Jean Pierre Lafon
Université Paris XIII

Algèbre commutative.
Langages géométrique et algébrique

Hermann

JEAN PIERRE LAFON est ancien élève de l'Ecole Normale Supérieure. Agrégé de mathématiques en 1952, il soutient une thèse de doctorat d'état à l'Université de Paris en 1960. Après avoir enseigné dans les Universités de Clermont-Ferrand, Montpellier, Toulouse, il devient professeur à l'Université Paris-Nord. Ses travaux portent essentiellement sur l'algèbre commutative et, notamment, la théorie des anneaux henséliens.

ISBN 2 7056 5849 1

1977, Hermann, 293 rue Lecourbe, 75015 Paris

Table

INTRODUCTION

Cet ouvrage et le suivant "*Algèbre locale*" proposent un exposé se suffisant à lui-même des résultats les plus classiques de l'algèbre commutative. Le lecteur trouvera dans le livre "*les formalismes fondamentaux de l'algèbre commutative*" les définitions de base et les éléments d'algèbre multilinéaire et homologique qui y sont utilisés.

L'*algèbre commutative* est la discipline mathématique qui traite des anneaux commutatifs. Elle a des liens étroits avec plusieurs théories fondamentales et, notamment, la théorie algébrique des nombres, la géométrie algébrique et la géométrie analytique locale.

La *théorie algébrique des nombres* est, en gros, l'étude des extensions finies ou, plus généralement, algébriques du corps des rationnels et de celle de ces cas particuliers d'anneaux de Dedekind que sont les anneaux d'entiers algébriques. Les éléments de la théorie des entiers algébriques sont donnés dans le chapitre 4. Une étude arithmétique des anneaux de Dedekind sera entreprise dans le livre "*Algèbre locale*".

Sous la forme la plus classique, la *géométrie algébrique* est l'étude des ensembles des zéros d'une famille de polynômes à coefficients dans un corps. La notion de courbe algébrique plane qui en relève est introduite dès le chapitre 2. Un exposé plus général est donné dans le chapitre 6. On y montre, en particulier, comment un ensemble algébrique s'interprète, après définition d'une notion convenable de point, comme le spectre d'une algèbre de type fini réduite sur un corps.

La plupart des résultats de ce livre ont un support ou une interprétation géométrique. La théorie des anneaux de fractions (chapitre 1) est liée à un processus de localisation à un ouvert ou au passage à un anneau de germes de fonctions. Le chapitre 2 contient des résultats de finitude dont le plus frappant est le théorème de Hilbert qui affirme qu'un ensemble algébrique est l'ensemble des zéros d'un nombre fini de polynômes. Le chapitre 3 qui traite de la décomposition primaire et des idéaux premiers associés correspond sous sa forme la plus simple à la décomposition d'un ensemble algébrique en réunion d'ensembles algébriques irréductibles. La théorie des extensions de type fini d'un corps est équivalente à la partie de la géométrie algébrique dite birationnelle, i.e. à l'étude des invariants par le groupe des transformations biration-

nelles. Les éléments de théorie des corps sont donnés dans le chapitre 5: existence des bases de transcendance, construction d'extensions remarquables dont la clôture algébrique, théorie de Galois des extensions finies, questions d'inséparabilité utiles en théorie de la multiplicité. Le chapitre 7 traite des morphismes d'ensembles algébriques et de quelques résultats particulièrement importants : lemme de normalisation d'E. Noether, constructibilité de l'image d'un morphisme. Le chapitre 9 aborde l'étude des espaces tangents.

La *géométrie analytique locale* est l'étude locale des ensembles analytiques, i.e. des ensembles des zéros de fonctions analytiques. Elle est équivalente à l'étude des algèbres analytiques qui sont les quotients des anneaux de séries convergentes. Le lecteur trouvera en exercices les théorèmes de base de cette théorie et, notamment, le théorème de préparation de Weierstrass et ses conséquences : théorèmes de la fonction implicite et de la fonction réciproque, lemme de Hensel. Le chapitre 8 traite d'une géométrie analogue : *la géométrie formelle* où les anneaux qui interviennent sont les anneaux locaux complets et surtout du passage de la géométrie algébrique locale à cette géométrie formelle.

Le livre "Algèbre locale" qui fait suite contient des résultats plus fins liés aux propriétés locales ou à des globalisations simples de celles-ci.

Je tiens à remercier ici toutes les personnes qui m'ont aidé dans la rédaction de cet ouvrage et, notamment, M. Alain Bouvier qui en a lu une première version et Mme Marie-Lise Pham et M. Laurie Mascle qui ont rédigé un appendice sur des résultats de Höchster. Je ne saurais oublier Mmes Simon et Das Chagas qui ont apporté toute leur compétence et dévouement à la dactylographie définitive.

NOTATIONS

Le livre : *les formalismes fondamentaux de l'algèbre commutative* est noté dans le suite (FFAC).

Voici le rappel de quelques notations utilisées dans ce livre.

$\mathbb{N}$ ensemble des entiers naturels

$\mathbb{N}^*$ ensemble des entiers naturels non nuls

$\mathbb{Z}$ anneau des entiers

$\mathbb{Q}$ corps des rationnels

$\mathbb{R}$ corps des réels

$\mathbb{C}$ corps des complexes

Ens catégorie des ensembles

Ab catégorie des groupes abéliens

Ann catégorie des anneaux commutatifs

Loc catégorie des anneaux locaux

Top catégorie des espaces topologiques

$\oplus$ somme directe

$\prod$ produit

$\otimes$ produit tensoriel

$\varinjlim$ limite inductive

$\varprojlim$ limite projective

Ext^n_A n-ième foncteur Ext

Tor^A_n n-ième foncteur Tor

H^n n-ième groupe de cohomologie

H_n n-ième groupe d'homologie

Quelques définitions sur les algèbres

Soient A *un anneau,* B *une* A*-algèbre.*

1. On dit que B est une A-algèbre *finie* si le A-module B est de type fini.

2. On dit que B est une A-algèbre *de type fini* si elle est *quotient d'une* A*-algèbre de polynômes à un nombre fini d'indéterminées.*

3. On dit que B est une A-algèbre *de présentation finie* si elle est *quotient d'une* A*-algèbre de polynômes à un nombre fini d'indéterminées par un idéal de type fini.*

4. On dit que B est une A-algèbre *essentiellement de type fini* si

elle est la localisée *en un idéal premier d'une A-algèbre de type fini.*

On a les implications évidentes : finie $\Longrightarrow$ de type fini

de présentation finie $\Longrightarrow$ de type fini

Ce sont les seules implications vraies en toute généralité.

Le lecteur est prié d'apporter à (FFAC) *les modifications suivantes*

Chapitre 4. Corollaire du théorème I.5

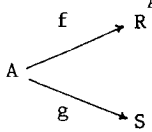
Soit N *un* A*-module.*

Les applications $\Phi_{M,N;P} \circ \chi^{-1}_{M,N;P}$ *de* $\mathrm{Hom}_A(M \underset{A}{\otimes} N, P)$ *dans* $\mathrm{Hom}_A(M, \mathrm{Hom}_A(N,P))$ *définissent le foncteur* $(M \longmapsto M \underset{A}{\otimes} N,\ v \longrightarrow v \otimes N)$ *comme foncteur adjoint à gauche du foncteur* $\mathrm{Hom}_A(N,-)$.

Proposition I.12

Soient A,R,S *des anneaux commutatifs,* f (resp. g) *un homomorphisme d'anneaux de* A *dans* R (resp. A *dans* S), u *l'homomorphisme d'anneaux :* $x \longmapsto x \otimes 1$ *de* R *dans* $R \underset{A}{\otimes} S$, v *l'homomorphisme d'anneaux :* $y \longmapsto 1 \otimes y$ *de* S *dans* $R \underset{A}{\otimes} S$.

Alors, $((R \underset{A}{\otimes} S), u, v)$ *est la somme amalgamée dans Ann du diagramme :*



Démonstration

Le fait que u et v soient des homomorphismes d'anneaux, $R \underset{A}{\otimes} S$ étant muni de la structure d'anneau défini dans la proposition I.11, est évident

Il est clair que uof = vog car

$(uof)(a) = f(a) \otimes 1 = a(1 \otimes 1) = 1 \otimes g(a) = (vog)(a)$ ... .

Chapitre 2. Proposition II.10 (fin de démonstration)

Soient alors $x \in \mathfrak{a} p_1 \cdots p_{n-1}$, $x \notin p_n$ et $y \in a$, $y \notin p_1 \cup \cdots \cup p_{n-1}$ dont l'existence résulte de l'hypothèse de récurrence.

Index des principales notations du livre dans l'ordre où elles se présentent :

CHAPITRE 1

Anneaux et modules de fractions
Localisation et globalisation

Le problème algébrique qui consite à rendre inversibles certains éléments d'un anneau se présente déjà à propos de la construction du corps $\mathbb{Q}$ des rationnels à partir de l'anneau $\mathbb{Z}$ des entiers et, plus généralement, du corps des fractions d'un anneau intègre.

En théorie des nombres, on considère souvent le sous-anneau $\mathbb{Z}_{(p)}$ de $\mathbb{Q}$, où p est un nombre premier, des fractions n/m où m n'est pas divisible par p et surtout son complété, l'anneau des entiers p-adiques (chap. 8). Dans l'anneau $\mathbb{Z}_{(p)}$, tout nombre premier différent de p devient inversible. On localise ainsi les problèmes en le nombre premier p.

Un processus analogue est fondamental en géométrie algébrique. En voici un exemple simple. L'anneau $\mathbb{C}[X_1,\ldots,X_n]$ des polynômes en les n indéterminées $X_1,\ldots,X_n$ à coefficients complexes s'identifie à l'anneau des fonctions polynômes de $\mathbb{C}^n$ dans $\mathbb{C}$.

Une fraction rationnelle $f(X_1,\ldots,X_n)/g(X_1,\ldots,X_n)$, où $f,g \in \mathbb{C}[X_1,\ldots,X_n]$, définit une fonction :

$$(x_1,\ldots,x_n) \longmapsto f(x_1,\ldots,x_n)/g(x_1,\ldots,x_n)$$

de l'ouvert $D(g) = \{(x_1,\ldots,x_n) \in \mathbb{C}^n / g(x_1,\ldots,x_n) \neq 0\}$ de $\mathbb{C}^n$ dans $\mathbb{C}$.

Soit $h \in \mathbb{C}[X_1,\ldots,X_n]$. Le sous-anneau du corps $\mathbb{C}(X_1,\ldots,X_n)$ des fractions rationnelles f/g, où f, g $\in \mathbb{C}[X_1,\ldots,X_n]$ et g n'est pas divisible par h, s'identifie à l'anneau des fonctions rationnelles définies sur tout l'ouvert $D(h)$. On démontrera ultérieurement que c'est le sous-anneau des fractions k/h^r, où $k \in \mathbb{C}[X_1,\ldots,X_n]$, obtenu en rendant inversibles les puissances de h.

Le passage de l'anneau $\mathbb{C}[X_1,\ldots,X_n]$ à ce sous-anneau constitue bien un processus de localisation à l'ouvert $D(h)$ de $\mathbb{C}^n$.

Plus généralement, à un anneau A on associe un espace topologique, son spectre, Spec(A) qui est l'ensemble des idéaux premiers de A muni d'une topologie convenable. On verra au chapitre 6 que cet espace a une signification géométrique simple si A est une algèbre réduite de type fini sur un corps. Le passage de A à l'anneau A_h, obtenu en rendant inversible l'élément h de A comme ci-dessus, est un processus de localisation à l'ouvert $D(h)$ de Spec(A), $D(h) = \{p \in \mathrm{Spec}(A) / h \notin p\}$.

Si p est un idéal premier de A, l'anneau A_p, obtenu en rendant in-

versibles les éléments de A n'appartenant pas à p, est un anneau local qui rend compte des propriétés de Spec(A) au voisinage du point p. Si $A = \mathbb{C}[X_1,\ldots,X_n]$ et p est l'idéal $(X_1,\ldots,X_n)$, l'anneau A_p est l'anneau des fractions rationnelles f/g, où f, g $\in \mathbb{C}[X_1,\ldots,X_n]$ et $g(0,\ldots,0) \neq 0$. Il permet de lire les propriétés de $\mathbb{C}^n$ considéré comme ensemble "algébrique" au voisinage de l'origine.

La construction générale des anneaux de fractions se présente comme suit.

Soient A *un anneau,* S *une partie de* A.

Un anneau de fractions de A *par rapport à* S *est la donnée d'un anneau* B *et d'un homomorphisme* $f : A \longrightarrow B$ *universel pour la propriété que, pour tout* $s \in S$, f(s) *soit inversible dans* B.

L'existence d'un tel anneau peut être démontrée, en toute généralité, par plusieurs procédés. Deux sont proposés dans le texte. Un troisième est donné en exercice.

Voici le plan de ce chapitre.

Dans I, on introduit la notion de partie multiplicative et de partie multiplicative saturée.

Dans II, on explicite deux constructions des anneaux de fractions et on démontre une importante propriété de platitude.

Le paragraphe III étudie la correspondance entre certains idéaux d'un anneau de fractions.

Dans IV, on compare les anneaux de fractions relatifs à deux parties multiplicatives.

Le processus de localisation suggéré dans l'introduction admet parfois un processus inverse, le processus de globalisation étudié dans V.

Le paragraphe VI concerne la localisation des Ext et des Tor. Il peut être laissé en première lecture.

I. Parties multiplicatives

Un produit d'éléments d'un anneau est inversible si et seulement si chaque facteur est inversible. Donc pour rendre inversible tout élément d'un ensemble S il faut rendre inversible tout produit d'éléments de S et c'est évidemment suffisant. L'ensemble de tels produits et de l'élément unité est multiplicativement stable. On dit que c'est une partie multiplicative.

On peut donc se limiter au problème de rendre inversibles les éléments de parties *multiplicatives*. L'avantage de cette restriction apparaîtra clairement dans la deuxième construction donnée ici d'un anneau de fractions : on peut alors réduire les fractions au même dénominateur.

Définition

Une partie S *d'un anneau* A *est dite multiplicative si* 1 *appartient à* S *et si le produit de deux éléments de* S *appartient à* S.

Exemples

1. *Soit* p *un idéal de* A.

Les assertions suivantes sont équivalentes : (i) p est premier

(ii) A-p est une partie multiplicative

2. *Soit* $f \in A$.

La partie $S_f = \{1, f, \ldots, f^n, \ldots\}$ est multiplicative.

3. *Soit* a *un idéal de* A.

La partie $1+a = \{1+x \ / \ x \in a\}$ est multiplicative.

4. Une intersection de parties multiplicatives est une partie multiplicative.

5. *Soit* S *une partie de* A.

L'intersection des parties multiplicatives de A contenant S est *la plus petite partie multiplicative de* A *contenant* S. Elle est l'ensemble des produits finis d'éléments de $S \cup \{1\}$.

On l'appelle la *partie multiplicative engendrée par* S.

Définition

Une partie multiplicative S *de* A *est dite saturée si la condition* $ss' \in S$ $(s, s' \in A)$ *implique la condition* $s \in S$ *et* $s' \in S$.

Exemples

1. *Soit* p *un idéal premier de* A.

La partie multiplicative A-p est saturée.

2. Une intersection de parties multiplicatives saturées est saturée.

3. *Soit* $(p_i)_{i \in I}$ *une famille d'idéaux premiers.*

La partie multiplicative $\bigcap_{i \in I} (A - p_i) = A - \bigcup_{i \in I} p_i$ est saturée.

4. *Soit* S *une partie de* A.

L'intersection des parties multiplicatives saturées contenant S est la plus petite partie multiplicative saturée contenant S. On l'appelle *la partie multiplicative saturée engendrée par* S. C'est aussi la partie multiplicative saturée engendrée par la partie multiplicative engendrée par S Si S est une partie multiplicative, la partie multiplicative saturée engendrée par S est l'ensemble $\{s \in A \mid \exists\ t \in A$ tel que $st \in S\}$.

Proposition I.1

Soit S *une partie multiplicative de l'anneau* A, *avec* $0 \notin S$.

Un idéal p *maximal, pour la relation d'inclusion, dans l'ensemble des idéaux de* A *disjoints de* S *est un idéal premier.*

Démonstration

Soient a et b n'appartenant pas à p. Par maximalité de p, $(p+Aa) \cap S$ et $(p+Ab) \cap S$ sont non vides. Il existe donc des éléments u, v de p et x, y de A tels que $u+xa$ et $v+yb$ appartiennent à S. L'élément ab ne peut appartenir à p car sinon le produit $(u+xa)(v+yb)$ appartiendrait à $p \cap S$.

Donc, l'idéal p est premier.

Corollaire

Soit S *une partie de* A.

La partie multiplicative saturée engendrée par S *est* $\bigcap_{i \in I}(A-p_i)$ *où* $(p_i)_{i \in I}$ *est la famille des idéaux premiers disjoints de* S.

Démonstration

Comme un idéal premier est disjoint d'une partie si et seulement si il est disjoint de la partie multiplicative saturée qu'elle engendre, on peut supposer S *multiplicative saturée* et démontrer alors *l'égalité*

$$S = \bigcap_{i \in I}(A-p_i) .$$

L'inclusion $S \subset \bigcap_{i \in I}(A-p_i)$ est claire et le second membre est une partie multiplicative saturée.

Soit $a \notin S$. Puisque S est saturée, $aA \cap S = \emptyset$. Le théorème de Zorn montre alors l'existence d'un idéal maximal p dans l'ensemble des idéaux de A contenant Aa et disjoints de S. Cet idéal p est premier et a n'appartient pas à $A-p$ et donc, a fortiori, à $\bigcap_{i \in I}(A-p_i)$.

II. Anneaux et modules de fractions

1. Première construction

Le lecteur peut considérer cette construction comme un exercice. La proposition II.2 est essentielle. On y verra bien où intervient l'hypothèse que la partie est multiplicative.

Problème

Soient A *un anneau,* S *une partie de* A.

Construire un anneau $A[S^{-1}]$ *et un homomorphisme* i_A^S *de* A *dans* $A[S^{-1}]$ *tels que, pour tout* $s \in S$, $i_A^S(s)$ *soit inversible dans* $A[S^{-1}]$ *qui soient universels pour cette propriété* en un sens précisé dans la proposition II.1.

On suppose le problème résolu.

Soit x_s *l'inverse de* $i_A^S(s)$ *dans* $A[S^{-1}]$.

Il existe un homomorphisme u de A-algèbre et un seul de $A[X_s]_{s\in S}$, où $(X_s)_{s\in S}$ est une famille d'indéterminées indexée par S, dans $A[S^{-1}]$ tel que $u(X_s) = x_s$. Le noyau de u contient évidemment l'idéal $(sX_s - 1)_{s\in S}$.

Le lecteur se persuadera que la minimalité de $A[S^{-1}]$ permet de supposer que $(x_s)_{s\in S}$ engendre la A-algèbre $A[S^{-1}]$: on ne rajoute que les inverses d'éléments de S.

Ceci signifie que u est surjectif.

On doit donc prendre $A[S^{-1}] = A[X_s]_{s\in S}/(sX_s - 1)_{s\in S}$ *et définir* i_A^S *comme le composé de l'injection canonique de* A *dans* $A[X_s]_{s\in S}$ *et de la surjection canonique de* $A[X_s]_{s\in S}$ *sur* $A[S^{-1}]$.

On laisse le soin au lecteur de vérifier la propriété universelle énoncé ci-dessous.

Proposition II.1

Soit, avec les notation ci-dessus, f *un homomorphisme de* A *dans un anneau* B *tel que, pour tout* $s \in S$, $f(s)$ *soit inversible dans* B.

Il existe un homomorphisme $\overline{f}$ *d'anneaux et un seul de* $A[S^{-1}]$ *dans* B *rendant le diagramme*

$$\begin{array}{ccc} A & \xrightarrow{i_A^S} & A[S^{-1}] \\ & \searrow^{f} & \downarrow{\scriptstyle \overline{f}} \\ & & B \end{array}$$

commutatif.

Cet homomorphisme se déduit, par passage au quotient, de l'unique homomorphisme f' de A-algèbres de $A[X_s]_{s\in S}$ dans B tel que $f'(X_s) = f(s)^{-1}$.

Soit $\overline{S}$ *la partie multiplicative engendrée par* S.

Un produit d'éléments est inversible si et seulement si chaque facteur l'est. Le couple $(A[S^{-1}], i_A^S)$ est donc solution du problème universel associé à la partie $\overline{S}$ et on peut identifier $A[\overline{S}^{-1}]$ à $A[S^{-1}]$ et $i_A^{\overline{S}}$ à i_A^S .

On supposera donc dans la suite de ce paragraphe la partie S *multiplicative.*

Voici alors quelques propriétés fondamentales du couple $(A[S^{-1}], i_A^S)$.

Proposition II.2.

1. Le noyau de i_A^S *est* $\{a\in A \mid \exists s\in S \text{ tel que } sa = 0\}$

2. Un élément de $A[S^{-1}]$ *s'écrit* $i_A^S(a)\, i_A^S(s)^{-1}$ *où* $a\in A$, $s\in S$.

Démonstration

1. Il résulte de la construction même que $\ker(i_A^S) = (sX_s - 1)_{s\in S} \cap A$. Soit alors $a\in\ker(i_A^S)$. Il existe $s_1,\ldots,s_n\in S$ tels que a appartienne à l'idéal

$$(s_1X_{s_1} - 1, \ldots, s_nX_{s_n} - 1)A[X_{s_1}, \ldots, X_{s_n}] \cap A$$

de A.

Ceci s'exprime en disant que l'image de a dans l'application naturelle de A dans l'anneau quotient $A[X_{s_1},\ldots,X_{s_n}]/(s_1X_{s_1}-1,\ldots,s_nX_{s_n}-1)$ est 0. Soient $t = s_1\ldots s_n$, $t_i = \prod_{j\neq i} s_j$ $(i=1,\ldots,n)$, u l'homomorphisme de A-algèbres de $A[X_{s_1},\ldots,X_{s_n}]$ dans $A[X_t]$ tel que $u(X_{s_i}) = t_iX_t$.

Comme $u(s_iX_{s_i} - 1) = tX_t - 1$, u définit par passage au quotient un homomorphisme v de l'anneau $A[X_{s_1},\ldots,X_{s_n}]/(s_1X_{s_1}-1,\ldots,s_nX_{s_n}-1)$ dans l'anneau $A[X_t]/(tX_t-1)$ rendant commutatif le diagramme

$$\begin{array}{ccc} A & \xrightarrow{\lambda} & A[X_{s_1},\ldots,X_{s_n}]/(s_1X_{s_1},\ldots,s_nX_{s_n}) \\ & \searrow^{\mu} & \downarrow v \\ & & A[X_t]/(tX_t-1) \end{array}$$

où λ et μ sont les homomorphismes naturels.

L'image de a dans $A[X_t]/(tX_t-1)$ est donc nulle, i.e. a appartient à $(tX_t-1)A[X_t]\cap A$.

Ainsi, $a = (tX_t-1)(a_0+a_1X_t+\ldots+a_rX_t^r)$, d'où

$$a = -a_0,\ ta = -a_1,\ldots,t^na = -a_n,\ t^{n+1}a = -ta_n = 0.$$

L'élément $s = t^{n+1}$ appartient à S et on a donc démontré l'inclusion

$$\mathrm{Ker}(i_A^S) \subset \{a \in A \mid \exists\ s \in S \text{ tel que } sa = 0\}$$

Réciproquement, s'il existe $s \in S$ tel que $sa = 0$, $i_A^S(s)\, i_A^S(a) = 0$ et, comme $i_A^S(s)$ est inversible, $i_A^S(a) = 0$ et a appartient à $\ker(i_A^S)$.

2. Un élément de $A[S^{-1}]$ est unesomme finie d'éléments

$$i_A^S(a_{i_1 \ldots i_n})\, i_A^S(s_{i_1} \ldots s_{i_n})^{-1}$$

où $a_{i_1 \ldots i_n} \in A$, $s_{i_j} \in S$. (Un tel élément est $i_A^S(a_{i_1 \ldots i_n}) x_{s_{i_1}} \ldots x_{s_{i_n}}$ où $x_{s_{i_j}}$ est la classe de $X_{s_{i_j}}$, i.e. l'inverse de $i_A^S(s_{i_j})$).

Soit s un multiple commun des produits $s_{i_1} \ldots s_{i_n}$ apparaissant dans cette somme. Il est clair que l'élément considéré de $A[S^{-1}]$ est de la for- $i_A^S(a) i_A^S(s)^{-1}$.

Notation

On convient de noter a/s *ou simplement* a/s *s'il n'y a pas de risque de confusion l'élément* $i_A^S(a)\, i_A^S(s)^{-1}$ ($a \in A$, $s \in S$).

Le résultat ci-dessous conduit à la deuxième construction de l'annea des fractions.

Proposition II.3

Soient $a, a' \in A$, $s, s' \in S$.

Les assertions suivantes sont équivalentes :

(i) $a/s = a'/s'$

(ii) *il existe* $t \in S$ *tel que* $t(s'a - sa') = 0$.

Démonstration

(i) équivaut à l'égalité $(s'a)(ss') = (sa')/(ss')$, i.e. $(s'a - sa')/(ss') = 0$ soit à l'appartenance de $s'a - sa'$ à $\ker(i_A^S)$.

Remarque

Le problème posé initialement peut se traduire sous la forme suivante qui a l'avantage de garder un sens pour un A-module quelconque : *trouver un anneau* $A[S^{-1}]$ *et un homomorphisme* i_A^S *d'anneaux de* A *dans* $A[S^{-1}]$ *tels que l'homothétie*

$$\delta^{S}_{A[S^{-1}]} : y \longmapsto s.y = (i^{S}_{A})(s)y$$

soit bijective, ces données étant universelles.

Le problème analogue pour les modules est étudié dans le paragraphe suivant.

2. Deuxième construction

Cette construction généralise celle donnée dans ((FFAC)) du corps des fractions d'un anneau intègre.

Soit S la partie multiplicative de l'anneau A dont on veut rendre les éléments inversibles. On introduit des fractions a/s, où $a \in A$, $s \in S$, ou si l'on préfère des couples (s,a).

Contrairement à ce qui se passe dans le cas où l'anneau A est intègre et plus généralement où tout élément de S est régulier, la relation naturelle R définie par (s,a)R(s',a') si et seulement si s'a = sa', qui est réflexive et symétrique, n'est pas toujours transitive : les égalités s'a = sa' et s"a' = s'a" permettent d'obtenir l'égalité s'(s"a-sa")=0 mais pas toujours l'égalité s"a-sa" = 0. Il faut donc considérer la relation d'équivalence R' engendrée par la relation R, i.e. définie par (s,a)R'(s',a') si et seulement si il existe $s'' \in S$ tel que s"(s'a-sa')=0.

Pour les modules de fractions, cette complication apparaît même si l'anneau A est intègre, en raison de l'existence éventuelle d'un sous-module de torsion non nul.

Soient A un anneau, S une partie multiplicative de A, M un A-module.

La relation R_M définie sur S×M par : $(s,m)R_M(s',m')$ si et seulement si il existe $t \in S$ tel que t(s'm-sm') = 0 est une *relation d'équivalence.*

On note $S^{-1}M$ (ou $M[S^{-1}]$) *l'ensemble quotient* $S\times M/R_M$ *et* m/s *la classe de* (s,m).

De nombreuses vérifications ultérieures sont simplifiées si l'on remarque que, pour tout $s' \in S$, m/s = s'm/ss', ce qui permet de réduire au même dénominateur.

Si $m/s = m'/s'$ et $m_1/s_1 = m'_1/s'_1$, on vérifie que :

$$(ss', s'm + sm')R_M(s_1s'_1, s'_1m_1 + s_1m'_1)$$

On définit donc une loi de composition sur $S^{-1}M$ en posant:

$$m/s + m'/s' = (s'm + sm')/(ss')$$

On vérifie que $S^{-1}M$ est ainsi muni d'une structure de *groupe abélien*.

Si de plus $M = A$, *on munit* $S^{-1}A$ *d'une structure d'anneau* en posant :

$$(a/s)(a'/s') = (aa')/(ss')$$

On munit enfin $S^{-1}M$ *d'une structure de* $S^{-1}A$*-module* en posant :

$$(a/s)(m'/s') = (am')/(ss')$$

On note i_M^S *l'application* : $x \longmapsto x/1$ *de* M *dans* $S^{-1}M$.

L'application i_M^S est A-linéaire de M dans le A-module $(i_A^S)_*(S^{-1}M)$ déduit du $S^{-1}A$-module $S^{-1}M$ par restriction des scalaires à A.

L'application i_A^S est un *homomorphisme d'anneaux*.

Soient enfin M *et* M' *deux* A*-modules,* f *une application* A*-linéaire de* M' *dans* M. *L'application* : $x'/s \longmapsto f(x')/s$ *de* $S^{-1}M'$ *dans* $S^{-1}M$ *est bien définie. Elle est* $S^{-1}A$*-linéaire.* On la note $S^{-1}f$.

Le diagramme

$$\begin{array}{ccc} M' & \xrightarrow{i_{M'}^S} & S^{-1}M' \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle S^{-1}f} \\ M & \xrightarrow[i_M^S]{} & S^{-1}M \end{array}$$

est commutatif.

Avec des notations évidentes, $S^{-1}(g \circ f) = (S^{-1}g) \circ (S^{-1}f)$, $S^{-1}(1_M) = 1_{S^{-1}M}$.

Les applications : $M \longrightarrow S^{-1}M$, $f \longrightarrow S^{-1}f$ *définissent un foncteur covariant de* $\mathrm{Mod}(A)$ *dans* $\mathrm{Mod}(S^{-1}A)$.

Proposition II.4

Les notations sont celles définies ci-dessus.

1. Pour tout $s \in S$, $i_A^S(s)$ *est inversible dans* $S^{-1}A$.

Soit f *un homomorphisme d'anneaux de* A *dans un anneau* B *tel que, pour tout* s *de* S, $f(s)$ *soit inversible dans* B.

Il existe un homomorphisme $\overline{f}$ *et un seul de* $S^{-1}A$ *dans* B *tel que* $f = \overline{f} \circ i_A^S$.

2. Pour tout $S^{-1}A$*-module* N, *il existe un homomorphisme de groupes abéliens*

$$\Phi_{M,N} : \mathrm{Hom}_A(M, (i_A^S)_*(N)) \longrightarrow \mathrm{Hom}_{S^{-1}A}(S^{-1}M, N)$$

qui associe à f *une application* $S^{-1}A$*-linéaire* $\overline{f}$ *telle que* $\overline{f}(x/s) = (1/s)f(x)$.

Cet homomorphisme est un isomorphisme fonctoriel en M *et* N.

Démonstration

1. L'inverse de $i_A^S(s)$ est l'élément $1/s$.

Un élément de $S^{-1}A$ s'écrit $a/s = (a/1)(1/s) = i_A^S(a)i_A^S(s)^{-1}$. On doit donc poser $\bar{f}(a/s) = (\bar{f}\circ i_A^S)(a)((\bar{f}\circ i_A^S)(s))^{-1} = f(a)f(s)^{-1}$.

On vérifie que l'application $\bar{f}$ est ainsi bien définie et que c'est un homomorphisme d'anneaux.

2. Si $x/s = x'/s'$, il existe $t\in S$ tel que $ts'x = tsx'$. Donc $ts'f(x) = tsf(x')$ dans $(i_A^S)_*(N)$ soit, dans N, $((ts')/1)f(x)=((ts)/1))f(x')$. Multipliant par $1/(ss't)$, on obtient $(1/s)f(x) = (1/s')f(x')$. Ainsi, l'application $\bar{f}$ est bien définie.

On vérifie facilement qu'elle est $S^{-1}A$-linéaire.

La fonctorialité en M et N est immédiate.

L'application $\bar{f} \longmapsto f$ de $\mathrm{Hom}_{S^{-1}A}(S^{-1}M,N)$ dans $\mathrm{Hom}_A(M,(i_A^S)_*(N))$ définie par $f(x) = \bar{f}(x/1)$ est l'inverse de $\Phi_{M,N}$.

Corollaire

Soit N *un* $S^{-1}A$*-module.*

L'application : $x/s \longmapsto (1/s)x$ *de* $S^{-1}((i_A^S)_*(N))$ *dans* N *est un isomorphisme de* $S^{-1}A$*-modules.*

Démonstration

Cette application est $\Phi_{(i_A^S)_*(N),N}(1_{(i_A^S)_*(N)})$.

La vérification directe est d'ailleurs immédiate.

On peut donner la variante suivante à la proposition II.4.2.

Proposition II.4'

Soient A *un anneau,* S *une partie multiplicative,* M *un* A*-module.*

1. Pour tout $s\in S$, *l'homothétie* $\delta_s^{S^{-1}M}$ *est bijective.*

2. Soient N *un* A*-module tel que, pour tout* $s\in S$, *l'homothétie* δ_s^N *soit bijective,* f *une application* A*-linéaire de* M *dans* N.

Il existe une application A*-linéaire* $\bar{f}$ *et une seule de* $(i_A^S)_*(S^{-1}M)$ *dans* N *telle que* $f = \bar{f}\circ i_S^M$.

Démonstration

Il est commode de remarquer le résultat suivant.

Lemme

Soit N *un* A*-module. Les assertions suivantes sont équivalentes :*

(i) Il existe un $S^{-1}A$*-module* P *tel que* $N = (i_A^S)_*(P)$.

(ii) Pour tout $s \in S$, *l'homothétie* $\delta_s^N : x \longrightarrow sx$ *est bijective.*

Démonstration du lemme

(i) $\Longrightarrow$ (ii). L'homothétie $\delta^P_{(1/s)}$ de P est une *application* inverse de δ_s^N.

(ii) $\Longrightarrow$ (i). On définit P comme suit : le groupe additif de P est celui de N ; la structure de $S^{-1}A$-module de P est donnée par l'application : $(a/s,x) \longmapsto (\delta_s^N)^{-1}(ax)$ de $S^{-1}A \times P$ dans P.

Démonstration de II.4'

Si $x \in M$, on doit avoir $\overline{f}(x/1) = (\overline{f} \circ i_S^M)(x) = f(x)$. Si $s \in S$, on doit avoir $\overline{f}(s(x/s)) = s\overline{f}(x/s)$, soit $s\overline{f}(x/s) = \overline{f}(x/1) = f(x)$.

On munit alors N de la structure de $S^{-1}A$-module du lemme. On doit avoir $\overline{f}(x/s) = (1/s)f(x)$. Ceci démontre l'unicité et donne la forme de $\overline{f}$. On laisse au lecteur le soin d'achever la démonstration.

On remarquera que l'application $\overline{f}$ *est* $S^{-1}A$*-linéaire.*

Remarques

1. L'homomorphisme i_A^S est un *épimorphisme*, en général non surjectif, de la catégorie des anneaux commutatifs. Ceci signifie que, si f_1 et f_2 sont des homomorphismes d'anneaux de $S^{-1}A$ dans un anneau B tels que $f_1 \circ i_A^S = f_2 \circ i_A^S$, alors $f_1 = f_2$: posant $g = f_i \circ i_A^S$ $(i = 1, 2)$, on voit que $f_i(a/s) = f_i(a/1)f_i(1/s) = g(a)g(s)^{-1}$ $(a \in A, s \in S)$ et donc $f_1 = f_2$.

2. L'égalité $S^{-1}A = 0$ équivaut à l'égalité $(i_A^S)(1) = 0$ et donc à l'existence de $s \in S$ tel que $s1 = s = 0$. Elle signifie donc que 0 appartient à S.

Définition

L'anneau $S^{-1}A$ (resp. *le* $S^{-1}A$*-module* $S^{-1}M$) *est appelé l'anneau* (resp. le *module*) *des fractions de* A (resp. M) *défini par* S (ou *associé à* S ou *par rapport à* S) .

Notations

Soient $f \in A$, p *un idéal premier de* A. *Il est traditionnel de noter* A_f *et* M_f *respectivement* $S^{-1}A$ *et* $S^{-1}M$ *où* $S = \{f^n\}$ *et* A_p *et* M_p *respectivement* $S^{-1}A$ *et* $S^{-1}M$ *où* $S = A - p$. *On appelle* M_p *le localisé de* M *en* p.

Exemples

1. Si S est la partie multiplicative (saturée) des éléments réguliers de A, l'anneau $S^{-1}A$ est appelé *l'anneau total des fractions de* A. Alors i_A^S est injective.

2. Si l'anneau A est *intègre*, l'anneau de fractions $S^{-1}A$ est intègre dès que S ne contient pas 0. L'anneau total des fractions de A est alors le *corps des fractions* de A ((FFAC). chap. 2.II.§2).

3. Platitude des anneaux de fractions

On a défini un foncteur : $M \longmapsto S^{-1}M$, $f \longmapsto S^{-1}f$ de Mod(A) dans $Mod(S^{-1}A)$. Ce foncteur est additif, i.e., si $f,g \in Hom_A(M,M')$, $S^{-1}(f+g) = S^{-1}f+S^{-1}g$.

On va démontrer ici qu'il est exact et endéduire que le A-module $S^{-1}A$ est plat.

Proposition II.5

Le foncteur $S^{-1}(-)$ *est exact.*

Démonstration

Soit $M' \xrightarrow{f} M \xrightarrow{g} M''$ une suite exacte de Mod(A).

On déduit de l'additivité de $S^{-1}(-)$ les égalités $S^{-1}(g\circ f) = S^{-1}(0) = 0 = S^{-1}g\circ S^{-1}f$.

Par conséquent, $im(S^{-1}f) \subset Ker(S^{-1}g)$.

Soit $m/s \in ker(S^{-1}g)$, i.e. tel que $g(m)/s = 0$. Il existe $t\in S$ tel que $tg(m) = 0$ soit $g(tm) = 0$, puis $m'\in M'$ tel que $tm = f(m')$. Donc, $m/s = (tm)/(ts) = (S^{-1}f)(m' / ts)$ appartient à $im(S^{-1}f)$.

En particulier, soient M un A-module, N un sous-module, i l'injection de N dans M. L'application $S^{-1}A$-linéaire injective $S^{-1}i$ permet d'identifier $S^{-1}N$ à un sous-module du $S^{-1}A$-module $S^{-1}M$.

Si a est un idéal de A, $S^{-1}a$ *s'identifie ainsi à l'idéal* $a(S^{-1}A)$ *de* $S^{-1}A$.

Proposition II.6

Il existe un isomorphisme fonctoriel (λ_M) *du foncteur* $S^{-1}-$ *dans le foncteur* $S^{-1}A \underset{A}{\otimes} -$ *tel que, pour tout* $x\in M$, *tout* $s\in S$, $\lambda_M(x/s) = (1/s)\bullet x$.

Démonstration

Compte tenu de la proposition II.4, il est possible de donner une

démonstration utilisant le lemme de Yoneda. Le lecteur préférera peut-être une démonstration plus élémentaire.

1ère démonstration

On a défini un isomorphisme fonctoriel en le A-module M et le $S^{-1}A$-module N :

$$\Phi_{M,N} : \mathrm{Hom}_A(M,(i_A^S)_*(N)) \longrightarrow \mathrm{Hom}_{S^{-1}A}(S^{-1}M,N)$$

qui à $f : M \longrightarrow (i_A^S)_*(N)$ fait correspondre $\overline{f}:S^{-1}M \longrightarrow N$ tel que $\overline{f}(x/s) = (1/s)f(x)$.

Il existe, d'autre part, un isomorphisme fonctoriel ((FFAC). chap.4.prop.I.13)

$$\Psi_{M,N} : \mathrm{Hom}_{S^{-1}A}(S^{-1}A \underset{A}{\otimes} M,N) \longrightarrow \mathrm{Hom}_A(M,(i_A^S)_*(N))$$

qui à $g : S^{-1}A \underset{A}{\otimes} M \longrightarrow N$ fait correspondre $f : M \longrightarrow (i_A^S)_*(N)$ tel que $f(x) = g((1/1) \underset{A}{\otimes} x)$. Le composé $\Lambda_{M,N} = \Phi_{M,N}\circ\Psi_{M,N}$ est un isomorphisme fonctoriel de $\mathrm{Hom}_{S^{-1}A}(S^{-1}A \underset{A}{\otimes} M,N)$ dans $\mathrm{Hom}_{S^{-1}A}(S^{-1}M,N)$ qui à $g : S^{-1}A \underset{A}{\otimes} M \longrightarrow N$ fait correspondre $\overline{f} : S^{-1}M \longrightarrow N$ tel que $\overline{f}(x/s) = (1/s)g((1/1) \underset{A}{\otimes} x) = g((1/s) \underset{A}{\otimes} x)$.

Il résulte du lemme de Yoneda que cet isomorphisme fonctoriel est $(\mathrm{Hom}(\lambda_M,N))$ où $\lambda_M = \Lambda_{M,S^{-1}A \underset{A}{\otimes} M}(1_{S^{-1}A \underset{A}{\otimes} M})$. Donc, $\lambda_M(x/s) = (1/s) \underset{A}{\otimes} x$.

2ème démonstration

L'application $(a/s,x) \longrightarrow (ax)/s$ de $S^{-1}A\times M$ dans $S^{-1}M$ est bien définie et est A-bilinéaire. Il existe donc une aplication A-linéaire μ_M de $S^{-1}A \underset{A}{\otimes} M$ dans $S^{-1}M$ telle que $\mu_M(\Sigma(a_i/s_i) \underset{A}{\otimes} x_i) = \Sigma(a_ix_i)/s_i$. Elle est évidemment surjective. On remarque que $\Sigma(a_i/s_i)\underset{A}{\otimes}x_i = \Sigma(1/s)\underset{A}{\otimes}a_it_ix_i$ où $s = \pi s_i$ et $t_i = \prod_{j\neq i} s_j$. Tout élément de $S^{-1}A \underset{A}{\otimes} M$ est donc de la forme $(1/s) \underset{A}{\otimes} y$. Dire que $(1/s) \underset{A}{\otimes} y$ appartient à $\mathrm{Ker}(\mu_M)$ c'est dire que $y/s=0$, i.e. qu'il existe $t\in S$ tel que $ty = 0$. Mais alors $(1/s) \underset{A}{\otimes} y=(1/st) \underset{A}{\otimes} (ty)=0$. Donc, μ_M est injective. On vérifie facilement la fonctorialité de μ_M. L'application λ_M est μ_M^{-1}.

Corollaire 1

Le A-module $S^{-1}A$ est plat.

Démonstration

Soit $M' \xrightarrow{f} M \xrightarrow{g} M''$ une suite exacte de Mod(A).

Dans le diagramme commutatif

$$\begin{array}{ccccc} S^{-1}M' & \xrightarrow{S^{-1}f} & S^{-1}M & \xrightarrow{S^{-1}g} & S^{-1}M'' \\ \downarrow{\scriptstyle \lambda_{M'}} & & \downarrow{\scriptstyle \lambda_{M}} & & \downarrow{\scriptstyle \lambda_{M''}} \\ S^{-1}A\otimes_A M' & \xrightarrow[S^{-1}A\otimes f]{} & S^{-1}A\otimes_A M & \xrightarrow[S^{-1}A\otimes g]{} & S^{-1}A\otimes_A M'' \end{array}$$

les flèches verticales sont des isomorphismes et la ligne supérieure est exacte (prop. II.5.). La ligne inférieure est donc exacte.

Corollaire 2

Le foncteur $S^{-1}(-)$ *commute aux limites inductives et, en particulier, aux sommes directes finies ou infinies.*

Démonstration

Le foncteur produit tensoriel commute aux limites inductives ((FFAC).chap.4.I.§7)

Corollaire 3

Soit $(M_i)_{i\in I}$ *une famille de sous-modules du* A*-module* M.

Alors $S^{-1}(\Sigma_{i\in I} M_i)$ (resp. $S^{-1}(\bigcap_{i\in I} M_i)$) *s'identifie à* $\sum_{i\in I} S^{-1}M_i$ (resp. $\bigcap_{i\in I} S^{-1}M_i$).

Démonstration

Il suffit d'appliquer le foncteur *exact* S^{-1}- au diagramme à ligne et colonne exactes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \bigcap_{i\in I} & \longrightarrow & \bigoplus_{i\in I} M_i & \longrightarrow & \sum_{i\in I} M_i & \longrightarrow & 0 \\ & & & & & & \downarrow & & \\ & & & & & & M & & \end{array}$$

et d'utiliser le corollaire 2.

III. Sous-modules de modules de fractions

Le résultat suivant est un des cas particuliers les plus importants des résultats obtenus dans ce paragraphe.

Soient A *un anneau,* f *un élément de* A. *L'application* : $p \longmapsto pA_f$ *est une bijection de l'ouvert* $D(f) = \{p\in \mathrm{Spec}(A)/f\notin p\}$ *de* Spec(A) *sur* $\mathrm{Spec}(A_f)$. C'est même un homéomorphisme.

On étudie ici plus généralement la structure des idéaux d'un anneaux de fractions. Soient A un anneau, S une partie multiplicative de A. *On suppose, pour simplifier, l'application* i_A^S *injective*, ce qui permet d'identifier A à un sous-anneau de $S^{-1}A$.

Exemple simple : $A = \mathbb{Z}$, $S = \mathbb{Z} - \{0\}$, $S^{-1}A = Q$.

A un idéal b de $S^{-1}A$ correspond sa trace $b \cap A$ sur A, qui est un idéal de A, appelé *contracté* de b.

A un idéal a de A correspond l'*idéal étendu* $a(S^{-1}A) = S^{-1}a$ de l'anneau $S^{-1}A$.

Partant d'un idéal b de $S^{-1}A$, l'idéal étendu $S^{-1}(b \cap A)$ de l'idéal contracté $b \cap A$ est égal à l'idéal b.

Par contre, si l'on part d'un idéal a de A, l'idéal contracté $S^{-1}a \cap A$ de l'idéal étendu $S^{-1}a$ n'est pas toujours égal à a. Une raison évidente est que, même si l'idéal a est distinct de A, il peut rencontrer S ; alors, $S^{-1}a = S^{-1}A$ et $S^{-1}a \cap A = A$. Ce n'est pas la seule difficulté qui se présente. On verra ci-dessous que l'égalité $S^{-1}a \cap A = a$ signifie que $a = \bigcup_{s \in S}(a:s)$ où $a : s = \{x \in A / sx \in a\}$. Un tel idéal est dit *saturé* pour S. Des exemples importants d'idéaux saturés pour S sont les idéaux premiers ne rencontrant pas S et, plus généralement, les idéaux primaires pour les idéaux premiers ne rencontrant pas S.

En résumé, la contraction est une bijection croissante de l'ensemble des idéaux de l'anneau $S^{-1}A$ sur l'ensemble des idéaux saturés de A. La bijection réciproque est l'extension.

La généralisation aux modules ne présente pas de difficulté spéciale. Le lecteur peut s'il le désire se limiter dans un premier temps au cas des idéaux.

1. Sous-modules saturés pour une partie multiplicative

Proposition III.1

1. Les assertions suivantes sont équivalentes pour un sous-module N *du* A*-module* M :

(i) il existe un sous-module P *du* S^{-1}A*-module* S^{-1}M *tel que* $N = (i_M^S)^{-1}(P)$

(ii) les conditions : $s \in S$, $x \in M$ *et* $sx \in N$ *impliquent l'appartenance de* x *à* N.

Autrement dit, $N = \bigcup_{s\in S}(N:s)$ *où* $(N : s) = \{x\in M / sx\in N\}$. *On dit alors que* N *est saturé pour* S.

2. L'application $P \longmapsto (i_M^S)^{-1}(P)$ *est une bijection croissante de l'ensemble* (ordonné par inclusion) *des sous-modules du* $S^{-1}A$*-module* $S^{-1}M$ *sur l'ensemble* (ordonné par inclusion) *des sous-modules de* M *saturés pour* S.

La bijection réciproque est l'application $N \longmapsto S^{-1}N$.

Démonstration

1. (i) $\Longrightarrow$ (ii). Dire que sx appartient à $N = (i_M^S)^{-1}(P)$, où $s\in S$, $x\in M$, c'est dire que $(sx)/1$ appartient à P. Il en résulte que $(1/s)(sx/1) = x/1$ appartient à P et donc que x appartient à N.

(ii) $\Longrightarrow$ (i). *On va démontrer que, si* N *est saturé pour* S, $N = (i_S^M)^{-1}(S^{-1}N)$. (On peut donc prendre pour module P le $S^{-1}A$-module $S^{-1}N$)

On a les équivalences : $x \in (i_M^S)^{-1}(S^{-1}N) \Longleftrightarrow x/1 \in S^{-1}N \Longleftrightarrow \exists y\in N$, $t\in S$ tels que $x/1 = y/t \Longleftrightarrow \exists y\in N$, $t\in S$, $t'\in S$ tels que $xtt' = t'y$.

Comme $t'y$ appartient à N et tt' à S, cette condition implique que x appartient à N, d'où l'inclusion $N \supset (i_M^S)^{-1}(S^{-1}N)$.

L'inclusion $N \subset (i_M^S)^{-1}(S^{-1}N)$ est vraie sans hypothèse sur N : si $x\in N$, $x/1 \in S^{-1}N$.

2. *Il suffit,* compte tenu de ce qui précède, *de démontrer que si* P *est un sous-module du* $S^{-1}A$*-module* $S^{-1}M$, $S^{-1}(i_M^S)^{-1}(P) = P$.

Soient $s\in S$, $x \in (i_M^S)^{-1}(P)$. Alors $x/1$ appartient à P ; il est de même de $x/s = (1/s)(x/1)$. Donc $S^{-1}(i_M^S)^{-1}(P)$ est contenu dans P.

Un élément de P s'écrit x/s, où $x\in M$, $s\in S$. Alors $(s/1)(x/s) = x/1$ appartient à P et x appartient à $(i_M^S)^{-1}(P)$. Donc, P est contenu dans $(i_M^S)^{-1}(P)$.

Corollaire 1

Soit b *un idéal de* $S^{-1}A$. *Alors* $b = S^{-1}(i_A^S)^{-1}(b)$.

Corollaire 2

L'application $b \longmapsto (i_A^S)^{-1}(b)$ *est une bijection croissante de l'ensemble des idéaux de* $S^{-1}A$ *sur l'ensemble des idéaux de* A *saturés pour* S.

2. Un exemple important de sous-modules saturés : les sous-modules primaires

La notion de sous-module primaire apparaît aussi à propos de la *décomposition primaire* étudiée au chapitre 3.

L'idéal (p^r) de $\mathbb{Z}$, où p est premier et r un entier $\geqslant 2$, n'est pas premier. Il possède néanmoins la propriété suivante : soient $a,b \in \mathbb{Z}$ tels que $ab \in (p^r)$, i.e. ab soit divisible par p^r. Si a n'appartient pas à (p^r) il existe une puissance de b appartenant à (p^r). L'idéal (p^r) est dit primaire.

Définitions

Soit A *un anneau,* a *un idéal,* p *un idéal premier de* A.

On dit que a *est* p*-primaire si ;*

1. $r(a) = p$ (ce qui implique l'inclusion $a \subset p$ et, en particulier, le fait que $a \neq A$).

2. $a,x \in A$, $ax \in a$ et $x \notin a \Longrightarrow a \in p$.

Proposition III.2

Soit a *un idéal de* A, *distinct de* A.

On suppose vérifiée la condition suivante :

$a,x \in A$, $ax \in a$ et $x \notin a \Longrightarrow \exists\, n(x) \in \mathbb{N}^* \;/\; a^{n(x)} \in a$

Alors $r(a)$ *est un idéal premier* p *de* A *et* a *est* p*-primaire.*

Démonstration

L'idéal $r(a)$ *est premier* : si $ab \in r(a)$ $(a,b \in A)$, il existe $n \in \mathbb{N}^*$ tel que $a^n b^n$ appartienne à a ; si $a \notin (a)$, a^n n'appartient pas à a ; il existe donc $m \in \mathbb{N}^*$ tel que $(b^n)^m$ appartienne à a et alors b appartient à $r(a)$.

La suite de la démonstration est immédiate.

Exemples

1. Un idéal premier p est p-primaire. On verra, par contre, dans le chapitre 3, des exemples d'idéaux dont la racine est un idéal premier mais qui ne sont pas primaires.

2. *Idéaux primaires de* $\mathbb{Z}$

Soit $a = (n)$ où $n \in N$ un idéal de $\mathbb{Z}$. Si $n = 0$, a est premier et donc primaire.

Si $n \neq 0$, soit $n = p_1^{r_1} \ldots p_s^{r_s}$ la décomposition de n en produit de nombres premiers distincts. La racine de a est l'idéal $(p_1 \ldots p_s)$ qui est

premier si et seulement si s = 1. L'idéal a est alors primaire.

3. Soit A un anneau tel que, pour tout $p \in \mathrm{Spec}(A)$, l'anneau A_p soit un corps.

Alors, tout idéal primaire de A est premier : soit, en effet, q un idéal primaire de racine l'idéal premier p. Par hypothèse, $qA_p = pA_p$ et il résulte de la proposition III.3. Corollaire 3 démontrée plus loin que $q = p$.

L'hypothèse est satisfaite si l'anneau A est *absolument plat*, i.e. tel que, pour tout $a \in A$, il existe $x \in A$ tel que $a = a^2x$, par exemple est un, produit fini ou non de corps. (Confer. Chapitre 3.I.1.).

Sous-modules primaires

On peut interpréter le fait que l'idéal a est p-primaire en terme du A-module A/a en disant que si $a \notin p$ l'homothétie $\delta_a^{A/a}$ est injective et si $a \in p$ l'homothétie $\delta_a^{A/a}$ est nilpotente.

Soit a un idéal distinct de A tel que, pour tout $a \in A$, $\delta_a^{A/a}$ soit injective ou nilpotente. L'ensemble $p = \{a \in A,\ \delta_a^{A/a}$ nilpotente$\}$ est alors un idéal premier p et a est p-primaire.

On peut généraliser au cas où le A-module A est remplacé par un A-module M et l'idéal a par un sous-module N de M. La généralisation la plus utile dans le cas où le module quotient M/N n'est pas de type fini, est un peu plus compliquée que celle qui est naturelle.

Définition

1. Soient M *un* A*-module,* $a \in A$. *On dit que l'homothétie* δ_a^M *est presque nilpotente* (ou que a est presque nilpotent dans M) *si, pour tout* $x \in M$, *il existe* $n(x) \in N^*$ *tel que* $a^{n(x)}x = 0$.

Si M est *de type fini*, a est presque nilpotent si et seulement si il est nilpotent.

2. Soient N *un sous-module de* M, p *un idéal premier de* A.

On dit que N *est* p*-primaire si, pour tout* $a \in A$, $\delta_a^{M/N}$ *est injective* (resp. *presque nilpotente*) *si* a *n'appartient pas* (resp. *appartient*) *à* p.

Voici l'analogue de la proposition III.2.

Proposition III.2'

Soit N *un sous-module de* M *distinct de* M.

On suppose que, pour $a \in A$, *l'homothétie* $\delta_a^{M/N}$ *est injective ou presque nilpotente. L'ensemble* $p = \{a \in A / \delta_a^{M/N}$ *presque nilpotente*$\}$ *est un idéal premier de* A *et* N *est* p*-primaire.*

Démonstration

Soient $a,b \in A$ tels que ab appartienne à p et $a \notin p$.

Si $x \in M/N$, il existe $n \in N^*$ tel que $a^n b^n x = 0$. Comme l'homothétie $\delta_a^{M/N}$ est injective, il en est de même de $\delta_a^{M/N} = (\delta_a^{M/N})^n$. Donc, $b^n x = 0$. L'homothétie $\delta_b^{M/N}$ est presque nilpotente.

Remarque

Si le sous-module N de M est p-primaire et si M/N est *de type fini*, $p = r(\mathrm{Ann}(M/N))$

Proposition III.3

Soient A *un anneau,* S *une partie multiplicative de* A, p *un idéal premier de* A *tel que* $S \cap p = \emptyset$, M *un* A*-module,* N *un sous-module* p*-primaire de* M.

Alors N *est saturé pour* S.

Démonstration

Comme $S \subset A\text{-}p$, il suffit de démontrer que N est saturé pour $A\text{-}p$. Ceci résulte de la définition même d'un sous-module primaire : soient $s \in A\text{-}p$, $x \in M$ tel que sx appartienne à N ; si $\bar{x}$ est la classe de x modulo N, $s\bar{x} = 0$; comme $\delta_s^{M/N}$ est injective, $\bar{x} = 0$, i.e. x appartient à N.

Corollaire

Soient A *un anneau,* S *une partie multiplicative.*

L'application : $p \longmapsto S^{-1}p$ *est une bijection croissante de l'ensemble des idéaux premiers de* A *disjoints de* S *sur l'ensemble des idéaux premiers de* $S^{-1}A$.

Démonstration

Il suffit de vérifier que l'idéal $S^{-1}p$ *est premier.*

D'abord $S^{-1}p \neq S^{-1}A$ car sinon on aurait une égalité $a/s = 1/1$ où $a \in p$, $s \notin p$ et donc une égalité $ta = ts$ pour un élément t de S, égalité impossible car ts appartient à S, ts à p et $p \cap S = \emptyset$.

On laisse au lecteur les autres vérifications. On peut d'ailleurs procéder autrement en utilisant le lemme suivant.

Lemme

Soient A *un anneau,* S *une partie multiplicative de* A, a *un idéal de* A, p *la surjection canonique de* a *sur* A/a.

Alors $p(S)$ *est une partie multiplicative de* A/a *et* $S^{-1}a$ *est isomorphe à* $p(S)^{-1}(A/a)$.

Démonstration du lemme

On définit un homomorphisme θ de $S^{-1}A$ dans $p(S)^{-1}p(A)$ par $\theta(a/s) = p(a)/p(s)$.

Il est *surjectif* comme p et *son noyau* est $S^{-1}a$.

On applique le lemme au cas où a est un idéal premier p disjoint de S. Alors, 0 n'appartient pas à $p(S)$. L'anneau $p(S)^{-1}p(A)$ est intègre comme anneau de fractions de l'anneau intègre $p(A) = A/p$ par rapport à une partie multiplicative ne contenant pas 0.

On remarquera que les idéaux *maximaux* de $S^{-1}A$ correspondent aux idéaux de A maximaux dans l'ensemble des idéaux de A disjoints de S.

Corollaire 2

Soient A *un anneau,* p *un idéal premier de* A.

L'anneau A_p *des fractions de* A *par rapport à la partie multiplicative* A-p *est local d'idéal maximal* pA_p *et de corps résiduel isomorphe au corps des fractions de* A/p.

Démonstration

Il résulte de ce qui précède que pA_p est l'unique idéal maximal de A_p. On déduit du lemme que A_p/pA_p est le corps des fractions de l'anneau intègre A/p.

Corollaire 3

Soient A *un anneau,* S *une partie multiplicative de* A, p *un idéal premier de* A *ne rencontrant pas* S, M *un* A*-module.*

L'application $N \longrightarrow S^{-1}N$ *est une bijection croissante de l'ensemble des sous-modules* p*-primaires de* M *sur l'ensemble des sous-modules* $S^{-1}p$*-primaires de* $S^{-1}M$.

Démonstration

Le sous-module $S^{-1}N$ *de* $S^{-1}M$ *est* $S^{-1}p$*-primaire.* Soit, en effet, $a/s \in S^{-1}A$ $(a \in A, s \in S)$. Si $a/s \notin S^{-1}p$, a n'appartient pas à p ; si $(a/s)\bar{y} = 0$ où $\bar{y} = \bar{x}/t$ $(\bar{x} \in M/N,\ t \in S)$, il existe $u \in S$ tel que $(ua)\bar{x} = 0$ mais $u \notin p$ puisque $p \cap S = \emptyset$ et donc ua n'appartient pas à p et $\bar{x} = 0$. Ainsi, l'homothétie $\delta^{S^{-1}M/S^{-1}N}_{a/s}$ est injective. Il est clair, par contre, que si a/s appartient à $S^{-1}p$, i.e. si a appartient à p, l'homothétie de rapport a/s est presque nilpotente comme celle de rapport a.

Il reste à démontrer que *si* P *est un sous-module* $S^{-1}p$*-primaire de* $S^{-1}M$, $(i_A^S)^{-1}(P)$ *est un sous-module* p*-primaire de* M.

Soient $a\in A$, $x\in M$ tels que ax appartienne à $(i_M^S)^{-1}(P)$, i.e. tels que $(a/1)(x/1)$ appartienne à P.

Si $a\notin p$, $a/1$ n'appartient pas à $S^{-1}p$ et donc $x/1$ appartient à P et x appartient à $(i_M^S)^{-1}(P)$.

Si $a\in p$, il existe $n(x)\in N$ tel que $(a/1)^{n(x)}(x/1)$ appartienne à P. Il existe donc $s\in S$ tel que $sa^{n(x)}x$ appartienne à $(i_M^S)^{-1}(P)$ et, puisque ce sous-module est saturé pour S, $a^{n(x)}x$ appartient à $(i_M^S)^{-1}(P)$.

IV. Changement de parties multiplicatives

Proposition IV.1 (*transitivité des anneaux de fractions*)

Soient A *un anneau,* S *et* T *deux parties multiplicatives telles que* $S\subset T$, M *un* A*-module.*

1. La partie $S^{-1}T = \{t/s \text{ où } t\in T,\ s\in S\}$ *de l'anneau* $S^{-1}A$ *est multiplicative.*

2. Il existe un isomorphisme θ *de l'anneau* $T^{-1}A$ *dans l'anneau* $(S^{-1}T)^{-1}(S^{-1}A)$ *qui applique l'élément* a/t *sur l'élément* $(a/1)/(t/1)$.

3. Il existe un isomorphisme de $T^{-1}A$*-modules du module* $T^{-1}M$ *sur le module* $\theta_*((S^{-1}T)^{-1}(S^{-1}M))$ *qui applique l'élément* x/t *sur l'élément* $(x/1)/(t/1)$.

Démonstration

1. Est évident.

2. Soit u l'homorphisme composé $i_{S^{-1}A}^{S^{-1}T}\circ i_A^S$ de A dans $(S^{-1}T)^{-1}(S^{-1}A)$. Il applique $s\in A$ sur $(a/1)/(1/1)$. Si $t\in T$, u(t) est inversible d'inverse $(1/1)/(t/1)$. Il existe donc un homomorphisme θ de l'anneau $T^{-1}A$ dans l'anneau rendant commutatif le diagramme

$$\begin{array}{ccc} A & \xrightarrow{i_A^S} & S^{-1}A \\ {\scriptstyle i_A^T}\downarrow & & \downarrow{\scriptstyle i_{S^{-1}A}^{S^{-1}T}} \\ A & \xrightarrow[\theta]{} & (S^{-1}T)^{-1}(S^{-1}A) \end{array}.$$

Il est clair que $\theta(a/t) = u(a)/u(t) = (a/1)/(t/1)$.

L'homomorphisme θ *est injectif* : en effet, l'égalité $\theta(a/t) = 0$ implique l'existence d'un élément t'/s' où $t'\in T$, $s'\in S$ tel que

$(t'/s')(a/1) = 0$, i.e. $t'a/s' = 0$, et donc l'existence de $s'' \underset{S}{\in} S$ tel que $(s''t')a \underset{S}{=} 0$. Comme $S \subset T$, $s''t'$ appartient à T et donc $a/t \underset{T}{=} 0$.

L'homomorphisme θ *est surjectif* : il suffit de remarquer que l'élément $(a/s)/(t/s')$ de $(S^{-1}T)^{-1}(S^{-1}A)$ s'écrit $((as'/1)/(st)/1)$ et est donc $\underset{S}{=}$ $\underset{S}{=}$ $\theta((as')/(st))$.
$\underset{T}{=}$

3. La démonstration est laissée au soin du lecteur.

Exemple : On peut, en particulier, appliquer ce résultat au cas où $M = A$ et T est la *partie multiplicative des éléments réguliers de* A.

Il est clair qu'un élément de $S^{-1}T$ où S est une partie multiplicative contenue dans T est régulier dans $S^{-1}A$.

L'application $i^{S^{-1}T}_{S^{-1}A}$ est donc un homomorphisme *injectif* de l'anneau $S^{-1}A$ dans l'anneau $(S^{-1}T)^{-1}(S^{-1}A)$ isomorphe à l'anneau $T^{-1}A$, c'est à dire à l'anneau total des fractions de A.

Ainsi, *tous les anneaux de fractions de* A *par rapport à des parties formées d'éléments réguliers de* A *s'identifient à des sous anneaux de l'anneau total des fractions de* A.

En particulier, si *l'anneau* A *est intègre, tout anneau de fractions de* A *s'identifie à un sous-anneau du corps des fractions de* A.

Corollaire 1

Soient A *un anneau,* S *une partie multiplicative de* A, q *un idéal premier de* A *ne rencontrant pas* S, M *un* A*-module.*

1. Les anneaux $(S^{-1}A)_{S^{-1}q}$ *et* A_q *sont isomorphes.*

2. Les A_q*-modules* $(S^{-1}M)_{S^{-1}q}$ *et* M_q *sont isomorphes.*

Démonstration

Il suffit d'appliquer la proposition IV.1 au cas où $T = A\text{-}q$.

Le corollaire suivant est la justification du fait remarquable que, dans certaines questions, la seule considération des idéaux premiers qui sont *maximaux* est suffisante.

Corollaire 2

Soient A *un anneau,* p *et* q *des idéaux premiers tels que* $q \subset p$, M *un* A*-module.*

1. Les anneaux $(A_p)_{qA_p}$ *et* A_q *sont isomorphes.*

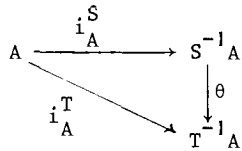
2. *Les* A_q*-modules* M_q *et* $(M_p)_{qA_p}$ *sont isomorphes.*

En particulier, pour tout idéal maximal m contenant un idéal premier q, l'anneau A_q (resp. A_q-module M_q) est un localisé de l'anneau A_m (resp. du A_m-module M_m).

Proposition IV.2 (*égalité d'anneaux de fractions*)

Soient A *un anneau,* S *et* T *des parties multiplicatives telles que* $S \subset T$.

1. *Il existe un homomorphisme d'anneaux* θ *et un seul de* $S^{-1}A$ *dans* $T^{-1}A$ *tel que la diagramme*



soit commutatif. Il est tel que $\theta(a/s) = a/s$.

2. *Les assertions suivantes sont équivalentes :*

(*i*) θ *est un isomorphisme*

(*ii*) *l'ensemble des idéaux premiers ne rencontrant pas* T *est égal à celui des idéaux premiers ne rencontrant pas* S.

(*iii*) S *et* T *engendrent la même partie multiplicative saturée.*

Démonstration

1. L'existence et l'unicité de θ résulte de ce que, pour tout $s \in S$, $i_A^T(s)$ est inversible et de la propriété universelle de i_A^S.

2. L'implication (i) $\Longrightarrow$ (ii) résulte de l'existence d'une bijection de l'ensemble des idéaux premiers ne rencontrant pas T (resp. S) sur l'ensemble des idéaux premiers de $T^{-1}A$ (resp. $S^{-1}A$).

L'implication (ii) $\Longrightarrow$ (iii) résulte de ce que la partie multiplicative saturée engendrée par S (resp. T) est $\bigcap A\text{-}p$ où p parcourt l'ensemble des idéaux premiers ne rencontrant pas S (resp. T).

(iii) $\Longrightarrow$ (i) : on peut évidemment supposer que T est la partie multiplicative saturée engendrée par S. *L'application* θ *est surjective* : soit a/t de $T^{-1}A$; il existe t' de T tel que tt' appartienne à S ; comme $a/t = t'a/t't$, $a/t = \theta(t'a/t't)$. *L'application* θ *est injective* : si $a/s = 0$, il existe t' dans T tel que $t'a = 0$. Si t" est un élément de T tel que $t"t' \in S$, $t"t'a = 0$ et donc $a/s = 0$.

Complément : Sous les hypothèses de la proposition III.2. si M est un A-module, l'application $x/s \longrightarrow x/s$ *de* $S^{-1}M$ *dans* $T^{-1}M$ *est bien définie Si S et T engendrent la même multiplicative saturée, c'est un isomorphisme de* $S^{-1}A$*-modules.*

V. Le principe de globalisation

On verra, chapitre 4, que l'on peut considérer un idéal premier p d'un anneau A comme un point d'un espace topologique attaché à A : son spectre. Si M est un A-module, le A_p-module M_p rend compte des propriétés de M en le point p.

Soit $P(A,M)$ *une propriété définie pour tout couple* (A,M) *d'un anneau* A *et d'un* A*-module* M.

On dit qu'elle est *ponctuellement*(*) vérifiée par le couple (A,M) si, pour tout $p \in \mathrm{Spec}(A)$, la propriété $P(A_p,M_p)$ est vraie.

Le principe de globalisation permet, dans certains cas, d'affirmer que la propriété $P(A,M)$ est vraie si et seulement si elle est vraie ponctuellement. Tel est le cas par exemple pour la propriété P(A,M) : M est un A-module plat.

1. Le principe de globalisation

Proposition V.1

Soient A *un anneau,* M *un* A*-module.*

L'application A*-linéaire :* $x \longmapsto ((i_A^p)(x)$ *de* M *dans* $\prod_{p\in\mathrm{Spec}(A)} M_p$ *(resp.* $\prod_{p\in\mathrm{Max}(A)} M_p$*) est injective.* (On désigne par Max(A) l'ensemble des idéaux maximaux).

Démonstration

Soit x un élément du noyau de cette application.

Pour tout $p \in \mathrm{Spec}(A)$ (resp. tout p maximal), il existe $s_p \in A$ n'appartenant pas à p tel que $s_p x = 0$.

(*) La plupart des auteurs disent *localement* au lieu de ponctuellement. On verra qu'a tout $f\in A$ correspond un ouvert $D(f)$ du spectre, $D(f) = \{p\in\mathrm{Spec}(A)/f\notin p\}$. On devrait dire que (A,M) vérifie *localement* P si, tout $p \in \mathrm{Spec}(A)$, il existe un voisinage ouvert $D(f)$ de p tel que $P(A_f,M_f)$ soit vérifiée. Il se trouve que ces deux points de vue sont souvent équivalents

L'annulateur de x n'est donc contenu dans aucun idéal premier (resp. maximal). Il est égal à A et x = 0.

Le lecteur pourra déduire les corollaires 1 et 2 soit de la proposition V.1 soit de la proposition ci-dessous qui fait, elle, intervenir la somme et non le produit.

Proposition V.2

Soit A *un anneau. Le* A*-module* $\oplus_{p\in Max(A)} A_p$ *est fidèlement plat.*

Démonstration

La platitude résulte de ce qu'une somme directe de modules plats est un module plat. Il suffit donc de vérifier que le A-module $\oplus_{p\in Max(A)} A_p$ est *fidèlement* plat et, à cet effet, que, pour tout idéal maximal m de A, $m(\oplus_{p\in Max(A)} M_p)$ est distinct de $\oplus_{p\in Max(A)} M_p$. Ceci résulte de ce que $mA_m \neq A_m$.

Corollaire 1

Soient A *un anneau,* M *un* A*-module. Les assertions suivantes sont équivalentes :*

(i) $M = 0$

(ii) $M_p = 0$ *pour tout idéal premier* p *de* A.

(iii) $M_p = 0$ *pour tout idéal maximal* p *de* A.

Corollaire 2

Soient A *un anneau,* f *une application* A*-linéaire du* A*-module* M *dans le* A*-module* N. *Les assertions suivantes sont équivalentes :*

(i) f *est injective* (resp. *surjective* ; resp. *bijective*)

(ii) f_p *est injective* (resp. *surjective* ; resp. *bijective*) *pour tout idéal premier* p *de* A.

(iii) f_p *est injective* (resp. *surjective* ; resp. *bijective*) *pour tout idéal maximal* p *de* A.

Démonstration

De la suite exacte $0 \longrightarrow \ker(f) \longrightarrow M \xrightarrow{f} N \longrightarrow \operatorname{coker}(f) \longrightarrow 0$ on déduit, pour tout idéal premier p de A, la suite exacte

$0 \longrightarrow (\ker(f))_p \longrightarrow M_p \xrightarrow{f_p} N_p \longrightarrow (\operatorname{coker}(f))_p \longrightarrow 0.$

Donc, $\ker(f)_p = \ker(f_p)$ et $\operatorname{coker}(f)_p = \operatorname{coker}(f_p)$.

Dire que f est injective (resp. surjective) c'est dire que $\ker(f)=0$ (resp. $\operatorname{coker}(f) = 0$) soit, pour tout $p \in \operatorname{Spec}(A)$, $\ker(f)_p = 0$ (resp. $\operatorname{coker}(f)_p = 0$), i.e. f_p injective (resp. surjective).

Corollaire 3

Soient A *un anneau,* M *un* A*-module,* x *un élément de* M, N *un sous module de* M. *Les assertions suivantes sont équivalentes :*

(i) x *appartient à* N

(ii) pour tout idéal premier p (resp. *maximal*), *l'image de* x *dans* M_p *appartient à* N_p.

Démonstration

Soit $\overline{x}$ l'image de x dans A-module M/N. L'assertion (i) se traduit par la nullité du A-module $P = A\overline{x}$. La condition (ii) se traduit par le fait que le A_p-module P_p est nul pour tout idéal premier (resp. maximal) p de A. Il suffit d'appliquer le corollaire 1.

Appliquant le corollaire 3 au cas particulier où le A-module M est A et où N est donc un idéal a de A, on voit qu'*un élément* x *de* A *appartient à* a *si et seulement si, pour tout idéal premier* (resp. *maximal*) p *de* A, *l'image de* x *dans* A_p *appartient à* a_p.

Proposition V.3

Soient A *un anneau intègre,* K *son corps des fractions.*

On identifie, pour tout idéal maximal m *de* A, A_m *à un sous-anneau de* K.

Alors $A = \bigcap_{m \in \mathrm{Max}(A)} A_m$ *où* Max(A) *désigne l'ensemble des idéaux maximaux de* A.

Démonstration

L'inclusion $A \subset \bigcap_{m \in \mathrm{Max}(A)} A_m$ est claire.

Soit $x \in \bigcap_{m \in \mathrm{Max}(A)} A_m$.

Pour tout $m \in \mathrm{Max}(A)$, il existe $s_m \in A-m$ et $y_m \in A$ tel que $x = y_m/s_m$. Alors, $s_m x$ appartient à A.

L'idéal $\{b \in A / bx \in A\}$ est égal à A car il n'est contenu dans aucun idéal maximal.

Donc, 1 appartient à cet idéal et x appartient à A.

2. Support d'un module

Soient A *un anneau,* a *un idéal de* A.

On note Spec(A) (resp. $V(a)$) l'ensemble des idéaux premiers de A (resp. des idéaux premiers de A contenant a).

Il est facile d'interpréter $V(a)$ grace au A-module monogène A/a :

$V(a) = \{p \in \mathrm{Spec}(A)/(A/a)_p \neq 0\}$

Ceci suggère la définition générale suivante.

Définition

Soit M *un* A*-module.*

On appelle support de M *et on note* $\mathrm{Supp}_A(M)$ *le sous-ensemble* $\{p \in \mathrm{Spec}(A)/M_p \neq 0\}$ *de* Spec(A).

Proposition V.4 *(premières propriétés du support)*

1. *Si le* A*-module* M *est monogène* $\simeq A/a$, $\mathrm{Supp}_A(M) = V(\mathrm{Ann}(M)) = V(a)$.
2. *Les assertions suivantes sont équivalentes :*
   (i) $M = (0)$
   (ii) $\mathrm{Supp}_A(M) = \emptyset$
3. *Si* $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ *est une suite exacte,* $\mathrm{Supp}_A(M) = \mathrm{Supp}_A(M') \cup \mathrm{Supp}_A(M'')$.
4. *Soit* $(M_i)_{i \in I}$ *une famille de sous-modules du* A*-module* M.

   $\mathrm{Supp}_A(\sum_{i \in I} M_i) = \bigcup_{i \in I} \mathrm{Supp}_A(M_i)$

5. *Soit* $(e_i)_{i \in I}$ *un système de générateurs du* A*-module* M.

   $\mathrm{Supp}_A(M) = \bigcup_{i \in I} \mathrm{Supp}_A(Ae_i) = \bigcup_{i \in I} V(\mathrm{Ann}(e_i)) \subset V(\mathrm{Ann}(M))$

Si le A*-module* M *est de TYPE FINI,* $\mathrm{Supp}_A(M) = V(\mathrm{Ann}(M))$ *et donc,* $\mathrm{Supp}_A(M)$ *est un fermé de* Spec(A).

6. *Soit* $(M_i)_{i \in I}$ *une famille de* A*-modules.*

   $\mathrm{Supp}_A(\bigoplus_{i \in I} M_i) = \bigcup_{i \in I} \mathrm{Supp}_A(M_i)$.

Démonstration

1. Est clair.

2. Si $M \neq (0)$, soit x un élément non nul de M. Il est clair que $\mathrm{Supp}_A(Ax)$ est non vide et contenu dans $\mathrm{Supp}_A(M)$.

3. Résulte de ce que, pour tout $p \in \mathrm{Spec}(A)$, la suite $0 \longrightarrow M'_p \longrightarrow M_p \longrightarrow M''_p \longrightarrow 0$ est exacte.

4. Résulte de ce que, pour tout $p \in \mathrm{Spec}(A)$,

   $(\sum_{i \in I} M_i)_p = \sum_{i \in I} (M_i)_p$

5. Résulte de 4. appliqué à $M_i = Ae_i$, de ce que $\mathrm{Ann}(Ae_i) = \mathrm{Ann}(e_i)$ et de l'égalité $\mathrm{Ann}(M) = \bigcap_{i \in I} \mathrm{Ann}(e_i)$.

Si M est de type fini, on peut choisir I *fini* et alors $V(\bigcap_{i\in I} \mathrm{Ann}(e_i)) = \bigcup_{i\in I} V(\mathrm{Ann}(e_i))$ soit $V(\mathrm{Ann}(M)) = \bigcup_{i\in I} \mathrm{Supp}(Ae_i) = \mathrm{Supp}_A(M)$.

6. Résulte de ce que, pour tout $p \in \mathrm{Spec}(A)$, $(\bigoplus_{i\in I} M_i)_p = \bigoplus_{i\in I}(M_i)_p$.

VI. Modules de fractions, produit tensoriel et modules Hom

1. Modules de fractions et produit tensoriel

Proposition VI.1

Soient M *et* N *des* A*-modules.*

Il existe un isomorphisme ν *de* $S^{-1}A$*-modules de* $(S^{-1}M) \underset{S^{-1}A}{\otimes} (S^{-1}N)$ *sur* $S^{-1}(M \underset{A}{\otimes} N)$ *tel que* $\nu((x/s) \otimes (y/t)) = (x \otimes y)/(st)$.

En particulier, si p *est un idéal premier de* A*, on a un isomorphisme de* A_p*-modules de* $M_p \underset{A_p}{\otimes} N_p$ *sur* $(M \underset{A}{\otimes} N)_p$.

Démonstration

Il suffit en utilisant l'associativité du produit tensoriel d'écrire la suite d'isomorphismes :

$$(S^{-1}M) \underset{S^{-1}A}{\otimes} (S^{-1}N) \xrightarrow{\sim} (S^{-1}M) \underset{S^{-1}A}{\otimes} (S^{-1}A \underset{A}{\otimes} N) \xrightarrow{\sim} (S^{-1}M) \underset{A}{\otimes} N \xrightarrow{\sim} S^{-1}A \underset{A}{\otimes} M \underset{A}{\otimes} N$$

$$\downarrow$$

$$S^{-1}(M \underset{A}{\otimes} N)$$

Corollaire 1

Soient M *et* M' *des* A*-modules DE TYPE FINI.*

Alors $\mathrm{Supp}_A(M \underset{A}{\otimes} M') = \mathrm{Supp}_A(M) \cap \mathrm{Supp}_A(M')$.

Démonstration

Il suffit de démontrer l'assertion suivante :

Soit A *un anneau local d'idéal maximal* m.

Si M *et* M' *sont des* A*-modules de type fini, les assertions suivantes sont équivalentes :*

1. $M \underset{A}{\otimes} N = (0)$
2. $M = 0$ *ou* $N = 0$.

Il est clair que 2. implique 1. *sans hypothèse de finitude.*

1. $\Longrightarrow$ 2. Tensorisant $M \underset{A}{\otimes} N$ à droite et à gauche par A/m et tenant compte de ce que $A/m \underset{A}{\otimes} M$ (resp. $N \underset{A}{\otimes} A/m$) s'identifie à M/mM (resp. N/mN), on obtient $(0) = M/mM \underset{A}{\otimes} N/mN$.

Mais $M/mM \underset{A}{\otimes} N/mN \simeq M/mM \underset{A/m}{\otimes} N/mN$. L'égalité $M/mM \underset{A/m}{\otimes} N/mN = (0)$ implique $M/mM = (0)$ ou $N/mN = (0)$. Il suffit d'appliquer alors le lemme de Nakayama. ((FFAC). chap.3 prop.IV.8).

Corollaire 2

Soient A *un anneau,* U_A *l'un des foncteurs* T_A (algèbre tensorielle), S_A (algèbre symétrique), Λ_A (algèbre extérieure), S *une partie multiplicative de* A. *Il existe un isomorphisme fonctoriel* (en le A-module M) *de* $U_{S^{-1}A}(S^{-1}M)$ *sur* $S^{-1}(U_A(M))$.

Démonstration

Posant $T^n_A(M) = \overbrace{M \underset{A}{\otimes} \dots \underset{A}{\otimes} M}^{n}$ en sorte que $T_A(M) = \bigoplus_{n=0}^{\infty} T^n_A(M)$, on voit que $S^{-1}T^n_A(M)$ est isomorphe (fonctoriellement) à $T^n_{S^{-1}A}(S^{-1}M)$. On en déduit l'assertion pour $U_A = T_A$.

Les autres assertions résultent de ce que $S_A(M)$ (resp. $\Lambda_A(M)$) est le quotient $T_A(M)/I_M$ où I_M est l'idéal engendré par les tenseurs $x\otimes y - y\otimes x$ (resp. $x\otimes x$), où x et y parcourent M, et de ce que $S^{-1}I_M$ s'identifie, dans l'isomorphisme de $S^{-1}T_A(M)$ sur $T_{S^{-1}A}(S^{-1}M)$ à l'idéal $I_{S^{-1}M}$.

2. *Foncteurs* Tor *et modules de fractions*

Proposition VI.2

Soient A *et* B *des anneaux,* $f : A \longrightarrow B$ *un homomorphisme plat.*

Pour tout entier naturel n, *il existe un isomorphisme fonctoriel du foncteur* $B \underset{A}{\otimes} \mathrm{Tor}^A_n(-,-)$ *sur le foncteur* $\mathrm{Tor}^B_n(B \underset{A}{\otimes} -\ ,\ B \underset{A}{\otimes} -)$.

Démonstration

Si un A-module P est projectif et donc facteur direct d'un A-module libre, le B-module $B \underset{A}{\otimes} P$ est facteur direct d'un B-module libre et donc projectif.

Soit $\dots \longrightarrow P_n \xrightarrow{d_n} P_{n-1} \longrightarrow \dots \longrightarrow P_1 \xrightarrow{d_1} P_o \xrightarrow{\varepsilon} M \longrightarrow 0$

la résolution projective du A-module M telle que :

$$\mathrm{Tor}^A_n(M,N) = H_n((P_i \underset{A}{\otimes} N\ ,\ d_i \otimes N)) \quad \text{(FFAC. chap.6)}$$

Comme B est plat sur A, la suite :

$$\dots \longrightarrow B \underset{A}{\otimes} P_n \xrightarrow{B\otimes d_n} B \underset{A}{\otimes} P_{n-1} \longrightarrow \dots \longrightarrow B \underset{A}{\otimes} P_1 \xrightarrow{B\otimes d_1} B \underset{A}{\otimes} P_o \xrightarrow{B\otimes\varepsilon} B \underset{A}{\otimes} M \longrightarrow 0$$

est une résolution projective du B-module $B \underset{A}{\otimes} M$.

Cette résolution est évidemment fonctorielle.

On en déduit aisément l'existence d'un isomorphisme, fonctoriel en M et N, du B-module $H_n((B \underset{A}{\otimes} P_i) \underset{B}{\otimes} (B \underset{A}{\otimes} N)$, $(B \bullet d_1) \bullet (B \bullet N))$ sur le B-module $\mathrm{Tor}_n^B(B \underset{A}{\otimes} M$, $B \underset{A}{\otimes} N)$.

Il existe, d'autre part, un isomorphisme fonctoriel en M et N du B-module $B \underset{A}{\otimes} \mathrm{Tor}_n^A(M,N) = B \underset{A}{\otimes} (\ker(d_n \bullet N)/\mathrm{im}(d_{n+1} \bullet N))$ sur le B-module $H_n((B \underset{A}{\otimes} P_i) \underset{B}{\otimes} (B \underset{A}{\otimes} N), \ldots)$.

En composant les deux isomorphismes précédents, on obtient l'isomorphisme cherché.

Corollaire 1

Soient A *un anneau,* p *un idéal premier de* A, M *et* N *des* A*-modules. Alors,* $\mathrm{Tor}_n^A(M,N)_p$ *est isomorphe à* $\mathrm{Tor}_n^{A_p}(M_p,N_p)$.

Corollaire 2

Soit M *un* A*-module.*

Les assertions suivantes sont équivalentes :

(i) M *est un* A*-module plat*

(ii) pour tout $p \in \mathrm{Spec}(A)$, M_p *est un* A_p*-module plat*

(iii) pour tout $m \in \mathrm{Max}(A)$, M_m *est un* A_m*-module plat*

Démonstration

(i) $\Longrightarrow$ (ii). Il suffit d'utiliser la caractérisation des modules plats en termes de Tor_1 ((FFAC), chap.6, th.V.2), le fait qu'un A_p-module N est $((i_A^p)_*(N))_p$.

(ii) $\Longrightarrow$ (iii) est clair.

(iii) $\Longrightarrow$ (i) . Soit N un A-module. Pour tout $m \in \mathrm{Max}(A)$, $\mathrm{Tor}_1^A(M,N)_m = \mathrm{Tor}_1^{A_m}(M_m,N_m) = 0$.

Donc, $\mathrm{Tor}_1^A(M,N) = 0$ (prop.V.2 ; cor.1) et M est plat.

3. Foncteurs Ext et modules de fractions

La situation est plus compliquée pour les Ext que pour les Tor. On doit supposer éventuellement certains modules *de présentation finie.*

Proposition VI.3

Soient A *un anneau,* S *une partie multiplicative de* A.

Pour tout couple (M,N) *de* A*-modules, il existe une application li-*

néaire $\phi_{M,N}$ *du* $S^{-1}A$*-module* $S^{-1}\mathrm{Hom}_A(M,N)$ *dans le* $S^{-1}A$*-module* $\mathrm{Hom}_{S^{-1}A}(S^{-1}M,S^{-1}N)$ *telle que :*

$$\phi_{M,N}(u/s)(x/t) = u(x)/(st) \qquad (u \in \mathrm{Hom}_A(M,N),\ x\in M, s,t\in S)$$

Les applications $\phi_{M,N}$ *définissent un morphisme du foncteur* $S^{-1}\mathrm{Hom}_A(-,-)$ *dans le foncteur* $\mathrm{Hom}_{S^{-1}A}(S^{-1}-,S^{-1}-)$.

Si le A-module M est de présentation finie, $\phi_{M,N}$ *est un isomorphisme*

Démonstration

On vérifie que si $u/s = u'/s'$, les éléments v et v' de $\mathrm{Hom}_{S^{-1}A}(S^{-1}M,S^{-1}N)$ tels que $v(x/t) = u(x)/(st)$ et $v'(x/t) = u'(x)/(st)$ sont égaux La définition de $\phi_{M,N}$ a donc un sens. On vérifie aisément la fonctorialité.

Les foncteurs $F = S^{-1}\mathrm{Hom}_A(-,N)$ et $G = \mathrm{Hom}_{S^{-1}A}(S^{-1}-,S^{-1}N)$ commutent aux sommes directes finies. Ils sont exacts à gauche.

L'application $\phi_{A,N}$ est un isomorphisme comme il résulte du diagramme commutatif dont les flèches horizontales sont les isomorphismes canoniques

$$\begin{array}{ccc} S^{-1}\mathrm{Hom}_A(A,N) & \longrightarrow & S^{-1}N \\ \downarrow{\scriptstyle \phi_{A,N}} & & \downarrow{\scriptstyle 1_{S^{-1}N}} \\ \mathrm{Hom}_{S^{-1}A}(S^{-1}A,S^{-1}N) & \longrightarrow & S^{-1}N \end{array}$$

Un raisonnement dual de celui de la proposition IV.9 de (FFAC) chap.3 prouve le fait que $\phi_{M,N}$ est un isomorphisme si M est de présentation finie.

Proposition VI.4

Les notations sont celles de la proposition VI.3.

On suppose que le A-module M a une résolution libre

$$\ldots \longrightarrow P_n \xrightarrow{d_n} P_{n-1} \longrightarrow \ldots \longrightarrow P_1 \xrightarrow{d_1} P_o \xrightarrow{\varepsilon} M \longrightarrow 0$$

où les modules P_n *sont de type fini.*

Pour tout entier naturel n*, il existe un isomorphisme fonctoriel du foncteur* $S^{-1}\mathrm{Ext}^n_A(M,-)$ *dans le foncteur* $\mathrm{Ext}^n_{S^{-1}A}(S^{-1}M,S^{-1}-)$.

Démonstration

Il suffit de remarquer, si $R_n = \mathrm{im}(d_n)$ (avec la convention $R_o = \mathrm{im}(\varepsilon) = M$), l'existence d'un isomorphisme fonctoriel de

$\mathrm{Ext}^n_{S^{-1}A}(S^{-1}M, S^{-1}-)$ (resp. $S^{-1}\mathrm{Ext}^n_A(M,-)$) dans $\mathrm{Hom}_{S^{-1}A}(S^{-1}R_n, S^{-1}-)$ (resp. $S^{-1}\mathrm{Hom}_A(R_n,-)$) et d'appliquer la proposition précédente.

Corollaire

Soient A *un anneau,* p *un idéal premier de* A, M *un* A*-module satisfaisant à la condition de la proposition VI.4,* N *un* A*-module.*

Alors, $\mathrm{Ext}^n_A(M,N)_p$ *est isomorphe à* $\mathrm{Ext}^n_{A_p}(M_p, N_p)$.

Remarques

1. Comme la proposition VI.3, la proposition VI.4 peut être démontrée par un procédé de décalage.

2. On appliquera surtout la proposition VI.4 sous l'hypothèse A *noethérien*. L'hypothèse faite sur le A-module M devient alors que M est *de type fini*.

Exercices du chapitre 1

(1). Une partie multiplicative saturée d'un anneau A contient-elle l'ensemble des éléments inversibles de A ?

(2). Quel est l'anneau des fractions de l'anneau A par rapport à la partie multiplicative des éléments inversibles de A ?

(3). Soient k un anneau, X une indéterminée, n un entier positif, $A = k[X]/(X^n)$, f la classe de X modulo (X^n). Calculer A_f.

(4). Soient A un anneau *intègre*, f un élément *non nul* de A. Démontrer que, si A n'est pas un corps, l'anneau A_f des fractions de A par rapport à {f} n'en est pas un.
(Utiliser la proposition I.1).

(5). Soient A un anneau, M un A-module de *type fini*, $\{e_1,\ldots,e_n\}$ un système fini de générateurs de M, f l'application : $a \longmapsto (ae_1,\ldots,ae_n)$ de A dans M^n.

Quel est le noyau de f ?

En déduire que, si B est une A-algèbre *plate*, $\mathrm{Ann}_B(B \otimes_A M) = B \otimes_A \mathrm{Ann}(M)$

Retrouver ainsi le fait que, si M est un A -module de type fini et S une partie de A, $\mathrm{Ann}(S^{-1}M) = S^{-1}\mathrm{Ann}(M)$.

(6). 1. Soient A un anneau *intègre*, K son corps des fractions, M un A-module.

Démontrer que le noyau de l'application $x \longmapsto 1 \otimes x$ de M dans

$K \underset{A}{\otimes} M$ est le sous-module de torsion $t(M) = \{x \in M / a \in A,\ a \neq 0$ tel que $ax = 0\}$ de M.

2. On ne suppose plus l'anneau A intègre. Soit K son anneau total des fractions.

Quel est alors le noyau de l'application : $x \longmapsto 1 \otimes x$ de M dans $K \underset{A}{\otimes} M$?

(7). Soient B un anneau, A un sous-anneau, q un idéal premier de B, b un idéal q-primaire de B, $p = q \cap A$, $a = b \cap A$.

L'idéal a est-il p-primaire ?

(8). Soient A un anneau, S une partie multiplicative de A, a un idéal projectif de A.

L'idéal $S^{-1}a$ de l'anneau $S^{-1}A$ est-il projectif ?

Un anneau de fractions d'un anneau de Dedekind ((FFAC).Chap.5.II.2) est-il un anneau de Dedekind ?

(9). Soient A un anneau, S une partie (multiplicative) de A, M un A-module.

1. Démontrer l'existence d'une application A-linéaire μ_M de $S^{-1}A \underset{A}{\otimes} M$ dans $S^{-1}M$ telle que $\mu_M((a/s) \otimes x) = (ax)/s$ $(a \in A\ ;\ s \in S\ ;\ x \in M)$ et sa fonctorialité. Que peut-on dire de μ_A ?

2. Démontrer que le foncteur $S^{-1}(-)$ commute aux sommes directe quelconques. Que peut-on dire de $\mu_A(I)$, où I est un ensemble ?

3. Utiliser une présentation d'un A-module M pour démontrer que μ_M est un isomorphisme. (Utiliser la prop.IV.9 du chapitre 3 de (FFAC)

Les exercices 10, 11, 12, 13, proposent une construction d'un module de fractions différente de celle indiquée dans le texte. Les exercices 10, 11 sont des cas particuliers qui doivent faciliter la compréhension. Le cas général est traité dans l'exercice 14.

(10). Soient A un anneau, a un élément de A, M un A-module.

Pour tout $n \in N$, on pose $M_n = M$. Si $n \leqslant m$, on définit l'application g_{mn} de M_n dans M_m comme étant δ_s^M m-n. On note $(\overline{M}, g_n)_{n \in N}$ le limite inductive du système inductif $(M_n, g_{mn})_{m,n \in N}$.

1. Démontrer, en utilisant les égalités $\overline{M} = \bigcup_{n \in N} g_n(M_n)$ et $\ker(g_n) = \bigcup_{m \geqslant n} \ker(g_{mn})$ que l'homothétie $\delta_s^{\overline{M}}$ est bijective.

On munit $\overline{M}$ de la structure de $S^{-1}A$-module correspondante.

2. On suppose que M est $(i_A^S)_*(P)$ où P est un $S^{-1}A$-module.

Démontrer que l'on peut alors prendre $\overline{M} = P$ et $g_n = \delta^P_{1/s^n}$.

3. Revenant au cas général, soient N un $S^{-1}A$-module, f une application A-linéaire de M dans $(i_A^S)_*(N)$ (noté N dans la suite).

On définit M_n, N_n comme étant M, N et f_n comme étant f.

Démontrer que l'application $\overline{f} = \varinjlim(f_n)$ est l'unique application $S^{-1}A$-linéaire de $\overline{M}$ dans N telle que $f = \overline{f} \circ g_o$.

En déduire que $(\overline{M}, g_o)$ est un module de fractions de M par rapport à $S = \{s^n\}_{n \in \mathbb{N}}$.

(11). Soient A un anneau, S une partie multiplicative de A, M un A-module.

On suppose que tout élément de S est régulier.

La relation $\leqslant$ définie dans S par $s \leqslant t$ si il existe $a \in A$ tel que $t = as$ est une relation de préordre. Il sera utile pour la compréhension de l'exercice 14 de considérer la catégorie $\mathcal{S}$ dont les objets sont les éléments de S et l'ensemble des morphismes de $s \in S$ dans $t \in S$ est vide si s n'est pas $\leqslant$ t et l'ensemble réduit à a si $t = as$.

Si $s \in S$, on pose $M_s = M$. Si $s, t \in S$ et $s \leqslant t$, on définit l'application A-linéaire g_{ts} de M_s dans M_t comme étant S_a^M où $t = as$. Soit $(\overline{M}, g_s)_{s \in S}$ la limite inductive du système inductif $(M_s, g_{ts})_{s,t \in S}$.

Démontrer, comme dans l'exercice 10, que $(\overline{M}, g_1)$ est un module de fractions de M par rapport à S.

(12). (préliminaire catégoriques à l'étude du cas général)

Soient $\mathcal{C}$ une catégorie, A un anneau.

On suppose que la classe $\mathrm{Ob}(\mathcal{C})$ *des objets de* $\mathcal{C}$ *est un ensemble.*

Un système inductif de A-modules suivant $\mathcal{C}$ est un foncteur F covariant de $\mathcal{C}$ dans Mod(A).

Exemple : Un ensemble préordonné I définit une catégorie $\mathcal{I}$ ((FFAC). chap.1.ex.1) et un système inductif de A-module suivant $\mathcal{I}$ n'est autre qu'un système inductif de A-module indexé par l'ensemble préordonné I.

Une *limite inductive* du système inductif F est la donnée :

d'un A-module M

pour tout $s \in \mathrm{Ob}(\mathcal{C})$, d'une application A-linéaire g_s de $F(s)$ dans M, tels que, pour tout couple (s,t) d'objets de $\mathcal{C}$ et tout $a \in \mathrm{Hom}_{\mathcal{C}}(s,t)$, le diagramme

$$\begin{array}{ccc} F(s) & \xrightarrow{F(a)} & F(t) \\ & {\scriptstyle g_s} \searrow \quad \swarrow {\scriptstyle g_t} & \\ & M & \end{array}$$

soit commutatif,

cette donnée étant universelle en un sens que l'on laisse le soin au lecteur de préciser, à partir du cas classique.

1. Soit M *le* A*-module quotient de la somme directe* $\bigoplus_{s\in Ob(C)} F(s)$ *par le sous-module engendré par les éléments* $x_s - F(a)(x_s)$, *où* s *parcourt* $Ob(C)$ *a l'ensemble des morphismes de source* s *et où on a noté, abusivement,* $x_s - x_t$ l'élément de la somme directe dont toutes les coordonnées sont nulles sauf la s-ième qui est x_s et la t-ième qui est $-x_t$.

Soit, pour $s \in Ob(C)$, g_s *l'application* A*-linéaire composée de l'injection canonique de* $F(s)$ dans $\bigoplus_{t\in Ob(C)} F(t)$ *et de la surjection canonique de ce module sur* M.

Démontrer que $(M, g_s)_{s\in Ob(C)}$ est limite inductive de F,

2. On suppose que la catégorie C *vérifie la propriété suivante: pour tout ensemble fini* $s_1,\ldots,s_n$ *d'objets de* C, *il existe un objet* t *de* C *et des morphismes* $a_1,\ldots,a_n$ *respectivement de* $s_1,\ldots,s_n$ *dans* t.

Reprenant les démonstrations de ((FFAC). Chap. 1.II.7), démontrer alors les égalités :

$M = \bigcup_{s\in Ob(C)} g_s(F(s))$

$\ker(g_s) = \bigcup_a \ker(F(a))$, où a parcourt l'ensemble des morphismes de C de source s.

(13). Soient A un anneau, S une partie multiplicative, M un A-module.

On définit une catégorie S *comme suit:*

Les objets de S sont les éléments de S.

Si, $s,t \in S$, $\mathrm{Hom}_S(s,t) = \{a\in A / t = as\}$

La composition des morphismes est naturelle.

Cette catégorie S vérifie la propriété de l'exercice 12, question 2.

On définit un système inductif F *suivant* S *comme suit :*

pour tout $s\in S$, $F(s) = M$

pour tout $a\in \mathrm{Hom}_S(s,t)$, $F(a)$ est l'homothétie δ_a^M de rapport a de M.

Soit $(M, g_s)_{s\in S}$ *la limite inductive de* F.

Démontrer, comme dans l'exercice 11, que (M, g_1) est un module de fractions de M par rapport à S.

(14). Une sous-catégorie pleine C de Mod(A) est dite *localisante* si:

1) Pour toute suite exacte $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ de $\mathrm{Mod}(A)$ M appartient à $\mathrm{Ob}(\mathcal{C})$ si et seulement si M' et M'' appartiennent à $\mathrm{Ob}(C)$.

2) $\mathcal{C}$ est stable par limites inductives

1. Soient A un anneau, S une partie multiplicative.

Démontrer que la sous-catégorie pleine de $\mathrm{Mod}(A)$ dont les objets sont les A-modules M tels que $S^{-1}M = 0$ est localisante.

2. Démontrer qu'une sous-catégorie localisante $\mathcal{C}$ de $\mathrm{Mod}(A)$ est parfaitement déterminée par l'ensemble $I(\mathcal{C})$ des idéaux a tels que A/a soit objet de $\mathcal{C}$.

3. Caractériser les ensembles I d'idéaux de A de la forme $I(\mathcal{C})$.

(Le lecteur pourra se reporter à l'artcle de P. Gabriel. *Des catégories abéliennes. Bull. Soc. Math. France*, 90,1962,323-448, dans lequel est étudiée une théorie de la localisation valable pour les anneaux non commutatifs et fondée sur la considération de telles sous-catégories localisantes).

(15). La géométrie algébrique projective fait usage d'anneaux gradués, de modules gradués et, en particulier, d'idéaux homogènes. Il est donc indispensable d'étendre à ces objets gradués les résultats usuels.

Soient $A = \bigoplus_{i \in \mathbb{Z}} A_i$ un anneau gradué de type $\mathbb{Z}$, $M = \bigoplus_{i \in \mathbb{Z}} M_i$ un A-module gradué, S *une partie multiplicative de* A *dont tous les éléments sont homogènes*, par exemple, l'ensemble des puissances d'un élément homogène.

1. Démontrer qu'il existe une structure et une seule d'anneau gradué de type $\mathbb{Z}$ sur l'anneau de fractions $S^{-1}A$ telle que l'application i_A^S soit homogène de degré 0.

(On définit $(S^{-1}A)_i$ comme le sous-ensemble de $S^{-1}A$ des fractions a/s où a appartient à A_j et s à $S \cap A_{j-i}$).

2. Démontrer qu'il existe alors sur le $S^{-1}A$-module $S^{-1}M$ une structure et une seule de $S^{-1}A$-module gradué telle que l'application A-linéaire i_M^S soit homogène de degré 0.

(On remarquera qu'un anneau (resp. un module) peut toujours être muni de la graduation évidente où tout est concentré en degré 0. La théorie graduée contient donc la théorie usuelle comme cas particulier).

(16). Soit A un anneau.

1. Démontrer les équivalences :

(i) A est local et tout idéal de type fini de A est principal

(ii) l'ensemble des idéaux principaux de A est totalement ordonné par inclusion

(iii) l'ensemble des idéaux de A est totalement ordonné par inclusion

Un anneau satisfaisant à ces conditions est dit *local arithmétique*

2. On suppose l'anneau local arithmétique A intègre. Soit K son corps des fractions. Démontrer que, pour tout élément x de K, $x \in A$ ou $x^{-1} \in A$.

Réciproque ? (voir anneaux de valuation. chap. 4).

(17). Un anneau A est dit *arithmétique* si, pour tout idéal premier p de A, l'anneau local A_p est arithmétique (ex.16).

1. Démontrer qu'un anneau A est arithmétique si et seulement si l'anneau local A_p est arithmétique pour tout idéal *maximal* p de A, qu'un anneau de fractions d'un anneau arithmétique est arithmétique, qu'un quotient d'un anneau arithmétique est arithmétique.

2. Soit $(A_i, f_{ji})_{i,j \in I}$ un système inductif filtrant d'anneaux arithmétiques A_i.

Démontrer que l'anneau $\varinjlim (A_i)$ est arithmétique.

3. Utilisant le lemme de globalisation, démontrer les équivalences suivantes pour un anneau A :

(i) A est arithmétique

(ii) $(a+b) \cap c = a \cap c + b \cap c$ *pour tout triplet* (a,b,c) *d'idéaux de* A

(iii) $a+(b \cap c) = (a+b) \cap (a+c)$ *pour tout triplet* (a,b,c) *d'idéaux de* A

(iv) $(a+b):c = (a:c) + (b:c)$ *pour tout triplet* (a,b,c) *d'idéaux de* A *où* c *est de type fini.*

4. Démontrer que deux idéaux premiers sans relation d'inclusion d'un anneau arithmétique A sont étrangers.

5. Soient A un anneau arithmétique, K son anneau total des fractions, B un sous anneau de K contenant A. Démontrer que B est arithmétique.

6. Démontrer que si A est un anneau arithmétique semi-local tout idéal de type fini de A est principal.

7. Démontrer qu'un anneau dans lequel tout idéal *de type fini* est principal est un anneau arithmétique. Un tel anneau est appelé un *anneau de* Bezout.

(Deux exemples d'anneaux de Bezout intègres sont bien connus : l'anneau des fonctions entières (FFAC).chap.2.ex.16) et l'anneau des entiers

algébriques. Ces anneaux ne sont pas noethériens).

(18). Démontrer les équivalences pour un anneau A

(i) A_p est intègre pour tout idéal premier (resp. maximal) p de A

(ii) pour tout couple (a,b) d'éléments de A tel que ab = 0, Ann(a) et Ann(b) sont étrangers.

(19). Soient A un anneau, M, N, P des A-modules, f (resp. g) une application A-linéaire de M dans N (resp. P dans N).

On suppose M de présentation finie. Démontrer les équivalences :

(i) il existe une application A-linéaire $h : M \longrightarrow P$ telle que $f = g \circ f$

(ii) pour tout $m \in \mathrm{Max}(A)$, il existe une application A_m-linéaire h_m telle que $f_m = g_m \circ h_m$, f_m (resp. g_m) désignent les applications $f \circ A_m$ (resp. $g \circ A_m$) .

(20).1. Soient A un anneau, P un A-module projectif de type fini, S une partie multiplicative de A. Démontrer que $S^{-1}P$ est un $S^{-1}A$-module projectif.

En particulier, pour tout $p \in \mathrm{Spec}(A)$, P_p est un A_p-module projectif de type fini et donc un A_p-module libre de rang fini. *On note* $\mathrm{rg}_p(P)$ *le rang du* A_p*-module* M_p (i.e. le cardinal d'une base de M_p).

2. Démontrer que la fonction : $p \longmapsto \mathrm{rg}_p(P)$ de Spec(A), muni de la topologie spectrale ((FFAC),chap.2.II), dans $\mathbb{N}$, est localement constante et que, si Spec(A) est connexe, elle est constante.

On dit qu'*un A-module projectif est de rang l'entier naturel* n si il est de type fini et si, pour tout $p \in \mathrm{Spec}(A)$, $\mathrm{rg}_p(P) = n$.

3. Démontrer les équivalences pour un A-module de type fini M :

(i) M est projectif de rang 1

(ii) il existe un A-module N tel que $M \underset{A}{\otimes} N$ soit isomorphe à A

(indication : pour démontrer (i) $\Longrightarrow$ (ii), prendre $N = M^* = \mathrm{Hom}_A(M,A)$ et considérer l'application $\Sigma x_i \otimes x_i^* \longmapsto \Sigma x_i^*(x_i)$ de $M \underset{A}{\otimes} M^*$ dans A ; pour démontrer (ii) $\Longrightarrow$ (i), se ramener au cas où A est local).

4. Démontrer que si M et N sont des A-modules projectifs de rang 1, les A-modules $M \underset{A}{\otimes} N$, $\mathrm{Hom}_A(M,N)$ sont projectifs de rang 1.

On définit le *groupe de Picard de* A, noté Pic(A), comme l'ensemble des classes d'isomorphismes de A-modules projectifs de rang 1 muni du produit tensoriel.

CHAPITRE 2

Conditions de chaînes et de finitude

Le théorème, dit *de la base finie*, de Hilbert affirme que tout idéal de l'anneau $k[X_1,\ldots,X_n]$ des polynômes à n indéterminées, à coefficients dans un corps k, est de type fini.

Ce théorème, démontré pour résoudre un problème essentiel de la théorie des invariants, a une interprétation *géométrique* simple et intéressante :

Soit $(f_i(X_1,\ldots,X_n))_{i\in I}$ une famille d'éléments de $k[X_1,\ldots,X_n]$. Le sous-ensemble $\{(x_1,\ldots,x_n) \in k^n / \forall i\in I,\ f_i(x_1,\ldots,x_n) = 0\}$ de k^n est appelé *l'ensemble algébrique* de k^n d'équations $f_i(X_1,\ldots,X_n) = 0$ $(i\in I)$.

Soit a l'idéal de $k[X_1,\ldots,X_n]$ engendré par les polynômes f_i $(i\in I)$. L'ensemble algébrique H d'équations $f = 0$ $(i\in I)$ est aussi l'ensemble algébrique d'équations $g = 0$, où g parcourt a. Le théorème de Hilbert montre qu'il existe une partie *finie* J de I telle que les éléments f_i, où i parcourt J, forment un système de générateurs de a, et, par suite, que H est l'ensemble algébrique défini par un *nombre fini* d'équations $f_i = 0$ $(i \in J)$.

C'est Emmy Noether qui a fait l'étude systématique des anneaux dont tout idéal est de type fini. Elle a démontré que cette *condition de finitude* équivaut à la non-existence de suites *infinies strictement croissantes* d'idéaux (*condition de chaîne croissante*) ou encore au fait que tout ensemble non vide d'idéaux admet un (au moins) élément maximal (*condition maximale*).

Les anneaux satisfaisant à ces conditions sont dits *noethériens*.

La classe des anneaux noethériens est stable par passage au quotient ou à un anneau de fractions ; elle contient l'anneau $k[X_1,\ldots,X_n]$ des polynômes à coefficients dans un corps k et donc les anneaux de la *géométrie algébrique classique* qui s'en déduisent par quotient et localisation; elle contient également l'anneau $k[[X_1,\ldots,X_n]]$ des séries formelles et l'anneau des séries convergentes à coefficients réels ou complexes et, donc, les anneaux de la *géométrie analytique locale* réelle ou complexe.

Les anneaux ne possédant pas de *suites infinies strictement décroissantes* d'idéaux ont été étudiés, en particulier, par E. Artin et sont pour cette raison dits *artiniens*. Ils jouent un rôle important en théorie de la multiplicité et de la dimension.

On démontre que ce sont les *anneaux noethériens de dimension de* Krull 0, i.e. dont les seuls idéaux premiers sont maximaux. Un corps et, donc, le quotient d'un anneau par un idéal maximal sont des anneaux artiniens. Plus généralement, le quotient d'un anneau noethérien par un idéal *primaire pour un idéal maximal* (par exemple, puissance d'un idéal maximal) est un anneau artinien.

Les anneaux artiniens ont un *spectre fini* (la réciproque est fausse). Ils sont, en fait, produits d'anneaux artiniens locaux.

Comme d'habitude, on a intérêt à étendre aux modules les notions définies ci-dessus. C'est, d'ailleurs, dans ce cadre que l'on retrouve une "dualité" raisonnable entre les conditions de chaînes croissante et décroissante, perdue pour les anneaux puisqu'il existe des anneaux noethériens non artiniens (par exemple, l'anneau $k[X]$ des polynômes à une indéterminée à coefficients dans le corps k) alors que tout anneau artinien est noethérien. Un module artinien (resp. noethérien) n'est pas noethérien (resp. artinien) en général.

Un module qui est, à la fois, noethérien et artinien est dit de *longueur finie*. On peut lui associer un invariant numérique, sa *longueur*, qui redonne, dans le cas où l'anneau de base est un corps, la dimension d'un espace vectoriel (de dimension finie).

La *condition de chaîne croissante pour les idéaux principaux* apparait naturellement dans la théorie des anneaux *factoriels* qui sont les anneaux *intègres* dont tout élément non nul et non inversible est, de manière unique, produit d'éléments irréductibles. Une première étude de ces anneaux est donnée en fin de chapitre.

Nous avons cru bon d'adjoindre à cette étude algébrique une application géométrique simple : une première étude des *courbes algébriques planes*.

Le plan de ce chapitre est le suivant :

Dans I, on donne la définition et les premières propriétés des modules noethériens et artiniens.

Le paragraphe II est consacré aux anneaux noethériens, le paragraphe III aux modules de longueur finie, le paragraphe IV aux anneaux artiniens.

Dans V, on s'intéresse aux premières propriétés des anneaux fac-

toriels et, notamment, à la factorialité des anneaux de polynômes à coefficients dans un corps.

I. Modules noethériens et artiniens

1. Ensembles ordonnées avec conditions de chaîne

Proposition I.1

Soit E *un ensemble ordonné.*

Les assertions suivantes sont équivalentes :

(i) tout sous ensemble non vide de E *a un élément minimal* (resp. *maximal*)

(ii) toute partie totalement ordonnée non vide de E *a un plus petit*(*) (resp. *plus grand*) *élément.*

(iii) toute suite décroissante (resp. *croissante*) $(x_n)_{n\in N}$ *d'éléments de* E *est stationnaire,* i.e. *telle qu'il existe* $n_o \in N$ *avec* $x_n = x_{n_o}$ *si* $n \geqslant n_o$.

Démonstration

Les implications (i) $\Longrightarrow$ (ii) et (ii) $\Longrightarrow$ (iii) sont claires.

(iii) $\Longrightarrow$ (i). Soit F un sous-ensemble non vide de E. Soit $x_o \in F$. S'il n'est pas minimal, il existe $x_1 \in F$ tel que $x_1 < x_o$. Si x_1 n'est pas minimal, il existe $x_2 \in F$ tel que $x_2 < x_1$. On suppose obtenue ainsi une suite strictement décroissante :

$$x_n < \ldots < x_2 < x_1 < x_o$$

d'éléments de F. Si x_n n'est pas minimal, il existe $x_{n+1} \in F$ tel que $x_{n+1} < x_n$.

Le procédé fournit au bout d'un nombre fini d'opérations un élément minimal de F car sinon on obtiendrait une suite *infinie* strictement décroissante et donc non stationnaire.

La condition (i) est dite condition *minimale* (resp. *maximale*).

La condition (iii) est dite de *chaîne décroissante* (resp. *croissante*).

Il existe une méthode de démonstration applicable aux ensembles ordonnés satisfaisant à la condition minimale (resp. maximale), appelée *principe de récurrence noethérienne.* On l'énonce ci-dessous pour un en-

(*) i.e. E est bien ordonné.

semble E satisfaisant à la condition minimale. Dans la pratique, on l'applique souvent à l'ensemble des *fermés* de certains *espaces topologiques* dit *noethériens* définis dans le chapitre 6.

Principe de récurrence noethérienne

Soit E *un ensemble ordonné satisfaisant à la condition minimale. Soit* P *une propriété d'un élément de* E.

On suppose :

$a \in E$ *et, pour tout* $x \in E$, $x < a$ *et* $P(x)$ *vraie* $\Longrightarrow P(a)$ *vraie*.

Alors, $P(x)$ *est vraie pour tout* $x \in E$.

La démonstration est immédiate : Dire que la conclusion est fausse c'est dire que $F=\{x \in E / P(x)$ fausse$\}$ est un sous-ensemble *non vide* de E. Soit $a \in F$ un élément minimal. Pour tout $x \in E$ tel que $x \in a$, $P(x)$ est vraie. Donc, par hypothèse, $P(a)$ est vraie. Contradiction.

2. Définition des modules noethériens et artiniens

Soient A *un anneau,* M *un* A*-module.*

On dit que M *est noethérien* (resp. *artinien*) *si l'ensemble des sous-modules de* M *ordonné par inclusion satisfait à la condition maximale* (resp. *minimale*) *ou ce qui est équivalent à la condition de chaine croissante* (resp. *décroissante*).

Donc, le A-module M est *noethérien* (resp. *artinien*) s'il satisfait aux conditions équivalentes suivantes :

(i) tout sous-ensemble non vide de sous-modules de M *admet un élément maximal* (resp. *minimal*)

(ii) toute suite croissante (resp. *décroissante*) *de sous-modules de* M *est stationnaire.*

Exemples :

1. Le module 0 est noethérien et artinien.

2. L'ensemble $\mathbb{Z}/n\mathbb{Z}$, où n est un entier >0, est *fini*. Il admet donc un nombre fini de sous-ensembles. Le $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ a donc un nombre fini de sous-modules. Il est par conséquent artinien et noethérien.

3. Soit k un corps. Un k-espace vectoriel est noethérien (resp. artinien) si et seulement si il est de dimension finie.

4. Une somme directe *infinie* de modules *non nuls* est un module non noethérien et non artinien.

Proposition I.2

Soient A *un anneau,* M *un* A*-module.*

Les assertions suivantes sont équivalentes :

(i) M *est noethérien*

(ii) tout sous-module de M (et, en particulier, M) *est de type fini.*

Démonstration

(i) $\Longrightarrow$ (ii) : soit N un sous module de M. L'ensemble des sous-modules *de type fini* de N est non vide car il contient (0). Soit N' un élément maximal de cet ensemble. Il est égal à N : sinon, soit x de N n'appartenant pas à N' ; le A-module N' + Ax est un sous module de type fini de N contenant N' strictement, ce qui contredit la maximalité de N'.

(ii) $\Longrightarrow$ (i) : soit $(N_n)_{n\in N}$ une suite croissante de sous-modules de M. Le sous-module $N = \bigcup_{n\in N} N_n$ est de type fini par hypothèse. Soit $(x_1,\ldots,x_r)$ un système fini de générateurs de N. Il existe $n_o \in N$ tel que x_i appartienne à N_{n_o}. Alors $N = N_{n_o}$ et donc $N_n = N_{n_o}$ si $n \geqslant n_o$.

3. Comportement par suites exactes

Proposition I.3.

Soit $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ *une suite exacte de* A*-modules.*

Les assertions suivantes sont équivalentes :

(i) M *est noethérien* (resp. *artinien*)

(ii) M' *et* M'' *sont noethériens* (resp. *artiniens*)

Démonstration

(i) $\Longrightarrow$ (ii) : une suite croissante (resp. décroissante) de sous modules de M' est une suite croissante (resp. décroissante) de sous modules de M. Elle est donc stationnaire. Une suite croissante (resp. décroissante) de sous modules de M'' a pour image réciproque par g une suite croissante (resp. décroissante) et donc stationnaire de sous modules de M. Elle est donc stationnaire.

(ii) $\Longrightarrow$ (i) : soit $(M_n)_{n\in N}$ une suite croissante (resp. décroissante) de sous modules de M. On pose $M'_n = M_n \cap M'$ et $M''_n = g(M_n)$. Les suites croissantes (resp. décroissantes) $(M'_n)_{n\in N}$ et $(M''_n)_{n\in N}$ de sous modules respectifs de M'et M'' sont stationnaires. Il est possible de

trouver n_o tel que $M'_n = M'_{n_o}$ et $M''_n = M''_{n_o}$ si $n \geqslant n_o$. Alors, $M_n = M_{n_o}$ si $n \geqslant n_o$: en effet, si $x_n \in M_n$, $g(x_n)$ appartient à M''_{n_o} et il existe donc x_{n_o} appartenant à M_{n_o} tel que $g(x_n) = g(x_{n_o})$.

Il en résulte que $x_n - x_{n_o}$ appartient à M'_n et donc à M'_{n_o}. Par suite, x_n appartient à M_{n_o} et $M_n = M_{n_o}$.

Corollaire 1

Soient $M_1, \ldots, M_n$ *des* A*-modules. Les assertions suivantes sont équivalentes :*

(i) M_i *est noethérien* (resp. *artinien*) ($i = 1, \ldots, n$)

(ii) $M_1 \oplus \ldots \oplus M_n$ *est noethérien* (resp. *artinien*)

Démonstration

(ii) $\Longrightarrow$ (i) : résulte de ce que M_i est quotient de $M_1 \oplus \ldots \oplus M_n$.

(i) $\Longrightarrow$ (ii) : la preuve se fait par récurrence sur n. comme

$$M_1 \oplus \ldots \oplus M_{n-1} \oplus M_n = (M_1 \oplus \ldots \oplus M_{n-1}) \oplus M_n$$

il suffit de prouver le cas $n = 2$. On a alors une suite exacte

$$0 \longrightarrow M_1 \longrightarrow M_1 \oplus M_2 \longrightarrow M_2 \longrightarrow 0$$

et il suffit d'appliquer la proposition I.3.

Corollaire 2

Soient M *un* A*-module,* $M_1, \ldots, M_n$ *des sous modules de* M*. Les assertions suivantes sont équivalentes :*

(i) M_i *est noethérien* (resp. *artinien*) ($i = 1, \ldots, n$)

(ii) $M_1 + \ldots + M_n$ *est noethérien* (resp. *artinien*)

Démonstration

(ii) $\Longrightarrow$ (i) : en effet, M_i est un sous module de $M_1 + \ldots + M_n$.

(i) $\Longrightarrow$ (ii) : on sait que $M_1 + \ldots + M_n$ est un quotient de $M_1 \oplus \ldots \oplus M_n$ ((FFAC)chap.II.§4). Il suffit donc d'appliquer le corollaire I.4 puis la proposition I.3.

II. Anneaux noethériens

1. Définitions équivalentes

Un anneau A *est dit noethérien si le* A*-module* A *est noethérien.*

Il revient au même de dire que *tout idéal de* A *est de type fini* ou que *toute suite croissante d'idéaux de* A *est stationnaire* ou que *tout ensemble non vide d'idéaux de* A *a un élément maximal.*

Exemples :

1. *Un quotient d'un anneau noethérien est noethérien* : soit, en effet, a un idéal de l'anneau A. Les sous-modules du A/a-module A/a ne sont autres que les sous-modules du A-module A/a.

2. *Un produit fini d'anneaux noethériens est noethérien* : la démonstration se fait par récurrence sur le nombre de facteurs à partir du cas $A = A_1 \times A_2$. On utilise la suite exacte de A-modules $0 \longrightarrow A_1 \longrightarrow A \longrightarrow A_2 \longrightarrow 0$ et le fait que, si A_i est noethérien, il est un A-module noethérien.

3. *Un anneau de fractions d'un anneau noethérien est noethérien* :

Soit S une partie multiplicative de l'anneau noethérien A. Tout idéal de $S^{-1}A$ est de type fini puisque de la forme $S^{-1}a$ où a est un idéal de A.

4. Un *corps* est un anneau noethérien.

Il en est de même d'un anneau *principal*.

5. Il sera prouvé ultérieurement (théorème de Hilbert) qu'un anneau de polynômes à un nombre fini d'indéterminées sur un anneau noethérien est noethérien.

6. Les anneaux de la géométrie algébrique classique, qui se déduisent des anneaux de polynômes à un nombre fini d'indéterminées à coefficients dans un corps par passage au quotient et passage à un anneau de fractions, sont noethériens.

7. Il en est de même en géométrie analytique où les polynômes sont remplacés par les séries convergentes (ex. 17)

8. La situation est différente en géométrie différentielle : l'anneau $\mathcal{E}^n$ des germes à l'origine de fonctions de classe C^∞ dans un voisinage de l'origine de $\mathbb{R}^n$ n'est pas noethérien (ex. 19).

Voici d'autres exemples d'anneaux non noethériens

9. L'anneau des fonctions entières d'une variable complexe n'est pas noethérien ((FFAC).chap.2.ex.16. On démontre que l'idéal engendré par les fonctions $x \longrightarrow \sin(x/n)$ où n parcourt N n'est pas de type fini).

10. L'anneau des entiers algébriques, i.e. des $x \in \mathbb{C}$ racines d'un polynôme *unitaire* $\in \mathbb{Z}[X]$ n'est pas noethérien. (Un polynôme est dit unitaire si le coefficient de son terme de plus haut degré est 1).

11. Soient k un corps, $(X_n)_{n \in N}$ une suite d'indéterminées. L'anneau

$k[X_n]_{n\in N}$ n'est pas noethérien. Il existe, en effet, une suite strictement croissante infinie : $(X_o) \subset (X_o, X_1) \subset \ldots$ d'idéaux.

On peut aussi remarquer que l'idéal $(X_n)_{n\in N}$ n'est pas de type fini.

2. Modules noethériens sur un anneau non nécessairement noethérien

Proposition II.1

Soient A *un anneau,* M *un* A*-module.*

Les assertions suivantes sont équivalentes :

(i) le A*-module* M *est noethérien*

(ii) le A*-module* M *est de type fini et l'anneau* A/Ann(M) *est noethérien.*

Démonstration

(ii) $\Longrightarrow$ (i) : un sous-module du A-module M est aussi un sous-module du (A/Ann(M))-module M.

(i) $\Longrightarrow$ (ii). Soit $\{x_1, \ldots, x_r\}$ un système fini de générateurs du A-module M.

Le sous-module Ax_i de M est noethérien comme M. Il est isomorphe à $A/\mathrm{Ann}(x_i)$.

On en déduit que *l'anneau* $A/\mathrm{Ann}(x_i)$ est noethérien. Or, $\mathrm{Ann}(M) = \bigcap_{i=1}^{r} \mathrm{Ann}(x_i)$.

Il suffit alors d'utiliser la suite exacte de A-modules :

$$0 \longrightarrow A/\bigcap_{i=1}^{r} \mathrm{Ann}(x_i) = A/\mathrm{Ann}(M) \longrightarrow \bigoplus_{i=1}^{r} A/\mathrm{Ann}(x_i).$$

Le A-module $\bigoplus_{i=1}^{r} A/\mathrm{Ann}(x_i)$ est noethérien. Il en est donc de même du A-module A/Ann(M) et de *l'anneau* A/Ann(M).

Corollaire

Soit A *un anneau noethérien. Les assertions suivantes sont équivalentes pour un* A*-module* M :

(i) M *est noethérien.*

(ii) M *est de type fini.*

3. Caractérisation d'un anneau noethérien par des idéaux premiers

Théorème II .2 (Cohen)

Soit A *un anneau. Les assertions suivantes sont équivalentes :*

(i) A *est noethérien.*

(ii) tout idéal premier de A *est de type fini.*

Démonstration

(i) $\Longrightarrow$ (ii). Clair.

(ii) $\Longrightarrow$ (i). On raisonne par l'absurde supposant A *non noethérien*. L'ensemble F des idéaux non de type fini de A est non vide. Ordonné par inclusion, il est inductif. Soit b un élément maximal de F. Il n'est pas premier (condition (ii)). Soient $x,y\in A$ tels que $xy\in b$, $x\notin b$, $y\notin b$. Les idéaux $b+Ax$ et $(b:Ax)$ contiennent strictement b : en effet, $(b:Ax) = \{z\in A / xz\in b\}$ contient y et b. Ils sont doncde type fini. Il existe un système fini de la forme $\{u_1,\ldots,u_r,x\}$ où $u_i\in b$ de générateurs de $b+Ax$. Soit $(v_1,\ldots,v_s)$ un système fini de générateurs de $(b:Ax)$.

Un élément de b s'écrit $\sum_{i=1}^{r} a_i u_i + zx$ où $a_i\in A$ et $z\in(b:Ax)$: on écrit qu'untel élément est élément de $b+Ax$, donc sous la forme ci-dessus, puis qu'il appartient à b, i.e. que zx appartient à b et donc que z appartient à $(b:Ax)$.

On exprime z comme combinaison linéaire à coefficients dans A de $v_1,\ldots,v_s$.

On en déduit que $\{u_1,\ldots,u_r,xv_1,\ldots,xv_s\}$ est un système de générateurs de b qui est donc de type fini, contrairement au fait qu'il appartient à F.

4. Un théorème de Hilbert

Théorème II.3 (*Théorème dit de la base finie*)

Soit A *un anneau. Les assertions suivantes sont équivalentes :*

(i) L'anneau A *est noethérien.*

(ii) L'anneau $A[X]$ *des polynômes à une indéterminée* X *est noethérien.*

Démonstration

(ii) $\Longrightarrow$ (i) : plus généralement, *si* B *est un anneau noethérien fidèlement plat sur un anneau* A, *l'anneau* A *est noethérien.*

En effet, si a est un idéal de A, $aB\cap A = a$ (FFAC). Il suffit alors d'appliquer une quelconque caractérisation des anneaux noethériens.

(i) implique (ii) : Le A-module M_n des éléments de $A[X]$ de degré inférieur ou égal à n est de type fini, engendré par $1,X,\ldots,X^n$, donc noethérien.

L'application ϕ_n de M_n dans A qui applique un élément de M_n sur le coefficient de son terme de degré n est une formule linéaire sur M_n.

Soit a un idéal de $A[X]$. Le sous module $a_n = a\cap M_n$ de M_n est de type fini.

Il en est de même de l'idéal $b_n = \phi_n(a_n)$ de A. La suite $(b_n)_{n\in\mathbb{N}}$ est croissante : en effet, si $c\in b_n$, il existe un polynôme $f(X) = cX^n + \Sigma_{i<n} c_i X^i$ dans a_n. Le polynôme $Xf(X)$ appartient à a_{n+1} et donc c à a_{n+1}.

Il existe donc un entier m tel que $b_m = b_n$ si $m\leqslant n$. *On va prouver que a_m engendre l'idéal a. Il suffit, à cet effet, de prouver par récurrence sur n que tout élément de a_n est combinaison linéaire à coefficients dans $A[X]$ d'éléments de a_m. C'est clair si $n\leqslant m$. On suppose la propriété établie pour $n\geqslant m$.* Soit $f(X) = cX^{n+1}+\ldots$ un élément de a_{n+1}. L'élément c appartient à b_m. Il existe donc un élément de a_m de la forme $cX^m + \Sigma_{i<m} c_i X^i$. Le polynôme $f(X) - X^{n-m}g(X)$ appartient à a_n et est donc combinaison linéaire à coefficients dans $A[X]$ d'éléments de a_m. Il en est de même de $f(X)$.

Un système *fini* de générateurs du A-module a_m engendre l'idéal a qui est ainsi de type fini.

Corollaire 1

Soit A *un anneau noethérien. L'anneau* $A[X_1,\ldots,X_n]$ *des polynômes à* n *indéterminées à coefficients dans* A *est noethérien.*

En particulier, l'anneau des polynômes à n *indéterminées à coefficients dans un corps est noethérien.*

La preuve est immédiate par récurrence sur n.

En utilisant le fait qu'un anneau quotient d'un anneau noethérien est noethérien on obtient le corollaire.

Corollaire 2

Soit A *un anneau noethérien. Soit* B *une* A*-algèbre de type fini. L'anneau* B *est noethérien.*

Démonstration

Une A-algèbre de type fini est, par définition, un quotient d'un anneau de polynômes à un nombre fini d'indéterminées à coefficients dans A.

En particulier, *une algèbre finie sur un anneau noethérien est un anneau noethérien.*

Il existe une réciproque due à Eakin (Math. Annalen 177,1968,

278-282) et Nagata. La démonstration ci-dessous est due à Edward Formanek (Faithful noetherian Modules. Proc. of the Amer.Math.soc. 41, n°2, 1973, 381-383).

Théorème II.4

Soient A *un anneau,* B *un* A*-module de type fini fidèle.* (i.e. $\{a \in A / aB = 0\} = (0)$).

Les assertions suivantes sont équivalentes :

(i) A *est noethérien.*

(ii) B *est un* A*-module noethérien.*

(iii) L'ensemble des sous-modules de B *de la forme* aB (a idéal quelconque de A) *satisfait à la condition maximale.*

Démonstration

(i) $\Longrightarrow$ (ii). Clair.

(ii) $\Longrightarrow$ (i). Résulte du fait que si B est un A-module noethérien, A/Ann(B) est un anneau noethérien (prop. II.V) et que, par hypothèse, Ann(B) = (0).

(ii) $\Longrightarrow$ (iii). Clair.

(iii) $\Longrightarrow$ (ii). *On raisonne par l'absurde supposant le* A*-module* B *non noethérien.*

On va démontrer que l'on peut de plus supposer :

1) que, pour tout idéal non nul a *de* A, *le* A*-module* B/aB *est noethérien,*

2) que, pour tout sous-module non nul U *de* B, *le* A*-module* B/U *n'est pas fidèle*

1. L'ensemble F des sous-modules de B de la forme aB, où a est un idéal de A, tel que le A-module B/aB ne soit pas noethérien est non vide: il contient, en effet, (0). Il admet donc un élément maximal aB.

Le A-module B/aB n'est donc pas noethérien mais pour tout idéal b contenant strictement a, le A-module B/bB = (B/aB)/(bB/aB) est noethérien. Ce A-module B/aB n'est pas fidèle si $a \neq (0)$. On considère donc c = Ann(B/aB) et le A/c-module B/aB. Il n'est pas noethérien. Un idéal non nul de A/c est de la forme d/c où d est un idéal de A contenant strictement c et donc, a fortiori, a. Le A-module B/dB est donc noethérien. Il en est de même du A/c-module B/dB .

L'ensemble des sous-modules du A/c-module B/aB de la forme

$(d/c)(B/aB) = (dB/aB)$ où (d/c) est un idéal de A/c satisfait évidemment à la condition maximale.

Remplaçant A par A/c et B par B/aB, on voit que l'on peut supposer 1) satisfaite.

2. L'ensemble G des sous-modules U de B tels que B/U soit fidèle est non vide. Il est inductif. Soit, en effet, $(U_i)_{i\in I}$ une famille totalement ordonnée d'éléments de G et soit $U = \bigcup_{i\in I} U_i$.

On a les équivalences pour un élément $a\in A$:

(i) $a \in \mathrm{Ann}(B/U)$

(ii) $aB \subset U$

(iii) il existe $i\in I$ tel que $aB \subset U_i$ (parce que B est un A-*module de type fini*)

(iv) $a \in \mathrm{Ann}(B/U_i)$ et donc $a = 0$.

Soit U un élément maximal de G. Alors, B/U est un A-module fidèle non noethérien car sinon A serait noethérien et donc B qui est un A-module de type fini le serait aussi.

On remplace B par B/U.

On suppose donc maintenant les conditions 1) et 2) satisfaites.

On va démontrer que tout quotient différent de B de B est noethérien. Il en résultera, évidemment, que B est noethérien, i.e. une contradiction.

Soit B/U un quotient de B distinct de B. Le sous-module U est non nul. En raison de 2), B/U n'est pas fidèle. Il existe donc un élément non nul a de A tel que $aB \subset U$.

En raison de 1), B/aB est un A-module noethérien. Il en est de même du A-module B/U qui en est un quotient.

Corollaire (Théorème d'Eakin-Nagata)

Soient B un anneau, A un sous-anneau tel que B soit une A-algèbre finie. Les assertions suivantes sont équivalentes :

(i) L'anneau A est noethérien.

(ii) L'anneau B est noethérien.

Démonstration

(i) $\Longrightarrow$ (ii). Clair.

(ii) $\Longrightarrow$ (i). Le A-module B satisfait à la condition (iii) du théorème.

5. Anneaux et modules cohérents

Les anneaux cohérents jouent un rôle important dans certaines questions d'algèbre commutative non noethérienne.

Un exemple d'anneau cohérent non noethérien est celui des polynômes à une infinité d'indéterminées à coefficients dans un anneau noethérien.

Les résultats exposés ci-dessous sont extraits de S.U.Chase (41), Bourbaki (2) et J.P. Soublin (57).

Définition

Soient A *un anneau,* M *un* A*-module.*

On dit que M *est pseudo-cohérent* (resp. *cohérent*) *si tout sous-module de type fini de* M *est de présentation finie* (resp. *s'il est pseudo-cohérent et de type fini*).

Le A-module est cohérent si et seulement si il est pseudo-cohérent. On dit alors que *l'anneau* A *est cohérent.* l'anneau A est donc cohérent si tout idéal de type fini de A est de présentation finie.

Lemme

Soit $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ *une suite exacte de* A*-module.*

1. Si M' *et* M'' *sont de type fini,* M *est de type fini* .

2. Si M'' *est de présentation finie et* M *est de type fini,* M' *est de type fini.*

3. Si M *est de présentation finie,* M' *est de type fini,* M'' *est de présentation finie* .

4. Une somme directe finie de modules de présentation finie est un module de présentation finie.

Démonstration

1. Dire que M' (resp. M'') est de type fini c'est dire qu'il existe un homomorphisme surjectif $\varepsilon' : A^n \longrightarrow M'$ (resp. $\varepsilon'' : A^m \longrightarrow M''$). Il existe un homomorphisme surjectif $\varepsilon : A^{n+m} \longrightarrow M$ tel que le diagramme

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A^n & \longrightarrow & A^{n+m} & \longrightarrow & A^m & \longrightarrow & 0 \\
 & & \varepsilon' \downarrow & & \varepsilon \downarrow & & \varepsilon'' \downarrow & & \\
0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

soit commutatif à lignes exactes.

((FFAC).Chap.5.prop.I.10). Donc M est de type fini.

2. Soit $L_1 \xrightarrow{\phi} L_o \xrightarrow{\psi} M'' \longrightarrow 0$ une présentation finie de M''. Il existe un diagramme commutatif :

$$\begin{array}{ccccccc} L_1 & \xrightarrow{\phi} & L_o & \xrightarrow{\psi} & M'' & \longrightarrow & 0 \\ \downarrow{\scriptstyle a_1} & & \downarrow{\scriptstyle a_o} & & \downarrow{\scriptstyle 1_{M''}} & & \\ 0 \longrightarrow M' & \xrightarrow[f]{} & M & \xrightarrow[g]{} & M'' & & \end{array} \qquad \text{à lignes exactes}$$

On a alors une suite exacte $0 = \ker(1_{M''}) \longrightarrow \operatorname{coker}(a_1) \longrightarrow \operatorname{coker}(a_o) \longrightarrow \operatorname{coker}(1_{M''}) = 0$.

Donc, $\operatorname{coker}(a_1) = M'/\operatorname{im}(a_1) = \operatorname{coker}(a_o) = M/\operatorname{im}(a_o)$ est de type fini. Comme $\operatorname{im}(a_1)$ est de type fini comme L_1, M' est de type fini d'après 1.

3. Le A-module M est de la forme A^n/R, où R est de type fini.

Il existe un sous-module de type fini S de A^n contenant R tel que $M' = S/R$. Donc, $M'' = A^n/S$ est de présentation finie.

4. Laissé au soin du lecteur.

Proposition II.5

Soient A *un anneau,* M *un* A*-module.*

Les assertions suivantes sont équivalentes :

(i) M *est pseudo-cohérent.*

(ii) (α) *l'annulateur de tout élément de* M *est un idéal de type fini*

(β) *l'intersection de tout sous-module monogène et tout sous-module de type fini de* M *est un sous-module de type fini*

(iii) (α) *et l'intersection de deux sous-modules de type fini de* M *est un sous-module de type fini.*

Démonstration

(i) $\Longrightarrow$ (iii). Si $x \in M$, $A/\operatorname{Ann}(x)$ est de présentation finie puisque isomorphe au sous-module monogène Ax. Donc, en vertu du lemme 2., $\operatorname{Ann}(x)$ est de type fini. D'où (α).

Soit N_1 et N_2 des sous-modules de type fini de M. On déduit de la suite exacte $0 \longrightarrow N_1 \cap N_2 \longrightarrow N_1 \oplus N_2 \longrightarrow N_1 + N_2 \longrightarrow 0$, du fait que $N_1 \oplus N_2$ est de type fini et $N_1 + N_2$ de présentation finie, comme sous module de type fini de M, que $N_1 \cap N_2$ est de type fini.

(iii) $\Longrightarrow$ (ii). Evident.

(ii) $\Longrightarrow$ (i). On démontre par récurrence sur le cardinal n d'un système fini de générateurs d'un sous-module de type fini N de M que N

est de présentation finie. C'est vrai si n = 1 : c'est la condition (α). On suppose l'assertion vraie pour n-1. Soit N un sous-module ayant un système de n générateurs avec n>1. Si x est un élément de ce système, N = N' + Ax où N' est engendré par n - 1 éléments. Le résultat se déduit de la suite exacte $0 \longrightarrow N' \cap Ax \longrightarrow N' \oplus Ax \longrightarrow N = N' + Ax \longrightarrow 0$, où $N' \cap Ax$ est de type fini par hypothèse, $N' \oplus Ax$ est de présentation finie comme N' et Ax (hypothèse de récurrence) et du lemme 3.

Corollaire 1

Soit A *un anneau intègre.*

Les assertions suivantes sont équivalentes :

(i) A *est cohérent.*

(ii) l'intersection d'un idéal principal et d'un idéal de type fini de A *est un idéal de type fini de* A.

(iii) l'intersection de deux idéaux de type fini de A *est un idéal de type fini.*

Corollaire 2

Soit A *un anneau.*

Les assertions suivantes sont équivalentes :

(i) pour toute famille $(X_i)_{i\in I}$ *d'indéterminées, l'anneau* $A[X_i]_{i\in I}$ *est cohérent*

(ii) pour toute famille FINIE $(X_i)_{i\in I}$ *d'indéterminées, l'anneau* $A[X_i]_{i\in I}$ *est cohérent.*

Démonstration

Il est clair que (i) implique (ii).

(ii) $\Longrightarrow$ (i). Soit $x \in A[X_i]_{i\in I}$. Il existe un sous-ensemble *fini* J de I tel que x appartienne à $A[X_i]_{i\in J}$. Soit a l'annulateur de x dans $A[X_i]_{i\in J}$. C'est un idéalde type fini. Il en est de même de l'annulateur de x dans $A[X_i]_{i\in I}$ qui est $aA[X_i]_{i\in I}$.

Soient c et b deux idéaux de type fini de $A[X_i]_{i\in I}$. Il existe un sous-ensemble J *fini* de I tel que c et b admettent des systèmes de générateurs dans $A[X_i]_{i\in J}$.

Soient c_J et b_J les idéaux de $A[X_i]_{i\in J}$ engendrés par ces systèmes. L'idéal $c_J \cap b_J$ est de type fini. Il en est de même de l'idéal $c \cap b$ qui est $(c_J \cap b_J)\, A[X_i]_{i\in I}$, puisque $A[X_i]_{i\in I}$ étant (fidèlement) plat sur

$A[X_i]_{i\in J}$, $c_J A[X_i]_{i\in I} \cap b_J A[X_i]_{i\in I}$, i.e. $c \cap b$, est égal à $(c_J \cap b_J)A[X_i]_{i\in I}$.

Corollaire 3

Soit A *un anneau noethérien (par exemple, un corps).*

Pour toute famille $(X_i)_{i\in I}$ *d'indéterminées, l'anneau* $A[X_i]_{i\in I}$ *est cohérent.*

Théorème II.6 (S.U. Chase)

Soit A *un anneau.*

Les assertions suivantes sont équivalentes :

(i) A *est cohérent*

(ii) un produit d'une famille de A*-modules plats est un* A*-module plat*

(iii) un produit d'une famille de copies de A *est un module plat*

(iv) un sous-module de type fini d'un A*-module libre est de présentation finie.*

Démonstration

On va procéder suivant le schéma (ii) $\Longrightarrow$ (iii), (iii) $\Longrightarrow$ (iv), (iv) $\Longrightarrow$ (i), (i) $\Longrightarrow$ (ii)

(iv) $\Longrightarrow$ (i) : clair

(ii) $\Longrightarrow$ (iii) : clair car A est un A-module plat.

(iii) $\Longrightarrow$ (iv). Soit M un sous-module de type fini du A-module libre L que l'on peut choisir de type fini égal à A^s. On a un diagramme à lignes et colonne exacte :

$$\begin{array}{ccccc} & & 0 & & \\ & & \downarrow & & \\ & & K & & \\ & & f\downarrow & & \\ & & F=A^r & & \\ & & g\downarrow & & \\ 0 & \longrightarrow & M & \longrightarrow & A^s=L \\ & & \downarrow & & \\ & & 0 & & \end{array}$$

Soit $N = A^K$.

On va déduire du fait que le A*-module* N *est plat* (par hypothèse) *que le* A*-module* K *est de type fini.*

Soient $\{\varepsilon_1,\ldots,\varepsilon_r\}$ la base canonique de F, $x_i = g(\varepsilon_i)$ $(i = 1,\ldots,r)$, $x_i = (\lambda_{i1},\ldots,\lambda_{is}) \in A^S$.

Un élément y de K s'écrit $a_1(y)\varepsilon_1+\ldots+a_r(y)\varepsilon_r$. L'égalité $0 = g(y)$ se traduit par les équations linéaires :

$$\Sigma_{k=1}^{r} a_k(y)\lambda_{kj} = 0 \qquad (1 \leqslant j \leqslant s)$$

Soit a_k l'élément $(a_k(y))_{y\in K}$ de N. On a donc :

$$\Sigma_{k=1}^{r} a_k\lambda_{kj} = 0 \qquad (1 \leqslant j \leqslant s)$$

Il existe alors ((FFAC).chap.6.ThéorèmeV.3) $b_1,\ldots,b_n \in N$, $\mu_{ik} \in A$ $(i\leqslant n,\ k\leqslant r)$ tels que $a_k = \Sigma_{i=1}^{n} b_i\mu_{ik}$ et $\Sigma_{k=1}^{r} \mu_{ik}\lambda_{kj} = 0$.

L'élément $z_i = \Sigma_{k=1}^{r} \mu_{ik}\varepsilon_k$ de F appartient à K car $g(z_i) = 0$ $(i = 1, \ldots, n)$.

On va démontrer que $z_1,\ldots,z_n$ *engendrent* K.

Soit $b_i = (b_i(y))_{y\in K}$ où $b_i(y) \in A$. Puisque $a_k = \Sigma_{i=1}^{n} b_i\mu_{ik}$ $(1\leqslant k\leqslant r)$, pour tout $y\in K$, $a_k(y) = \Sigma_{i=1}^{n} b_i(y)\mu_{ik}$. Donc, pour tout $y\in K$,

$$y = \Sigma_{k=1}^{r} a_k(y)\varepsilon_k = \Sigma_{i=1}^{n} b_i(y)z_i.$$

(i) $\Longrightarrow$ (iii)

Soit $M = A^I$. *On va démontrer que* M *est plat en utilisant la caractérisation* (iii) *du théorème* V.3. *de* (FFAC).

Soient $x_i \in M$, $a_i \in A$ $(i = 1,\ldots,r)$ tels que $\Sigma_{i=1}^{r} a_i x_i = 0$. Soit $x_j(\alpha)$ la α-ème composante de x_j en sorte que $x_j = (x_j(\alpha))_{\alpha\in I}$.

On a une suite exacte $0 \longrightarrow K \longrightarrow A^r \xrightarrow{g} a \longrightarrow 0$ où a est l'idéal $(a_1,\ldots,a_r)$ et où $\{\varepsilon_1,\ldots,\varepsilon_r\}$ désignant la base canonique de A^r, $g(\varepsilon_i) = a_i$. Par hypothèse, le sous-module K de A^r est de type fini engendré par des éléments $z_1,\ldots,z_n$ où $z_i = \Sigma_{k=1}^{r} \mu_{ik}\varepsilon_k$.

L'élément $u_\alpha = \Sigma_{k=1}^{r} x_k(\alpha)\varepsilon_k$ de A^r appartient à K car $g(u_\alpha) = \Sigma_{k=1}^{r} a_k x_k(\alpha)$.

Il existe donc $b_i(\alpha) \in A$ tel que $u_\alpha = \Sigma_{i=1}^{n} b_i(\alpha)z_i = \Sigma_{k=1}^{r}(\Sigma_{i=1}^{n} b_i(\alpha)\mu_{ik})\varepsilon_k$.

Alors, pour tout $\alpha \in I$, $x_k(\alpha) = \Sigma_{i=1}^{r} b_i(\alpha)\mu_{ik}$. Posant $b_i = (b_i(\alpha))_{\alpha\in I}$, on voit que $x_k = \Sigma_{i=1}^{n} b_i\mu_{ik}$. D'autre part, l'égalité $g(z_i) = 0$ montre que $\Sigma_{k=1}^{r} \mu_{ik}a_k = 0$.

(iv) $\Longrightarrow$ (ii)

Soient $(M_i)_{i\in I}$ une famille de A-modules plats, $M = \prod_{i\in I} M_i$.

Pour démontrer que M *est un* A*-module plat on va démontrer que, pour tout* A*-module* N *de présentation finie,* $\mathrm{Tor}_1^A(M,N) = 0$. ((FFAC).chap.6. prop.V.1 et chap.3. prop.V.2).

Soit F *le foncteur additif de* Mod(A) *dans* Mod(A) tel que $F(N) = \prod_{i\in I} (M_i \underset{A}{\otimes} N)$ et $F(f) = \prod_{i\in I} (M_i \bullet f)$. Comme, pour tout $i\in I$, M_i est plat, ce foncteur est *exact*.

Il existe un morphisme fonctoriel ϕ de $M \underset{A}{\otimes} -$ dans F tel que, pour un A-module N, $\phi_N((x_i)_{i\in I} \bullet y) = (x_i \bullet y)_{i\in I}$.

Soit N un A-module de présentation finie. On a par conséquent une suite exacte $0 \longrightarrow K \longrightarrow L \longrightarrow N \longrightarrow 0$ où L est un A-module libre de type fini, K est un sous-module de type fini .

On en déduit un diagramme commutatif à ligne exactes :

$$\begin{array}{ccccccccc}
 & & M \underset{A}{\otimes} K & \longrightarrow & M \underset{A}{\otimes} L & \longrightarrow & M \underset{A}{\otimes} N & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \phi_K} & & \downarrow{\scriptstyle \phi_L} & & \downarrow{\scriptstyle \phi_N} & & \\
0 & \longrightarrow & F(K) & \longrightarrow & F(L) & \longrightarrow & F(N) & \longrightarrow & 0
\end{array}$$

Il est clair que ϕ_A est un isomorphisme et donc qu'il en est de même de ϕ_L.

Il résulte alors du diagramme du serpent que ϕ_N est surjectif.

Mais, *par hypothèse*, K qui est de type fini est de présentation finie. Donc, ϕ_K est surjectif. Le lemme des quatre indique alors que ϕ_N est injectif et donc un isomorphisme. Il en est de même de ϕ_K. L'application $M \underset{A}{\otimes} K \longrightarrow M \underset{A}{\otimes} L$ est donc injectif et son noyau $\mathrm{Tor}_1^A(M,N)$ est 0.

Définition

Un anneau A *est dit absolument plat si tout* A*-module est plat.*

(Le lecteur pourra se reporter à (FFAC).chap.2.exercice 14. Un exemple simple d'anneau absolument plat est un produit quelconque de corps.)

Corollaire

Un anneau absolument plat est cohérent.

Remarque :

On trouvera dans l'exercice 12 une caractérisation des anneaux noethériens de même nature que celle donnée pour les anneaux cohérents dans le théorème II.6.

III. Modules de longueur finie

La notion introduite ci-dessous de module de longueur finie généralise celle d'espace vectoriel de dimension finie sur un corps. A certains modules, les modules qui sont à la fois noethériens et artiniens, on peut attacher un invariant numérique, leur longueur. Ceci permet, par exemple, de faire des démonstrations par récurrence.

Définitions

1. Soient A *un anneau,* M *un* A*-module.*

Une suite de composition de M *est une suite strictement décroissante :*

(1) $M=M_0 \supset M_1 \supset \ldots \supset M_n = (0)$

de sous-modules de M.

L'entier n *est appelé la longueur de la suite de composition.*

On définit sur l'ensemble des suites de composition de M une relation d'ordre comme suite :

On dit que la suite

(2) $M=M'_0 \supset M'_1 \supset \ldots \supset M'_m = (0)$

est *plus fine* que la suite (1) s'il existe une application, injective, τ de $\{0, \ldots, n\}$ dans $\{0, \ldots, m\}$ telle que $M_i = M'_{\tau(i)}$.

2. Un élément maximal de l'ensemble des suites de composition de M *est appelé une suite de Jordan-Hölder de* M.

Dire que la suite (1) est une suite de Jordan-Hölder de M c'est à dire que les quotients successifs M_i/M_{i+1} sont des A-modules simples.

3. On définit la longueur du A*-module* M *comme étant infinie si* M *n'admet pas de suite de* Jordan-Hölder *et comme la borne inférieure des longueurs des suites de*Jordan-Hölder *de* M *si* M *admet de telle suites*

On note $\text{long}_A(M)$ *ou* long(M) *cette longueur.*

Exemple :

Soit n un entier > 0. Le $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ est de longueur finie. On laisse le soin de calculer sa longueur.

Proposition III.1

On suppose que le A*-module* M *admet une suite de* Jordan-Hölder *de longueur* n.

1. Toutes les suites de Jordan-Hölder *de* M *ont même longueur* n *et donc* long(M) = n.

2. Toute suite de composition de M *peut-être raffinée en une suite de* Jordan-Hölder.

Démonstration

On utilise le lemme suivant.

Lemme

Si $N \subset M$, $\text{long}(N) \leqslant \text{long}(M)$. *L'égalité* $\text{long}(N) = \text{long}(M)$ *implique l'égalité* $n = M$.

Démonstration du lemme

Soit (M_i) une suite de Jordan-Hölder de M de longueur long(M). Si $N_i = N \cap M_i$, N_{i-1}/N_i est un sous-module du module simple M_{i-1}/M_i ; donc ou $N_{i-1} = N_i$ ou N_{i-1}/N_i est égal à M_{i-1}/M_i et est donc simple.

La suite obtenue à partir de la suite (N_i) en retirant N_j s'il est égal à N_{j-1} est une suite de Jordan-Hölder de N. Par définition de long(N), $\text{long}(N) \leqslant \text{long}(M)$.

L'égalité $\text{long}(N) = \text{long}(M)$ implique que, pour tout i, $N_{i-1}/N_i = M_{i-1}/M_i$. On en déduit $N_{n-1} = M_{n-1}$, puis $N_{n-2} = M_{n-2}$ et, par récurrence sur i, $M_{n-i} = N_{n-i}$ pour tout i. En particulier, $M = M_o = M_o = N$.

Démonstration de 1).

Soit $M_o = M \supset M_1 \supset \ldots \supset M_n = 0$ une suite de composition de M. Il résulte du lemme les inégalités strictes

$$\text{long}(M) > \text{long}(M_1) > \ldots > \text{long}(M_n) = 0$$

qui prouvent que $\text{long}(M) \geqslant n$.

Ainsi, la longueur d'une suite de composition de M est inférieure ou égale à long(M). Il en résulte que la longueur de toute suite de Jordan-Hölder de M est long(M).

Démonstration de 2).

Une suite de composition $M_o = M \supset M_1 \supset \ldots \supset M_n = 0$ est une suite de Jordan-Hölder si et seulement si $n = \text{long}(M)$. Si $n < \text{long}(M)$, un des quotients M_{i-1}/M_i n'est pas simple et il est donc possible d'intercaler un sous module entre M_{i-1} et M_i, augmentant de 1 la longueur de la suite de composition. Au bout de long(M)-n opérations de ce type, on obtient une suite de Jordan-Hölder plus fine que la suite de composition de départ.

Proposition III.2

Soient A *un anneau,* M *un* A*-module.*

1. Les assertions suivantes sont équivalentes :

(i) $\text{long}_A(M) < \infty$

(ii) M *est noethérien et artinien*

2. Si A *est un corps et* M *un* A*-espace vectoriel,* $\text{long}_A(M) < \infty$ *si et seulement si* $[M:A] < \infty$ *et alors* $\text{long}_A(M) = [M:A]$.

Démonstration

1. (i) $\Longrightarrow$ (ii) : clair

(ii) $\Longrightarrow$ (i). Clair si $M = 0$. Si $M \neq 0$, l'ensemble des sous-modules de M distincts de M est non vide. Comme M est noethérien, il a un élément maximal M_1, noethérien comme M. Si $M_1 = 0$, $\text{long}_A(M) = 0$. Si $M_1 \neq 0$, M_1 admet un sous-module maximal M_2. On construit ainsi une suite strictement décroissante $M_0 = M \supset M_1 \supset M_2 \supset \ldots$ qui, puisque M est artinien, ne peut-être infini. Il existe donc $n \in \mathbb{N}$ tel que $M_n = 0$ et on a obtenu une suite de Jordan-Hölder de M.

2. Laissé au soin du lecteur.

Proposition III.3 (additivité de la longueur)

Soit $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ *une suite exacte de* A*-modules.*

1) Les assertions suivantes sont équivalentes :

(i) M *est de longueur finie.*

(ii) M' *et* M'' *sont de longueur.*

2) S'il en est ainsi, $\text{long}_A(M) = \text{long}_A(M') + \text{long}_A(M'')$.

Démonstration

1) Résulte immédiatement de la proposition III.1 et de la proposition I.3.

2) Soit $M_0 = M \supset \ldots \supset M_r = M' \supset \ldots \supset M_n = 0$ une suite de Jordan-Hölder de M contenant M' (proposition III.1.2).

La suite $M_0/M' \supset \ldots \supset M_r/M' = 0$ est une suite de Jordan-Hölder de M/M' et la suite $M_r \supset \ldots \supset M_n$ est une suite de Jordan-Hölder de M'.

Corollaire

Soit $0 \longrightarrow M_1 \longrightarrow \ldots \longrightarrow M_n \longrightarrow 0$ *une suite exacte de* A*-modules de longueur finie.*

Alors, $\sum_{i=1}^{n} (-1)^i \text{long}(M_i) = 0$.

Démonstration

On fait une récurrence sur n. Le cas $n < 3$ est évident. Le cas $n = 3$ résulte de la proposition III.3. Soit $n > 3$. On a les deux suites exactes

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M'_3 \longrightarrow 0$$
$$0 \longrightarrow M'_3 \longrightarrow M_3 \longrightarrow M_n \longrightarrow 0$$

Par hypothèse de récurrence, on a :

$$- \text{long}(M'_3) + \Sigma_{i>3}(-1)^{i+1} \text{long}(M_i) = 0$$

Remplaçant $\text{long}(M'_3)$ par $\text{long}(M_2) - \text{long}(M_1)$ et changeant de signe, on obtient l'inégalité cherchée.

Définition

Soient A *un anneau,* M *un* A*-module,* $(N_i)_{0\leqslant i\leqslant n}$ *et* $(P_j)_{0\leqslant j\leqslant m}$ *deux suites de composition de* M.

On dit que ces deux suites sont équivalentes si $m = n$ *et s'il existe une permutation* π *de* $\{0,\ldots,n-1\}$ *telle que les* A*-modules* M_i/M_{i+1} *et* $N_{\pi(i)}/N_{\pi(i+1)}$ *soient isomorphes pour tout* $i = 0,\ldots,n-1$.

Théorème III.4 (Schreier)

Soient S_1 *et* S_2 *deux suites de composition d'un* A*-module* M. *Il existe deux suites de composition* S'_1 *et* S'_2 *de* M *équivalentes et respectivement plus fines que* S_1 *et* S_2.

Démonstration

Soient $S_1 = (N_i)_{0\leqslant i\leqslant n}$ et $S_2 = (P_j)_{0\leqslant j\leqslant m}$.

Le A-module $N_{i+1} + (N_i \cap P_j) = N'_{ij}$ (resp. $P_{j+1} + (N_i \cap P_j) = P'_{ij}$) contient N_{i+1} (resp. P_{j+1}) et $N'_{i0} = N_i$ (resp. $P'_{0j} = P_j$).

On a un isomorphisme (canonique) de $(N_i \cap P_j)/(N'_i \cap P_{j+1})$ sur $(P_{j+1} + (N_i \cap P_j))/P_{j+1}$ puisque $N_i \cap P_{j+1} = (N_i \cap P_j) \cap P_{j+1}$. Cet isomorphisme induit un isomorphisme de $(N_i \cap P_{j+1}) + (N_{i+1} \cap P_j)/(N_i \cap P_{j+1})$ sur $(P_{j+1} + (N_{i+1} \cap P_j))/P_{j+1}$.

On en déduit un isomorphisme de :

$(N_i \cap P_j)/(N_i \cap P_{j+1}) + (N_{i+1} \cap P_j)$ sur $P_{j+1} + (N_i \cap P_j)/P_{j+1} + (N_{j+1} \cap P_j) = P'_{ij}/P'_{i+1,j}$.

On a de même un isomorphisme de ce module sur $N'_{ij}/N'_{i+1,j}$, d'où le résultat.

Corollaire

Deux suites de Jordan-Hölder d'un module sont équivalentes.

Démonstration

Il existe deux suites de composition plus fines que les suites de

Jordan-Hölder considérées qui sont équivalentes. Elles sont égales à ces suites de Jordan-Hölder qui sont donc équivalentes.

IV. Anneaux artiniens

1. Définition et exemples

Définition

Un anneau A *est dit artinien si le* A*-module* A *est artinien.*

Il revient au même de dire que *toute suite décroissante d'idéaux de* A *est stationnaire* ou que *tout ensemble non vide d'idéaux de* A *a un élément minimal.*

1. Un quotient d'un anneau artinien est artinien.

2. Un produit fini d'anneaux artiniens est artinien.

3. Un anneau de fractions d'un anneau artinien est artinien.

Soit $(b_n)_{n\in N}$ une suite décroissante d'idéaux de l'anneau $S^{-1}A$ des fractions de l'anneau artinien A par rapport à la partie multiplicative S

Soit $a_n = (i_A^S)^{-1}(b_n)$. La suite $\{a_n\}_{n\in N}$ d'idéaux de A est décroissante et donc stationnaire. Il en est de même de la suite $\{b_n\}_{n\in N}$ puisque $b_n = S^{-1}a_n$.

Exemples :

1. Un corps est un anneau artinien.

Plus généralement, *une algèbre* A *sur un corps* k *finie sur* k *est un anneau artinien* : en effet, un idéal de A est en particulier un sous-espace vectoriel du k-espace vectoriel de A.

2. Un anneau fini est artinien : en particulier, si n est un entier ≥ 1, l'anneau quotient $\mathbb{Z}/(n)$ est artinien.

3. L'anneau $k[X]$ des polynômes à une indéterminée X à coefficients dans le corps k *est noethérien mais n'est par artinien* : en effet, la suite décroissante $\{X^n\}_{n\in N}$ d'idéaux n'est pas stationnaire.

On verra ultérieurement qu'un anneau artinien est noethérien.

2. Spectre premier d'un anneau artinien

Proposition IV.1

Un idéal premier d'un anneau artinien est maximal.

Démonstration

Il suffit, par passage au quotient, de démontrer qu'*un anneau artinien intègre est un corps.*

Soit donc A un anneau artinien intègre. Si a est un élément non nul de A, il résulte de ce que la suite $\{(a^n)\}_{n\in N}$ d'idéaux est stationnaire qu'il existe $r\in N$ tel que $(a^r) = (a^{r+1})$. Il existe donc $b\in A$ tel que $a^r = ba^{r+1}$ et donc $1 = ba$, puisque A est intègre. L'élément a est donc inversible.

Remarque

Il existe des anneaux dans lesquels tout idéal premier est maximal mais qui ne sont pas artiniens.

Soient, par exemple, k *un corps*, $(X_n)_{n\in N}$, *une suite d'indéterminées*, A *l'anneau quotient* $k[X_n]_{n\in N}/(X_iX_j)_{i,j\in N}$, x_i *la classe de* X_i $(i\in N)$.

Le seul idéal premier de $A = k[x_n]_{n\in N}$ est l'idéal maximal $(x_n)_{n\in N}$.

La suite $(x_o) \subset (x_o,x_1) \subset \ldots$ est *strictement* croissante et donc l'anneau A n'est pas noethérien.

Il résulte alors du théorème IV.4, démontré plus loin, que a fortiori l'anneau A n'est pas artinien.

Proposition IV.2

Le spectre premier d'un anneau artinien est fini.

Démonstration

Soit F l'ensemble, non vide, des idéaux de l'anneau A qui sont intersection d'un nombre fini d'idéaux premiers.

Si A est artinien, F possède un élément minimal a qui s'écrit $m_1 \cap \ldots \cap m_n$ où $m_1,\ldots, m_n$ sont des idéaux premiers distincts.

On va démontrer que $\mathrm{Spec}(A) = \{m_1,\ldots,m_n\}$.

Soit, en effet, $m\in \mathrm{Spec}(A)$. L'idéal $m \cap a$ est élément de F. Puisque il est contenu dans a, il doit être égal à a.

Par conséquent, $m_1 \cap \ldots \cap m_n \subset m$. Il existe donc $i\in\{1,\ldots,n\}$ tel que $m_i \subset m$ et puisque m_i est maximal (proposition IV.1), $m_i = m$.

Remarque

La réciproque de la proposition IV.2 est fausse.

Exemple :

L'anneau $A = k[X_o,\ldots,X_n,\ldots]/(X_iX_j)_{i,j\in N}$ a un spectre premier réduit à un élément, son idéal maximal, mais il n'est pas artinien.

3. Nilradical et radical d'un anneau artinien

Proposition IV.3

Le radical d'un anneau artinien est égal à son nilradical.

Il est nilpotent, i.e. *il existe un entier* $n \geq 1$ *tel que la puissance* n-ème *du radical soit* (0).

Démonstration

Soient A un anneau artinien, r son radical. Ce radical qui est l'intersection des idéaux maximaux de A est l'intersection des idéaux premiers de A, i.e. le nilradical.

La suite $(r^n)_{n \in N}$ d'idéaux de A est stationnaire.

Soit n tel que $r^n = r^{n+1}$. On va démontrer que $r^n = (0)$.

On pose $a = r^n$ *et on suppose* $a \neq (0)$. On remarque l'égalité $a = a^2$.

L'ensemble F des idéaux b de A tels que $ba \neq (0)$ est alors non vide. Il admet donc un élément minimal c. Il existe $x \in c$ tel que $xa \neq (0)$.

Par minimalité de c, on a $c = (x)$.

Or, $(xa)a = xa^2 = xa \neq (0)$. Par suite, $(x) = xa$ et il existe $z \in a$ tel que $x = xz$.

On en déduit $x = xz^n$ pour tout $n \in N$. Comme z appartient au radical, c'est-à-dire ici au nilradical, il existe $n \in N$ tel que $z^n = 0$. Donc, $x = 0$ et ceci contredit le fait que xa est supposé non nul.

Corollaire (théorème de structure des anneaux artiniens)

Un anneau artinien est un produit fini d'anneaux artiniens locaux.

Démonstration

Soient $m_1, \ldots, m_n$ les idéaux maximaux de l'anneau artinien A.

Il existe $s \in N$ tel que $(m_1 \cap \ldots \cap m_n)^s = (0)$. Mais $(m_1 \cap \ldots \cap m_n)^s = (m_1 \ldots m_n)^s = m_1^s \ldots m_n^s = m_1^s \cap \ldots \cap m_n^s$ (par comaximalité).

L'anneau A est isomorphe à $A/(m_1^s \cap \ldots \cap m_n^s)$ et donc au produit $\Pi_{i=1}^n (A/m_i^s)$.

L'anneau A/m_i^s est artinien et a pour seul idéal premier m_i/m_i^s. Il est donc local.

Remarque

Le lecteur pourra vérifier à titre d'exercice que l'anneau A/m_i^s est isomorphe à l'anneau $S_i^{-1}(\Pi_{j=1}^n A/m_j^s)$ où $S_i = A - m_i$ puis à l'anneau A_{m_i}.

Ainsi l'anneau artinien A est isomorphe au produit de ces localisés en les idéaux maximaux.

Ce résultat sera généralisé aux anneaux semi-locaux complets dans le chapitre 8 puis aux algèbres finies sur les anneaux locaux henséliens dans le chapitre 13.

4. Une caractérisation des anneaux artiniens

Théorème IV.4

Soit A *un anneau.*

Les assertions suivantes sont équivalentes :

(i) A *est noethérien et tout idéal premier de* A *est maximal*

(ii) A *est artinien*

(iii) le A*-module* A *est de longueur finie*

Démonstration

On commence par remarquer que *l'idéal* (0) *d'un anneau artinien est un produit d'idéaux maximaux* : si $m_1,\ldots,m_n$ sont les idéaux maximaux de l'anneau il existe un entier s tel que $(m_1 \cap \ldots \cap m_n)^s = (0)$. Or, on a déjà remarqué que $(m_1 \cap \ldots \cap m_n)^s = m_1^s \ldots m_1^s$.

On démontre d'abord le lemme suivant, qui est une forme affaiblie du théorème.

Lemme 1

Soit A *un anneau dans lequel* (0) *est produit d'idéaux maximaux.*

Les assertions suivantes sont équivalentes :

(i) A *est noethérien*

(ii) A *est artinien*

(iii) le A*-module* A *est de longueur finie*

Démonstration du lemme 1

On sait que (iii) implique (i) et (ii) *sans hypothèse sur l'idéal* (0).

On va démontrer que (i) ou (ii) implique (iii).

Soit $(0) = m_1 \ldots m_n$ une représentation de (0) comme produit d'idéaux maximaux avec n *minimal* en sorte que $\Pi_{j=1}^{i} m_j$ contient *strictement* $\Pi_{j=1}^{i+1} m_j$ $(i = 1,\ldots,n-1)$.

On a donc une suite de composition de A-modules :

$$A_o = A \supset A_1 = m_1 \supset A_2 = m_1\, m_2 \supset \ldots \supset A_n = m_1 \ldots m_n = (0)$$

Le A-module A_i/A_{i+1} est annulé par m_{i+1} $(i = 0,\ldots,n-1)$ et est donc muni d'une structure naturelle de A/m_{i+1}-espace vectoriel.

L'hypothèse (i) ou (ii) implique que cet espace vectoriel est de dimension finie.

Relevant dans A une suite de Jordan-Hölder de cet espace vectoriel on obtient une suite de Jordan-Hölder du A-module A (raffinant la suite de composition) qui est donc de longueur finie.

La démonstration du théorème résulte alors du lemme suivant.

Lemme 2

Soit A *un anneau noethérien.*

Un idéal de A *contient un produit d'idéaux premiers de* A.

En particulier, (0) *est un produit d'idéaux premiers.*

Démonstration du lemme 2

Soit F l'ensemble des idéaux de A ne contenant pas un produit d'idéaux premiers.

Si F est non vide il possède un élément maximal a.

L'idéal a n'est pas premier. Il existe donc x et y n'appartenant pas à a tel que xy appartienne à a.

Les idéaux a+Ax et a+Ay qui contiennent strictement a contiennent des produits d'idéaux premiers. Il en est de même de leur produit. Or, ce produit est contenu dans a en sorte que a contient un produit d'idéaux premiers, contrairement au fait qu'il appartient à F.

Corollaire

Soient A *un anneau noethérien,* $m_1,\ldots,m_n$ *des idéaux maximaux de* A, r *l'idéal* $m_1 \cap \ldots \cap m_n$, q *un idéal de* A *tel que, pour un entier* $s \geqslant 1$, $r^s \subset q \subset r$.

L'anneau A/q *est artinien.*

Démonstration

Comme l'anneau A/q est quotient de l'anneau A/r^s, il suffit de prouver que l'anneau A/r^s est artinien.

Ceci résulte de ce que l'anneau A/r^s est noethérien d'idéaux premiers les idéaux maximaux m_i/r^s (i = 1,...,n).

Remarque

Soient A un anneau (noethérien), m un idéal maximal.

On peut considérer le corps quotient A/m comme une approximation de l'anneau A.

On obtient une meilleure approximation en considérant un quotient A/m^n pour $n \in N$ supérieur à 1. L'approximation est d'ailleurs d'autant meilleure que n est grand.

Les anneaux artiniens fournissent donc des approximations des anneaux noethériens plus satisfaisantes que celles que l'on obtiendrait en ne considérant que des corps.

5. Notions sur les modules artiniens

On a, donné dans la proposition II.2, la structure des modules noethériens. La structure des modules artiniens est plus compliquée. Elle a été élucidée par E. Matlis dans le cas où l'anneau de base A est noethérien (52) et par B. Ballet dans le cas général.

On va ici se contenter d'indiquer les résultats les plus faciles.

Proposition IV.5 (*modules de type fini sur un anneau artinien*)

Soient A *un anneau artinien,* M *un* A*-module.*

Les assertions suivantes sont équivalentes :

(i) M *est de type fini*

(ii) M *est artinien*

(iii) M *est noethérien*

(iv) M *est de longueur finie*

Démonstration

Elle est laissée au soin du lecteur.

Socle d'un module

Soient A *un anneau,* M *un* A*-module.*

On désigne par Max(A) l'ensemble des idéaux maximaux de A.

On appelle socle de M *et on note* $s(M)$ *le sous-module* $\Sigma_{m\in \mathrm{Max}(A)} \mathrm{Ann}(m)$ *où* $\mathrm{Ann}(m)$ *est* $\{x\in M / mx = 0\}$.

En fait, $s(M)$ est somme directe interne des sous-modules $\mathrm{Ann}(m)$: si $m_1,\ldots,m_n \in \mathrm{Max}(A)$, on vérifie aisément que $\mathrm{Ann}(m_1) \cap (\mathrm{Ann}(m_2)+\ldots+\mathrm{Ann}(m_n)) = (0)$.

Lemme

Soient A *un anneau noethérien,* M *un* A*-module artinien.*

Les assertions suivantes sont équivalentes :

(i) $M = 0$

(ii) $s(M) = 0$

Démonstration

(i) $\Longrightarrow$ (ii) : évident.

(ii) $\Longrightarrow$ (i). On démontre non(i) $\Longrightarrow$ non(ii). Soit x non nul de M. Alors, $\mathrm{Ann}(x) \neq A$.

L'anneau A/Ann(x) est artinien : en effet, le A-module A/Ann(x)

est artinien comme M et donc le A/Ann(x)-module A/Ann(x) est artinien. Par conséquent, le socle de A/Ann(x) est non nul et il en est de même, a fortiori, de $s(M)$.

Il résulte alors du fait que, si N est un sous-module de M, $s(N) = N \cap s(M)$ que *si M est un module artinien sur un anneau noethérien* A, M *est extension essentielle de son socle* $s(M)$.

De plus, *ce socle est un* A*-module artinien et donc somme finie* $\bigoplus_{i=1}^{n} A/m_i$ *où* $m_i \in \mathrm{Max}(A)$ (les idéaux maximaux m_i n'étant pas forcément distincts) : en effet, pour tout $m \in \mathrm{Max}(A)$, Ann(m) est un A/m-module artinien et donc un A/m-espace vectoriel de dimension finie.

Ainsi, l'enveloppe injective E(M) de M ((FFAC).chap.5,I.§5) est égale à l'enveloppe injective $E(\bigoplus_{i=1}^{n} A/m_i)$, i.e. à $\bigoplus_{i=1}^{n} E(A/m_i)$.

Ainsi, *un* A*-module artinien est un sous-module d'un* A*-module de la forme* $\bigoplus_{i=1}^{n} E(A/m_i)$.

La réciproque est exacte : il suffit de démontrer que si l'anneau A est noethérien, pour tout idéal maximal m de A, E(A/m) est artinien. Ceci est proposé en exercice. (chapitre II. ex. 4.7.).

V. Généralités sur les anneaux factoriels

1. Définitions

Soit A *un anneau.*

L'ensemble des éléments inversibles de A est un groupe multiplicatif, *le groupe des unités de* A.

Soient $x, y \in A$. On dit que x est *associé à* y si $x = yz$ où z est inversible dans A.

Alors, y est associé à x. On dit aussi que x et y *sont associés*.

On dit que y *divise* x s'il existe $z \in A$ tel que $yz = x$. Ceci équivaut à la condition $x \in (y)$ ou encore à l'inclusion $(x) \subset (y)$ d'idéaux principaux.

Il en résulte que, *si* x *et* y *sont associés*, $(x) = (y)$.

La réciproque est vraie si l'anneau A *est intègre* : si $(x) = (y)$, x et y sont associés. En effet, si $x = 0$, il en est de même de y. Il suffit donc de considérer le cas $x \neq 0$; il existe alors $z, t \in A$ tels que $x = yz$, $z = xt$; comme $x(1-zt) = 0$, $zt = 1$ et z est inversible.

Définition

Un élément x *de* A *est dit premier* (resp. *irréductible*) *si*

1. il est non nul et non inversible, c'est à dire si l'idéal (x) est différent de (0) et A,

2. l'idéal (x) *est premier*, ce qui revient à dire que, si x divise un produit de deux éléments de A, il divise l'un de ces éléments (resp. *une égalité* $x = yz$, *où* $y,z \in A$, *implique que* y *ou* z *est inversible*).

Autrement dit, un élément irréductible est un élément x non nul et non inversible n'admettant que les diviseurs évidents, les éléments inversibles et les éléments associés à x.

Dans l'anneau $\mathbb{Z}$, les notions d'élément irréductible et d'élément premier coïncident : un élément irréductible ou premier est de la forme p ou -p, où p est un nombre premier au sens usuel.

Si l'anneau A *est intègre, un élément* x *premier est irréductible* :

Soient, en effet, $y,z \in A$ tels que $yz = x$. Par exemple, y appartient à (x), i.e. il existe $t \in A$ tel que $y = tx$ et on en déduit $tz = 1$.

La réciproque est, en général, fausse. Tel sera le cas notamment dans un anneau noethérien non factoriel. Elle est vraie pour une classe importante d'anneaux intègres : les anneaux factoriels.

La notion d'élément irréductible se traduit en terme d'idéaux principaux.

On a les équivalences pour un élément $x \in A$:

(i) x *est irréductible.*

(ii) *l'idéal* (x) *est non nul, différent de* A *et une inclusion* $(x) \supset (y)$ *implique l'égalité* (y) = (x), i.e. y *est associé à* x, *ou* (y) = A, i.e. y *est inversible.*

(iii) *l'idéal* (x) *est maximal dans l'ensemble des idéaux principaux non nuls et distincts de* A.

Définitions

1. Un anneau intègre A *est dit factoriel si*

1°) tout élément non nul et non inversible est produit d'éléments irréductibles

2°) une égalité $x_1 \ldots x_n = y_1 \ldots y_m$ *où* x_i, y_j *sont irréductibles, implique l'égalité* $n = m$ *et l'existence d'une permutation* π *de* $\{1,\ldots,n\}$ *telle que* x_i *soit associée à* $y_{\pi(i)}$.

Un élément associé à un élément irréductible est évidemment irréductible.

2. Un ensemble P d'éléments irréductibles d'un anneau A est appelé un ensemble de représentants de classes d'éléments irréductibles associés de A si tout élément irréductible de A est associé à un élément de P et si deux éléments distincts de P ne sont pas associés.

Proposition V.1

Soient A un anneau intègre, P un ensemble d'éléments irréductibles de A. Les assertions suivantes sont équivalentes :

(i) L'anneau A est factoriel et P est un ensemble de représentants de classes d'éléments irréductibles associés

(ii) Tout élément non nul x de A s'écrit de manière unique sous la forme :

$$(1) \qquad x = \varepsilon_x \prod_{p \in P} p^{n_p(x)}$$

où ε_x est inversible et $n_p(x)$ est nul sauf pour un nombre fini de $p \in P$.

Démonstration

(ii) $\Longrightarrow$ (i).

Soit q un élément irréductible de A. On l'écrit sous la forme (1). Puisqu'il est irréductible, il existe $p \in P$ tel que $n_p(q) = 0$ pour tout $p \in P$ distinct de q. Donc, q est associé à p. En raison de l'unicité de l'écriture (1), deux éléments distincts de P ne sont pas associés. Par suite, P est un ensemble de représentants de classes d'éléments irréductibles associés.

On déduit de (ii) que tout élément non nul et non inversible x de A est produit d'éléments irréductibles : il suffit de regrouper l'élément inversible ε_x avec un élément $p \in P$ tel que $n_p(x)$ soit non nul.

Soient $q_1 \ldots q_r = u_1 \ldots u_s$ deux représentations d'un même élément non nul et non inversible de A comme produit d'éléments irréductibles. Il existe alors p_i (resp. p'_j) $(i = 1,\ldots,r)$ (resp. $j = 1,\ldots,s$) appartenant à P tel que $q_i = \varepsilon_i p_i$ (resp. $u_j = \varepsilon'_j p'_j$) avec ε_i (resp. ε'_j) inversible.

On déduit de l'égalité :

$$(\varepsilon_1 \ldots \varepsilon_r) p_1 \ldots p_r = (\varepsilon'_1 \ldots \varepsilon'_s) p'_1 \ldots p'_s$$

et de l'unicité de l'écriture (1) l'égalité $r = s$ et l'existence d'une permutation π de $\{1,\ldots,r\}$ telle que $p_i = p'_{\pi(i)}$.

Il en résulte que q_i et $u_{\pi(i)}$ sont associés. Ceci achève la démonstration de la factorialité de A.

(i) $\Longrightarrow$ (ii).

Il est clair qu'un élément non nul x de A s'écrit sous la forme (1)

L'unicité, facile, est laissée au soin du lecteur.

Proposition V.2

Soient A *un anneau factoriel,* P *un ensemble de représentant des classes d'éléments irréductibles associés de* A.

1. Pour tout couple (x,y) *d'éléments non nuls de* A *et tout* $p \in P$, $n_p(xy) = n_p(x) + n_p(y)$.

2. Pour tout couple (x,y) *d'éléments non nuls de* A, *on a les équivalences :*

(i) y *divise* x

(ii) pour tout $p \in P$, $n_p(y) \leqslant n_p(x)$

3. Deux éléments non nuls x *et* y *de* A *admettent un plus grand commun diviseur* (p.g.c.d.) *et un plus petit commun multiple* (p.p.c.m.), *définis à association près, et que l'on prendra dans la suite sous la forme*

$$\text{p.g.c.d.}(x,y) = \prod_{p \in P} p^{\inf(n_p(x), n_p(y))}$$

$$\text{p.p.c.m.}(x,y) = \prod_{p \in P} p^{\sup(n_p(x), n_p(y))}$$

Démonstration

Elle est laissé au soin du lecteur.

Proposition V.3 (*Une caractérisation des anneaux factoriels*)

Soit A *un anneau intègre.*

Les assertions suivantes sont équivalentes :

(i) A *est factoriel*

(ii) A *satisfait aux deux conditions suivantes :*

(F1) *toute suite croissante d'idéaux principaux de* A *est stationnaire*

(F2) *tout élément irréductible de* A *est premier*

Démonstration

(i) $\Longrightarrow$ (ii).

(i) $\Longrightarrow$ (F1).

Un élément x non nul de A n'admet qu'un nombre fini de classes de diviseurs associés : les classes d'éléments $\prod_{p \in P} p^{m_p}$ où $m_p \geqslant n_p(x)$.

Il n'existe donc qu'un nombre fini d'idéaux principaux de A contenant (x).

(F1) en résulte immédiatement.

(i) $\Longrightarrow$ (F2) soient $y,z \in A$ tels que yz appartienne à (x).

Dire que x est irréductible c'est dire qu'il est associé à un élément p de P.

Dire que $yz \in (x)$ c'est alors dire que $n_p(yz) \geqslant 1$, soit $n_p(y) + n_p(z) \geqslant 1$ et donc $n_p(y) \geqslant 1$ ou $n_p(z) \geqslant 1$, soit $y \in (x)$ ou $z \in (x)$.

(ii) $\Longrightarrow$ (i).

Soit Φ l'ensemble des idéaux principaux, distincts de A et (0), qui ne sont pas produits d'idéaux principaux engendrés par des éléments irréductibles (i.e. d'idéaux principaux maximaux dans l'ensemble des idéaux principaux distincts de A).

Dire qu'il existe t, non nul et non inversible de A, non produit d'éléments irréductibles c'est dire que Φ est non vide.

L'ensemble Φ admet alors un élément maximal (x). (Condition (F1)).

L'élément x n'est pas irréductible ; il est donc de la forme yz où (y) et (z) contiennent (x) *strictement* et sont donc produits d'idéaux principaux engendrés par des éléments irréductibles. Il en est de même de (x), contrairement à l'hypothèse.

Ainsi tout élément non nul et non inversible de A *est produit d'éléments irréductibles.*

L'unicité se démontre par récurrence sur le nombre minimal n de facteurs dans une décomposition d'un élément (non nul et non inversible) en produit d'éléments irréductibles.

Supposant l'unicité vérifiée pour $n-1$, soit $x_1 \ldots x_n = y_1 \ldots y_m$ où les éléments x_i et y_j sont irréductibles.

Utilisant (F2), on voit qu'il existe $i \in \{1,\ldots,n\}$ tel que $(x_i) \subset (y_1)$ et, comme (x_i) est maximal (dans l'ensemble des idéaux principaux de A), $(x_i) = (y_1)$.

On peut supposer $i = 1$. Divisant par x_1, on se ramène au cas $n-1$.

Corollaire

Un anneau principal est factoriel.

Démonstration

Un anneau principal A est noethérien et vérifie donc (F1).

Un élément irréductible de A engendre un idéal *maximal* dans l'ensemble des idéaux principaux, et donc *dans l'ensemble des idéaux* de A

dictincts de A. Il engendre donc un idéal premier. Il vérifie donc (F2).

2. Le théorème de Gauss

D'abord une définition.

Soient A *un anneau factoriel,* X *une indéterminée,* f(X) *un élément non nul de* A[X].

On appelle *contenu de* f *et on note* c(f) le p.g.c.d. des coefficients de f(X) écrit sous la forme (1). (Proposition V.1).

On dit que f est *primitif* si c(f) = 1.

Lemme

Soient A *un anneau factoriel,* f(X) *et* g(X) *deux éléments non nuls de* A[X]. *Alors* c(fg) = c(f) c(g).

Démonstration

Si f et g sont primitifs, il en est de même de fg. Sinon, soit p un facteur irréductible de fg. En vertu de (F2), l'anneau A/(p) est intègre. Il en est de même de l'anneau (A/(p))[X]. Désignant par $\overline{f}(X)$ et $\overline{g}(X)$ les images de f(X) et g(X) dans (A/(p))[X], on déduirait de l'égalité $\overline{f}(X)\overline{g}(X) = 0$ l'égalité $\overline{f}(X) = 0$ ou l'égalité $\overline{g}(X) = 0$, qui signifierait que p divise c(f) ou c(g), contrairement à l'hypothèse.

Le cas général résulte de ce que $f(X) = c(f)f_1(X)$ et $g(X)=c(g)g_1(X)$ où f_1 et g_1 sont primitifs, et donc de l'égalité $f(X)g(X) = c(f)c(g)f_1(X)g_1(X)$ d'où l'on déduit, parce que $f_1(X)g_1(X)$ est primitif, l'égalité cherchée c(fg) = c(f)c(g).

Théorème V.4 (*théorème de Gauss*)

Soient A *un anneau factoriel,* $X_1,\ldots,X_n$ *des indéterminées.*

L'anneau $A[X_1,\ldots,X_n]$ *est factoriel.*

Démonstration

Il suffit d'examiner le cas n = 1. On pose alors $X_1 = X$.

Soit K le corps des fractions de A. Il existe un ensemble Q de représentants des classes d'éléments irréductibles associés de K[X] formé d'éléments de A[X] et même d'éléments *primitifs* de A[X].

Soit, d'autre part, P un ensemble de représentants de classes d'éléments irréductibles associés de A.

On va démontrer que $P \cup Q$ *est un ensemble de représentants des classes d'éléments irréductibles associés de* A[X].

Un élément non nul $f(X) \in A[X]$ s'écrit $a \prod_{g \in Q} g(X)^{n_g}$ avec $a \in K$. On écrit $a = b/d$ avec $b, d \in A$. On obtient $df(X) = b \prod_{g \in Q} g(X)^{n_g}$ et, prenant le contenu des deux membres, $dc(f) = b$, d'où $a = c(f)$. Par conséquent, a est un élément de A.

On écrit alors $a = \varepsilon \prod_{p \in P} p^{n_p}$, avec ε inversible dans A, et on obtient une représentation de $f(X)$ sous la forme

$$(1) \quad f(X) = \varepsilon \prod_{p \in P} p^{n_p} \prod_{g \in Q} g(X)^{n_g}$$

On laisse au lecteur la vérification de l'unicité de cette représentation par utilisation successive de la factorialité de $K[X]$ et de celle de A.

Pour démontrer la factorialité de $A[X]$, il suffit de démontrer que tout élément p de P et tout élément $g(X)$ de Q sont irréductibles. D'abord une égalité $p = h(X)k(X)$, où $h(X)$ et $k(X)$ appartiennent à $A[X]$, implique l'égalité $0 = d°h + d°k$. Donc, $h(X)$ et $k(X)$ appartiennent à A. Il en résulte que $h(X)$ ou $k(X)$ est inversible dans A et donc, a fortiori, dans $A[X]$. Ensuite, une égalité $g(X) = h(X)k(X)$ avec $h(X), k(X) \in A[X]$ implique, par exemple, que $h(X)$ est un élément inversible de $K[X]$ et donc un élément de K et, en définitive, de A. Comme $g(X)$ est primitif, cet élément de A n'admet pas de diviseur irréductible et est ainsi un élément inversible de A.

Corollaire

Soient k *un corps ou un anneau principal* (par exemple, $\mathbb{Z}$), $X_1, \ldots, X_n$ *des indéterminées.*

L'anneau $k[X_1, \ldots, X_n]$ *est factoriel.*

Remarques

1. Dans : *On unique factorization domains. III.J.math.*5,1961,1-17, P. Samuel a donné des exemples d'anneaux noethériens factoriels A tels que l'anneau $A[[X]]$ des séries formelles ne soit pas factoriel, résolvant ainsi un problème posé par W. Krull.

2. L'étude des anneaux factoriels noethériens sera reprise dans le chapitre 12 à propos des anneaux locaux réguliers.

3. Application aux courbes algébriques planes

Des objets géométriques plus généraux que les courbes algébriques planes seront étudiés dans le chapitre 6.

On va, de plus, se limiter ici au cas où le corps de base est le corps $\mathbb{C}$ des complexes. Les résultats de ce paragraphe s'étendent d'ailleurs sans difficulté au cas où le corps de base k est *algébriquement clos*, i.e. possède l'une des propriétés équivalentes suivantes :

(i) tout polynôme non constant à une indéterminée X à coefficient dans k se décompose en facteurs du premier degré

(ii) les seuls polynômes irréductibles de l'anneau $k[X]$ sont les polynômes du premier degré

Elle implique que le corps k est *infini* mais l'exemple $k = \mathbb{R}$ montre que la réciproque est fausse. [chap. 5]

Définition

Soient X *et* Y *des indéterminées,* $f(X,Y)$ *un polynôme non constant de* $\mathbb{C}[X,Y]$.

Le sous-ensemble

$V(f) = \{(x,y) \in \mathbb{C}^2 / f(x,y) = 0\}$

est appelé la courbe algébrique plane d'équation $f(X,Y) = 0$.

Exemples

1. La courbe d'équation $aX + bX + c = 0$, où $a,b,c, \in \mathbb{C}$ et a et b ne sont pas simultanément nuls, est une droite.

Plus généralement, la courbe d'équation $c(X-a_1)\ldots(X-a_r)$, où $a_1,\ldots,a_r,c \in \mathbb{C}$ et c est non nul, est la réunion des droites d'équations $X - a_i = 0$ $(i = 1,\ldots,r)$ qui sont parallèles à l'axe OY.

2. La courbe d'équation $X^2 + Y^2 + aX + bY + c = 0$ est un cercle.

Proposition V.5

Soit $f(X,Y)$ *un polynôme non constant de* $\mathbb{C}[X,Y]$.

La courbe algébrique $V(f)$ *d'équation* $f(X,Y) = 0$ *est un ensemble infini.*

Démonstration

1er cas : $f(X,Y)$ est de la forme $c(X-a_1)\ldots(X-a_r)$, où $a_1,\ldots,a_r,c \in \mathbb{C}$, $c \neq 0$.

Alors $V(f)$ est infini comme réunion de droites, infinies puisqu'en bijection avec $\mathbb{C}$.

2ème cas : $f(X,Y)$ est de la forme $a_r(X)+\ldots+a_0(X)Y^r$ avec $a_i(X) \in \mathbb{C}[X]$, $a_0(X) \neq 0$.

Le complémentaire E dans $\mathbb{C}$ de l'ensemble des racines de $a_o(X)$ est infini.

Pour tout $x \in E$, il existe $y \in \mathbb{C}$ tel que $f(x,y) = 0$ et donc un point (x,y) de $V(f)$.

Remarque

L'analogue de la proposition V.5 avec $\mathbb{R}$ au lieu de $\mathbb{C}$ est faux, bien que $\mathbb{R}$ soit infini : le sous-ensemble $\{(x,y) \in \mathbb{R}^2 / x^2 + y^2 + 1 = 0\}$ est vide !

Utilisation de la factorialité de $\mathbb{C}[X,Y]$.

Soient $f(X,Y)$ *un polynôme non constant de* $\mathbb{C}[X,Y]$, $f(X,Y) = \prod_{i=1}^{s} f_i(X,Y)^{r_i}$ *une décomposition de* $f(X,Y)$ *en produit de facteurs irréductibles distincts.*

Il est clair que $V(f) = \bigcup_{i=1}^{s} V(f_i)$.

L'étude des courbes algébriques planes se ramène donc à celle des courbes algébriques planes d'équations $f(X,Y) = 0$ où f est *irréductible*.

On va voir l'interprétation géométrique de cette condition sur F.

Définition

1. Une courbe algébrique plane C *est dite réductible s'il existe des courbes algébriques planes* C_1 *et* C_2 *telles que* $C = C_1 \cup C_2, C \neq C_1$ *et* $C \neq C_2$.

Par exemple, $V(X^2 - Y^2)$ est réductible, réunion des droites $V(X-Y)$ et $V(X+Y)$.

2. Une courbe algébrique plane qui n'est pas réductible est dite irréductible.

Comme si f et g sont associés, $V(f) = V(g)$, il est naturel de considérer l'ensemble des classes d'équivalence de polynômes associés.

On note $\overline{f}$ *la classe d'équivalence de* f *et* $V(\overline{f})$ *la courbe algébrique plane* $V(f)$.

Théorème V.6 (*courbes et polynômes irréductibles*)

L'application : $\overline{f} \longmapsto V(\overline{f})$ *est une bijection de l'ensemble des classes de polynômes irréductibles associés sur l'ensemble des courbes algébriques planes irréductibles.*

Démonstration

Elle se déduit de la proposition suivante.

Proposition V.7

Soient $f(X,Y)$, $g(X,Y) \in \mathbb{C}[X,Y]$. *On suppose* f *irréductible.*

Si f *ne divise pas* g, $V(f) \cap V(g)$ *est un ensemble fini.*

Démonstration

On démontre que $V(f) \cap V(g)$ *est contenu dans l'intersection d'un nombre fini de droites parallèles à* OX *et d'un nombre fini de droites parallèles à* OY.

Puisque f est irréductible et ne divise pas g, 1 est p.g.c.d. de f et g dans $\mathbb{C}[X,Y]$. Il l'est encore dans $\mathbb{C}(X)[Y]$: sinon, il existe un facteur commun $h(X,Y)$ dans $\mathbb{C}(X)[Y]$, non constant, i.e. $\notin \mathbb{C}(X)$,de f et g ; donc, $f = uh$ et $g = vh$ où u,v appartiennent à $\mathbb{C}(X)[Y]$. On peut, évidemment, supposer, par multiplication par un élément convenable de $\mathbb{C}[X]$, que $h(X,Y)$ appartient à $\mathbb{C}[X,Y]$.

Soit $d(X) \in \mathbb{C}[X]$ un dénominateur commun de u et v. Il existe $u_1, v_1 \in \mathbb{C}[X,Y]$ tels que $df = u_1 h$ et $dg = v_1 h$. Un facteur irréductible de h n'appartenant pas à $\mathbb{C}[X]$ ne peut diviser d. Il doit donc diviser f et g. C'est impossible.

L'identité de Bezout, appliqué à f et g dans $\mathbb{C}(X)[Y]$, s'écrit

$$1 = \frac{a(X,Y)}{m(X)} f(X,Y) + \frac{b(X,Y)}{m(X)} g(X,Y) \text{ où}$$

$a(X,Y)$, $b(X,Y) \in \mathbb{C}[X,Y]$, $m(X) \in \mathbb{C}[X]$, soit

$$m(X) = a(X,Y)f(X,Y) + b(X,Y)g(X,Y)$$

Donc, $V(f) \cap V(g) \subset V(m)$.

Echangeant les rôles de X et Y, on voit qu'il existe $n(Y) \in \mathbb{C}[Y]$ tel que $V(f) \cap V(g) \subset V(n)$. Donc, $V(f) \cap V(g)$ est contenu dans l'ensemble *fini* $V(m) \cap V(n)$.

Démonstration du théorème V.6

Si f *est irréductible, la courbe* $V(f)$ *est irréductible.*

En effet, une égalité $V(f) = V(g) \cup V(h) = V(gh)$ implique, comme $V(f) \cap V(gh)$ est infini, que f divise gh et donc, par exemple, divise g. Mais alors $V(f) \subset V(g)$ et donc $V(f) = V(g)$.

L'application : $\overline{f} \longmapsto V(\overline{f})$ *est injective.*

L'égalité $V(\overline{f}) = V(\overline{g})$ signifie, pour des représentants f et g, l'égalité $V(f) = V(g)$.

Comme $V(f) \cap V(g) = V(f) = V(g)$ est infini, f divise g et g divise f. Donc, f et g sont associés, i.e. $\overline{f} = \overline{g}$.

L'application : $\bar{f} \longmapsto V(\bar{f})$ *est surjective.*

On a déjà remarqué qu'une courbe algébrique plane est de la forme $V(f)$ où le polynôme $f(X,Y)$ est le produit $f_1 \ldots f_s$ de polynômes irréductibles $f_1,\ldots,f_s$ deux à deux non associés.

Si $s \geqslant 2$, $V(f)$ *est réductible* : Soit, en effet, $g_1 = f_2 \ldots f_s$ en sorte que $V(f) = V(f_1) \cup V(g_1)$. Comme f_1 ne divise pas g_1, $V(f_1) \cap V(g_1)$ est fini. Comme $V(f_1)$ et $V(g_1)$ sont infinis, $V(f_1)$ (resp. $V(g_1)$) n'est pas contenu dans $V(g_1)$ (resp. $V(f_1)$) et donc, $V(f_1)$ et $V(g_1)$ sont distincts de $V(f)$.

Par conséquent, une courbe algébrique plane irréductible est de la forme $V(\bar{f})$ où $\bar{f}$ est la classe d'un polynôme f irréductible.

Corollaire 1

Une courbe algébrique plane est, de manière unique, réunion de courbes algébriques planes irréductibles.

Démonstration

Une courbe algébrique plane est de la forme $V(f_1) \cup \ldots \cup V(f_s)$ où $f_1,\ldots,f_s$ sont des polynômes irréductibles deux à deux non associés et est donc réunion des courbes algébriques planes irréductibles $V(f_1),\ldots,V(f_s)$.

Une égalité $V(f_1) \cup \ldots \cup V(f_s) = V(g_1) \cup \ldots \cup V(g_t)$, où $g_1,\ldots,g_t$ sont des polynômes irréductibles deux à deux non associés implique que les polynômes $f_1 \ldots f_s$ et $g_1 \ldots g_t$ sont associés : en effet, comme $V(f_i) = V(f_i) \cap V(g_1 \ldots g_t)$ est infini, f_i divise $g_1 \ldots g_t$ $(i = 1,\ldots,s)$; donc, $f_1 \ldots f_s$ divise $g_1 \ldots g_t$. De la même manière, $g_1 \ldots g_t$ divise $f_1 \ldots f_s$.

Ainsi, $s = t$ et il existe, par factorialité de $\mathbb{C}[X,Y]$, une permutation π de $\{1,\ldots,s\}$ telle que f_i et $g_{\pi(i)}$ soient associés et donc que $V(f_i) = V(g_{\pi(i)})$.

Corollaire 2

L'application : $\bar{f} \longmapsto V(\bar{f})$ *est une bijection de l'ensemble des classes de produits de polynômes irréductibles deux à deux non associés sur l'ensemble des courbes algébriques planes.*

Algèbre affine d'une courbe algébrique plane

Soient C *une courbe algébrique plane,* $f(X,Y) \in \mathbb{C}[X,Y]$, *produit de polynômes* $f_1,\ldots,f_r$ *irréductibles et deux à deux non associés tel que* $C = V(f)$.

Ce polynôme f est déterminé, à élément inversible près de $\mathbb{C}[X,Y]$, par C.

La $\mathbb{C}$-algèbre $\mathbb{C}[X,Y]/(f(X,Y))$ ne dépend que de C.

On l'appelle la $\mathbb{C}$-algèbre affine de C. On la note $\mathbb{C}[C]$.

Il résulte de la factorialité de $\mathbb{C}[X,Y]$ que (f) est égal à $(f_1) \cap \ldots \cap (f_r)$.

Comme les idéaux (f_i) sont premiers, l'algèbre affine $\mathbb{C}[C]$ est *réduite*.

Elle est *intègre* si et seulement si $r = 1$, i.e. si f est irréductible et donc si et seulement si la courbe C est irréductible.

On va démontrer l'existence d'une bijection de C sur l'ensemble des idéaux maximaux de $\mathbb{C}[C]$. Voici d'abord un lemme, cas particulier d'un résultat plus général démontré dans le chapitre 5 (proposition I.2.2.) par une autre méthode.

Lemme

Un idéal maximal de $\mathbb{C}[X,Y]$ est de la forme $(X-a, Y-b)$ où $a,b \in \mathbb{C}$.

Démonstration

L'idéal $(X-a, Y-b)$, où $a,b \in \mathbb{C}$, est maximal comme noyau de l'homomorphisme *surjectif* de $\mathbb{C}$-algèbres de $\mathbb{C}[X,Y]$ sur $\mathbb{C}$ appliquant X sur a et Y sur b.

Soit, réciproquement, m un idéal maximal de $\mathbb{C}[X,Y]$. Comme $m \cap \mathbb{C} = (0)$ on peut identifier $\mathbb{C}$ à un sous-corps du corps quotient $\mathbb{C}[X,Y]/m$.

Soient a et b les classes respectives de X et Y modulo m en sorte que $\mathbb{C}[X,Y]/m = \mathbb{C}[a,b]$. Les éléments a et b sont algébriques (algébriquement dépendants sur $\mathbb{C}$ au sens de (FFAC)) sur $\mathbb{C}$. Ils appartiennent donc à $\mathbb{C}$ en sorte que $m = (X-a, Y-b)$.

Supposons, en effet, a transcendant que $\mathbb{C}$, i.e. tel que l'homomorphisme de $\mathbb{C}[X]$ sur $\mathbb{C}[a]$ appliquant X sur a soit injectif et donc un isomorphisme. On peut alors identifier a à X.

Les éléments $\frac{1}{a-\lambda}$ où λ parcourt $\mathbb{C}$ sont *linéairement indépendants* sur $\mathbb{C}$: une égalité

$$\Sigma_{i=1}^{r} \frac{b_i}{a-\lambda_i} = 0 \quad , \quad \text{où} \quad b_i \in \mathbb{C} \ ,$$

implique, en effet, par multiplication par $a - \lambda_i$ et spécialisation de a en λ_i , l'égalité $b_i = 0$.

Il en résulte que $[\mathbb{C}[a]:\mathbb{C}]$ est un cardinal *non dénombrable* comme le cardinal de $\mathbb{C}$.

Or, $[\mathbb{C}[X]:\mathbb{C}]$ est dénombrable. On obtient ainsi une contradiction.

Proposition V.7 (*idéaux maximaux de l'algèbre affine*)

Soient x *et* y *les classes respectives de* X *et* Y *dans l'algèbre affine* $\mathbb{C}[C]$.

L'application : $(a,b) \longmapsto (x-a,y-b)$ *est une bijection de* C *sur l'ensemble des idéaux maximaux de* $\mathbb{C}[C]$.

Démonstration

L'application : $(a,b) \longmapsto (X-a,Y-b)$ est une bijection de C sur l'ensemble des idéaux maximaux de $\mathbb{C}[X,Y]$ contenant $f(X,Y)$, où f est un polynôme produit de polynômes irréductibles distincts tel que $C = V(f)$ et $\mathbb{C}[C] = \mathbb{C}[X,Y]/(f)$.

La proposition V.7. est un cas particulier du théorème des zéros de Hilbert, démontré plus généralement dans le chapitre 6.

Exercices du chapitre 2

(1). Un sous-anneau d'un anneau artinien est-il artinien ? noethérien ?

(2). Soient A un anneau, B une A-algèbre finie, M un B-module. Comparer la propriété pour M d'être un B-module noethérien (resp. de longueur finie) et celle d'être un A-module noethérien (resp. de longueur finie).

Si M est une B-module artinien, est-il aussi un A-module artinien ?

(3). Que peut-on dire d'un anneau noethérien intègre dont tout idéal de type fini est principal ?

(4). Que peut-on dire d'un anneau n'ayant qu'un idéal premier, celui-ci étant de type fini ?

(5). Soient A un anneau, M un A-module, I un ensemble. On suppose le A-module $M^{(I)}$ noethérien.

Que peut-on dire de I? de M?

Même question avec M^I.

(6). Démontrer les équivalences pour un anneau A.

(i) A est cohérent

(ii) la catégorie des A-modules de type fini est abélienne

A-t-on une caractérisation analogue avec la catégorie des A-modules de présentation finie ?

(7). Démontrer qu'un anneau de fractions d'un anneau cohérent est cohérent.

(8). Démontrer qu'une algèbre finie sur un anneau cohérent intègre est un anneau cohérent.

(9). Soit A le sous-anneau de $\mathbb{Q}^{\mathbb{N}}$ des suites stationnaires.

Démontrer que l'anneau A est cohérent.

Soit e_n l'élément $(a_i)_{i\in\mathbb{N}}$ de A où $a_{2j+1} = 1$ $(j = 0,\ldots,n-1)$, $a_i = 0$ si $i \neq 1,\ldots,2n-1$.

Démontrer que l'annulateur de l'élément $\Sigma_{n\geqslant 1} e_n X^n$ de l'anneau $A[X]$ n'est pas de type fini . En déduire que l'anneau $A[[X]]$ n'est pas cohérent.

(10). Soit A un anneau. Un A-module M est dit *indécomposable* s'il est $\neq(0)$ et s'il n'est pas somme directe de deux sous-modules non nuls.

1. Démontrer que si l'ensemble des sous-modules de M satisfait à la condition minimale, M est nul ou somme directe d'un nombre fini de sous-modules indécomposables.

2. Démontrer que si l'anneau A est artinien, tout A-module non nul de type fini est somme directe d'un nombre fini de sous-modules indécomposables.

3. Soit M un A-module non nul indécomposable de longueur finie. Démontrer que l'ensemble des éléments non inversibles à gauche de l'anneau $\mathrm{End}_A(M)$ des A-endomorphismes de M est un idéal maximal à gauche, que c'est aussi l'ensemble des éléments non-inversibles à droite (Une situation analogue se trouvera dans le chap. 11.III. prop. III.1).

4. Soient M un A-module de longueur finie, $M_1\oplus\ldots\oplus M_n$ et $N_1\oplus\ldots\oplus N_m$ deux décompositions de M comme sommes directes de sous-modules indécomposables. Démontrer que $m = n$ et qu'il existe une permutation s de $\{1,\ldots,n\}$ telle que, pour tout i, M_i soit isomorphisme à $N_{s(i)}$. (Ce résultat est connu sous le nom de théorème de Krull-Schmidt).

(11). (Groupes résolubles)

Cet exercice est une généralisation aux groupes non nécessairement commutatifs des résultats de III (pour les $\mathbb{Z}$-modules, i.e. les groupes abéliens). Il sera utilisé dans le chapitre 6 pour démontrer l'impossibilité de la résolution par radicaux de l'équation générique de degré $\geqslant 5$.

Soit G *un groupe* (non nécessairement commutatif). On désigne par e son élément neutre.

Une *suite de composition* de G est une suite *strictement décroissante* :

(1) $G_o = G > G_1 > \ldots > G_n = (e)$

de sous-groupes de G tels que, pour tout $i = 0,\ldots,n-1$, G_{i+1} soit *normal* dans G_i.

Les quotients G_i/G_{i+1} sont appelés les *facteurs* de la suite de composition.

Un élément maximal de l'ensemble des suites de composition de G, pour la relation d'ordre naturelle , est appelé une *suite* de Jordan-Hölder de G.

1. Démontrer que, si G a une suite de Jordan-Hölder, toutes les suites de Jordan-Hölder de G ont la même longueur et que toute suite de composition de G peut être raffinée en une suite de Jordan-Hölder.

2. On dit que la groupe G est *résoluble* s'il admet une suite de Jordan-Hölder dont les facteurs sont abéliens. Démontrer qu'alors ces facteurs sont des groupes cycliques d'ordres des nombres premiers (groupes abéliens simples).

Démontrer que si H est sous-groupe normal de G, les assertions suivantes sont équivalentes : (i) G est résoluble

(ii) H et G/H sont résolubles

3. Démontrer que les facteurs de deux suites de Jordan-Hölder d'un groupe G (admettant de telles suites) sont deux à deux isomorphes.

4. Démontrer que le groupe alterné A_n est simple pour $n \geqslant 5$ et en déduire que pour $n \geqslant 5$ le groupe symétrique S_n n'est pas résoluble.

Indications : une permutation π de $\{1,\ldots,n\}$ est appelée un cycle d'ordre m s'il existe $a_1,\ldots,a_m \in \{1,\ldots,n\}$ tels que $\pi(a) = a$ si $a \notin \{a_1,\ldots,a_m\}$, $\pi(a_i) = a_{i+1}$ si $i = 1,\ldots,m-1$, $\pi(a_m) = a_1$. On écrit alors $\pi = (a_1,\ldots,a_m)$ et l'ensemble $\{a_1,\ldots,a_m\}$ est appelé le support du cycle π. Deux cycles sont dits disjoints si leurs supports sont disjoints. On démontre que tout $\pi \in S_n$ est, de manière unique, produit de cycles disjoints.

On démontre d'abord qu'un sous-groupe H *normal du groupe alterné* A_n (avec n>2) *qui contient un cycle* (ijk) *d'ordre* 3 *est égal à* A_n : supposant (ijk) = (123), on remarque, en effet, que

$(12k) = (12)(3k)(123)^2(12)(3k)$ appartient à H et on utilise le fait que les cycles $(12k)$ $(k\geqslant 3)$ engendrent A_n.

On démontre ensuite que si $n\geqslant 5$ *tout sous-groupe normal de* A_n *distinct de* $\{e\}$ *contient un cycle d'ordre* 3 *en examinant les différents cas suivants :*

1. Il existe $\pi\in H$ tel que $\pi = \theta\rho$ où $\theta = (a_1 \ldots a_m)$ avec $m>3$ et ρ produit de cycles disjoints de θ. Calculer alors $\pi_1 = \sigma\pi\sigma^{-1}$ où $\sigma = (a_1a_2a_3)$ puis $\pi^{-1}\pi_1$.

2. On n'est pas dans le cas 1. mais il existe $\pi\in H$ tel que π soit produit de deux cycles disjoints d'ordre 3 et de cycles (d'ordre $\leqslant 3$) disjoints de ceux-ci ; on peut supposer $\pi = (123)(456)\theta$. Calculer $\pi_1 = (234)\pi(432)$ et $\pi^{-1}\pi_1$. Obtenir une contradiction.

3. Démontrer que s'il existe dans H un élément π de la forme $(123)\theta$ où θ est un produit de transpositions (cycles d'ordre 2) disjointes et disjointes de (123), $\pi^2 = (132)$.

4. Tout élément de H est produit de transpositions disjointes ; on peut supposer qu'il existe $\pi\in H$ de la forme $(12)(34)\theta$ où θ est un produit de transpositions disjointes et disjointes de (12) et (34). Calculer $\pi_1 = (234)\pi(432)$, $\pi_2 = \pi^{-1}\pi_1$, $\pi_3 = (145)\pi_2(541)$ et enfin $\pi_2^{-1}\pi_3$.

(12). Démontrer pour un anneau A les équivalences suivantes dues à H. Bass.

*(Injective Dimension in Noetherian Rings. Trans.Amer.Math.Soc.*102, 18.29,1962).

(i) A est noethérien

(ii) une somme directe de A-modules injectifs est un A-module injectif

(iii) une limite inductive filtrante de A-modules injectifs est un A-module injectif

((i) $\Longrightarrow$ (iii). Utiliser la caractérisation d'un module injectif ((FFAC).chap.5.prop.I.4).

(iii) $\Longrightarrow$ (ii). Utiliser le fait que le A-module $\bigoplus_{i\in I} M_i$ est limite inductive filtrante des A-modules $\bigoplus_{i\in J} M_i$ où J parcourt l'ensemble des parties finies de I.

(ii) $\Longrightarrow$ (i). Considérer une suite croissante $a_1 \subset a_2 \subset \cdots \subset a_n \subset \cdots$ d'idéaux de A, pour tout $n\in N^*$, un A-module injectif I_n contenant A/a_n, I

la somme directe $\bigoplus_{n\in N^*} I_n$, a l'idéal $\bigcup_{n\in N^*} a_n$. Soit f_n la surjection canonique de a sur a/a_n composée avec l'injection de a/a_n dans I_n. Définir $f : a \longrightarrow I$ par $f(x) = \Sigma_{n\in N^*} f_n(x)$. Prolonger f en $g : A \longrightarrow I$. En déduire l'existence de $n\in N^*$ tel que $f(a)$ soit contenu dans $I_1\oplus\ldots\oplus I_n$ puis l'égalité $a = a_{n+1}$).

(13). L'exercice suivant est tiré de l'article : *Subrings of Artnian and Noetherian Rings*. D.Eisenbud. Math.Ann.185, 247-249, 1970.

Soient B un anneau, A un sous-anneau de B tel que B soit un A-algèbre finie, E l'enveloppe injective du A-module sous-jacent à un B-module M.

1. Démontrer que,si le B-module $\mathrm{Hom}_A(B,M)$ est injectif, le A-module M est injectif.

(Démontrer que l'application naturelle $u : \mathrm{Hom}_A(B,M) \longrightarrow \mathrm{Hom}_A(B,E)$ est essentielle. Utiliser le diagramme commutatif

$$\begin{array}{ccc} \mathrm{Hom}_A(B,M) & \xrightarrow{u} & \mathrm{Hom}_A(B,E) \\ \downarrow & & \downarrow \\ M=\mathrm{Hom}_A(A,M) & \longrightarrow & E=\mathrm{Hom}_A(A,E) \end{array}$$

pour démontrer que l'injection : $M \longrightarrow E$ est surjective, en utilisant le fait que u l'est).

2. Utiliser la caractérisation des anneaux noethériens données dans l'exercice 12 pour démontrer que si B est noethérien il en est de même de A.

(Soit $\{I_k\}_{k\in K}$ une famille de A-modules injectifs. Utiliser la finitude de B sur A pour démontrer l'égalité $\bigoplus_{k\in K} \mathrm{Hom}_A(B,I_k)=\mathrm{Hom}_A(B,\bigoplus_{k\in K} I_k)$. Déduire de 1. que $\bigoplus_{k\in K} I_k$ est un A-module injectif).

(14). Soient A un anneau, $X_1,\ldots,X_n$ des indéterminées.

1. Démontrer que si A est noethérien, l'anneau $A[[X_1,\ldots,X_n]]$ est noethérien.

(Se ramener au cas n=1. Reprendre alors la démonstration du théorème II.3 en remplaçant le degré d'un polynôme par l'ordre d'une série formelle).

2. Etudier la réciproque.

Les exercices 15, 16, 17, 18 qui suivent sont consacrés à la démonstration du fait que l'anneau $\mathbb{C}\{\{X_1,\ldots,X_n\}\}$ des séries convergentes à n indéterminées à coefficients complexes est noethérien et factoriel. On a suivi l'exposé de [37].

La démonstration repose sur un théorème dû à Weierstrass et appelé

théorème de préparation. La validité d'un tel théorème dans l'anneau des séries formelles sera démontré dans le chapitre 8 (théorème IV.3). On peut en déduire le théorème de préparation pour les séries convergentes par une méthode de fonctions majorantes.

(15). 1. Soient D un polydisque $\{|z_i| < R\}$ de $\mathbb{C}^n$, ϕ une fonction analytique dans D telle que $|\phi(z_1,\ldots,z_n)| \leqslant M$ pour tout $(z_1,\ldots,z_n)$ de D, ϕ_2 et ϕ_1 les fonctions analytiques dans D

$$\phi_2(z_1,\ldots,z_n) = \Sigma_0^{p-1} \frac{\partial^j \phi(z_1,\ldots,z_{n-1},0)}{\partial z_n^j} \frac{z_n^j}{j!}$$

$$\phi_1(z_1,\ldots,z_n) = (\phi(z_1,\ldots,z_n) - \phi_2(z_1,\ldots,z_n))/z_n^p$$

où p est un entier $\geqslant 1$.

Déduire des inégalités de Cauchy que $|\phi_2(z_1,\ldots,z_n)| \leqslant pM$ pour tout $(z_1,\ldots,z_n) \in D$ puis du lemme de Schwarz l'inégalité

$$|\phi_1(z_1,\ldots,z_n)| \leqslant (p+1)M/R^p \text{ pour tout } (z_1,\ldots,z_n) \in D$$

2. Soit h une fonction analytique dans D telle que :

$$h(0,\ldots,0,z_n^p) = 0 \text{ pour tout } z_n \text{ tel que } |z_n| < R$$

$$|h(z_1,\ldots,z_n)| \leqslant c \text{ pour tout } (z_1,\ldots,z_n) \in D$$

On choisira D suffisamment petit pour que $c(p+1) \leqslant R^{p/2}$. (Ceci est évidemment possible puisque h s'annule à l'origine et est agréable pour la suite).

Soit g *une fonction analytique dans* D *et bornée dans* D.

Démontrer l'existence de deux suites $s_0 = 0, s_1, \ldots, s_k, \ldots$ de fonctions analytiques et bornées dans D et $r_1, \ldots, r_k, \ldots$ de fonctions analytiques dans D *polynomiales de degré* $<p$ en z_n (ceci signifie que la série de Taylor de r_j est un polynôme de degré $<p$ en l'indéterminée X_n) telles que, pour tout $(z_1,\ldots,z_n) \in D$,

$$g(z_1,\ldots,z_n) = z_n^p s_k(z_1,\ldots,z_n) + h(z_1,\ldots,z_n)s_{k-1}(z_1,\ldots,z_n) + r_k(z_1,\ldots,z_n)$$

Démontrer la majoration :

$$\sup_D |s_{k+1} - s_k| \leqslant 2^{-k} \sup_D |s_1|$$

Démontrer que la série de terme général $(s_{k+1} - s_k)$ converge uniformément dans D.

Soit s la somme de cette série. C'est une fonction analytique dans D et

$$\sup_D |s| \leqslant 2(p+1)R^{-p} \sup_D |g|$$

En déduire l'existence de r analytique dans D, bornée dans D et polynomiale en z_n de degré $<p$ telle que, pour tout $(z_1,\ldots,z_n)$ dans D,

$$g(z_1,\ldots,z_n) = (h(z_1,\ldots,z_n) + z_n^p)s(z_1,\ldots,z_n) + r(z_1,\ldots,z_n)$$

3. Soient g et f des fonctions analytiques dans un voisinage de 0 de $\mathbb{C}^n$ telles que $f(0,\ldots,0,z_n)/z_n^p$ soit analytique non nulle à l'origine de $\mathbb{C}^n$. On définit f_1 et f_2 analytiques au voisinage de l'origine de $\mathbb{C}^n$ par

$$f(z_1,\ldots,z_n) = f_1(z_1,\ldots,z_n) + z_n^p\, f_2(z_1,\ldots,z_n)$$

où f_1 est polynomiale de degré p en z_n s'annulant pour $z_1=\ldots=z_{n-1} = 0$.

Posant $h = f_1 f_2^{-1}$ et appliquant ce qui précède démontrer l'existence d'un polydisque D telle que g et f soient analytiques et bornées dans D et de fonctions q et r analytiques et bornées dans D telles que $g=qf+r$ et r soit polynomiale de degré $<p$ en z_n.

Démontrer l'unicité du couple (q,r).

(16). *Soit* A *l'anneau des germes de fonctions analytiques en l'origine de* $\mathbb{C}^n$.

On note $\tilde{f}$ le germe de la fonction analytique.

Si f est analytique au voisinage de 0 de $\mathbb{C}^n$, on désigne par $T(f)$ la série de Taylor de f en 0. C'st la série formelle

$$\Sigma_{(i_1,\ldots,i_n)\in\mathbb{N}^n} \frac{\partial^{i_1+\ldots+i_n}}{\partial z_1^{i_1}\ldots\partial z_n^{i_n}} f(0,\ldots,0)\, \frac{X_1^{i_1}\ldots X_n^{i_n}}{i_1!\ldots i_n!}$$

On remarque que si $\tilde{f} = \tilde{g}$, $T(f) = T(g)$.

On définit donc la série de Taylor d'un élément a de A comme $T(\tilde{f})$ où $a = \tilde{f}$. On la note $T(a)$.

1. Démontrer que l'application : $a \longmapsto T(a)$ est un isomorphisme de $\mathbb{C}$-algèbres de A sur l'anneau $\mathbb{C}\{\{X_1,\ldots,X_n\}\}$ des séries convergentes (sous-anneau de $\mathbb{C}[[X_1,\ldots,X_n]]$ des séries formelles dont les coefficients satisfont à des inégalités de Cauchy).

En déduire que $\mathbb{C}\{\{X_1,\ldots,X_n\}\}$ est local d'idéal maximal $(X_1,\ldots,X_n)$.

2. Déduire de l'exercice 15 le *théorème de préparation pour les séries convergentes* :

Une série $f(X_1,\ldots,X_n)$ est dite *régulière d'ordre* p *en* X_n si $f(0,\ldots,0,X_n)$ est une série d'ordre p.

Soient f une série convergente régulière d'ordre p en X_n, g une série convergente.

Il existe un couple (q,r) et un seul d'éléments de $\mathbb{C}\{\{X_1,\ldots,X_n\}\}$ tel que $g = qf + r$ et r soit un polynôme de degré $<p$ en X_n à coefficients dans $\mathbb{C}\{\{X_1,\ldots,X_{n-1}\}\}$.

Un polynôme unitaire en X_n est dit *distingué* (ou de Weierstrass) s'il s'écrit

$$a_p(X_1,\ldots,X_{n-1})+a_{p-1}(X_1,\ldots,X_{n-1})X_n+\ldots+a_1(X_1,\ldots,X_{n-1})X_n^{p-1}+X_n^p$$

où $a_i(X_1,\ldots,X_{n-1}) \in \mathbb{C}\{\{X_1,\ldots,X_{n-1}\}\}$ et $a_i(0,\ldots,0) = 0$ $(i = 1,\ldots,p)$.

3. Appliquant le théorème de préparation à f (régulière d'ordre p en X_n) et $g = X_n^p$ démontrer que f est associée à un polynôme distingué de degré p en X_n.

(Ce polynôme distingué est appelé le *polynôme distingué de* f).

4. Démontrer l'existence d'un automorphisme ϕ de $\mathbb{C}$-algèbres de $\mathbb{C}\{\{X_1,\ldots,X_n\}\}$ tel que $\phi(h(X_1,\ldots,X_n)) = h(X_1,X_2+a_2X_1,\ldots,X_n+a_nX_1)$, où $a_2,\ldots,a_n \in \mathbb{C}$.

Démontrer qu'il existe un tel automorphisme tel que, *pour une série convergente donnée* f, $\phi(f)$ soit régulière en X_n.

(C'est l'analogue de la proposition II.1. du chapitre 7, l'ordre remplaçant le degré).

(17). (Démonstration de la noethérianité de l'anneau des séries convergentes)

Soit a un idéal de l'anneau $\mathbb{C}\{\{X_1,\ldots,X_n\}\}$. On veut démontrer qu'il est de type fini. C'est clair si $a = (0)$. On suppose donc $a \neq (0)$. Soit f non nul $\in a$.

1. Utilisant le 4 de l'exercice 16, démontrer que l'on peut supposer f régulière en X_n.

2. Démontrer que le $\mathbb{C}\{\{X_1,\ldots,X_{n-1}\}\}$-module $\mathbb{C}\{\{X_1,\ldots,X_n\}\}/(f)$ est alors de type fini.

Raisonner alors par récurrence supposant $\mathbb{C}\{\{X_1,\ldots,X_{n-1}\}\}$ noetérien pour en déduire que l'idéal $a/(f)$ est de type fini et qu'il en est de même de l'idéal a.

(18). (Démonstration de la factorialité des anneaux de séries convergentes)

On procède par récurrence sur n. On suppose donc démontré que $\mathbb{C}\{\{X_1,\ldots,X_{n-1}\}\}$ est factoriel. *On veut alors démontrer* que $\mathbb{C}\{\{X_1,\ldots,X_n\}\}$ est factoriel et, comme il est noethérien, *que tout élément irréductible est premier.*

Soit f un élément irréductible de $\mathbb{C}\{\{X_1,\ldots,X_n\}\}$. Remarque : pour tout automorphisme ϕ de $\mathbb{C}$-algèbres de $\mathbb{C}\{\{X_1,\ldots,X_n\}\}$, $\phi(f)$ est irréductible.

En déduire que l'on peut supposer que l'élément irréductible f est régulier en X_n.

Démontrer alors que le polynôme distingué de f est irréductible dans $\mathbb{C}\{\{X_1,\ldots,X_{n-1}\}\}[X_n]$. Déduire de la factorialité de $\mathbb{C}\{\{X_1,\ldots,X_{n-1}\}\}$ que ce polynôme distingué est premier et qu'il en est de même de f.

(19). Soit $\mathcal{E}^1$ l'anneau des germes en 0 des fonctions numériques de classe C^∞ dans un voisinage de 0. On note $\tilde{f}$ le germe de la fonction f de classe C^∞.

1. L'anneau $\mathcal{E}^1$ est local. Quel est son idéal maximal $m(\mathcal{E}^1)$?

2. Soit, pour $n\in N$, f_n la fonction définie par $f_n(0) = 0$, $f_n(x) = x^{-n}\exp(-1/x^2)$ si $x \neq 0$.

Démontrer que f_n est de classe C^∞ sur R.

3. Démontrer que l'idéal $(\tilde{f}_n)_{n\in N}$ n'est pas de type fini.

(Remarquer que sinon il serait engendré par un nombre fini d'éléments $\tilde{f}_n$ et serait par conséquent principal).

4. Comment s'interprète l'idéal $\bigcap_{n=0}^{\infty} m(\mathcal{E}^1)^n$? Démontrer que cet idéal est non nul. (Utiliser, par exemple, $\tilde{f}_o$).

(Cet idéal est l'idéal des germes de fonctions *plates* à l'origine. On démontre que si A est un anneau local *noethérien* d'idéal maximal m, $\bigcap_{n=0}^{\infty} m^n = (0)$ (théorème de Krull. Chap.8.1. Théorème 1.4. Corollaire 2). On retrouve ainsi que l'anneau $\mathcal{E}^1$ n'est pas noethérien).

5. Démontrer que l'anneau $\mathcal{E}^n$ des germes de fonctions numériques de classe C^∞ dans un voisinage de l'origine dans $\mathbb{R}^n$ est local non noethérien ($n\geq 1$).

(20). Soit k un corps de caractéristique le nombre premier p.

On le suppose non parfait. Ceci signifie qu'il existe un élément de k sans racine p-ème. Il existe un corps $k^{p^{-\infty}}$ formé des racines p^n-èmes

(pour n parcourant N) des éléments de k. (Chapitre 5.IV.§1).

1. Démontrer l'existence, pour tout $n \in N^*$, de $x_n \in k^{p^{-\infty}}$ tel que $x_n^{p^n}$ appartienne à k mais que $x_n^{p^{n-1}}$ n'appartienne pas à k.

Soit A l'anneau $k^{p^{-\infty}} \underset{k}{\otimes} k^{p^{-\infty}}$. On pose $z_n = 1 \otimes x_n - x_n \otimes 1$.

2. Démontrer que $z_n^{p^n} = 0$ et $z_n^{p^{n-1}} \neq 0$.

En déduire qu'il n'existe pas d'entier naturel r tel que, $n(A)$ désignant le nilradical de A, $n(A)^r = (0)$.

Démontrer que l'anneau A n'est pas noethérien. (Si A était noethérien, il existerait r tel que $n(A)^r = (0)$.)

(21). Soient A un anneau factoriel, p un élément irréductible de A, X une indéterminée, $f(X) = X^n + a_1 X^{n-1} + \ldots + a_n$ un polynôme $\in A[X]$, K le corps des fractions de A.

On suppose a_i divisible par p pour tout $i = 1, \ldots, n$ mais a_n non divisible par p^2.

Démontrer que f(X) est irréductible dans $K[X]$ (*Critère d'irréductibilité* d'Eisenstein).

En déduire l'irréductibilité dans $\mathbb{Q}[X]$ des polynômes suivants, où p est un nombre *premier*.

1. $X^n - p$

2. du polynôme cyclotomique $X^{p-1} + X^{p-2} + \ldots + X + 1 = f(X)$

(On démontrera l'irréductibilité de $f(X+1)$).

Démontrer directement cette irréductibilité.

(22). Soient k un corps, $T_1, \ldots, T_n, X_1, \ldots, X_n$ des indéterminées, $K = k(T_1, \ldots, T_n)$, $f_i(X_1, \ldots, X_n)$ $(i = 1, \ldots, n)$ des polynômes sans diviseur non constant de $k[X_1, \ldots, X_n]$.

Démontrer que le polynôme $f(X_1, \ldots, X_n) = \sum_{i=1}^{n} T_i f_i(X_1, \ldots, X_n)$ est irréductible dans $K[X_1, \ldots, X_n]$.

CHAPITRE 3

Idéaux premiers associés
Décomposition primaire

La plupart des questions traitées dans ce chapitre (diviseurs de zéro, éléments nilpotents, décomposition primaire) se traduisent simplement dans le cas où l'anneau de base est l'anneau $\mathbb{Z}$ des entiers et où le module considéré est un idéal de $\mathbb{Z}$. Voici donc un exposé des principaux résultats dans ce cas particulièrement simple.

Soient n un entier distinct de 0,1 et -1, $\varepsilon \prod_{i=1}^{s} \Pi_i^{r_i}$ *sa décomposition en produit de nombres premiers distincts* Π_i *et d'un des éléments inversibles* +1 *ou* -1.

La racine de l'idéal $q_i = (\Pi_i^{r_i})$ est l'idéal premier $p_i = (\Pi_i)$. L'idéal q_i est p_i-primaire. La décomposition (n) $= \bigcap_{i=1}^{s} q_i$ de l'idéal (n) est appelée la *décomposition primaire réduite* de cet idéal.

Soit M *le* $\mathbb{Z}$*-module* $\mathbb{Z}/(n)$ isomorphe à $\bigoplus_{1}^{s} \mathbb{Z}/q_i$.

L'annulateur d'un élément non nul de M est de la forme $(\prod_{i=1}^{s} \Pi_i^{t_i})$ où $0 \leqslant t_i \leqslant r_i$ et l'un au moins des t_i est non nul. *Les éléments maximaux* pour la relation d'inclusion de *l'ensemble de ces annulateurs sont justement des idéaux premiers* p_i. *On les appelle les idéaux premiers associés au* $\mathbb{Z}$*-module* M.

Un élément a de $\mathbb{Z}$ est dit *diviseur de zéro* (resp. *nilpotent*) dans M s'il existe $\overline{b}$ non nul de M tel que $a\overline{b} = 0$, i.e. $b \in \mathbb{Z}$, $b \notin (n)$ tel que ab appartienne à (n). (resp. s'il existe $m \in \mathbb{N}^*$ tel que a^m annule M, i.e. tel que a^m appartienne à l'annulateur (n) de M).

Il est facile de vérifier que *l'ensemble des diviseurs de zéro* (resp. *des nilpotents*) *dans* M *est* $\bigcup_{i=1}^{s} p_i$ (resp. $\bigcap_{i=1}^{s} p_i$).

E. Lasker puis E. Noether ont démontré des résultats analogues dans d'autres anneaux. E. Lasker (50) a démontré que *si* A *est l'anneau* $k[X_1,\ldots,X_r]$ *des polynômes à* r *indéterminées à coefficients dans un corps* k, tout idéal *a*, distinct de $k[X_1,\ldots,X_r]$, est de la forme $\bigcap_{i=1}^{s} q_i$, où q_i est p_i-primaire, les idéaux premiers $p_1,\ldots p_s$ étant distincts et, pour tout i, q_i ne contient pas $\bigcap_{j \neq i} q_j$.

On obtient alors des assertions analogues à celles obtenues pour le $\mathbb{Z}$-module $\mathbb{Z}/(n)$ pour le A-modulo A/a à propos des annulateurs d'éléments non nuls, des diviseurs de zéro et des éléments nilpotents.

E. Noether (54) *a démontré la validité de résultats analogues pour tout anneau noethérien* A *et tout idéal a distinct de* A.

Il existe alors des idéaux premiers $p_1,\ldots,p_s$, dits *associés au*

A-*module* A/a, des idéaux $q_1,\ldots,q_s$ tels que q_i soit p_i-primaire, ne contienne pas $\bigcap_{j\neq i} q_j$ et que $a = \bigcap_{i=1}^{s} q_i$ (décomposition primaire reduite de l'idéal a). Les idéaux premiers associés à A/a sont les annulateurs d'éléments de A/a qui sont maximaux parmi les annulateurs d'éléments non nuls de A/a. L'ensemble des diviseurs de zéro (resp. des éléments nilpotents) de A/a est $\bigcup_{i=1}^{s} p_i$ (resp. $\bigcap_{i=1}^{s} p_i$).

La présentation de la notion d'idéal premier associé adoptée ici n'est pas la présentation historique, issue de la théorie de la décomposition primaire. Le lecteur trouvera dans l'exercice 21 une telle présentation.

On part ici de l'étude des diviseurs de zéro. La notion d'idéal premier faiblement associé, due à Bourbaki et indispensable en l'absence d'hypothèses noethériennes, s'introduit alors naturellement. Signalons que nous avons cru bon d'appeler idéal premier associé ce que Bourbaki appelle idéal premier faiblement associé, réservant le nom d'ideal premier fortement associé à ce qu'il appelle idéal premier associé. Les deux notions coincident d'ailleurs quand des hypothèses noethériennes sont satisfaites.

La partie I est consacrée à l'introduction des idéaux premiers associés et à l'étude de leurs propriétés les plus naturelles.

La partie II traite de la décomposition primaire sous hypothèses noethériennes.

La partie III plus technique étudie le comportement du support et de l'ensemble des idéaux premiers associés par changement de base.

I. Idéaux premiers associés

1. Diviseurs de zéro d'un module

Soient A *un anneau,* M *un* A*-module.*

Un élément a de A est dit *diviseur de zéro dans* M s'il existe un élément x *non nul* de M tel que $ax = 0$ ou, ce qui est équivalent, si l'homothétie $\delta_a^M : x \longmapsto ax$ n'est pas injective.

Par définition même, l'ensemble D(M) des diviseurs de zéro de M est $\bigcup_{\substack{x\in M\\ x\neq 0}} \mathrm{Ann}(x)$ où $\mathrm{Ann}(x) = \{a \in A / ax = 0\}$ est l'annulateur de x.

En fait, $D(M) = \bigcup_{\substack{x\in M\\ x\neq 0}} r(\mathrm{Ann}(x))$, où $r(a)$ désigne la racine de l'idéal a:

Soit en effet, $z \in r(\mathrm{Ann}(x))$, $z \notin \mathrm{Ann}(x)$.

Il existe un entier $n > 1$ tel que z^{n-1} n'appartienne pas à Ann(x) et z^n appartienne à Ann(x). Alors, $z \in \mathrm{Ann}(z^{n-1}x)$.

Ainsi *l'étude des diviseurs de zéro du A-module M se ramène à celle des idéaux de la forme $r(\mathrm{Ann}(x))$ et donc des idéaux premiers minimaux d'idéaux de la forme* Ann(x) *pour x non nul.* On est donc conduit à la définition suivante:

Définition

Un idéal premier p de A est dit associé au A-module M s'il existe un élément x non nul de M tel que p soit idéal premier minimal de Ann(x).

On dit alors que l'élément x correspond à l'idéal premier associé p

L'ensemble des idéaux premiers associés à M est noté $\mathrm{Ass}_A(M)$, *ou simplement* Ass(M) *s'il n'y a pas de risque de confusion.*

On remarque que $\mathrm{Ass}_A(0)$ est $\emptyset$. La réciproque est vraie (prop. I.6)

La proposition suivante fournit des exemples d'idéaux premiers associés.

Proposition I.1

Soient A un anneau, M un A-module, $E = \{\mathrm{Ann}(x)/x \in M, x \neq 0\}$.

Un élément maximal de E ordonné par inclusion est un idéal premier. C'est donc un idéal premier associé à M.

Démonstration

Soit $p = \mathrm{Ann}(x)$ un élément maximal de E.

Soient a, $b \in A$ tels que ab appartienne à p et b n'appartienne pas à p. Alors $bx \neq 0$ et a appartient à Ann(bx). Mais, $\mathrm{Ann}(bx) \supset \mathrm{Ann}(x)$ et, par maximalité de Ann(x), $\mathrm{Ann}(bx) = \mathrm{Ann}(x)$. Donc, a appartient à p et p est premier.

Proposition I.2 (idéaux premiers associés quand l'anneau est noethérien)

Soient A un anneau noethérien, M un A-module.

Tout idéal premier associé à M est de la forme Ann(x).

Démonstration

Soient $p \in \mathrm{Ass}_A(M)$, x un élément de M correspondant à p.

On va démontrer que pA_p appartient à $\mathrm{Ass}_{A_p}(M_p)$ et est de la forme Ann(y/1) *pour $y \in M$ puis en déduire que p est de la forme* Ann(x).

Soit $S = A - p$.

On déduit de la croissance de l'application : $q \longrightarrow S^{-1}q$

que $p' = S^{-1}p$ est un idéal premier minimal de $S^{-1}\mathrm{Ann}(x)$. Or, $S^{-1}\mathrm{Ann}(x) = \mathrm{Ann}(x')$ où $x' = x/1$ est non nul parce que $\mathrm{Ann}(x) \subset p$. L'anneau $S^{-1}A$ est noethérien. Il existe donc un élément maximal q' de $\{\mathrm{Ann}(a'x')/a' \in A_p, a'x' \neq 0\}$. Il résulte de la proposition I.1 que q' appartient à $\mathrm{Ass}_{A_p}(A_p x')$. *On a l'égalité* $q' = p'$: en effet, $q' = \mathrm{Ann}(y')$ où y' est un élément non nul de $A_p x'$, on a les inclusions $\mathrm{Ann}(x') \subset \mathrm{Ann}(y') = q'$ et $q' \subset p'$, par maximalité de l'idéal p'. Comme p' est idéal premier minimal de $\mathrm{Ann}(x')$, on a l'égalité, $p' = q'$.

Donc, p' est de la forme Ann (y') et, par suite, de la forme Ann(y/1 où $y \in M$.

Soit $\{a_1, \ldots, a_n\}$ un système fini de générateurs de p. De l'égalité $(a_i/1)(y/1) = 0$, on déduit l'existence de $s_i \in S$ tel que $s_i a_i y = 0$. On pose $s = s_1 \ldots s_n$. Pour tout $a \in p$, say $= 0$ et donc $p \subset \mathrm{Ann}(sy)$. Réciproquement, soit $b \in \mathrm{Ann}(sy)$. Alors, $bsy = 0$ et donc $b/1$ appartient à $p' = \mathrm{Ann}(y/1)$. Par conséquent, b appartient à p. Finalement, $p = \mathrm{Ann}(sy)$.

Définition

Soient A *un anneau,* M *un* A*-module. Un idéal premier de la forme* Ann(x) *où* $x \in M$ *est dit fortement associé.*

Un idéal fortement associé est associé. On vient de voir que la réciproque est vraie si l'anneau A est noethérien.

Remarques

Nous n'avons pas respecté la terminologie de N. Bourbaki qui appelle idéal premier associé (resp. faiblement associé) ce qui est appelé ici idéal premier fortement associé (resp. associé).

La notion d'idéal premier fortement associé ne semble guère utilisable en algèbre *commutative non noethérienne*. La bonne notion est celle d'idéal premier associé.

Exemples

1. Cas d'un module monogène

On peut supposer le module monogène de forme A/a où a est un idéal de A.

Soient x *un élément non nul de* A/a, b *un représentant de* x *dans* A.

L'idéal Ann(x) est $(a:b) = \{c \in A/cb \in a\}$.

Un idéal premier p *de* A *est donc associé (resp. fortement associé) à* A/a *si et seulement si il existe* $b \in A$, $b \notin a$ *tel que* p *soit idéal premier minimal de* (a:b) *(resp. soit égal à* (a:b)).

On remarque que, si l'idéal a est *premier*, pour tout élément x non nul de A/a, on a l'égalité $\mathrm{Ann}(x) = a$. Il en résulte qu'alors $\mathrm{Ass}_A(A/a) = \{a\}$.

2. Exemple d'idéal premier associé mais non fortement associé

Définition

Un anneau A *est dit absolument plat (ou régulier au sens de* Von-Neumann) *si, pour tout* $a \in A$, *il existe* $x \in A$ *tel que* $a = a^2x$.

Cette définition n'est pas celle donnée dans le chapitre 2.11.§5: tout A-module est plat, mais on démontre qu'elle est équivalente (ex.8)

Voici quelques propriétés simples

1. *Si* A *est absolument plat et si* S *est une partie multiplicative de* A, *alors* $S^{-1}A$ *est absolument plat.*

2. *Un produit (fini ou infini) d'anneaux absolument plats est absolument plat.*

En particulier, comme un corps k est absolument plat, pour tout ensemble I, l'anneau k^I est absolument plat. *L'anneau* k^N *est absolument plat* non noethérien: on a, en effet, une suite strictement croissante $k^1 \subset k^2 \subset \ldots \quad k^n \subset \ldots$ d'idéaux où k^n désigne l'idéal des éléments dont toutes les coordonnées de rang $>n$ sont nulles. Il résulte donc du théorème de Cohen *qu'il existe dans* k^N *des idéaux premiers qui ne sont pas de type fini.* (voir aussi l'exercice 9).

3. *Un anneau absolument plat local* A *est un corps:* soient a non nul de A et $x \in A$ tel que $a = a^2x$. Alors $ax = (ax)^2$ est un idempotent. Comme ax est non nul comme a et A n'a pour seuls idempotents que 0 et 1, $ax = 1$.

Il en résulte que, *si* A *est absolument plat, pour tout* $p \in \mathrm{Spec}(A)$, *l'anneau* A_p *est un corps.*

4. *Si* A *est absolument plat,* $\mathrm{Ass}_A(A) = \mathrm{Spec}(A)$.

Soit, en effet, $p \in \mathrm{Spec}(A)$. Alors, $\mathrm{Ass}_{A_p}(A_p) = \{pA_p\}$ car A_p est un corps. Il en résulte que p appartient à $\mathrm{Ass}_A(A)$. (proposition I.4 plus loin).

5. *Un idéal premier fortement associé d'un anneau absolument plat* A *est de type fini:* un tel idéal p est de la forme Ann(x) et, donc, si $a = a^2x$, de la forme Ann(ax) car a appartient à ax et ax appartient à (a) et donc (a) = (ax). Or, ax est un idempotent e et Ann(e) = (1-e).

Comme k^N *a des idéaux premiers non de type fini, il a des idéaux premiers associés qui ne sont pas fortement associés.*

Propriétés fonctorielles de l'ensemble des idéaux premiers associés

Proposition I.3 (idéaux premiers associés et suites exactes)

Soit $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ *une suite exacte de* A*-modules.*

Alors $\mathrm{Ass}_A(M') \subset \mathrm{Ass}_A(M) \subset A_{ss}(M') \cup \mathrm{Ass}_A(M'')$.

Démonstration

L'inclusion $\mathrm{Ass}_A(M') \subset \mathrm{Ass}_A(M)$ est claire.

Soient $p \in \mathrm{Ass}_A(M)$, x un élément de M correspondant à p.

1er cas : il existe $a \in A$*-*p *tel que* ax *appartienne à* M'.

Comme p contient Ann(x), ax est non nul. L'idéal premier p est un idéal premier minimal de Ann(ax) et donc appartient à $\mathrm{Ass}_A(M')$: en effet, p contient Ann(x) car si b appartient à Ann(ax), abx = 0; donc $ab \in \mathrm{Ann}(x) \subset p$. Comme $a \notin p$, b appartient à p. Puisque Ann(x) est contenu dans Ann(ax), p est idéal premier minimal de Ann(ax).

2ème cas : pour tout $a \in A$*-*p, ax *n'appartient pas à* M'

Soit $\bar{x}$ l'image de x dans M''. Il résulte de l'hypothèse les inclusions

$$\mathrm{Ann}(x) \subset \mathrm{Ann}(\bar{x}) \subset p$$

Donc, p est un idéal premier minimal de $\mathrm{Ann}(\bar{x})$ et comme $\bar{x}$ est non nul, p appartient à $\mathrm{Ass}_A(M'')$.

Corollaire

Soient A *un anneau,* $(M_i)_{i \in I}$ *une famille de* A*-modules.*

Alors $\mathrm{Ass}(\bigoplus_{i \in I} M_i) = \bigcup_{i \in I} \mathrm{Ass}(M_i)$

Démonstration

On utilise le fait que $\bigoplus_{i \in I} M_i = \bigcup_J (\bigoplus_{i \in J} M_i)$, où J parcourt l'ensemble filtrant des parties finies de I.

On en déduit immédiatement l'inclusion $\mathrm{Ass}(\bigoplus_{i \in I} M_i) \subset \bigcup_J (\mathrm{Ass}(\bigoplus_{i \in J} M_i))$.

Il suffit donc de démontrer le corollaire si I est fini puis, par une récurrence immédiate sur card(I), dans le *cas où* $I = \{i_1, i_2\}$.

On déduit alors de l'exactitude de la suite

$$0 \longrightarrow M_{i_1} \longrightarrow M_{i_1} \oplus M_{i_2} \longrightarrow M_{i_2} \longrightarrow 0$$

les inclusions

$$\mathrm{Ass}_A(M_{i_1}) \subset \mathrm{Ass}_A(M_{i_1} \oplus M_{i_2}) \subset \mathrm{Ass}_A(M_{i_1}) \cup \mathrm{Ass}_A(M_{i_2})$$

On a de même une inclusion

$\mathrm{Ass}_A(M_{i_2}) \subset \mathrm{Ass}_A(M_{i_1} \oplus M_{i_2})$, d'où le résultat

Corollaire 2

Soient A *un anneau,* M *un* A*-module,* $(Q_i)_{i\in I}$ *une famille finie de sous-modules de* M *telle que* $\bigcap_{i\in I} Q_i = 0$.

Alors $\mathrm{Ass}_A(M) \subset \bigcup_{i\in I} \mathrm{Ass}(M/Q_i)$.

Démonstration

Il suffit de remarquer que l'application naturelle: $M \longrightarrow \bigoplus_{i\in I} M/Q_i$ est injective.

Proposition I.4 (passage aux anneaux de fractions)

Soient A *un anneau,* S *une partie (multiplicative) de* A. Ψ *l'ensemble des idéaux premiers de* A *ne rencontrant pas* S *et* M *un* A*-module.*

1. L'application $p \longmapsto S^{-1}p$ *est une bijection de* $\mathrm{Ass}_A(M) \cap \Psi$ *sur* $\mathrm{Ass}_{S^{-1}A}(S^{-1}M)$

2. Soit $\Psi' = \mathrm{Ass}_A(M) \cap \Psi$, N le noyau de l'application canonique i_M^S de M dans $S^{-1}M$. Alors $\mathrm{Ass}_A(N) = \mathrm{Ass}_A(M) - \Psi'$ et $\mathrm{Ass}_A(M/N) = \Psi'$.

Démonstration

1. Soient $p \in \mathrm{Ass}_A(M) \cap \Psi$, $x \in M$ un élément correspondant à p.

Alors $S^{-1}p$ est idéal premier minimal de $S^{-1}\mathrm{Ann}(x) = \mathrm{Ann}(x/1)$ et $x/1$ est un élément non nul de $S^{-1}M$. Donc, $S^{-1}p$ appartient à $\mathrm{Ass}_{S^{-1}A}(S^{-1}M)$.

Soient, réciproquement, $p' \in \mathrm{Ass}_{S^{-1}A}(S^{-1}M)$, x/s où $x \in M$, $s \in S$ un élément correspondant à p', $p = (i_A^S)^{-1}(p')$.

Alors $\mathrm{Ann}(x) \subset (i_A^S)^{-1}(\mathrm{Ann}(x/s)) \subset p$. Soit, d'autre part, q un idéal premier de A contenant Ann(x) et contenu dans p. Alors, $S^{-1}\mathrm{Ann}(x) \subset S^{-1}q \subset S^{-1}p = p'$. Comme $S^{-1}\mathrm{Ann}(x) = \mathrm{Ann}(S^{-1})(Ax)) = \mathrm{Ann}(x/s)$, $S^{-1}q = p'$ et donc $q = (i_A^S)^{-1}(S^{-1}q) = (i_A^S)^{-1}(p') = p$.

Ainsi p est un idéal premier minimal de Ann(x) et p apapartient à $\mathrm{Ass}_A(M)$.

2. En vertu de la proposition I.3, il suffit de démontrer les inclusions

$\mathrm{Ass}_A(N) \subset \mathrm{Ass}_A(M) - \Psi'$ et $\mathrm{Ass}_A(M/N) \subset \Psi'$.

Soient $p \in \mathrm{Ass}_A(N)$, $x \in N$ un élement correspondant à p.

Puisque x appartient à N, il existe $s \in S$ tel que $sx = 0$. Alors, $s \in \mathrm{Ann}(x) \subset p$ et donc $p \cap S \neq \emptyset$ en sorte que p appartient à $\mathrm{Ass}_A(M) - \Psi'$.

Soient $q \in \mathrm{Ass}_A(M/N)$, $y \in M$ dont la classe $\bar{y}$ modulo N est un élément correspondant à q. Soit $a \in q$.

Il existe $b \in A$*-*q *et un entier* $n \geqslant 1$ *tel que* ba^n *appartienne à* $\mathrm{Ann}(\bar{y})$ *et donc tel que* $ba^n y$ *appartienne à* N:

En effet, qA_q est l'unique idéal premier minimal de $\mathrm{Ann}(\overline{y})_q$ et est donc la racine de cet idéal. Il existe donc un entier $n \geqslant 1$ tel que $a^n/1$ appartienne à $\mathrm{Ann}(\overline{y})_q$.

Il existe par conséquent $s \in S$ et $b \in A-S$ tels que $sba^n y = 0$. Si a appartenait à S, il en serait de même de sa^n. Donc, by appartiendrait à N et b appartiendrait à $\mathrm{Ann}(\overline{y})$ et, a fortiori, à q, contrairement au choix de b.

Donc, $q \cap S = \emptyset$ et q appartient à Ψ.

Il reste à démontrer que q appartient à $\mathrm{Ass}_A(M)$.

Soit q' un idéal premier tel que $\mathrm{Ann}(y) \subset q' \subset q$. Si q' était différent de q, il existerait $a \in q-q'$ et, avec les notation précédentes, on aurait une égalité $sa^n by = 0$. L'élément $sa^n b$ appartiendrait à Ann(y) et donc à q'. Ceci est impossible puisque s, a et b n'appartiennent à q'.

Donc, $q' = q$ et q est idéal premier minimal de Ann(y) et appartient à $\mathrm{Ass}_A(M)$.

Remarques

1. Si $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ est suite exacte de A-modules, on a *l'égalité*

$$\mathrm{Supp}_A(M) = \mathrm{Supp}_A(M') \cup \mathrm{Supp}_A(M'')$$

car, pour tout $p \in \mathrm{Spec}(A)$, la suite $0 \longrightarrow M'_p \longrightarrow M_p \longrightarrow M''_p \longrightarrow 0$ est exacte et $M_p \neq (0)$ si et seulement si M'_p ou M''_p est non nul.

L'exemple de la suite exacte $0 \longrightarrow p \longrightarrow A \longrightarrow A/p \longrightarrow 0$ où p est un idéal premier *non nul* d'un anneau *intègre* A (qui n'est pas un corps) montre qu'une telle égalité n'est pas forcément vraie pour les idéaux premiers associés: $\mathrm{Ass}_A(A) = \mathrm{Ass}_A(p) = \{(0)\}$ tandis que $\mathrm{Ass}_A(A/p) = \{p\}$.

2. La proposition ci dessous reste valable dans le cas où l'anneau A n'est pas noethérien à condition de remplacer l'ensemble des idéaux *premiers associés* par l'ensemble des idéaux *premiers fortement associés*.

Proposition 1.5

Soient A *un anneau NOETHERIEN,* M *un* A*-module,* Φ *un sous-ensemble de* $\mathrm{Ass}_A(M)$. *Il existe un sous-module* M' *de* M *tel que* $\mathrm{Ass}_A(M') = \mathrm{Ass}_A(M) - \Phi$ *et* $\mathrm{Ass}_A(M/M') = \Phi$.

Démonstration

Soit F l'ensemble des sous-modules P de M tels que $\mathrm{Ass}_A(P) \subset \mathrm{Ass}_A(M)$. Comme il contient (0) il est non vide. Il est inductif.

Soit M' un élément maximal de F. *On va démontrer,* ce qui est suffisant, que $\mathrm{Ass}_A(M/M')$ *est contenu dans* Φ.

Soit $p \in \mathrm{Ass}_A(M/M')$. Il existe un sous-module de M/M' isomorphe à A/p. Il est de la forme N/M' où N est un sous-module de M contenant M'.

On a les inclusions

$$\mathrm{Ass}_A(N) \subset \mathrm{Ass}_A(M') \cup \mathrm{Ass}_A(A/p) = \mathrm{Ass}_A(M') \cup \{p\}$$

Puisque M' est maximal dans F, N n'appartient pas à F. Il en résulte que p appartient à Φ (par définition de F).

3. Idéaux premiers associés et support

Proposition I.6

Soit M *un* A*-module.*

1. On a l'inclusion $\mathrm{Ass}_A(M) \subset \mathrm{Supp}_A(M)$

2. Les assertions suivantes sont équivalentes :

(i) $M = (0)$

(ii) $\mathrm{Supp}_A(M) = \emptyset$

(iii) $\mathrm{Ass}_A(M) = \emptyset$

3. Les ensembles, ordonnés par inclusion, $\mathrm{Ass}_A(M)$ *et* $\mathrm{Supp}_A(M)$ *ont mêmes éléments MINIMAUX.*

Démonstration

1. Soient $p \in \mathrm{Ass}_A(M)$, x un élément correspondant à p.

On a un diagramme à ligne et colonne exactes

$$\begin{array}{ccccccc} & & 0 & & & & \\ & & \downarrow & & & & \\ 0 & \longrightarrow & Ax & \xrightarrow{\sim} & A/\mathrm{Ann}(x) & \longrightarrow & A/p \longrightarrow 0 \\ & & \downarrow & & & & \\ & & M & & & & \end{array}$$

qui, par tensorisation par A_p, fournit un diagramme à ligne et colonne exactes de A_p-modules

$$\begin{array}{ccccc} & & 0 & & \\ & & \downarrow & & \\ (x/1) & A_p & \longrightarrow & A_p/pA_p & \longrightarrow 0 \\ & \downarrow p & & & \\ & M_p & & & \end{array}$$

Comme A_p/pA_p est non nul, il en est de même de $A_p(x/1)$ et donc de M_p et $p \in \mathrm{Supp}_A(M)$.

2. Il est clair que (i) implique (ii) et, compte tenu de 1., que (ii) implique (iii).

Il suffit de démontrer que (non i) implique (non iii).

Soit x un élément non nul de M. Alors Ann(x) est contenu dans un idéal maximal m et donc dans un idéal premier minimal p. Cet élément appartient à $\mathrm{Ass}_A(M)$.

3. Soit $p \in \mathrm{Supp}_A(M)$. Comme le A_p-module M_p est non nul, il résulte de 2. que $\mathrm{Ass}_{A_p}(M_p)$ est non vide. Soit $q' \in \mathrm{Ass}_{A_p}(M_p)$. L'idéal premier $q = (i_A^p)^{-1}(q')$ est donc contenu dans p et appartient à $\mathrm{Ass}_A(M)$ (prop. I.4.1).

Corollaire

Un idéal premier MINIMAL de A appartient à $\mathrm{Ass}_A(A)$

Démonstration

Un idéal premier minimal de A est un élément minimal de $\mathrm{Supp}_A(A) = \mathrm{Spec}(A)$. Il appartient donc à $\mathrm{Ass}_A(A)$.

4. Diviseurs de zéro et éléments nilpotents

Proposition I.7

Soient A un anneau noethérien, M un A-module.

L'ensemble $D(M)$ des diviseurs de zéro de M est $\bigcup_{p \in \mathrm{Ass}_A(M)} p$.

Démonstration

Soient $p \in \mathrm{Ass}_A(M)$, $a \in p$. Alors, $p = \mathrm{Ann}(x)$ avec $x \neq 0$, parce que A est noethérien, et $ax = 0$. Donc, $a \in D(M)$.

Soient $a \in D(M)$, x non nul $\in M$ tels que $ax = 0$. Comme $Ax \neq 0$, $\mathrm{Ass}_A(Ax$ est non vide.

Soit $p \in \mathrm{Ass}_A(Ax)$. Comme A est noethérien, p est de la forme Ann(bx) pour un élément convenable b de A. De $a(bx) = 0$, on déduit que a appartient à p.

Définition

Soient A un anneau, M un A-module, $a \in A$.

On dit que a est un élément presque nilpotent (resp. nilpotent) de M si, pour tout $x \in M$, il existe un entier $n(x) > 0$ tel que $a^{n(x)}x = 0$ (resp. s'il existe un entier $n > 0$ tel que $a^n M = (0)$).

Si M est un A-module de type fini, un élément presque nilpotent de M est nilpotent.

Proposition I.8

L'ensemble des éléments presque nilpotents du A-module M est

$$\bigcap_{p \in \mathrm{Ass}_A(M)} p = \bigcap_{p \in \mathrm{Supp}_A(M)} p$$

Démonstration

Comme $\mathrm{Ass}_A(M)$ et $\mathrm{Supp}_A(M)$ ont mêmes éléments minimaux, $\bigcap_{p\in \mathrm{Ass}_A(M)} p = \bigcap_{p\in \mathrm{Supp}_A(M)} p$. Il suffit donc de démontrer que l'ensemble des éléments presque nilpotents de M est $\bigcap_{p\in \mathrm{Supp}_A(M)} p$.

Il est clair que $\mathrm{Supp}_A(M) = \bigcup_{x\in M} \mathrm{Supp}(Ax)$. D'autre part, dire que a est presque nilpotent dans M c'est dire que, pour tout $x \in M$, a est nilpotent dans Ax.

Il suffit donc de vérifier que l'ensemble des éléments nilpotents de Ax est $\bigcap_{p\in \mathrm{Supp}_A(Ax)} p$. Or, $\mathrm{Supp}(Ax) = V(\mathrm{Ann}(x))$, $\bigcap_{p\in V(\mathrm{Ann}(x))} p$ est la racine de $\mathrm{Ann}(x)$ et cette racine est bien l'ensemble des éléments nilpotents de $Ax = A/\mathrm{Ann}(x)$.

Corollaire 1

Soit M *un* A*-module de type fini.*

Alors, $r(\mathrm{Ann}(M)) = \bigcap_{p\in \mathrm{Ass}_A(M)} p$

Corollaire 2

Le nilradical de A *est* $\bigcap_{p\in \mathrm{Ass}_A(A)} p$

Démonstration

Il suffit d'appliquer la proposition 1.8 au A-module *de type fini* A.

Remarque

Un élément MINIMAL de $\mathrm{Ass}_A(M)$ (ou ce qui est équivalent de $\mathrm{Supp}_A(M)$) *est appelé idéal premier isolé associé à* M.

Un idéal premier associé à M *qui n'est pas isolé est dit immergé.*

Dire que $p \in \mathrm{Ass}_A(M)$ est immergé c'est donc dire qu'il existe $q \in \mathrm{Ass}_A(M)$ strictement contenu dans p.

La terminologie d'idéal premier associé isolé ou immergé à une origine géométrique qui sera explicité plus loin. [chapitre 6. corollaire de la proposition I.4].

On remarquera que dans la proposition I.7 et ses corollaires on peut remplacer l'ensemble $\mathrm{Ass}_A(M)$ par le sous-ensemble des idéaux premiers associés isolés.

II. Décomposition primaire

1. Idéaux premiers associés d'un module de type fini sur un anneau noethérien

La proposition ci-dessous est très utile. Elle permet souvent de se ramener à des problèmes sur des modules monogènes d'annulateurs des idéaux premiers.

Proposition II.1

Soient A *un anneau noethérien,* M *un* A*-module de type fini.*

1. Il existe une suite de composition

$$M_0 = (0) \subset M_1 \subset \ldots \subset M_n = M$$

telle que, pour $i = 1,\ldots,n$, *le* A*-module* M_i/M_{i-1} *soit monogène d'annulateur un idéal premier* p_i *et donc isomorphe à* A/p_i.

2. On a les inclusions $\mathrm{Ass}_A(M) \subset \{p_1,\ldots,p_n\} \subset \mathrm{Supp}_A(M)$

Démonstration

1. Soit F l'ensemble des sous-modules de M admettant une telle suite de composition. Il est non vide car $(0) \in F$. Soit N un élément maximal de F. Si N était distinct de M, il existerait $p \in \mathrm{Ass}_A(M/N)$ et donc un sous-module P de M contenant N strictement tel que P/N soit isomorphe à A/p. Ce sous-module P appartiendrait à F, contrairement à la maximalité de N. Donc, $M = N$ et M a une suite de composition comme dans l'énoncé.

2. Des suites exactes

$$0 \longrightarrow M_{i-1} \longrightarrow M_i \longrightarrow A/p_i \longrightarrow 0 \quad (i = 1,\ldots,n)$$

on déduit l'égalité

$$\mathrm{Supp}_A(M_i) = \mathrm{Supp}_A(M_{i-1}) \cup \mathrm{Supp}_A(A/p_i) = \mathrm{Supp}_A(M_{i-1}) \cup V(p_i)$$

et donc

$$\mathrm{Supp}_A(M) = V(p_1) \cup \ldots \cup V(p_n)$$

En particulier, les idéaux premiers $p_1,\ldots,p_n$ appartiennent à $\mathrm{Supp}_A(M)$. On a de même l'inclusion

$$\mathrm{Ass}_A(M_i) \subset \mathrm{Ass}_A(M_{i-1}) \cup \mathrm{Ass}_A(A/p_i) = \mathrm{Ass}_A(M_{i-1}) \cup \{p_i\}$$

et donc

$$\mathrm{Ass}_A(M) \subset \{p_1,\ldots,p_n\}$$

Corollaire

Soient A *un anneau noethérien,* M *un* A*-module de type fini.*

Alors, $\mathrm{Ass}_A(M)$ *est fini.*

Exemple

Soient A un anneau local noethérien d'idéal maximal m possédant un idéal premier p distinct de m. Le sous-module $N = m/p$ a une suite de composition $M_{n-1} \supset \ldots \supset M_0 = (0)$ comme dans la proposition II.1. Or, m n'appartient pas à $\mathrm{Ass}_A(A/p) = \{p\}$. L'inclusion $\mathrm{Ass}_A(M) \subset \{p_1,\ldots,p_n\}$ de la proposition II.1 peut donc être stricte. On voit également qu'il n'y a pas en général unicité de l'ensemble $\{p_1,\ldots,p_n\}$.

Proposition II.2 (caractérisation des modules de longueur finie)

Soient A *un anneau noethérien,* M *un* A*-module de type fini.*

Les assertions suivantes sont équivalentes :

(i) M *est de longueur finie*

(ii) Tout $p \in \mathrm{Ass}_A(M)$ *est un idéal maximal*

(iii) Tout $p \in \mathrm{Supp}_A(M)$ *est un idéal maximal*

Démonstration

Il est clair que (ii) implique (iii)

(i) $\Longrightarrow$ (ii). Soit $p \in \mathrm{Ass}_A(M)$. Le A-module A/p qui est isomorphe à un sous-module de M est de longueur finie. *L'anneau* A/p est donc artinien. Comme il est intègre, c'est un corps et p est maximal.

(iii) $\Longrightarrow$ (i). Il résulte de la proposition II.1 qu'il existe une suite de composition

$$M_0 = (0) \subset \ldots \subset M_n = M$$

telle que M_i/M_{i-1} soit isomorphe à un A-module A/p_i, où p_i appartenant à $\mathrm{Supp}_A(M)$, est maximal par hypothèse.

Le A-module M_i/M_{i-1} est donc de longueur finie ($i = 1,\ldots,n$). Il en est de même du A-module M.

2 Sous-modules irréductibles

La théorie qui suit s'est d'abord développée pour les idéaux d'un anneau (noethérien) A, i.e. les sous-modules de A.

Des raisons techniques naturelles ont conduit à l'étendre aux sous-modules d'un A-module de type fini.

Définitions

Soient A *un anneau,* M *un* A*-module,* N *un sous-module de* M.

On dit que N *est irréductible (dans* M*) si une égalité* $N = P \cap Q$, *où* P *et* Q *sont des sous-modules de* M, *implique l'égalité* $P = N$ *ou* $Q = N$.

Un idéal a *de* A *est dit irréductible s'il est irréductible en tant que sous-module du* A*-module* A.

Exemples

1. Un idéal premier p de A est irréductible: une égalité $a \cap b = p$ implique, en effet, l'inclusion $ab \subset p$ et donc $a \subset p$ ou $b \subset p$ soit $a = p$ ou $b = p$.

2. L'idéal (6) de $\mathbb{Z}$ est réductible puisque égal à (2) $\cap$ (3).

3. L'idéal (X^2, XY) de $k[X,Y]$, où k est un corps et X et y sont des indéterminées est réductible car égal à $(X) \cap (Y, X^2)$.

Proposition II.3

Soient A *un anneau noethérien,* M *un* A*-module de type fini.*

Tout sous-module de M *est intersection d'un nombre fini de sous-modules irréductibles.*

Démonstration

Il suffit de démontrer que l'ensemble F des sous-modules de M non intersection d'un nombre fini de sous-modules irréductibles est vide.

S'il n'en était pas ainsi, puisque M est noethérien, F admettrait un élément maximal N qui ne serait pas irréductible. Il existerait donc des sous-modules P et Q de M contenant N *strictement* tels que $N = P \cap Q$. Mais alors P et Q n'appartiendraient pas à F, seraient donc intersection d'un nombre fini de sous-modules irréductibles.

Il en serait de même de N, contrairement au fait que N appartient à F.

On va démontrer ci dessous qu'un sous-module irréductible est primaire au sens du chapitre I.

On rappelle que le sous-module N *de* M *est dit primaire si, pour tout* $a \in A$, *l'homothétie* $\delta_a^{M/N}$ *de* M/N *est soit injective soit presque nilpotent.*

Proposition II.4

Soient A *un anneau noethérien,* M *un* A*-module de type fini,* N *un sous-module de* M *distinct de* M.

Si N *est irréductible dans* M, *il est primaire.*

Démonstration

On doit démontrer que, si $a \in A$ *est tel que l'homothétie* $\delta_a^{M/N}$ *ne soit pas injective, cette homothétie est presque nilpotente,* i.e., comme M/N est de type fini, *nilpotente.* La non-injectivité de $\delta_a^{M/N}$ se traduit par l'existence de $x \in M$ n'appartenant pas à N tel que ax appartienne à N.

La suite $(N:a^n)_{n \in N}$ de sous-modules de M est croissante, et donc, puisque M est noethérien, stationnaire. Soit $n \in N$ tel que $(N:a^n) = (N:a^{n+1})$.

On pose $P = N + ax$, $Q = N + a^n M$. *On démontre l'égalité* $N = P \cap Q$:

Soit $z \in P \cap Q$. Il existe $s \in N$, $b \in A$, $t \in N$, $y \in M$ tels que $z = s + bx = t + a^n y$.

Alors $az = as + b(ax)$ appartient à N. Comme d'autre part, $az = at + a^{n+1}y$, $a^{n+1}y$ appartient à N; donc, y appartient à $(N:a^{n+1}) = (N:a^n)$ et $a^n y$ appartient à N. Il en est de même de $z = t + a^n y$.

Puisque P contient N *strictement* et N est irréductible, Q = N. Par conséquent, $a^n M$ est contenu dans N, i.e. $\delta_a^{M/N}$ est nilpotente.

Corollaire (existence des décompositions primaires sous hypothèses noethériennes)

Soient A *un anneau noethérien,* M *un* A*-module de type fini.*

Tout sous-module de M *distinct de* M *est intersection d'un nombre fini de sous-modules primaires.*

Une représentation du sous-module N de M, distinct de M, comme intersection d'un nombre fini de sous-ensembles primaires est appelée une *décomposition primaire* de N.

On va achever ce paragraphe par une autre caractérisation en termes d'idéaux premiers associés d'un sous-module primaire, sans hypothèses noethériennes d'ailleurs.

Proposition II.5

Soient A *un anneau,* M *un* A*-module,* N *un sous-module de* M.

Les assertions suivantes sont équivalentes:

(i) N *est primaire*

(ii) $\mathrm{Ass}_A(M/N)$ *est réduit à un élément* (On dit alors que M/N est coprimaire)

Si $\mathrm{Ass}_A(M/N) = \{p\}$, *le sous-module* N *est p-primaire.*

Démonstration

(ii) $\Longrightarrow$ (i). Si $\mathrm{Ass}_A(M/N) = \{p\}$, l'ensemble des diviseurs de zéro de M/N est p.

C'est l'ensemble des éléments a de A tels que l'homothétie $\delta_a^{M/N}$ ne soit pas injective. On a vu aussi que p est l'ensemble des éléments $a \in A$ tels que l'homothétie $\delta_a^{M/N}$ soit presque nilpotente (prop. I.7). Donc, N est p-primaire.

(i) $\Longrightarrow$ (ii). Si N est p-primaire, $p = \bigcap_{q \in \mathrm{Ass}_A(M/N)} q$ (prop. I.7) et $p = \bigcup_{q \in} \mathrm{Ass}_A(M/N) q$ (prop. I.1). Donc, $\mathrm{Ass}_A(M/N) = \{p\}$.

3. Décompositions primaires réduites

On va démontrer, sous hypothèses noethériennes, l'existence de décompositions primaires privilégiées, les décompositions primaires réduites et démontrer certaines propriétés d'unicité.

Proposition II.6

Soient A *un anneau,* p *un idéal premier de* A, M *un* A*-module,* $\{N_i\}_{i\in I}$ *une famille finie de sous-modules* p*-primaires.*

Le sous-module $\bigcap_{i\in I} N_i$ *est* p*-primaire.*

Démonstration

Soient $a \in A$, $x \in M$ tels que ax appartienne à $\bigcap_{i\in I} N_i$ mais a n'appartienne pas à p.

Alors, puisque N_i est p-primaire, pour tout $i \in I$, x appartient à N_i et donc $x \in \bigcap_{i\in I} N_i$.

Définition

Une décomposition primaire $N = \bigcap_{i\in I} Q_i$ (I *fini*) *du sous-module* N *du* A*-module* M *est dite réduite si,* p_i *désignant l'unique élément de* $\mathrm{Ass}_A(M/Q_i)$, p_i *est différent de* p_j *si* $i \neq j$ *et si, pour tout* $i \in I$, $\bigcap_{j\neq i} Q_j$ *n'est pas contenu dans* Q_i.

Proposition II.7 (existence des décompositions primaires réduites)

Soient A *un anneau noethérien,* M *un* A*-module de type fini,* N *un sous-module de* M.

1. N *a (au moins) une décomposition primaire réduite*

2. Soit $N = \bigcap_{i\in I} Q_i$ *une décomposition primaire où* Q_i *est* p_i*-primaire (en sorte que* $\mathrm{Ass}_A(M/Q_i) = \{p_i\}$).

Les assertions suivantes sont équivalentes:

(i) la décomposition est réduite

(ii) Si $i \neq j$, $p_i \neq p_j$ *et* $\mathrm{Ass}(M/N) = \{p_i\}_{i\in I}$

Démonstration

1. Partant d'une décomposition primaire $N = \bigcap_{i\in I} Q_i$, on regroupe les sous-modules Q_i primaires pour le même idéal premier. On peut donc supposer $p_i \neq p_j$ si $i \neq j$.

Soient Φ l'ensemble des parties J de I telles que $\bigcap_{i\in J} Q_i = N$, J un élément de Φ ayant un nombre d'éléments *minimum*. La décomposition primaire $N = \bigcap_{i\in J} Q_i$ est réduite, car s'il existait $i \in J$ tel que Q_i contienne $\bigcap_{j\in J-\{i\}} Q_j$, l'élément $J-\{i\}$ de Φ aurait moins d'éléments que I.

2. (ii) $\Longrightarrow$ (i). L'inclusion $\bigcap_{j\neq i} Q_j \subset Q_i$ implique l'égalité $N = \bigcap_{j\neq i} Q_j$ et donc $\mathrm{Ass}_A(M/N) \subset \{p_j\}_{j\neq i}$ puisque $\mathrm{Ass}_A(M/\bigcap_{j\neq i} Q_j) \subset \bigcup_{j\neq i} \mathrm{Ass}_A(M/Q_j)$. Elle est impossible par hypothèse.

(i) $\Longrightarrow$ (ii). On sait que $\mathrm{Ass}_A(M/N)$ est contenu dans $\bigcup_{i\in I}\mathrm{Ass}_A(M/Q_i)$, i.e. $\{p_i\}_{i\in I}$.

Il faut démontrer que p_i appartient à $\mathrm{Ass}_A(M/N)$. Soit $Q_i' = \bigcap_{j\neq i} Q_j$ en sorte que $N = Q_i' \cap Q_i$ et $Q_i' \neq N$ puisque la décomposition est réduite.

De l'isomorphisme $Q_i'/N \xrightarrow{\sim} Q_i' + Q_i/Q_i$ on déduit que $\mathrm{Ass}_A(Q_i'/N)$ est contenu dans $\mathrm{Ass}(M/Q_i) = \{p_i\}$ et donc, puisque $\mathrm{Ass}_A(Q_i'/N)$ est non vide égal à $\{p_i\}$. Comme $\mathrm{Ass}_A(Q_i'/N)$ est contenu dans $\mathrm{Ass}_A(M/N)$, p_i appartient à $\mathrm{Ass}_A(M/N)$.

Etude de l'unicité des composantes primaires

Définition

Soient A un anneau noethérien, M un A-module de type fini, N un sous-module, $N = \bigcap_{i\in I} Q_i$ une décomposition primaire réduite de N, où Q_i est p_i primaire.

La composante Q_i est dite isolée (resp. immergée) si l'idéal p_i est idéal premier isolé (resp. immergé) de M/N.

On va démontrer que les composantes isolées sont déterminées de manière unique. Par contre, les composantes imérgées ne le sont pas.

Proposition II.8 (localisation des décompositions primaires réduites)

Soient A un anneau noethérien, M un A-module de type fini, $\bigcap_{i\in I} Q_i$ une décomposition primaire réduite du sous-module N de M, S une partie multiplicative de A.

Soit $J = \{i \in I / p_i \cap S = \emptyset\}$ *où* $\{p_i\} = \mathrm{Ass}_A(M/Q_i)$.

Alors, $S^{-1}N = \bigcap_{i\in J} S^{-1}Q_i$ *est une décomposition primaire réduite de* $S^{-1}N$ *(identifié à un sous-module de* $S^{-1}M$*)*

Démonstration

On sait que $S^{-1}N = \bigcap_{i\in I}(S^{-1}Q_i)$. Comme si $i \notin J$, $S^{-1}Q_i = S^{-1}M$, $S^{-1}N = \bigcap_{i\in J} S^{-1}Q_i$. Si $i \in J$, l'idéal $S^{-1}p_i$ est premier et $S^{-1}Q_i$ est $S^{-1}p_i$-primaire.

De plus, il résulte de la proposition I.4 que $\mathrm{Ass}_{S^{-1}A}(S^{-1}M/S^{-1}N) = \{S^{-1}p_i\}_{i\in J}$. La décomposition $S^{-1}N = \bigcap_{i\in J} S^{-1}Q_i$ est réduite (proposition II.7.2)

Corollaire

Les hypothèses et notations sont celles de la proposition II.8

Si Q_i est une composante isolée, $Q_i = (i_M^{p_i})^{-1}(N)$.

Les composantes isolées sont donc déterminées de manière unique.

Démonstration

Il suffit d'appliquer le résultat précédent à $S = A - p_i$, en remarquant qu'alors $J = \{i\}$.

Composantes immergées

La démonstration ci dessus n'est plus valable si la composante Q_i est immergée. Ceci signifie qu'il existe $j \in I$ tel que l'idéal premier p_j soit strictement contenu dans p_i et alors N_{p_i} n'est pas égal à $(Q_i)_{p_i}$ mais à l'intersection de $(Q_i)_{p_i}$ avec $\bigcap_{j\in I/p_j \; p_i} (Q_j)_{p_i}$.

L'exemple ci dessous montre qu'il n'y a pas forcément unicité de composantes immergées.

En fait, il n'y a *jamais* unicité des composantes immergées (exercice 15).

Exemple

Soient k *un corps,* X *et* Y *des indéterminées,* $A = k[X,Y]$, *a l'idéal* (X^2,XY).

On démontre, *pour tout élément* c *de* k, l'égalité $(X^2,XY) = (X) \cap (Y+cX,X^2)$.

L'idéal (X) est premier et donc (X)-primaire. L'idéal $(Y+cX,X^2)$ est (X,Y)-primaire.

On a donc une *décomposition primaire de a.* Elle est *réduite* car il n'y a pas de relation d'inclusion entre (X) et $(Y+cX,X^2)$. La composante (X) est isolée tandis que la composante $(Y+cX,X^2)$ est immergée. Cette composante immergée dépend de c.

4. Décomposition primaire des idéaux

Proposition II.9

Soit A *un anneau non nécéssairement noethérien.*

1. Soient p un idéal premier de type fini, q un idéal p-primaire.

Il existe $n \in N$ *tel que* $p^n \subset q \subset p$.

2. Soit p un idéal maximal. Si q est un idéal tel que $p^n \subset q \subset p$, *pour un entier naturel* n, *q est p-primaire.*

Démonstration

1. Soit $(a_1,\ldots,a_r)$ un système fini de générateurs de l'idéal p. Comme $p = r(q)$, il existe $n_i \in N$ $(i = 1,\ldots,r)$ tel que $a_i^{n_i}$ appartienne à q. Il suffit de prendre

$$n = n_1 + \ldots + n_r$$

2. Il est clair que $r(q) = p$. Soit $b \in A$. Si b n'appartient pas à p, $p^n + Ab = A$.

Il existe donc $u \in p^n$, $v \in A$ tels que $1 = u + vb$ et alors $a = au + vab$. Si ab appartient à q, il en est de même de a.

Si l'idéal premier p de A n'est pas maximal, l'idéal p^n, où n est un entier > 1, n'est pas nécessairement primaire, comme le montrent les exemples traités plus loin.

Par contre, l'idéal $p^n A_p$ de l'anneau A_p est pA_p-primaire. Il en résulte que l'idéal $(i_A^p)^{-1}(p^n A_p)$ est p-primaire.

Cet idéal est appelé la puissance symbolique n-ème de p et noté $p^{(n)}$.

(Si A est intègre, $p^{(n)} = p^n A_p \cap A$)

On verra ultérieurement que *si l'anneau A est noethérien*, on a une égalité

$$\bigcap_{n=0}^{\infty} p^n A_p = (0)$$ (théorème d'intersection de Krull) (ex. 13 du chap. 8, corollaire 2 du théorème I.4)

Par conséquent,

$$\bigcap_{n=0}^{\infty} p^n = (i_A^p)^{-1} \left(\bigcap_{n=0}^{\infty} p^n A_p\right) = (i_A^p)^{-1}(0)$$

est le saturé de l'idéal (0) *pour la partie multiplicative* $A-p$.

5. Quelques contre-exemples classiques sur les idéaux primaires.

1. *Exemple d'un idéal non primaire dont la racine est un idéal premier.*

Soient k un corps, X et Y des indéterminées, a l'idéal (X^2, XY) de $k[X,Y]$.

La racine de a est (X):

Si $f(X,Y) \in r(a)$, on a une égalité

$f(X,Y)^n = g(X,Y)X^2 + h(X,Y)XY$

Il en résulte que $f(X,Y)^n$ et donc $f(X,Y)$ est divisible par X, i.e. $f(X,Y) \in (X)$.

Réciproquement, si $f(X,Y) \in (X)$, $f(X,Y) = Xg(X,Y)$ et donc $f(X,Y)^2 \in (X^2) \subset a$.

L'idéal a n'est pas primaire car sinon il serait (X)-primaire. Or $XY \in a$, $Y \notin r(a)$ et $X \notin a$

2. Exemples d'idéaux puissances d'un idéal premier mais non primaires.

1er Exemple : *On va construire un exemple dans un anneau de polynômes à coefficients dans un corps,* à un nombre fini d'indéterminées. Un tel anneau est noethérien factoriel.

On verra au chapitre II qu'un idéal premier de hauteur 1 d'un anneau noethérien factoriel (i.e. tel qu'un idéal premier contenu dans cet idéal soit (0) ou cet idéal) est principal.

Or, il est facile de vérifier que *dans un anneau intègre une puissance d'un idéal principal premier est un idéal primaire.* D'autre part, une puissance d'un idéal maximal est un idéal primaire.

Il en résulte qu'un exemple ne peut être obtenu dans l'anneau $k[X]$ des polynômes à une indéterminée à coefficients dans le corps k (les idéaux premiers sont principaux), non plus que dans l'anneau $k[X,Y]$ des polynômes à deux indéterminées (on verra ultérieurement que les idéaux premiers sont ou principaux ou maximaux).

Soient la quintique de représentation paramétrique : $X = T^3$, $Y = T^4$, $Z = T^5$, *p l'idéal premier, noyau de l'homomorphisme:* $f(X,Y,Z) \longmapsto f(T^3,T^4,T^5)$ *de* $k[X,Y,Z]$ *dans* $k[T]$. *On va démontrer que l'idéal* p^2 *n'est pas primaire.*

On va expliciter un système de générateurs de l'idéal premier p.

On remarque que les polynômes

$f_1(X,Y,Z) = Y^2-XZ \quad f_2(X,Y,Z) = YZ-X^3 \quad f_3(X,Y,Z) = Z^2-X^2Y$

appartiennent à p.

On va démontrer qu'ils engendrent p.

A cet effet, on va trouver une forme canonique modulo l'idéal (f_1,f_2,f_3) d'un élément de $k[X,Y,Z]$. Il suffit de considérer un monôme $X^aY^bZ^c$.

Si $b > 2$, $X^aY^bZ^c = (X^aY^{b-2}Z^c)Y^2 \equiv (X^aY^{b-2}Z^c)(XZ) \equiv X^{a+1}Y^{b-2}Z^{c+1}$ modulo (f_1) soit $X^aY^bZ^c \equiv X^{a'}Y^{b'}Z^{c'}$ modulo (f_1) où $b'+c' = (b-2) + (c+1) = (b+c)-1 < b + c$.

Si $c \geqslant 2$, un calcul analogue, utilisant f_3, montre que $X^aY^bZ^c \equiv X^{a'}Y^{b'}Z^{c'}$ modulo (f_3) avec encore $b' + c' < b + c$.

Si $b \geqslant 1$ et $c \geqslant 1$, on obtient un résultat analogue en utilisant f_2.

Les seuls cas où il n'est pas possible d'appliquer l'un de ces trois procédés de réduction sont énumérés ci dessous :

$b = 1 \quad c = 0$ correspondant à un monôme X^aY

$b = 0 \quad c = 1$ correspondant à un monôme X^aZ

$b = 0 \quad c = 0$ correspondant à un monôme X^a

Ainsi un polynôme $f(X,Y,Z) \in k[X,Y,Z]$ est congru modulo (f_1,f_2,f_3) à

$$P(X)Y + Q(X)Z + R(X)$$

où $P(X)$, $Q(X)$, $R(X) \in k[X]$

Si $f(X,Y,Z) \in p$, on a

$$0 = f(T^3,T^4,T^5) = P(T^3)T^4 + Q(T^3)T^5 + R(T^3)$$

Les degrés des monômes apparaissant dans $P(T^3)T^4$, $Q(T^3)T^5$, $R(T^3)$ sont respectivement congrus modulo 3 à 1,2,0. Il n'y a donc pas de simplification possible et $P(T^3) = Q(T^3) = R(T^3) = 0$ et donc $P(X) = Q(X) = R(X) = 0$. Ainsi, f appartient à (f_1,f_2,f_3) et $p = (f_1,f_2,f_3)$.

On remarque que

$f_2^2 - f_1f_3 = X(X^5-3X^2YZ+XY^3+Z^3)$ *appartient à* p^2 *et que* X *n'appartient pas à* p. *Si* p^2 *était primaire, il serait* p*-primaire et par conséquent*

$$X^5 - 3X^2YZ + XY^3 + Z^3$$

appartiendrait à p^2. Or, c'est impossible car tous les monômes de coefficient non nul d'un élément de p^2 sont de degré au moins 4.

2ème exemple : *On peut obtenir un exemple à partir d'une courbe tracée sur une surface non factorielle,* i.e. d'algèbre affine non factorielle. Le cône d'équation $XY-Z^2 = 0$ est une telle surface. Son algèbre affine est $k[x,y,z] = A$ où $xy = z^2$. Le cône contient l'axe des Y dont l'idéal premier dans l'algèbreaffine est l'idéal premier non principal de hauteur 1, (x,z).

On remarque que $xy = z^2$ appartient à p^2 et que x n'appartient pas à p^2: en effet, une égalité

$$X = A(X,Y,Z)X^2 + B(X,Y,Z)XY + C(X,Y,Z)Z^2 + D(X,Y,Z)(XY - Z^2)$$

est impossible car, pour des raisons de degré, $XY-Z^2$ ne peut diviser $X - A(X,Y,Z)X^2 - B(X,Y,Z)XY - C(X,Y,Z)Z^2$.

D'autre part, y n'appartient pas à p car sinon p serait (x,y,z) et $k[x,y,z]/p$ serait isomorphe à k, ce qui n'est pas, puisqu'il est isomorphe à $k[X]$.

6. Anneau total des fractions d'un anneau noethérien réduit

Théorème II.10

Soient A *un anneau noethérien réduit,* $p_1,\ldots,p_n$ *les idéaux premiers minimaux de* A, A_i *l'anneau* A/p_i, K_i *le corps des fractions de* A_i $(i = 1,\ldots,n)$, K *l'anneau total des fractions de* A.

La surjection canonique $\Pi_i : A \to A_i$ *se prolonge de manière unique en un homomorphisme* ϕ_i *de* K *dans* K_i.

L'application $\phi : x \longrightarrow (\phi_1(x),\ldots,\phi_n(x))$ *est un isomorphisme d'anneaux de* K *sur* $\prod_{i=1}^{n} K_i$.

Démonstration

L'ensemble D *des diviseurs de zéro de* A *est* $\bigcup_{i=1}^{n} p_i$.

En effet, on sait que D est contenu dans $\bigcup_{i=1}^{n} p_i$, car $p_i \in \mathrm{Ass}(A)$.

Soient, d'autre part, b et c éléments de A tels que $c \neq 0$ et $bc=0$.

Comme $\bigcap_{i=1}^{n} p_i = (0)$, il existe $i \in \{1,\ldots,n\}$ tel que c n'appartienne pas à p_i et alors b appartient à p_i.

On sait donc que K est l'anneau de fractions de A associé à la partie multiplicative $S=A-\bigcup_{i=1}^{n} p_i$. C'est donc un anneau noethérien dont les idéaux maximaux sont les idéaux $p_iK (i = 1,\ldots,n)$ qui sont de hauteur 0. C'est donc un anneau artinien. *Les lignes qui suivent redémontrent dans ce cas particulier le théorème de structure des anneaux artiniens comme produits d'anneaux locaux.*

Il est clair que Π_i se prolonge de manière unique en un homomorphisme ϕ_i de K dans K_i défini par $\phi_i(a/s) = \Pi_i(a)/\Pi_i(s)$.

Cet homomorphisme est surjectif, i.e. $\Pi_i(S) = A_i - \{0\}$: soit, en effet, $\overline{x}$ un élément non nul de A_i. Si x' est un représentant de $\overline{x}$, soit $I = \{j \in 1,\ldots,n / x' \notin p_j\}$. Si $I = \{1,\ldots,n\}$, x' appartient à S. Sinon, soit x'' dans $\bigcup_{j\in I} p_j$ et non dans $\bigcup_{j\notin I} p_j$. Alors, si $x = x'+x''$, x appartient à S et $\Pi_i(x) = \overline{x}$. L'homomorphisme ϕ_i de $K = S^{-1}A$ dans $K_i = \Pi_i(S)^{-1}A_i$ a pour noyau $S^{-1}p_i$, i.e. p_iK. Il induit donc un isomorphisme $\overline{\phi}_i : K/p_iK \to K_i$.

D'autre part, on sait que les idéaux p_iK sont les idéaux maximaux de K.

L'application naturelle $\psi : K \longrightarrow \prod_{i=1}^{n} K/p_iK$ est donc *surjective*. Son noyau est (0) car il est $\bigcap_{i=1}^{n} p_iK$, c'est à dire, par platitude de K sur A, $(\bigcap_{i=1}^{n} p_i)K$. Donc ψ est surjective. C'est donc un isomorphisme d'anneaux. Il en est de même de ϕ qui s'en déduit au moyen des isomorphismes $\overline{\phi}_i$.

III. Support, idéaux premiers associés et changement d'anneaux

Cette partie assez technique peut être laissée en première lecture.

1. Support et changement d'anneaux

Proposition III.1

Soient $\phi : A \longrightarrow B$ *un homomorphisme d'anneaux*, M *un* A*-module.*

1. Alors $\mathrm{Supp}_B(M \otimes_A B)$ *est contenu dans* $\mathrm{Spec}(\phi)^{-1}(\mathrm{Supp}_A(M))$

2. Si le A*-module* M *est de type fini,* $\mathrm{Supp}_B(M \otimes_A B) = \mathrm{Spec}(\phi)^{-1}(\mathrm{Supp}_A(M))$

Démonstration

1. Soient $q = \mathrm{Supp}(M \otimes_A B)$, $p = \mathrm{Spec}(\phi)(q) = \phi^{-1}(q)$. Comme $(M \otimes_A B)_q$ est non nul, il en est de même de $M \otimes_A A_p = M_p$: en effet, $(M \otimes_A B)_q \simeq M \otimes_A B \otimes_B B_q \simeq M \otimes_A B_q \simeq M \otimes_A A_p \otimes_{A_p} B_q \simeq (M \otimes_A A_p) \otimes_{A_p} B_q$.

Donc, p appartient à Supp(M) et q appartient à $\mathrm{Spec}(\phi)^{-1}(\mathrm{Supp}_A(M))$.

2. Soit $q \in \mathrm{Spec}(\phi)^{-1}(\mathrm{Supp}_A(M))$, en sorte que si $p = \phi^{-1}(q)$, M_p est non nul.

On doit démonstrer que, *si* M *est de type fini* $(M \otimes_A B)_q$ est non nul, i.e. que $M \otimes_A B_q$ est non nul.

Remplaçant A *par* A_p, B *par* B_q *et* ϕ *par l'homomophisme de* A_p *dans* B_q *défini par* ϕ, *on se ramène à la démonstration du résultat suivant :*

Soient A *et* B *des anneaux locaux,* ϕ *un homomorphisme local de* A *dans* B, M *un* A*-module de type fini.*

Les assertions suivantes sont équivalentes :

(i) $M \simeq (0)$

(ii) $M \otimes_A B = (0)$

Il est clair que (i) implique (ii).

On démontre que (non i) implique (non ii). Soient k(A) et k(B) les corps résiduels respectifs de A et B. Le k(A)-espace vectoriel $k(A) \otimes_A M$ est non nul (lemme de Nakayama). Le k(B)-espace vectoriel $k(B) \otimes_B (B \otimes_A M)$ est non nul car il est isomorphe à $k(B) \otimes_{k(A)} (k(A) \otimes_A M)$. Il en est de même, a fortiori, de $M \otimes_A B$.

2. Idéaux premiers associés et changement d'anneaux

La proposition ci dessous sera utilisée dans le chapitre 13 (théorème II.5). Elle est un cas particulier de ((3) chap. 4 §2 n°6 th.2). On commence par un lemme.

Lemme

Soient A *et* B *des anneaux noethériens,* $f : A \longrightarrow B$ *un homomorphisme plat,* p *un idéal premier de* A, E *un* A*-module dont l'annulateur*

contient une puissance de p et tel que $\mathrm{Ass}(E) = \{p\}$.

Si $q \in \mathrm{Ass}_B(E \otimes_A B)$, $f^{-1}(q) = p$.

Démonstration

De $p^n E = 0$, on déduit que $p^n B$ est contenu dans $\mathrm{Ann}(B \otimes_A E)$. Donc, $p^n B \subset q$, d'où $p^n \subset f^{-1}(q)$ et, puisque $f^{-1}(q)$ est premier, $p \subset f^{-1}(q)$.

D'autre part, si $a \in A-p$, l'homothétie δ_a^E est injective. Par platitude de f, l'homothétie $\delta_{f(a)}^{B \otimes_A E}$ est injective. Donc, f(a) n'appartient pas à q.

Il en résulte $p = f^{-1}(q)$

Proposition III.2

Soient A *et* B *des anneaux noethériens,* $f: A \longrightarrow B$ *un homomorphisme plat, a un idéal de* A.

Alors, $\mathrm{Ass}_B(B/aB) = \bigcup_{p \in \mathrm{Ass}_A(A/a)} \mathrm{Ass}_B(B/pB)$

Démonstration

Soit $a = \bigcap_{i=1}^{r} q_i$ une décomposition primaire réduite de a, où l'idéal q_i est p_i-primaire. Le A-module A/a s'identifie à un sous-module du A-module $\bigoplus_{i=1}^{r} A/q_i$. Par platitude de B, B/aB s'identifie à un sous-module du B-module $\bigoplus_{i=1}^{r} B/q_i B$.

Il en résulte $\mathrm{Ass}_B(B/aB) \subset \bigcup_{i=1}^{r} \mathrm{Ass}_B(B/q_i B)$.

On va démontrer l'égalité $\mathrm{Ass}_B(B/q_i B) = \mathrm{Ass}_B(B/p_i B)$ $(i = 1,\ldots,r)$.

Comme $\mathrm{Ass}_B(B/p_i B)$ est contenu dans $\mathrm{Ass}_B(B/aB)$ puisque, de la suite exacte $0 \longrightarrow A/p_i \longrightarrow A/a$, se déduit par platitude la suite exacte $0 \longrightarrow B/p_i B \longrightarrow B/aB$, il en résultera l'inclusion $\bigcup_{i=r}^{r} \mathrm{Ass}_B(B/p_i B)$ $\mathrm{Ass}_B(B/aB)$ et donc l'égalité cherchée.

Il existe une puissance de p_i qui annule le A-module A/q_i. Il résulte du lemme que si $q \in \mathrm{Ass}_B(B/q_i B)$, $f^{-1}(q) = p_i$.

On a, d'autre part, une suite de composition

$$E_o = A/q_i \supset E_1 \supset \ldots \supset E_n = (0)$$

de A-modules où E_i/E_{i+1} est de la forme A/p_j' pour un idéal premier p_j' appartenant au support de A/q_i, qui est $V(p_i)$. Donc, $p_j' \supset p_i$.

On en déduit, par platitude, une suite de composition

$$B \otimes_A E_o = B/q_i B \supset B \otimes_A E_1 \supset \ldots \supset B \otimes_A E_n = (0)$$

avec $(B \otimes_A E_i)/(B \otimes_A E_{i+1}) = B/p_j' B$.

Alors, $\mathrm{Ass}_B(B/q_i B)$ est contenu dans $\bigcup_{i=0}^{n-1} \mathrm{Ass}_B(B/p_j' B)$.

Si $q' \in \mathrm{Ass}_B(B/p'_jB)$, il résulte du lemme appliqué au A-module A/p'_j que $f^{-1}(q') = p'_j$.

Ainsi, $\mathrm{Ass}_B(B/q_iB) \cap \mathrm{Ass}_B(B/p'_jB) = \emptyset$ si $p'_j \neq p_i$.

Donc, $\mathrm{Ass}_B(B/q_iB) = \mathrm{Ass}_B(B/p_iB)$

Exercices sur le chapitre 3

(1) Soit A un anneau *intègre*. Quel est $\mathrm{Ass}_A(A)$? Quelle est la décomposition primaire de (0) dans A ?

(2) Soient A un anneau, L un A-module libre. Comparer $\mathrm{Ass}_A(A)$ et $\mathrm{Ass}_A(L)$.

(3) Soient A un anneau, somme directe de deux idéaux a et b. Comparer $\mathrm{Ass}_A(A)$ et $\mathrm{Ass}_A(a) \cup \mathrm{Ass}_A(b)$.

Soient $A_1,\ldots,A_n$ des anneaux intègres. Calculer $\mathrm{Ass}_{A_1\times\ldots\times A_n}(A_1\times\ldots\times A_n)$

(4) Soit A un anneau noethérien intègre dont tout idéal premier non nul est maximal. Un idéal de A a-t-il des composante immergées ?

Donner des exemples de tels anneaux.

(5) Soient k un corps, X,Y,Z des indéterminées.

L'idéal (X^2,Y^3,Z^5) de $k[X,Y,Z]$ est-il primaire ?

(6) Soient k un corps, X et Y des indéterminées.

Quelle est la décomposition primaire de l'idéal (X^2+Y^2) dans le cas $k = \mathbb{R}$? $k = \mathbb{C}$? $k = \mathbb{F}_2$ corps à deux éléments.

(7) Soient A un anneau, M un A-module.

Démontrer que l'homomorphisme naturel de M dans $\prod_{p\in\mathrm{Ass}_A(M)} M_p$ est injectif.

(Utiliser le fait que si $x \in M$ est non nul, il existe $p \in \mathrm{Ass}_A(M)$ contenant $\mathrm{Ann}(x)$).

(8) *Anneaux absolument plats*

1. Soient A un anneau, $a \in A$.

Démontrer les équivalences: (i) il existe $x \in A$ tel que $a = a^2x$

(ii) l'idéal (a) est facteur direct de A

(iii) le A-module A/(a) est plat

(iv) pour tout idéal b de A, $(a)\cap b = ab$

((i) $\Longrightarrow$ (ii): remarquer que ax est un idempotent qui engendre (a);

(iii) $\Longrightarrow$ (iv): tensoriser par A/(a) la suite exacte

$0 \longrightarrow b \longrightarrow A \longrightarrow A/b \longrightarrow 0$;

(iv) $\Longrightarrow$ (i) appliquer à $b = (a)$)

2. Soit A un anneau tel que, pour tout $a \in A$, les conditions équivalentes ci dessus soient vérifiées. Démontrer que tout idéal de type fini A est principal facteur direct de A. Réciproque ?

(remarquer que si e et f sont deux idempotents, $(e,f) = (e+f - ef)$

3. Démontrer les équivalences pour l'anneau A:

(i) tout idéal de type fini de A est facteur direct de A

(ii) tout A- module est plat

(Utiliser le fait qu'une limite inductive filtrante de A-modules plats est un module plat pour démontrer que (ii) est équivalent à (ii'): pour tout idéal *de type fini* a de A, le A-module A/(a) est plat)

En déduire les équivalences des définitions d'un anneau absolument plat données dans le chapitre 2 (II.§5) et chapitre 3(I.§1).

4. Démontrer que tout idéal premier d'un anneau absolument plat est maximal.

Si m est un idéal maximal d'un anneau absolument plat A, comparer A_m et A/m.

Quels sont les anneaux absolument plats noethériens ?

(9) *Idéaux premiers de* k^N

Soit E un ensemble. On rappelle qu'un *filtre* sur E est un ensemble $\mathfrak{F}$ de parties de E, stable par intersection finie, stable par inclusion de $\mathfrak{F}$ et ne contenant pas $\emptyset$. Un *ultrafiltre* est un filtre maximal pour la relation d'ordre fournie par l'inclusion dans l'ensemble des ensembles de parties de E: *être plus fin que*. L'ensemble des parties contenant un élément de E est un ultrafiltre, appelé *ultrafiltre trivial*. On démontre, au moyen du théorème de Zorn, que, pour tout filtre $\mathfrak{F}$, il existe un (au moins) ultrafiltre plus fin que $\mathfrak{F}$. On peut aussi caractériser un ultrafiltre $\mathfrak{U}$ comme un filtre satisfaisant à l'une des propriétés équivalentes suivantes: (i) $A,B \subset E$, $A \cup B \in \mathfrak{U} \Rightarrow$ A ou B $\in \mathfrak{U}$

(ii) A E, A ou CA $\in \mathfrak{U}$

Dans N, le complémentaire des parties finies est un filtre, appelé *filtre de* Fréchet. On démontre que tout ultrafiltre non trivial de N est plus fin que le filtre de Fréchet.

Soient k un corps, A l'anneau k^N. On appelle Cossup (x), où $x = (x_n)_{n \in N}$, le sous-ensemble $\{n \in N / x_n = 0\}$.

Démontrer que, si a est un idéal de A *distinct de* A, l'ensemble $\{\text{Cossup } (x)/x \in a\}$ de parties de N est un filtre de N, et que ce filtre

est un ultrafiltre si et seulement si l'idéal a est premier. Réciproquement, si $\mathcal{U}$ est un ultrafiltre sur N, $\{x \in A / \mathrm{Cossup}(x) \in \mathcal{U}\}$ est un idéal premier de A.

Démontrer, sans utiliser le théorème de Cohen, l'existence dans A d'idéaux premiers qui ne sont pas de type fini. A quels utrafiltres de N correspondent les idéaux premiers de *type fini* de A ?

(10) L'exercice suivant est tiré de: E. Graham Evans, *Zero Divisors in noetherian-like Rings. Trans. Amer. Math. Soc., 155, n°2, p.505-512.*(*)

1. Soient A un anneau, S une partie multiplicative de A *formée d'éléments réguliers*, M un A-module. On rappelle que D(M) est l'ensemble des diviseurs de zéro de M.

Démontrer: 1. $D((i_A^S)_*(S^{-1}M)) = D(M)$

2. $D(S^{-1}M) = D(M)(S^{-1}A)$ (produit d'un élément de D(M) et d'un élément de $S^{-1}A$)

3. Si $D(S^{-1}M) = P_1 \cup \ldots \cup P_n$ où P_i est un idéal premier de $S^{-1}A$, $D(M) = p_1 \cup \ldots \cup p_n$ où $p_i = (i_A^S)^{-1}(P_i)$

On dit que le A-module M (resp. l'anneau A) est d'Evans *si* D(M) *est une réunion d'un nombre fini d'idéaux premiers* (resp. *si le A-module A est* d'Evans).

2. Démontrer: 1. Si le A-module M est d'Evans, pour toute partie multiplicative S, le $S^{-1}A$-module $S^{-1}M$ est d'Evans.

2. Soit $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ une suite exacte de Mod(A).

Les assertions suivantes sont équivalentes:

(i) M est d'Evans

(ii) M' et M" sont d'Evans

Déduire de 2. que si l'anneau A est d'Evans, tout A-module de type fini est d'Evans. Démontrer que s'il existe un A-module d'Evans *de type fini et fidèle*, l'anneau A est d'Evans.

Un anneau A est dit laskérien si tout idéal de A, distinct de A, est intersection d'un nombre fini d'idéaux primaires. (Un anneau noethérien est donc laskérien).

3. Démontrer qu'un anneau laskérien est d'Evans.

Une famille $(x_i)_{i \in I}$ *d'éléments d'un A-module M est dit faiblement indépendante si,* $\forall\, i \in I$, x_i *n'appartient pas au sous-module engendré*

par $(x_j)_{j\in I-\{i\}}$, *fortement indépendante si,* $\forall i \in I$, $x_i \neq 0$, *et si* ax_i *appartient au sous-module engendré par* $(x_j)_{j\in I-\{i\}}$ (où $a \in A$), *alors* $ax_i = 0$

4. Soient A un anneau *non noethérien*, $(a_1) \subset (a_1,a_2) \subset \ldots$ une suite *infinie* strictement croissante d'idéaux de A (où $a_i \in A$).

Démontrer: α. Soit X une indéterminée. La famille $(a_nX^n)_{n\ N^*}$ d'éléments de $A[X]$ est faiblement indépendante.

β. Soit I l'idéal engendré par les éléments ba_nX^n (où $b \in A$) qui appartiennent à l'idéal $(a_mX^m)_{m\in N^*-\{n\}}$. Soit $B = A[X]/I$, p la surjection de $A[X]$ sur B. Démontrer que la famille $(p(a_nX^n))_{n\in N}$ est fortement indépendante dans B.

5. Soient B un anneau, $(x_i)_{i\in I}$ une famille infinie fortement indépendante de B, $a_i = \mathrm{Ann}(x_i)$, m_i un idéal maximal de B contenant a_i, Y une indéterminée, M_i un idéal maximal de $B[Y]$ tel que $m_i = M_i \cap B$, I, l'idéal engendré par $\bigcup_{j\in J} r_jM_j$.

Démontrer $D(B/I) \supset \bigcup_{j\in J} M_j/I$. En déduire que $B[Y]$ n'est pas un anneau d'Evans.

On suppose l'anneau $A[X,Y]$ d'Evans. Que peut-on dire de l'anneau A?

(11) Soient A un anneau, a un idéal de A distinct de A, b un idéal de *type fini* de A. Démontrer les équivalences:

(i) il existe $a \in a$ tel que $(1-a)b = (0)$

(ii) $b \subset ab$

(Appliquer la méthode du déterminant de Krull. Chap.4 Théorème I.3)

(12) Soient A un anneau *noethérien*, a et b des idéaux de A distincts de A.

Soit $ab = \bigcap q_i \cap \bigcap q'_j$ une décomposition primaire réduite de l'idéal ab, où q_i est primaire pour un idéal premier p_i contenant a, q'_j est primaire pour un idéal premier p'_j ne contenant pas a.

Démontrer l'inclusion $b \subset q'_j$.

On pose $a' = \bigcap q_i$, $b_1 = \bigcap q'_j$. Démontrer l'inclusion $b \subset b_1$. En déduire l'égalité $ab = a' \cap b$. Démontrer l'existence d'un entier naturel r tel que $a' \subset a^r$.

(*) Nous n'avons pas gardé la terminologie, peu satisfaisante nous semble-t-il, de l'auteur de l'article.

(13) Soient A un anneau noethérien, a un idéal de A distinct de A.

On pose $b = \bigcap_{n=0}^{\infty} a^n$. On remarque $b \cap a^n = b$ pour tout n N.

Démontrer l'existence d'un idéal a', d'un entier naturel r tel que $a' \subset a^r$ et $a \cdot b = a' \cap b$

En déduire l'inclusion $b \subset ab$.

Démontrer que si A *est intègre ou si* a *est contenu dans le radical de* A, $b = (0)$.

(théorème d'intersection de Krull.

Ce théorème sera déduit d'un résultat plus général dans le chapitre 8. Corollaire 2 et 3 du tnéorème I.4.)

(14) Soient A un anneau *noethérien*, p un idéal *premier* de A.

Démontrer l'égalité $\bigcap_{n \in N} p^{(n)} = (0)$.

Que peut-on dire de l'intersection de l'ensemble des idéaux p-primaires ?

(15) Soient A un anneau *noethérien*, p et q des idéaux *premiers* de A, p contenant q *strictement*, b un idéal p-primaire, c un idéal q-primaire.

1. On suppose $b \cap c = (0)$ (exemple: $A = k[X,Y]/(X^2,XY)$ où k est un corps, $p = (X,Y)/(X^2,XY)$, $q = (X)/(X^2,XY)$, $b = (Y+X,X^2)/(X^2,XY)$, $c = q$).

Démontrer l'existence d'un idéal p-primaire b'' ne contenant pas b. (Utiliser le fait que b n'est pas contenu dans q et donc est non nul et le fait que l'intersection des idéaux p-primaires est (0))

En déduire l'existence d'un idéal p-primaire b' *strictement contenu dans* b.

2. En déduire dans le cas général (i.e. $b \cap c$ éventuellement $\neq (0)$) l'existence d'un idéal p-primaire b' strictement contenu dans b tel que $b' \cap c = b \cap c$.

3. Démontrer que si l'idéal a de A a une composante immergée, il existe une infinité de décompositions primaires réduites de a ne différant que par la composante immergée.

(16) Soient A un anneau noethérien, p un idéal premier A, q un idéal p-primaire.

1. Démontrer que la longueur n d'une suite strictement croissante

(1) $q_0 = q \subset q_1 \subset \ldots \subset q_n = p$ d'idéaux p-primaires d'origine q et d'extrémité p est majorée. La borne supérieure de ces longueurs est appelée la longueur de l'idéal primaire q. Démontrer l'existence d'une

suite (1) de longueur égale à la longueur de q. (Considérer l'anneau quotient A_p/qA_p)

2. Une suite (1) peut-elle être complétée en une suite strictement croissante d'idéaux p-primaires de longueur la longueur de q ?

(17) Soient A un anneau noethérien, a un idéal de A distinct de A et sans composantes immergées, $S = A - \bigcup_{p \in \mathrm{Ass}_A(A/a)} p$

Démontrer que l'anneau $S^{-1}A/S^{-1}a$ est de longueur finie.

La longueur de cet anneau est appelée la longueur de l'idéal a et noté $\lambda(a)$.

Démontrer que si $a = \bigcap_i q_i$ est une décomposition primaire réduite de a, $\lambda(a)$est égal à $\Sigma_i \lambda(q_i)$.

Démontrer que si a est un idéal primaire, $\lambda(a)$ est la longueur de a définie dans l'exercice 16.

(18) Cet exercice est tiré de l'article suivant :

W.Heinzer-J.Ohm. *Locally noetherian commutative Rings. Trans. Amer. Math. Soc., 158, n°2, p. 273-284.*

1. Soit $T_n (n \in N)$ une suite d'ensembles finis éventuellement vides.

On suppose que $T = \bigcup_{n \in N} T_n$ est muni d'une relation d'ordre partiel $\leqslant$, satisfait à la condition de chaîne croissante et que, pour tout $n \in N$, tout élément de T_{n+1} majore *strictement* un élément de T_n.

Démontrer qu'il existe $n_0 \in N$ tel que, pour tout $n \geqslant n_0$, T_n soit vide.

2. Soit p un idéal premier d'un anneau A. Démontrer les équivalences:

(i) p est de type fini

(ii) 1. pour tout idéal premier q de A contenant p, pA_q est de type fini

2. il existe un idéal de type fini b_o de A tel que $r(b_o) = p$ et que pour tout idéal b de type fini tel que $b_o \subset b \subset p$, $\mathrm{Ass}_A(A/b)$ soit fini.

3. l'ensemble $\bigcup_b \mathrm{Ass}_A(A/b)$ (où b parcourt l'ensemble des idéaux définis dans 2.) satisfait à la condition de chaîne croissante.

(*Définir par induction une suite* (a_n) *d'idéaux de type fini de* A *contenant* b_0 *telle que la suite* $T_n = \mathrm{Ass}_A(A/a_n) - \{p\}$ *satisfasse aux conditions de la question 1., en partant de* a_0 *engendré par* b_0 *et un nombre fini d'é-*

léments de A *dont les images dans* A_p *engendrent* pA_p.

Démontrer que, avec la notation de la question 1., $p = a_{n_0}$)

3. Démontrer que les assertions suivantes sont équivalentes pour un anneau A:

(i) A est noethérien

(ii) pour tout idéal premier p de A, l'anneau A_p est noethérien et, pour tout idéal a de type fini de A, $\mathrm{Ass}_A(A/a)$ est *fini.*

(Pour l'implication (ii) $\Longrightarrow$ *(i), démontrer l'existence pour un idéal premier* p *de* A *d'un idéal de type fini* b_o *tel que* $r(b_o) = p$.

A cet effet, définir par induction une suite (a_n)*croissante d'idéaux de* A *contenus dans* p *telle que la suite d'ensembles* $\mathrm{Isol}(A/a_n)-\{p\}$ *satisfasse aux conditions de la question 1.*(Isol(M) est l'ensemble des idéaux premiers isolés de (0) dans M) *et appliquer les résultats de cette question. En déduire que l'idéal premier* p *est de type fini. Conclure avec le théorème II.2 du chapitre 2).*

(19) L'exercice suivant est extrait de l'article: H. Bass. *Descending chains and the* Krull *ordinal of commutative Rings. Journal of pure and applied Algebra.* Vol. 1. n°4, 1971, 347-360.

On se propose de démontrer l'assertion suivante :

(P). *Soient* A *un anneau noethérien,* M *un* A*-module de type fini.*

Tout ensemble totalement ordonné de sous-modules M *est dénombrable.*

1. Démontrer que l'on peut se limiter à l'examen du cas M = A (prop.II.1)

On raisonne par l'absurde supposant que A *ne vérifie pas* (P).

Démontrer alors qu'en remplaçant A par un quotient convenable on peut supposer en outre que, pour tout idéal *non nul* a de A, A/a vérifie (P).

On désigne alors par C *un ensemble totalement ordonné non dénombrable d'idéaux non nuls.*

Démontrer que $\bigcap_{a\in C} a = (0)$ mais qu'il n'existe pas de suite infinie $(a_n)_{n\in N^*}$ d'éléments de C telle que $\bigcap_{n\in N^*} a_n = (0)$.

On note $\mathrm{Min}(C)$ *l'ensemble des éléments minimaux de* $\bigcup_{a\in C} \mathrm{Ass}_A(A/a)$. *(On admettra ici le fait que* $\mathrm{Min}(C)$ *est non vide.* Ceci résulte du fait que les idéaux premiers d'un anneau noethérien satisfont à la condition de chaîne descendante et donc à la condition minimale (confer. chap.10. Dimension et multiplicité))

2. Démontrer les équivalences pour $p \in \mathrm{Spec}(A)$:

(i) $p \in \mathrm{Min}(C)$

(ii) Il existe $b \in C$ tel que $a \in C$ et $a \subset b \Longrightarrow p \in \mathrm{Ass}_A(A/a)$

Supposer qu'il existe dans $\mathrm{Min}(C)$ une suite infinie $(p_n)_{n \in N^*}$ où $p_n \in \mathrm{Ass}_A(A/a_n)$ pour l'élément a_n de C.

Démontrer qu'il existe alors un idéal $b \in C$ (contenu dans $\bigcap_{n \in N^*} a_n$) tel que

$$\mathrm{Ass}_A(A/b) = \{p_n\}_{n \in N^*}$$

En déduire que $\mathrm{Min}(C)$ est *fini*.

Soit $a \in C$. On écrit $a = a' \cap a''$ où a' est l'intersection des composantes primaires associées à des éléments de $\mathrm{Min}(C)$, a'' est l'intersection des composantes primaires associées à des idéaux premiers n'appartenant pas à $\mathrm{Min}(C)$.

3. Démontrer (par récurrence transfinie) qu'il est possible de supposer l'application $a \longmapsto a''$ croissante. (Remplacer a'' par $\bigcap_{b \in C} b''$ où $a \subset b$).

4. Démontrer l'existence de $b \in C$ tel que, pour tout $a \in C$ contenu dans b, $a' = b'$.

(Considérer l'anneau B des fractions de A par rapport à la partie multiplicative $A - \bigcup_{p \in \mathrm{Min}(C)} p$. Utiliser le fait que, pour $a \in C$, $\mathrm{long}(B/aB)$ est finie pour démontrer l'existence d'une suite $(a_n)_{n \in N^*}$ d'éléments de C telle que la suite $(a_n N)_{n \in N}$ soit cofinale (pour la relation opposée à l'inclusion) à l'ensemble ordonné $(aB)_{a \in C}$.

En déduire que, pour tout $a \in C$ contenu dans tout a_n, a' ne dépend pas de a).

Soit C_1 l'ensemble totalement ordonné non dénombrable = $\{a \in C / a' = b'\}$ (avec les notation de 4.). *On pose $D(C) = \{a'' / a \in C_1\}$.*

5. Démontrer que tout élément de $\mathrm{Min}(D(C))$ contient *strictement* un élément de $\mathrm{Min}(C)$.

Construire une suite *infinie strictement croissante* d'idéaux premiers de A contredisant la noethérianité de A.

(20) Cet exercice propose l'extension aux anneaux et modules gradués des résultats concernant les idéaux premiers fortement associés, et la décomposition primaire, extension utile en géométrie algébrique projective.

Soient $A = \bigoplus_{n \in N} A_n$ un anneau gradué, $M = \bigoplus_{n \in N} M_n$ un A-module gradué.

1. Soient p un idéal premier fortement associé à M, x un élément de M

tel que $p = \mathrm{Ann}(x)$, $x_{i_1},\ldots,x_{i_r}$ avec $i_1 < \ldots < i_r$ les composantes homogènes non nulles de x.

Démontrer que l'idéal p est homogène.

(Soient $a = \Sigma a_n$, où $a_n \in A_n$, un élément de p, m le plus grand indice tel que a_m soit non nul. Calculant les composantes homogènes de ax, démontrer que a_m^r appartient à p).

Démontrer qu'il existe $j \in \{1,\ldots,r\}$ tel que $p = \mathrm{Ann}(x_{i_j})$

(Remarquer que $\bigcap_{n=1}^{r} \mathrm{Ann}(x_{i_j})$ est contenu dans $\mathrm{Ann}(x)$).

2. Soit p un idéal premier associé à M.

Démontrer que le plus grand idéal homogène p' contenu dans p est premier.

Démontrer que si un idéal premier contient l'annulateur d'un élément x de M, il contient aussi l'annulateur d'une au moins des composantes homogènes non nulles de x.

En déduire que l'idéal p est homogène et est idéal premier minimal de l'ensemble des idéaux premiers contenant l'annulateur d'un élément homogène de M.

3. *On suppose* A *noethérien.*

Soient p un idéal premier, N un sous-module de M, p' le plus grand idéal homogène contenu dans p (premier en vertu de 2.), N' le plus grand sous-module de N.

Démontrer que le sous-module N' de N est p'-primaire.

En déduire que si, N est sous-module homogène de M, admettant une décomposition primaire, N admet une décomposition primaire ne faisant intervenir que des sous-modules primaires homogènes.

(21) *On se propose dans cet exercice l'étude, dans le cas de modules monogènes, des idéaux premiers associés à partir de la décomposition primaire.*

Soient A un anneau noethérien, a un idéal de A distinct de A, $a = q_1 \cap \ldots \cap q_r$ une décomposition primaire réduite de a (dont l'existence est démontrée dans la proposition II.7), p_i l'idéal premier $r(q_i)$ $(i = 1,\ldots,r)$

1. Soit $a = q_1' \cap \ldots \cap q_s'$ une autre décomposition primaire réduite de a avec $p_i' = r(q_r')$.

Soient $p = p_m$ où, après renumérotation éventuelle, $p_i \subset p$ pour

$i = 1,\dots,m$, $p_i \not\subset p$ pour $i \geqslant m+1$, $p'_j \subset p$ pour $j = 1,\dots,n$, $p'_j \not\subset p$ pour $j \geqslant n+1$, $S = A-p$, $\overline{a}$ le saturé $(i_A^S)^{-1}(S^{-1}a)$ de a pour S.

Démontrer les égalités

$$a = q_1 \cap \dots \cap q_m = q'_1 \cap \dots \cap q'_n$$

Supposer $p \notin \{p'_1 \dots p'_n\}$. Justifier l'existence de $a \in p$ n'appartenant pas à $p_1 \cap \dots \cap p_{m-1} \cap p'_1 \cap \dots \cap p'_n$. Soit $u \in N^*$ tel que a^u appartienne à q_m.

Démontrer l'égalité

$$(\overline{a} : a^u) = q_1 \cap \dots \cap q_{m-1}$$

En déduire l'inclusion $q_1 \cap \dots \cap q_{m-1} \subset q_m$, contredisant le fait que la décomposition primaire $q_1 \cap \dots \cap q_r$ de a est réduite

En déduire l'égalité $r = s$ et l'égalité $\{p_1,\dots,p_r\} = \{p'_1,\dots,p'_s\}$.

Les idéaux $p_1,\dots,p_r$ sont dits associés au A-module A/a (ou à l'idéal a)

2. Démontrer les équivalences pour un idéal premier p de A:

(i) p est associé à a

(ii) il existe $\overline{x} \in A/a$ tel que $p = \mathrm{Ann}(\overline{x})$

(iii) il existe $x \in A$ tel que $p = (a : x)$

(Démontrer d'abord l'équivalence facile: (ii) $\Longleftrightarrow$ (iii).

(iii) $\Longrightarrow$ (i). Démontrer l'existence de $i \in \{1,\dots,r\}$ tel que $(a : x) = (q_i : x)$ et $(a : x) = p_i$.

(i) $\Longrightarrow$ (iii). Démontrer que l'idéal $q_1 \cap \dots \cap q_{m-1} \cap (q_m : p) \cap q_{m+1} \cap \dots \cap q_r$ contient strictement $a = q_1 \cap \dots \cap q_r$. Prendre x appartenant à cet idéal mais n'appartenant pas à a et démontrer l'égalité $(a : x) = p$).

(22) Traiter l'analogue de l'exercice 21 pour un sous-module N d'un A-module noethérien M.

CHAPITRE 4

Extensions d'anneaux
Dépendance algébrique et intégrale

Une des origines de la notion d'entier algébrique, exposée dans ce chapitre, est la conjecture célèbre de P. de Fermat que, *pour tout entier* $n > 2$, *l'équation diophantienne*: $x^n + y^n = z^n$ *n'a pas de solution* (x,y,z) *en nombres entiers (ou rationnels) telle que* xyz *soit non nul.*

Pour $n = 2$, cette équation a, par contre, une infinité de solutions et on en obtient la représentation paramétrique par des propriétés élémentaires de divisibilité dans $\mathbb{Z}$. Voici l'idée de la méthode. On écrit l'équation sous la forme $(z-x)(z+x) = y^2$; on peut se limiter à la recherche de solutions (x,y,z) où x,y,z sont premiers entre eux deux à deux; quitte à échanger x et y, on peut supposer alors x impair, y pair, z impair; posant $y = 2y'$, $z+x = 2x'$, $z-x = 2z'$, on remarque que $x' = u^2$, $z' = v^2$, où u et v sont des entiers. On en déduit la représentation paramétrique des solutions:

$$x = d(u^2-v^2) \quad y = 2duv \quad z = d(u^2+v^2)$$

Le succès de la méthode provient, en fait, *de la possibilité de décomposer dans l'anneau* $\mathbb{Z}[X,Z]$ *des polynômes le polynôme* Z^2-X^2 *en le produit* $(Z-X)(Z+X)$ *de deux facteurs du premier degré.*

Si $n > 2$, le polynôme Z^n-X^n ne se décompose plus en facteurs du premier degré dans $\mathbb{Z}[X,Z]$ mais une telle décomposition a lieu dans l'anneau $\mathbb{Z}[\zeta][X,Z]$, où ζ est une racine primitive n-ème de l'unité, sous la forme $Z^n-X^n = \prod_{i=0}^{n-1}(Z-\zeta^i X)$.

On peut démontrer que tout élément de $A = \mathbb{Z}[\zeta]$ est racine d'un polynôme à coefficients entiers *unitaire*, i.e. dont le coefficient du terme de plus haut degré est égal à 1: par exemple, ζ est racine de X^n-1.

On peut même démontrer que A est le sous-ensemble du corps $\mathbb{Q}(\zeta) = \{\sum_{i=0}^{n-1} a_i\zeta^i / a_i \in \mathbb{Q}\}$ des éléments de $\mathbb{Q}(\zeta)$ racines de tels polynômes. (Ceci est proposé en exercice dans le chapitre 5 dans le cas où n est un nombre premier mais est vrai en toute généralité).

L'idée de Kummer et, peut-être, de Fermat fut de remplacer l'anneau $\mathbb{Z}$, suffisant pour résoudre le problème dans le cas $n = 2$, par l'anneau $A = \mathbb{Z}[\zeta]$ et de démontrer l'inexistence de solutions (x,y,z) avec xyz non nul non seulement dans $\mathbb{Z}$ mais aussi dans A.(*)

(*) L'échec de la méthode tient, en premier lieu, au fait que l'anneau A n'est pas toujours factoriel (le plus petit nombre premier n pour lequel

La théorie générale des entiers algébriques se présente comme suit:

Soit A *un sous-anneau d'un anneau* B.

Un élément de B est dit *entier* (algébrique) *sur* A s'il est racine d'un polynôme *unitaire* à coefficients dans A. On démontre que l'ensemble des éléments de B entiers sur A est un sous-anneau de B contenant A, appelé *fermeture intégrale* de A dans B.

Certains anneaux, obtenus par ce procédé, apparaissent donc naturellement en *théorie algébrique des nombres*, d'autres en *géométrie algébrique*. Les indications qui suivent seront précisés dans d'autres chapitres.

Un *corps de nombres algébriques* (de degré fini) est un sous-corps de $\mathbb{C}$ de dimension finie en tant que $\mathbb{Q}$-espace vectoriel. La fermeture intégrale de $\mathbb{Z}$ dans un tel corps est *l'anneau des entiers algébriques du corps*.

Le même processus à partir de l'anneau $k[X]$ des polynômes à une indéterminée X à coefficients dans le corps k, au lieu de l'anneau $\mathbb{Z}$, conduit à des *algèbres affines de courbes algébriques non singulières*. Plus précisément, soit K un corps contenant le corps k(X) des fractions de $k[X]$ et de dimension finie en tant que k(X)-espace vectoriel. On démontrera dans le chapitre 7 qu'il existe $\mathbf{x}_1 = X_1,\ldots,x_n \in K$ tels que la fermeture intégrale de $k[X]$ dans K soit $k[\mathbf{x}_1,\ldots,x_n]$. Cette fermeture intégrale A est de la forme $k[X,\ldots X_n]/p$, où $X,\ldots,X_n$ sont des indéterminées et p un idéal premier. Le sous-ensemble de k^n

$$\{(a_1,\ldots,a_n) \in k^n / \forall f \in p,\ f(a_1,\ldots,a_n)\} = 0$$

est une courbe *algébrique irréductible de* k^n.

Le fait que l'anneau A soit intégralement clos implique que la courbe est *non singulière* en un sens qui sera précisé ultérieurement.

La notion d'entier algébrique a une autre interprétation géométrique plus au moins explicitée dans le paragraphe II sur les places. Cette interprétation est, par exemple, liée à la notion usuelle de direction asymptotique d'une courbe algébrique plane.

A n'est pas factoriel est 23) ou, ce qui est équivalent (pour les anneaux de ce type) principal.

I. Eléments transcendants, algébriques, entiers

1. Définitions

Soeint B *un anneau,* A *un sous-anneau de* B, $(x_i)_{i\in I}$ *une famille d'éléments de* B, $(X_i)_{i\in I}$ *une famille d'indéterminées,* indexée par le même ensemble d'indices I. On sait qu'il existe un homomorphisme et un seul ϕ de A-algèbres de $A[X_i]_{i\in I}$ dans B tel que $\phi(X_i) = x_i$ pour tout i de I. ((FFAC) chap. 2.II)

Définitions

On dit que la famille $(x_i)_{i\in I}$ *est algébriquement indépendante (resp. algébriquement dépendante) sur* A *si l'homomorphisme* ϕ *est injectif (resp. n'est pas injectif).*

Dire que la famille $(x_i)_{i\in I}$ *est algébriquement indépendante sur* A *c'est donc dire que* ϕ *est un isomorphisme de* A*-algèbres de* $A[X_i]_{i\in I}$ *sur* $A[x_i]_{i\in I}$.

Dire qu'elle est algébriquement dépendante sur A, c'est dire qu'il existe une partie *finie* $\{i_1,\ldots,i_n\}$ de I et un polynôme f non nul de $A[X_{i_1},\ldots X_{i_n}]$ tel que $f(x_{i_1},\ldots x_{i_n}) = 0$

Un élément x *de* B *est dit transcendant (resp. algébrique) sur* A *si la famille* {x} *est algébriquement indépendante (resp. algébriquement dépendante) sur* A.

Dire que x est algébrique sur A c'est dire que l'idéal $I = \{f(X) \in A[X]/f(x) = 0\}$ de $A[X]$ est non nul. La surjection canonique de $A[X]$ sur $A[x]$ définit alors, par passage au quotient, un isomorphisme de A-algèbres de $A[X]/I$ sur $A[x]$.

Définitions

1. *Soit* X *une indéterminée*

Un polynôme $f(X) \in A[X]$ *est dit unitaire si le coefficient du terme de plus haut degré de* f *est* 1. Un tel polynôme est donc de la forme $X^n + a_1X^{n-1} + \ldots + a_n$.

2. *Un élément* x *de* B *est dit entier (algébrique) sur* A *s'il existe un polynôme unitaire* f(X) *de* $A[X]$ *tel que* $f(x) = 0$.

L'équation $f(x) = 0$ est alors appelée *équation de dependance intégrale de* x *sur* A.

Exemples

Le nombre e (resp. π) est transcendant sur $\mathbb{Q}$ (démonstration due

à Hermite (resp. Lindemann)) (e.16 (resp. 17))

Un élément de A est entier sur A.

Un élément entier sur A est algébrique sur A.

Tout élément de $\mathbb{Q}$ est algébrique sur $\mathbb{Z}$. Il n'est entier sur $\mathbb{Q}$ que s'il appartient à $\mathbb{Z}$.

Proposition I.1

Soient B *un anneau,* k *un sous-corps de* B, x *un élément de* B.

1. Les conditions suivantes sont équivalentes: (i) x *est entier sur* k

(ii) x *est algébrique sur* k

2. Si elles sont satisfaites et si B *est intègre, l'anneau* $k[x]$ *est un corps.*

Démonstration

1. Il est clair que (i) $\Longrightarrow$ (ii).

(ii) $\Longrightarrow$ (i). Soit $f(X) = a_0X^n + \ldots + a_n \in k[X]$ avec $a_0 \neq 0$ tel que $f(x) = 0$.

Le polynôme $g(X) = a_0^{-1}f(X)$ est unitaire et $g(X) = 0$.

2. Soit $f(X) = X^n + a_1X^{n-1} + \ldots + a_n$ le polynôme unitaire de degré minimal de $k[X]$ tel que $f(y) = 0$. Il engendre l'idéal maximal $\{g(X) \in k[X] / g(x) = 0$. Cet idéal est le noyau de l'homomorphisme surjectif de k-algèbres de $k[X]$ sur $k[x]$ qui applique X sur x. Donc, $k[x]$ est un corps isomorphe au corps $k[X]/(f(X))$.

Pour des raisons historiques, dans la situation de la proposition 1.1, on préfèrera le terme algébrique au terme entier. On notera aussi, pour des raisons justifiées dans le chapitre suivant, $k(x)$ *le corps* $k[x]$.

Définition

Soient B *un anneau,* A *un sous-anneau de* B. *On dit que* B *est entier (resp. algébrique sur* A*) si tout élément de* B *est entier (resp. algébrique) sur* A.

Définition (morphisme entier)

Soient A *un anneau,* B *une* A*-algèbre,* ϕ *l'homomorphisme structural* $A \longrightarrow B$, $x \in B$. *On dit que* x *est entier sur* A *s'il est entier sur* $\phi(A)$.

On dit que B *est entière sur* A *ou que l'homomorphisme* ϕ *est entier si* B *est entier sur son sous-anneau* $\phi(A)$.

Il résulte de la définition même que l'on peut toujours se ramener

par remplacement éventuel de A par $\phi(A)$, au cas d'un homomorphisme *injectif*.

Si A est un corps, un homomorphisme $A \longrightarrow B$ est d'ailleurs injectif si B n'est pas l'anneau nul.

Proposition I.2

Soient B *un anneau,* A *un sous-anneau de* B *tel que* B *soit entier sur* A.

1. Soit u *un homomorphisme de* B *dans un anneau* B'. *L'anneau* u(B) *est entier sur l'anneau* u(A).

2. Soit S *une partie (multiplicative) de* A. *L'anneau* $S^{-1}B$ *est entier sur* $S^{-1}A$.

3. Soit $(B_i)_{i\in I}$ *une famille filtrante croissante de sous anneaux de* B *entiers sur* A. *L'anneau* $\bigcup_{i\in I} B_i$ *est entier sur* A.

Démonstration

1. Soit f(X) un polynôme unitaire $\in A[X]$ tel que f(x) = 0. Alors le polynôme $^{u}f(X)$ obtenu en appliquant u aux coefficients est unitaire et $^{u}f(u(x)) = 0$.

2. Soit $x^n + \sum_{i=0}^{n-1} a_{n-i}x^i = 0$ une équation de dépendance intégrale de x sur A.

Alors, $(x/s)^n + \sum_{i=0}^{n-i}(a_{n-i}/s^{n-i})(x/s)^i = 0$ est une équation de dépendance intégrale pour x/s sur $S^{-1}A$.

3. évident.

2. Caractérisation des éléments entiers

Théorème I.3 (linéarisation de la notion d'entier)

Soient B *un anneau,* A *un sous-anneau,* x *un élément de* B.

1. Les assertions suivantes sont équivalentes:

(i) x *est entier sur* A

(ii) A[x] *est un* A*-module de type fini*

(iii) Il existe un A[x]*-module fidèle* B' *qui est un* A*-module de type fini.*

2. La condition (iii) est, en particulier, satisfaite s'il existe un sous-anneau B' *de* B *contenant* A *et* x *et* A*-module de type fini*

Démonstration

(i) $\Longrightarrow$ (ii).

Soit $f(X) = X^n + \sum_{i=0}^{n-1} a_{n-i}X^i$ un élément de A[X] tel que f(x) = 0.

On démontre, par récurrence sur m, *que* x^m *appartient au* A*-module engendré par* $1, x, \ldots, x^{n-1}$.

C'est clair si $m < n$. On suppose donc $m \geqslant n$ et l'assertion vraie pour $m-1$.

De l'égalité $x^{m-1} = \sum_{i=0}^{n-1} \alpha_i x^i$ $(\alpha_i \in A)$, on déduit l'égalité

$$x^m = \sum_{i=0}^{n-1} \alpha_i x^{i+1} = \sum_{i=0}^{n-2} \alpha_i x^{i+1} - \alpha_{n+1}\left(\sum_{i=0}^{n-1} a_{n-i} x^i\right).$$

Il en résulte que $\{1, x, \ldots, x^{n-1}\}$ est un système de générateurs du A-module $A[x]$.

(ii) $\Longrightarrow$ (iii). Il suffit de prendre $B' = A|x|$.

(iii) $\Longrightarrow$ (i).

Soit $\{e_1, \ldots, e_n\}$ un système fini de générateurs du A-module B'.

On a des égalités

$$xe_i = \sum_{j=1}^{n} a_{ij} e_j \quad (a_{ij} \in A;\ i = 1, \ldots, n)$$

Posant $b_{ij} = \delta_{ij} x - a_{ij}$, où $\delta_{ij} = 1$ si $i = j$ et 0 si $i \neq j$ $(i, j = 1, \ldots, n)$ on obtient un système de n égalités.

$$(*_i) \quad \sum_{j=1}^{n} b_{ij} e_i = 0 \quad (i = 1, \ldots, n)$$

On fixe k et on multiplie l'égalité $(*_i)$ par le mineur B_{ik} de la matrice (b_{ij}) puis on ajoute.

On obtient $0 = \sum_{i=1}^{n} B_{ik}\left(\sum_{j=1}^{n} b_{ij} e_j\right) = \sum_{j=1}^{n}\left(\sum_{i=1}^{n} b_{ij} B_{ik}\right) e_j$ qui se réduit à

$$\det(b_{ij}) e_k = 0$$

Ainsi $\det(b_{ij})$ appartient à l'annulateur de B' et est donc nul.

Le polynôme $f(X) = \det(X\delta_{ij} - a_{ij})$ est *unitaire* car son terme de plus haut degré est celui de $\prod_{i=1}^{n}(X - a_{ii})$.

L'équation $f(x) = 0$ est une équation de dépendance intégrale de x sur A

Définition

Soient A et B des anneaux, u un homomorphisme d'anneaux de A dans B.

On dit que u est fini si B est un A-module (ou ce qui revient au même un $u(A)$-module) *de type fini.*

Corollaire 1

Un homomorphisme fini est entier.

On utilise dans les autres corollaires du théorème I.3 le lemme suivant dont la démonstration immédiate est laissée au lecteur.

Lemme

Soient A' *un anneau,* A *un sous-anneau,* M *un* A'*-module de type fini.*

Si A' *est un* A*-module de type fini, il en est de même de* M.

Corollaire 2

Soient B *un anneau,* A *un sous-anneau,* $(x_i)_{i\in I}$ *une famille d'éléments de* B *entiers sur* A.

L'anneau $A[x_i]_{i\in I}$ *est entier sur* A. *Si, de plus, l'ensemble* I *est fini,* $A[x_i]_{i\in I}$ *est un* A*-module de type fini.*

Démonstration

Comme $A[x_i]_{i\in I} = \bigcup_J A[x_i]_{i\in J}$ où J parcourt l'ensemble des parties finies de I, il suffit de démontrer l'assertion dans le cas où I est fini, $I = \{1,\ldots,n\}$.

On prouve par récurrence sur n que le A-module $A[x_1,\ldots,x_n]$ est de type fini (lemme) puis on utilise la caractérisation (iii) du théorème I.2.

Corollaire 3 (transitivité de la dépendance intégrale)

Soient C *un anneau,* B *un sous-anneau de* C, A *un sous-anneau de* B.

Si C *est entier sur* B *et* B *est entier sur* A, C *est entier sur* A.

Démonstration

Soient $x \in C$, $f(x) = 0$ une équation de dépendance intégrale de x sur B, où $f(X) = X^n + \sum_{i=0}^{n-1} b_{n-i} X^i$.

Le A-module $A' = A[b_0,\ldots,b_{n-1}]$ est de type fini. Il en est de même du A-module $A[b_0,\ldots,b_{n-1},x]$ et donc x est entier sur A.

Corollaire 4

Soient B *un anneau,* A *un sous-anneau de* B.

L'ensemble des éléments de B *entiers sur* A *est un sous-anneau de* B *contenant* A.

Démonstration

Soient x,y des éléments de B entiers sur A. Le A-module $A[x,y] = A[x][y]$ est de type fini. Donc, x-y et xy sont entiers sur A.

Définition

1. *Sous les hypothèses du corollaire 4, l'ensemble des éléments de* B *entiers sur* A *est appelé la fermeture intégrale de* A *dans* B.

2. *Si cet ensemble est égal à* A, *on dit que* A *est intégralement fermé dans* B.

3. *La fermeture intégrale d'un anneau intègre* A *dans son corps des fractions est appelé la clôture intégrale de* A.

4. *Si* A *est intégralement fermé dans son corps des fractions, on dit qu'il est intégralement clos.*

Proposition I.4

Un anneau factoriel (et donc un anneau principal) *est intégralement clos.*

Démonstration

Soit x un élément du corps K des fractions de l'anneau factoriel A.

Il s'écrit a/b où a,b $\in$ A et a et b n'ont pas de facteur irréductible commun.

Si x est entier sur A, soit $x^n + \sum_{i=0}^{n-1} a_i x^{n-i} = 0$ l'équation de dépendance intégrale de degré minimal de x sur A. Si $x \neq 0$, a_0 est non nul.

Remplaçant x par a/b on obtient une égalité $a^n = bc$ avec $c \in A$. L'élément b est inversible car sinon un de ses facteurs irréductibles devrait diviser a. Donc x appartient à A.

Exemples d'anneaux intégralement clos

Un corps est intégralement clos. L'anneau $\mathbb{Z}$ est intégralement clos.

L'anneau des polynômes à n indéterminées à coefficients dans un anneau factoriel (par exemple, $\mathbb{Z}$ ou un corps) est intégralement clos.

On reviendra, dans III, sur cette notion d'anneau intégralement clos en donnant d'autres exemples importants.

3. Changement de base

Proposition I.5

Soient A *un anneau,* B *et* A' *des* A*-algèbres.*

Si B *est entière sur* A, $B \underset{A}{\otimes} A'$ *est entière sur* A'.

Démonstration

Un élément de $B \underset{A}{\otimes} A'$ s'écrit $\sum_{i=1}^{n} b_i \otimes a'_i$ où $b_i \in B$, $a'_i \in A'$, soit $\sum_{i=1}^{n} (b_i \otimes 1)a'_i$.

Or, $b_i \otimes 1$ est entier sur A' car, si b_i est racine du polynôme unitaire

$$f(X) = X^{n_i} + a_{n-1}X^{n_i-1} + \ldots + a_{0} \quad \in A[X]$$

$b_i \otimes 1$ est racine du polynôme $X^{n_i} + a'_{n-1}X^{n_i-1} + \ldots + a'_0$, où $a'_i = a_i \otimes 1$ est identifié à l'image de a_i dans A'.

L'élément considéré de $B \otimes_A A'$ est donc bien entier sur A'.

Corollaire

Soient A *un anneau,* B *un anneau entier sur* A, $X_1,\ldots,X_n$ *des indéterminées.*

Alors l'anneau $B[X_1,\ldots,X_n]$ *est entier sur* $A[X_1,\ldots,X_n]$.

Démonstration

Résulte de ce que $B[X_1,\ldots,X_n]$ est isomorphe à $A[X_1,\ldots,X_n] \otimes_A B$.

Proposition I.6

Soient K *un corps,* L *un corps contenant* K *comme sous-corps et algébrique sur* K, $X_1,\ldots,X_n$ *des indéterminées.*

Le corps $L(X_1,\ldots,X_n)$ *des fractions rationnelles à coefficients dans* L (corps des fractions de l'anneau $L[X_1,\ldots,X_n]$) *est algébrique sur le corps* $K(X_1,\ldots,X_n)$.

Démonstration

C'est une conséquence immédiate du corollaire et du lemme suivant.

Lemme

Soient B *un anneau intègre,* A *un sous-anneau de* B.

Si B *est entier sur* A, *le corps des fractions* L *de* B *est algébrique sur le corps* K *des fractions de* A.

Démonstration du lemme

Soit $b/b' \in L$, où $b,b' \in B$, $b \neq 0$. Soit $b'^n + a_1 b'^{n-1} + \ldots + a_n = 0$ une équation de dépendance intégrale de b' sur A avec a_n non nul.

Soit $b'' = -(b'^{n-1} + a_1 b'^{n-2} + \ldots + a_{n-1})$. On a l'égalité $b'b'' = a_n$ L'élément b/b' s'écrit bb''/a_n.

On peut donc en changeant de notations, *supposer que* b' *est élément de* A.

On déduit facilement d'une équation de dépendance intégrale de b sur A une équation de dépendance algébrique de b/b' sur K.

La proposition suivante est un complément au théorème II 10 du chapitre 3.

Proposition I.7

Soient A *un anneau noethérien réduit,* $p_1,\ldots,p_n$ *les idéaux premiers minimaux de* A, A_i *L'anneau* A/p_i, ϕ_i *la surjection canonique de* A *sur* A_i, K_i *le corps des fractions de* A_i $(i = 1,\ldots,n)$, K *l'anneau total des fractions de* A, $\overline{A}_i$ *la clôture intégrale de* A_i, $\overline{A}$ *la fermeture intégrale de* A

dans K, ϕ_i *l'homomorphisme de* K *dans* K_i *prolongeant* ϕ_i. *On rappelle que l'application* $\phi : x \longrightarrow (\phi_1(x),\ldots,\phi_n(x))$ *est un isomorphisme de* K *sur* $\prod_{i=1}^{n} K_i$.

Alors, $\phi(\overline{A}) = \prod_{i=1}^{n} \overline{A}_i$.

Démonstration

L'inclusion $\phi(\overline{A}) \subset \prod_{i=1}^{n} \overline{A}_i$ est claire. Réciproquement, si (x_i) appartient à $\prod_{i=1}^{n} \overline{A}_i$, il existe, pour $i = 1,\ldots,n$, un polynôme unitaire $f_i(T) \in A[T]$ tel que $\phi_i(f_i(x)) = 0$ pour $x = \phi^{-1}((x_i))$. Donc, $f_i(x)$ appartient à $\ker(\phi_i)$. Il en résulte que, si $f(T) = \prod_{i=1}^{n} f_i(T)$, f(x) appartient à $\ker(\phi)$ et est, par suite, égal à 0. Par conséquent, x appartient à $\overline{A}$.

Corollaire 1

Soient A *un anneau noethérien réduit et intégralement fermé dans son anneau total des fractions.*

Alors, A *est un produit d'un nombre fini d'anneaux noethériens intégralement clos.*

Corollaire 2

Un anneau local noethérien réduit, intégralement fermé dans son anneau total des fractions est intègre.

Démonstration

Les seuls idempotents d'un anneau local A sont 0 et 1. Il suffit d'appliquer ((FFAC). chap.2.III).

4. Polynôme caractéristique d'un entier algébrique

Ce paragraphe sera utilisé dans le chapitre 13 théorème III.3. Pour une étude plus détaillée, le lecteur pourra consulter Bourbaki. *Algèbre commutative.* chapitre 5. Entiers. §1.n°6.

Proposition I.8

Soient B *un anneau,* A *un sous-anneau de* A, $u \in \mathrm{End}_B(B^n)$ (n *entier* ≥ 1).

Les assertions suivantes sont équivalentes:

(i) u *est entier sur* A

(ii) *il existe un sous-*A*-module de type fini* M *de* B^n *tel que* $u(M) \subset M$ *et que* M *soit un système de générateurs du* B*-module* B^n

(iii) *les coefficients du polynôme caractéristique* $\chi_u(X)$ *de* u *sont entiers sur* A.

Démonstration

On désigne par $(e_i)_{1\leqslant i\leqslant n}$ la base canonique de B^n. On rappelle que si (a_{ij}) est la matrice de u par rapport à cette base, $\chi_u(X) = \det(X\delta_{ij} - a_{ij})$. Le théorème d'Hamilton-Cayley affirme l'égalité $\chi_u(u) = 0$.

(iii) $\Longrightarrow$ (i)

Résulte du théorème d'Hamilton-Cayley et de la transitivité de la dépendance intégrale.

(i) $\Longrightarrow$ (ii)

On prend pour M le sous-module du A-module B^n engendré par les éléments $u^k(e_i)$ $(1\leqslant i\leqslant n;\ k\geqslant 0)$. Il est de type fini car $A[u]$ l'est.

Comme $e_i \in M$ pour tout i, M est bien un système de générateurs du B-module B^n.

(i) $\Longrightarrow$ (iii)

Comme u est entier sur A, il l'est, a fortiori, sur $A[X]$. Donc, $X\mathrm{I}_{B^n} - u$ est entier sur $A[X]$.

Remplaçant u par $X\mathrm{I}_{B^n} - u$ on est donc ramené à démontrer l'implication u *entier sur* A $\Longrightarrow$ det(u) *entier sur* A

Les éléments $x_1\wedge \ldots \wedge x_n$ $(x_i \in M;\ i = 1,\ldots,n)$ engendrent dans $\bigwedge^n(B^n)$ un sous A-module de type fini contenant $e_1 \ldots e_n$ et stable par $\bigwedge^n u$, c'est à dire par l'homothétie de rapport det(u). Ce sous-module est fidèle car l'annulateur de $e_1\wedge \ldots \wedge e_n$ est (0). Il résulte alors de la caractérisation (iii) du théorème I.3 que det(u) est entier sur A.

(ii) $\Longrightarrow$ (i)

Comme $u(M) \subset M$, M est muni d'une structure naturelle de $A[u]$-module. Ce module est, évidemment, fidèle. Il suffit d'utiliser la caractérisation (iii) du théorème I.3

Soient A *un anneau intègre,* K *son corps des fractions,* L *une* K*-algèbre telle que* $[L:K] < \infty$, $x \in L$.

L'élément x *définit un élément* $u \in \mathrm{End}_K(L)$ *par* $u(y) = xy$.

On appelle *polynôme caractéristique de* x *et on note* $\chi_x(X)$ le polynôme caractéristique $\chi_u(X)$

Corollaire de la proposition I.8

Si x *est entier sur* A, *les coefficients du polynôme caractéristique* $\chi_x(X)$ *sont entiers sur* A.

5. Le premier théorème de Cohen-Seidenberg

Théorème I.9 (appelé en anglais: lying over)

Soient B *un anneau,* A *un sous-anneau tel que* B *soit entier sur* A.

1. Pour tout idéal premier p *de* A, *il existe un* (au moins) *idéal premier* q *de* B *au dessus de* p, i.e. *tel que* $q \cap A = p$.

2. Soient q *et* q' *deux idéaux premiers de* B *au dessus du même idéal premier* p *de* A.

Si $q \subset q'$, $q = q'$. *Autrement dit, il n'y a pas de relation d'inclusion entre idéaux premiers de* B *au dessus du même idéal premier* p *de* A.

3. Si q *est un idéal premier de* B *au dessus d'un idéal maximal* p *de* A, q *est maximal. Réciproquement, si* q *est maximal,* $q \cap A$ *est maximal dans* A.

Démonstration

1. Cas où A *est local d'idéal maximal* p.

On remarque que $pB \neq B$: sinon, on aurait une égalité

$$1 = \sum_{i=1}^{n} p_i b_i \quad (p_i \in p,\ b_i \in B)$$

Posant, $B' = A[b_1, \ldots, b_n]$, on en déduirait l'égalité $pB' = B'$, contredisant le lemme de Nakayama puisque B' est un A-module de type fini.

Un idéal maximal q contenant pB est au dessus de p.

Cas général

Soit $S = A - p$. L'anneau $S^{-1}B$ est entier sur $S^{-1}A$. Il existe donc (cas précédent) un idéal premier q' de $S^{-1}B$ au dessus de l'idéal maximal de l'anneau local $S^{-1}A = A_p$. L'idéal premier $(i_B^S)^{-1}(q')$ est au dessus de p.

2. Quitte à passer au quotient par q, on peut supposer $q = (0)$, B et A intègres. Soient $x \in q'$, $x^n + \sum_{i=0}^{n-1} a_i x^i = 0$ l'équation de dependance intégrale de degré minimal de x sur A. Comme a_o appartient à $q' \cap A = q \cap A = (0)$, a_o est nul. Si n était >1, par division par x, nécéssairement non nul, on obtiendrait pour x une équation de dépendance intégrale de degré $n-1$. Donc $n = 1$ et $x = 0$.

3. Passant au quotient par q, on se ramène à la démonstration des points suivants.

Un anneau B *intègre entier sur un corps* A *est un corps:* soit x non nul $\in B$ et soit $x^n + \sum_{i=0}^{n-1} a_i x^i = 0$ une équation de dépendance intégrale

de degré minimal de x sur A; l'élément a_o de A est non nul et donc inversible; il en est de même de x qui a pour inverse $-(a_o)^{-1}(x^{n-1}+\ldots+a_1)$

Si le corps B *est entier sur le sous-anneau* A, A *est un corps:* soit a un élément non nul de A, x son inverse dans B. Utilisant une équation de dépendance intégrale de degré minimal $x^n + \sum_{i=0}^{n-1} a_i x^i = 0$ de x sur A, on obtient par multiplication par a^n une égalité $1 = ab$ où $b \in A$. Donc, $x = b$ appartient à A.

Corollaire

Avec les hypothèses du théorème I.12, *soient* r(A) *et* r(B) *les radicaux de* A *et* B. *Alors,* $r(A) = A \cap r(B)$.

Démonstration

Résulte immédiatement de la définition du radical comme intersection des idéaux maximaux.

Le résultat ci dessous, connu sous le nom de lemme de Kummer, précise le 3. du théorème I. 9 dans un cas particulier important, notamment en théorie algébrique des nombres.

Proposition I.10

Soient A *un anneau,* m *un idéal maximal de* A, k *le corps quotient* A/m, f(X) *un polynôme unitaire* $\in A[X]$, $\overline{f}(X) = \overline{f}_1(X)^{a_1}\ldots\overline{f}_r(X)^{a_r}$ *une décomposition de l'image de* f(X) *dans* $k[X]$ *en produit de puissances de polynômes* $\overline{f}_i(X)$ *irréductibles distincts,* $f_i(X)$ *un représentant de* $\overline{f}_i(X)$ *dans* $A[X]$ $(i = 1,\ldots,r)$, B *l'anneau* $A[X]/(f(X))$, x *la classe de* X *en sorte que* $B = A[x]$.

Les idéaux maximaux de B *au dessus de* m *sont les idéaux* $(m, f_i(x))B$ $(i = 1,\ldots,r)$

Démonstration

Soit p la surjection canonique de B sur $\overline{B} = B/mB$.

Un idéal maximal de B au dessus de m contient mB. L'application: $n \longmapsto p(n)$ est donc une bijection de l'ensemble des idéaux maximaux de B au dessus de m sur l'ensemble des idéaux maximaux de $\overline{B}$. Or, $\overline{B}$ est isomorphe à $k[X]/(\overline{f}(X))$ et un idéal maximal de $\overline{B}$ est donc de la forme $(\overline{f}_i(X))/(\overline{f}(X))$. Un idéal maximal de B au dessus de m est donc de la forme $((f_i(X)) + mA[X]/(f(X))$, i.e. de la forme $(m, f_i(x))B$.

Définition

On appelle chaîne d'idéaux premiers de l'anneau A *une suite finie*

strictement croissante $p_o \subset \ldots \subset p_n$ *d'idéaux premiers de* A.

L'idéal p_o est appelé l'origine de la chaîne , l'idéal p_n l'extremité de la chaîne. L'entier n, i.e. le nombre d'intervalles déterminés par la chaîne, est appelé la *longueur de la chaîne.*

Théorème I.11 (appelé en anglais: going up)

Soient f : A ⟶ B *un homomorphisme entier,* $p_1 \subset \ldots \subset p_n$ *une chaîne d'idéaux premiers de* A, m *un entier* ⩽n, $q_1 \subset \ldots \subset q_m$ *une chaîne d'idéaux premiers de* B *telle que* q_i *soit au dessus de* p_i *pour* i = 1,...,m.

On peut compléter la chaîne $q_1 \subset \ldots \subset q_m$ *en une chaîne* $q_1 \subset \ldots \subset q_n$ *d'idéaux premiers de* B *telle que* q_i *soit au dessus de* p_i *pour* i = 1,...,n.

Démonstration

Par une récurrence immédiate, on se ramène au cas n = 2, m = 1.

Soit f_1 l'homomorphisme de A/p_1 dans B/q_1 déduit de f par passage au quotient. Il est entier injectif. Il existe donc un idéal premier q_2/q_1 de B/q_1 au dessus de l'idéal premier p_2/p_1 et l'idéal premier q_2 de B contient q_1 et est au dessus de p_2.

Définition

La dimension de Krull *d'un anneau* A *est la borne supérieure des longueurs des chaînes d'idéaux premiers de* A: *c'est donc un entier naturel ou* + ∞. *On le note* dim(A).

Exemples

La dimension d'un corps est 0. La dimension de $\mathbb{Z}$ est 1. Plus généralement, la dimension d'un anneau principal est 1 si il n'est pas un corps.

Soient k un corps, $\{X_n\}_{n\in\mathbb{N}}$ une suite d'indéterminées. L'anneau $k[X_n]_{n\in\mathbb{N}}$ a pour dimension + ∞: on a, en effet, la suite infinie $(X_o) \subset (X_o, X_1) \subset \ldots$ d'idéaux premiers.

L'étude de la dimension de Krull d'un anneau sera reprise de manière plus détaillée dans le chapitre 10. On veut simplement signaler ici le résultat ci dessous.

Proposition I.12

Soit f : A ⟶ B *un homomorphisme entier.*

Alors, dim(B) ⩽ dim(A).

Si, de plus, f *est injectif,* dim(B) = dim(A).

Démonstration

Comme $\dim(A/\ker(f)) \leqslant \dim(A)$, il suffit de traiter le cas où f est injectif. Le théorème I.11 indique que $\dim(B) \geqslant \dim(A)$. Il résulte, d'autre part, du théorème I.9.2 que $\dim(A) \geqslant \dim(B)$. Donc, $\dim(B) = \dim(A)$.

II. Interprétation de la notion d'entier en termes de places ou de valuations

Les notions explicitées dans ce paragraphe ont un support géométrique que l'on se contentera ici de suggérer sur des exemples: places de $\mathbb{C}(X)$, points d'une hyperbole et places d'un corps associé naturellement à l'hyperbole. Le lecteur pourra se reporter à un livre sur les courbes algébriques pour l'étude plus générale de la correspondance entre points d'une courbe algébrique projective non singulière et places de son corps des fonctions rationnelles.

1. Places et anneaux de valuation

Corps projectif

Le corps projectif associé à un corps k *est* $k \cup \{\infty\}$, *où* ∞ *est un élément n'appartenant pas à* k. *On le note* k_∞.

Si $k = \mathbb{R}$, k peut être assimilée à la droite affine. On peut considérer R_∞ comme la droite projective obtenue par adjonction d'un point à l'infini.

On munit k_∞ *de lois de composition non partout définies prolongeant celles de* k *en posant:* si $a \neq \infty$, $a + \infty = \infty + a = \infty$

si $a \neq 0$, $a\infty = \infty a = \infty$

$-\infty = \infty$, $0^{-1} = \infty$, $\infty^{-1} = 0$

Les éléments $\infty + \infty$, $\infty 0$ *et* 0∞ *ne sont pas définis.*

Soient k *et* k' *deux corps.*

Un morphisme de k_∞ *dans* k'_∞ *est une application* ϕ *de* k_∞ *dans* k'_∞ *possédant les propriétés suivantes:*

1. Les éléments $\phi(x+y)$ et $\phi(x) + \phi(y)$ sont définis (resp. non définis) simultanément et s'ils sont définis, $\phi(x+y) = \phi(x) + \phi(y)$
2. Les éléments $\phi(xy)$ et $\phi(x)\,\phi(y)$ sont définis (resp. non définis) simultanément et s'ils sont définis $\phi(xy) = \phi(x)\,\phi(y)$.

Une place de k *dans* k' *est un morphisme* ϕ *de* k_∞ *dans* k'_∞ *tel que* $\phi(1) = 1$.

Alors, $\phi(\infty) = \phi(\infty + 1) = \phi(\infty) + 1$ et donc $\phi(\infty) = \infty$

Un élément x *de* k_∞ *est dit fini en la place* ϕ *si* $\phi(x) \neq \infty$. Un tel élément appartient alors à k.

Proposition II.1 (anneau de valuation d'une place)

Soient ϕ *une place du corps* k *dans le corps* k', A *l'ensemble des éléments de* k *finis en* ϕ.

L'ensemble A *est un sous-anneau de* k *possédant la propriété suivante:*

Si $x \in k$ *n'appartient pas à* A (ce qui implique $x \neq 0$), x^{-1} *appartient à* A.

L'anneau A *est local d'idéal maximal* $m = \{x \in k / \phi(x) = 0\}$. *Il admet* k *pour corps de fractions.*

Démonstration

Si a, a' $\in$ A, a-a' et aa' appartiennent à A. Comme $\phi(1) = 1$, 1 appartient à A qui est donc un sous-anneau de k.

Soit $x \in k$. Dire que x n'appartient pas à A c'est dire que $\phi(x) = \infty$. Il en résulte que $\phi(x^{-1}) = 0$ car sinon $\phi(x)\,\phi(x^{-1})$ serait défini et donc égal à $\phi(xx^{-1}) = \phi(1) = 1$. Or, $\phi(x)\phi(x^{-1})$ serait égal à ∞ comme $\phi(x)$.

Par conséquent, x^{-1} appartient à A.

On en déduit immédiatement que k est le corps des fractions de A.

Un raisonnement analogue prouve que dire que l'élément x de A n'est pas inversible dans A c'est dire que $\phi(x^{-1}) = \infty$, i.e. que $\phi(x) = 0$

Donc, A est local d'idéal maximal $\{x \in k / \phi(x) = 0\}$.

Définition

Soit k *un corps.*

Un anneau de valuation de k *est un sous-anneau* A *de* k *tel que, si* $x \in k$ *n'appartient pas à* A, *son inverse* x^{-1} *appartient à* A.

Le lien entre la notion de place et celle d'anneau de valuation est précisée ci dessous.

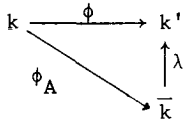
Proposition II.2 (place d'un anneau de valuation)

Soit k *un corps.*

1. Soient A *un anneau de valuation de* k, $\overline{k}$ *le corps résiduel de* A, ϕ_A *l'application de* k_∞ *dans* $\overline{k}_\infty$ *définie comme suit: la restriction de* ϕ_A *à* A *est la surjection canonique de* A *sur* $\overline{k}$ *et si* $x \notin A$, $\phi_A(x) = \infty$.

Alors, ϕ_A *est une place de* k *à valeurs dans* $\overline{k}$.

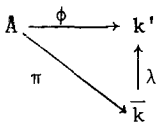
2. Soient k' *un corps,* ϕ *une place de* k *à valeurs dans* k', A *l'anneau de valuation associé à* ϕ, $\overline{k}$ *le corps résiduel de* A, ϕ_A *la place définie en* 1. *Il existe un homomorphisme d'anneaux et un seul* λ *de* $\overline{k}$ *dans* k' *rendant commutatif le diagramme*



Démonstration

1. Il suffit de vérifier les axiomes des places.

2. Comme, si m désigne l'idéal maximal de A, $\phi(m) = 0$, ϕ définit par passage au quotient un homomorphisme λ et un seul de $A/m = \overline{k}$ dans k' rendant commutatif le diagramme



où π est la surjection canonique.

Il est clair que λ satisfait à la condition imposée.

L'unicité est immédiate.

Soit ϕ une place du corps k à valeurs dans k'. Si λ est un homomorphisme de k' dans le corps k", le composé $\lambda \circ \phi$ est une place de k à valeurs dans k". Les anneaux de valuation de ϕ et $\lambda \circ \phi$ sont égaux.

L'application: place $\longmapsto$ anneau de valuation, *qui est surjective* (prop. II.1) *n'est donc pas bijective.*

Elle devient bijective si on se limite aux seules places de la forme ϕ_A. (avec les notations de la proposition II.2).

Il est clair que la considération des seules places de cette forme est suffisante dans la pratique.

2. Une caractérisation des anneaux de valuation

Définition

Soient C *et* D *deux anneaux locaux.*

On dit que C *domine* D *si* D *est un sous-anneau de* C *et si l'injection de* D *dans* C *est un homomorphisme local.*

Il revient au même de dire que D *est un sous-anneau de* C *et que l'idéal maximal de* D *est la trace sur* D *de l'idéal maximal de* C.

Proposition II.3 (caractérisation d'anneaux de valuation)

Soient k *un corps,* A *un sous-anneau de* k.

Les assertions suivantes sont équivalentes:

(*i*) A *est un anneau de valuation de* k

(*ii*) *l'ensemble des idéaux principaux de* A *est totalement ordonné par inclusion et* k *est le corps des fractions de* A

(*iii*) *l'ensemble des idéaux de* A *est totalement ordonné par inclusion et* k *est le corps de fractions de* A.

(*iv*) A *est un élément maximal de l'ensemble des sous anneaux locaux de* k *ordonné par la relation de domination.*

Démonstration

Il est clair que (ii) implique (i) et que (iii) implique (ii).

(i) $\Longrightarrow$ (ii): soient a et b ε A avec b $\neq$ 0. Si (a) n'est pas contenu dans (b), i.e. si x = a/b n'appartient pas à A, 1/x = b/a appartient à A, i.e. (b) est contenu dans (a).

(iii) $\Longrightarrow$ (ii): soient a et b deux idéaux de A tels que b ne soit pas contenu dans a. Si b de b n'appartient pas à a, on a, pour tout a de a, (a)$\subset$(b) et donc $a \subset$ (b) $\subset b$.

(iii) $\Longrightarrow$ (iv): il est clair que A est local. Si B est un sous anneau local de k dominant A, il est clair qu'il vérifie, a fortiori, la condition (i). Si b de B n'appartenait pas à A, 1/b appartiendrait à A et en fait à l'idéal maximal de A. Par conséquent, 1/b appartiendrait à l'idéal maximal de B. Ceci contredit l'inversibilité de 1/b dans B.

(iv) $\Longrightarrow$ (i): soit A un élément maximal de l'ensemble des sous anneaux locaux de k ordonné par domination. Si x appartient à k mais pas à A, mA$[$x$]$ = A$[$x$]$ où m désigne l'idéal maximal de A: sinon il existerait un idéal maximal n de A$[$x$]$ contenant mA$[$x$]$: l'idéal $n \cap$ A, distinct de A et contenant m, serait égal à m; l'anneau local A$[$x$]_n$ dominerait *strictement* l'anneau local A, contrairement à la maximalité de A.

On a donc une égalité $1 = \sum_{i=0}^{n} m_i x^i$ où $m_i \varepsilon m$. En la multipliant par l'inverse de $1 - m_o$, on se ramène au cas où $m_o = 0$.

On obtient alors l'équation de dépendance intégrale

$$(x^{-1})^n - \sum_{i=1}^{n-1} m_i (x^{-1})^{n-i} = 0$$

pour x^{-1} sur A.

L'anneau A$[x^{-1}]$ est donc entier sur A. En vertu du premier théorème

de Cohen-Seidenberg (théorème I. 9), il existe un idéal premier n de $A[x^{-1}]$ au dessus de m.

L'anneau local $A[x^{-1}]_n$ domine A et lui est donc égal. Par conséquent, x^{-1} appartient à A.

Etude des places de l'anneau $\mathbb{C}(X)$, où X est une indéterminée, finies sur $\mathbb{C}$.

Soit ϕ une place de $\mathbb{C}(X)$ finie sur $\mathbb{C}$. Soit A son anneau de valuation.

Deux cas sont possibles :

1er cas: X est finie en ϕ.

En ce cas, A contient l'anneau $\mathbb{C}[X]$ des polynômes. Soient m l'idéal maximal de A, p l'idéal premier $\mathbb{C}[X] \cap m$. *Deux cas sont possibles:*

1. $p = (0)$. Alors A contient $\mathbb{C}[X]_{(0)} = \mathbb{C}(X)$ et est donc égal à $\mathbb{C}(X)$.
2. *p est de la forme* $(X-a)$ *où* $a \in \mathbb{C}$.

L'anneau local A domine l'anneau $\mathbb{C}[X]_{(X-a)}$. Il est facile de vérifier que $\mathbb{C}[X]_{(X-a)}$ est un anneau de valuation. Il en résulte que $A = \mathbb{C}[X]_{(X-a)}$.

Le corps résiduel de $\mathbb{C}[X]_{(X-a)}$, isomorphe au corps quotient $\mathbb{C}[X]/(X-a)$, est isomorphe à $\mathbb{C}$.

On peut supposer que ϕ est la place ϕ_A. (proposition II.2)

Un élément $f(X)$ de $\mathbb{C}(X)$ s'écrit, de manière unique, $(X-a)^n g(X)$ où $g(X) \in \mathbb{C}(X)$ n'a ni pôle ni zéro en a. Alors,

$$\phi_A(f(X)) = \infty \text{ si } n < 0.$$
$$= 0 \text{ si } n > 0$$
$$= g(a) \text{ si } n = 0$$

2ème cas: X n'est pas finie en ϕ.

En ce cas, X^{-1} appartient à A et, même, comme X n'appartient pas à A, X^{-1} appartient à l'idéal maximal m de A. Alors, $A = \mathbb{C}[X^{-1}]_{(X^{-1})}$.

Un élément $f(X)$ de $\mathbb{C}(X)$ s'écrit de manière unique,

$$X^{-n} \frac{a_o + a_1 X^{-1} + \ldots + a_r X^{-r}}{b_o + b_1 X^{-1} + \ldots + b_s X^{-s}} .$$

On vérifie alors que

$$\phi_A(f(X)) = \infty \text{ si } n < 0$$
$$= 0 \text{ si } n > 0$$
$$= \frac{a_o}{b_o} \text{ si } n = 0$$

Ainsi si on écarte le cas où l'anneau de la place est $\mathbb{C}(X)$ (place triviale), on voit que *l'ensemble des classes de places de même anneau est en bijection avec le corps projectif* $\mathbb{C}_\infty$. A $a \in \mathbb{C}$ correspond la place définie dans le 1er cas (2). A ∞, on fait correspondre la place définie dans le 2ème cas.

Remarque

Les anneaux de valuation qui apparaissent ci dessus sont très particuliers. Ils sont principaux et donc noethériens. Ce sont des anneaux de valuation discrète dont l'étude plus détaillée sera abordée au chapitre 12.

3. Caractérisation des entiers en termes de places et valuations

Théorème II.4

Soient k *un corps,* A *un sous-anneau de* k, $x \in k$.

Les assertions suivantes sont équivalentes:

(i) x *est entier sur* A

(ii) x *appartient à tout anneau de valuation de* k *contenant* A

(iii) toute place de k *finie sur* A *est finie en* x

Démonstration

L'équivalence (ii) $\Longleftrightarrow$ (iii) résulte de la correspondance entre places et anneaux de valuation.

(i) $\Longrightarrow$ (iii). Soit x un élément non nul de k entier sur A. Une équation de dépendance intégrale de degré minimal de x sur A fournit, par multiplication par une puissance convenable de x^{-1}, une égalité:

$1 = \sum_{i=0}^{n-1} a_i x^{-i}$ où $a_i \in A$.

Si $\phi(x)$ était ∞, $\phi(x^{-1})$ serait 0. Comme $\phi(a_i)$ est fini, on obtiendrait une égalité, impossible, $\phi(1) = 0$.

(non i) $\Longrightarrow$ (non iii).

Lemme

Soit x *un élément* (non nul) *de* k *non entier sur* A.

Il existe un idéal maximal n *de* $A[x^{-1}]$ *contenant* x^{-1}.

Si, de plus, A *est local d'idéal maximal* m, $n \cap A = m$.

Démonstration du lemme

L'élément x^{-1} n'est pas inversible dans $A[x^{-1}]$ car sinon on aurait une égalité $1 = (x^{-1})(\sum_{i=0}^{n-1} a_i (x^{-1})^i)$ qui, par multiplication par x^n, donnerait une équation de dépendance intégrale de x sur A. L'existence de n en résulte.

L'anneau quotient $A[x^{-1}]/n$ est $A/(n \cap A)$. Si A est local d'idéal maximal m, l'idéal maximal $n \cap A$ est égal à m.

Il existe un élément V maximal dans l'ensemble des sous-anneaux locaux de k dominant l'anneau local $A[x^{-1}]_n$. C'est un anneau de valuation de k dont l'idéal maximal contient x^{-1}. L'inverse x de x^{-1} n'appartient pas à V et, a fortiori, à A.

Corollaire 1

Un anneau de valuation est intégralement clos.

Corollaire 2

Soient K *un corps,* A *un sous-anneau de* K.

La fermeture intégrale de A *dans* K *est l'intersection des anneaux de valuation de* K *contenant* A.

Théorème II.5 (prolongement des places)

Soient k *un corps,* A *un sous-anneau de* k, k' *un corps algébriquement clos,* ϕ *un homomorphisme de* A *dans* k'.

Il existe une place (au moins) *de* k *à valeurs dans* k' *prolongeant* ϕ.

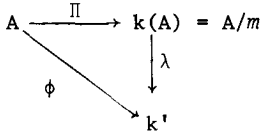
Démonstration

L'ensemble ordonné par inclusion-prolongement, des couples (B,ψ) d'un sous-anneau B de k contenant A et d'un homomorphisme ψ de B dans k' prolongeant ϕ est inductif. Il admet donc un élément maximal.

On peut donc supposer que (A,ϕ) *est maximal pour la relation d'inclusion-prolongement.*

L'anneau A *est alors local d'idéal maximal* $m = \ker(\phi)$: sinon, on pourrait prolonger ϕ en un homomorphisme $\overline{\phi}$ de A_m dans k' par $\overline{\phi}(a/b) = \phi(a)/\phi(b)$.

On a donc un diagramme commutatif :



où Π est la surjection canonique.

On va démontrer que A *est un anneau de valuation.*

L'homomorphisme Π se prolonge alors en la place canonique ϕ_A. On prolongera l'homomorphisme ϕ en la place $\lambda \circ \phi_A$.

On doit donc démontrer que, pour tout $x \in k$, x ou x^{-1} appartient à A.

1er cas: x est entier sur A

Soient alors I l'idéal $\{f(X) \in A[X]/f(x) = 0\}$ de $A[X]$, $\overline{I}$ l'idéal $\{\overline{f}(X)/f(X) \in I\}$ de $k(A)[X]$, où $\overline{f}(X)$ se déduit de $f(X)$ par application de Π aux coefficients de $f(X)$. Comme I contient un polynôme *unitaire*, $\overline{I}$ est non nul. Comme $A[x] = A[X]/I$ l'idéal I est premier. Par conséquent, l'idéal $\overline{I}$ est premier, i.e. de la forme $(\theta(X))$ où $\theta(X)$ est un polynôme irréductible de $k(A)[X]$. Ce polynôme a une racine a dans le corps algébriquement clos k'. On utilise alors le fait que le sous-corps $k(A)[a]$ de k' est isomorphe à $k(A)[X]/\theta(X))$. L'homomorphisme Π se prolonge en un homomorphisme Π_1 de $A[X]$ dans $k(A)[X]$ tel que $\Pi_1(I) = (\theta(X))$ et donc par passage au quotient ϕ se prolonge en un homomorphisme ψ de $A[x]$ dans k' tel que $\psi(x) = a$.

Par maximalité de (A,ϕ), $A = A[x]$ et donc x appartient à A.

2ème cas: x n'est pas entier sur A

Il existe alors (lemme de la proposition II.4) un idéal maximal n de $A[x^{-1}]$ contenant x^{-1} et tel que $n \cap A = m$. L'homomorphisme Π se prolonge en un homomorphisme de $A[x^{-1}]$ dans k(A) appliquant x^{-1} sur 0. Donc, ϕ se prolonge en un homomorphisme de $A[x^{-1}]$ dans k'. Par maximalité de (A,ϕ), $A[x^{-1}] = A$ et donc x^{-1} appartient à A.

Exemples

Les deux exemples ci dessous sont caractéristiques.

1. Soit H l'hyperbole d'équation $X^2 - Y^2 = 1$. Son algèbre affine (chapitre 2) $\mathbb{C}[H]$ est $\mathbb{C}[X,Y]/(X^2-Y^2-1) = \mathbb{C}[X,y]$ où y est la classe de X. Un élément du corps K des fractions de $\mathbb{C}[H]$ s'écrit de manière unique $a(X)+b(X)y$ où $a(X)$, $b(X) \in \mathbb{C}[X]$ et $y^2 = X^2-1$, les calculs se faisant de manière naturelle. L'anneau $\mathbb{C}[H]$ est entier sur l'anneau $\mathbb{C}[X]$ qui n'est autre que l'algèbre affine de la droite D, axe des X.

Un point a de D correspond à l'homomorphisme $\phi: f(X) \longmapsto f(a)$ de $A = \mathbb{C}[D]$ dans $\mathbb{C}$.

Soit ψ une place de K à valeurs dans $\mathbb{C}$ prolongeant ϕ. On doit avoir $\psi(y)^2 = a^2-1$.

On en déduit, si $a \neq 1$ l'existence de deux places ψ_1 et ψ_2 de K à valeurs dans $\mathbb{C}$ prolongeant ϕ: elles correspondent aux deux racines de a^2-1 et donc aux deux points d'abcisse a sur H; elles sont finies sur l'algèbre affine $\mathbb{C}[H]$.

2. Soit maintenant H l'hyperbole d'équation XY = 1. Son algèbre affine est $\mathbb{C}[X,Y]/(XY-1) = \mathbb{C}[X,1/X]$. Ce n'est plus un anneau entier sur $\mathbb{C}[D]$. A l'origine O de D correspond l'homomorphisme $\phi: f(X) \longmapsto f(0)$. Il se prolonge en la seule place évidente ψ du corps $K = \mathbb{C}(X)$ des fractions de $\mathbb{C}[H]$. Cette palce n'est plus finie sur $\mathbb{C}[H]$ puisque $\psi(1/X) = \infty$. Elle correspond au point à l'infini de H dans la direction de l'axe OY.

III. Anneaux intégralement clos

1. *Exemples d'anneaux intégralement clos. Anneaux d'entiers algébriques*

Proposition III.1

Soient A *un anneau intègre,* K *son corps des fractions,* L *un corps contenant* K *comme sous-corps et algébrique sur* K.

La fermeture intégrale B *de* A *dans* L *est un anneau intégralement clos de corps des fractions* L.

En particulier, la clôture intégrale de A *est un anneau intégralement clos de corps de fractions* K.

Démonstration

Soit $x \in L$. Il satisfait à une équation de la forme

(1) $\sum_{i=0}^{n} a_i x^i = 0$

où $a_i \in A$ et $a_n \neq 0$: il suffit de multiplier une équation de dépendance algébrique de degré minimal de x sur K par un dénominateur commun de ses coefficients.

On multiplie (1) par a_n^{n-1}, obtenant une équation de dépendance intégrale sur A de l'élément $y = a_n x$. L'élément y appartient à B, et par conséquent, x appartient au corps des fractions de B. Ce corps des fractions est donc égal à L.

Un élément de L entier sur B est entier sur A par transitivité de la dépendance intégrale et appartient donc à B.

Un exemple particulièrement important est celui où $A = \mathbb{Z}$, $K = \mathbb{Q}$ *et où* L *est une extension de degré fini de* $\mathbb{Q}$.

Un tel corps L est alors appelé un *corps de nombres algébriques*.(*)

On démontrera dans le chapitre II que l'anneau B est alors un *anneau* de Dedekind, i.e. un anneau héréditaire intègre (FFAC. chap.5). On démon-

(*) Cette terminologie est quelquefois étendue à une extension algébrique (non nécéssairement de degré fini) de $\mathbb{Q}$.

trera également que dans un tel anneau tout idéal (distinct de l'anneau) est, de manière unique, produit d'idéaux premiers.

Les exemples les plus classiques sont les suivants :

1. $L = \mathbb{Q}(\sqrt{d})$, où d est un entier sans facteur carré (*extension quadratique de* $\mathbb{Q}$).

On démontre (ex. 11) que la fermeture intégrale B de $\mathbb{Z}$ dans L est un $\mathbb{Z}$-module libre de base :

$(1,\sqrt{d})$ si d est congru à 2 ou 3 modulo 4

$(1, \frac{1+\sqrt{d}}{2})$ si d est congru à 1 modulo 4

2. $L = \mathbb{Q}(\zeta)$, où ζ est une racine primitive p-ème de l'unité (p nombre premier impair (*corps cyclotomique*)

On démontre (ex. 21 chap. 5) que la fermeture intégrale de $\mathbb{Z}$ dans L est le $\mathbb{Z}$-module libre de base $\{1,\zeta,\ldots,\zeta^{p-2}\}$.

Un autre exemple important est celui où A est l'anneau $k[X]$ des polynômes à une indéterminée dans un corps k et où L est une extension de degré fini de k(X), i.e. un corps L contenant k(X) comme sous corps et tel que la dimension $[L:k(X)]$ soit finie.

On verra au chapitre 6 que la fermeture intégrale B de A dans L est l'algèbre affine d'une courbe algébrique non nécéssairement plane irréductible définie sur k. Le fait que B soit intégralement clos implique que la courbe est non singulière.

Il est donc facile d'obtenir des exemples d'anneaux non intégralement clos, à partir de courbes algébriques admettant un point singulier. C'est la cas, par exemple, de la courbe algébrique plane (complexe) d'équation $X^2-Y^3 = 0$

Exemple d'anneau non intégralement clos

Soient k *un corps,* X *et* Y *des indéterminées. On va démontrer que l'anneau quotient* $A = k[X,Y]/(X^2-Y^3)$ *est intègre mais n'est pas intégralement clos.*

L'anneau A *est intègre*

On doit démontrer que l'idéal principal $p = (X^2-Y^3)$ de $k[X,Y]$ est premier ou, comme $k[X,Y]$ est factoriel, que X^2-Y^3 est irréductible.

1ère méthode

X^2-Y^3 *est irréductible.*

Soit $X^2-Y^3 = g(X,Y)h(X,Y)$ où $g,h \in k[X,Y]$. Alors,

$d^\circ(g) + d^\circ(h) = 3 \quad \omega(g) + \omega(h) = 2, \quad \omega(g) \leqslant d^\circ(g) \quad \omega(h) \leqslant d^\circ(h)$
(où ω désigne l'ordre en tant que série formelle)

Les seules possibilités sont $d^\circ(g) = \omega(g) = 0$, i.e. g est une constante, ou $d^\circ(h) = \omega(h) = 0$, i.e. h est une constante.

2ème méthode

L'idéal p est premier. Cette méthode est ici un peu plus compliquée.

On va démontrer que, T désignant une indéterminée, *p est le noyau de l'homomorphisme* ϕ *de k-algèbres:* $f(X,Y) \longmapsto f(T^3,T^2)$.

Un élément de $k[X,Y]$ s'écrit de manière unique

$a(Y) + b(Y)X$ modulo (X^2-Y^3) où $a(Y), b(Y) \in k[Y]$
division euclidienne par le polynôme X^2-Y^3, *unitaire en* X

L'image par ϕ d'un tel élément est $a(T^2) + b(T^2)T^3$. Cet élément appartient à $\ker(\phi)$ si et seulement si $a(T^2) = b(T^2) = 0$, i.e. $a(Y)=b(Y)=0$ (un monôme de $a(T^2)$ est de degré pair, un monôme de $b(T^2)T$ est de degré impair)

Donc, $\ker(\phi) \subset (X^2-Y^3)$ et $\ker(\phi) = (X^2-Y^3)$.

L'anneau A n'est pas intégralement clos.

Soient x et y les classes de X et Y modulo (X^2-Y^3) en sorte que $A = k[x,y]$ (après identification de k à un sous-corps de A).

L'élément $z = x/y$ du corps des fractions de A est *entier sur* A puisque $z^2-y = 0$. Il n'appartient pas à A car sinon $X-ZY$ devrait diviser X^2-Y^3, ce qui est impossible parce qu'on devrait avoir $X^2-Y^3 = (X-YZ)\,g(X,Y)$ avec $\omega(g) = 1$, contrairement à l'irréductibilité de X^2-Y^3.

Détermination de la clôture intégrale de A

On remarque que $a = k[T^3,T^2]$. Le corps des fractions de A contient $T = T^3/T^2$.

Il est donc égal à $k(T)$. Comme T est entier sur A, la clôture intégrale de A contient $k[T]$. Comme $k[T]$ est intégralement clos, cette clôture est $k[T]$.

2. Deux propriétés des anneaux intégralement clos

Proposition III.2 (le fait d'être intégralement clos est une propriété ponctuelle)

Soit A un anneau intègre.

Les assertions suivantes sont équivalentes:

(i) A *est intégralement clos*

(ii) A_p *est intégralement clos pour tout idéal premier* p *de* A.

(iii) A_p *est intégralement clos pour tout idéal maximal* m *de* A

Démonstration

Soit f l'injection de l'anneau A dans sa clôture intégrale.

L'assertion (i) (resp.(ii); resp.(iii)) équivaut à la surjectivité de f (resp. de f_p pour tout idéal premier de A; resp. de f_p pour tout idéal maximal m de A).

L'équivalence des trois assertions résulte alors du lemme de globalisation et du lemme suivant qui exprime le fait que la fermeture intégrale commute au passage à un anneau de fractions.

Lemme

Soient A *un sous-anneau d'un anneau* B, S *une partie multiplicative de* A, $\overline{A}$ *la fermeture intégrale de* A *dans* B.

Alors, $S^{-1}\overline{A}$ *est la fermeture intégrale de* $S^{-1}A$ *dans* $S^{-1}B$.

Démonstration du lemme

On sait déjà (proposition I.2) que $S^{-1}\overline{A}$ est entier sur $S^{-1}A$.

Soit x/s un élément de $S^{-1}B$ ($x \in B; s \in S$) entier sur $S^{-1}A$ et soit

$$(x/s)^n + \sum_{i=0}^{n-1} (a_{n-i}/s_{n-i})(x/s)^i = 0$$

une équation de dépendance de x/s sur $S^{-1}A$ ($a_{n-i} \in A$, $s_{n-i} \in S$)

Soit $y = x \prod_{i=0}^{n-1} s_{n-i}$. On obtient une égalité

$(y/1)^n + \sum_{i=0}^{n-1} (b_{n-i}/1)(y/1)^i = 0$ où b_{n-i} appartient à A.

Il existe donc un élément t de S tel que

$$t\left(y^n + \sum_{i=0}^{n-1} b_{n-i} y^i\right) = 0$$

Par multiplication par t^{n-1}, on en déduit que l'élément yt appartient à $\overline{A}$.

Par conséquent, l'élément $x/s = (xt \prod_{i=0}^{n-1} s_i)/(st \prod_{i=0}^{n-1} s_i)$ appartient à $S^{-1}\overline{A}$.

Le lecteur pourra reprendre, dans le cas où $k = \mathbb{C}$, l'exemple d'anneau A non intégralement clos du §1, vérifier que si m est l'idéal maximal $(x-a, y-b)$, où (a,b) appartient à la courbe d'équation $X^2-Y^3 = 0$, l'anneau local A_m est intégralement clos (resp. n'est pas intégralement clos) si $(a,b) \neq (0,0)$ (resp. $a = b = 0$, cas qui correspond à l'origine

qui est un point singulier de la courbe au sens de l'exercice du chapitre 2)

Proposition III.3 (transfert aux anneaux des polynômes)

Soit A *un anneau intégralement clos. L'anneau* $A[X_1,\ldots,X_n]$ *où* $X_1,\ldots,X_n$ *sont des indéterminées est intégralement clos.*

Démonstration (*On peut supposer* n = 1)

Il est commode d'introduire la définition suivante:

Soient A *un anneau intègre,* K *son corps des fractions,* $x \in K$.

On dit que x *est presque entier sur* A *s'il existe* $d \neq 0$, $d \in A$, *tel que, pour tout* $n \in N$, dx^n *appartienne à* A.

Il revient au même de dire que le A-module A[x] est contenu dans le sous-module monogène A(1/d) de K. Il est clair que si x, x' sont presque entiers sur A, il en est de même de x-x' et xx'.

Si l'élément x de K est *entier* sur A, il est *presque entier* sur A. La réciproque est vraie si l'anneau A est *noethérien* car alors le A-module A[x] est de type fini comme sous-module du module noethérien A(1/d).

Un anneau intègre A *est dit complétement intégralement clos si tout élément de son corps de fractions* K *qui est presque entier sur* A *appartient à* A.

On revient à la démonstration de la proposition en démontrant que si l'élément f(X) du corps des fractions de A[X] est presque entier sur A[X], ses coefficients sont presque entiers sur A. Ce corps des fractions est aussi le corps K(X) des fractions de l'anneau K[X].

Il est clair que K[X] est intégralement clos, donc complétement intégralement clos (il est, en effet, principal).

Donc, si f(X) est presque entier sur A|X|, $f(X) = a_r X^r + a_{r+1} X^{r+1} + \ldots$ où $a_i \in K$ et $a_r \neq 0$. Soit $d(X) = b_s X^s + \ldots$ où $b_j \in A$ tel que $d(X)f(X)^n \in A[X]$ pour tout n.

On en déduit que $b_s a_r^n \in A$, pour tout n, donc que a_r est presque entier sur A.

Alors, $f(X) - a_r X^r$ est presque entier sur A et on en déduit que a_{r+1} est presque entier sur A. On procède ainsi de proche en proche.

Soit $f(X) \in K(X)$ un élément entier sur A[X]. Il existe un sous-anneau noethérien A_o de A contenant les numérateurs et dénominateurs des coefficients de f(X) et les coefficients des polynômes A[X] apparaissant

dans une équation de dépendance intégrale de f(X) sur A[X]. Les coefficients de f(X) sont presque entiers sur A_o, donc entiers sur A_o. Si A est intégralement clos, ils appartiennent à A.

Exercices du chapitre 4

(1). Expliciter une équation de dépendance intégrale sur $\mathbb{Z}$ du nombre complexe $\sqrt{2}+i$ où $i^2 = -1$, 1°) directement, 2°) par utilisation du $\mathbb{Z}$-module engendré par les nombres 1, $\sqrt{2}$, i, $i\sqrt{2}$ suivant la démonstration de (iii) $\Longrightarrow$ (i) du théorème I.3.

(2). Les nombres complexes suivants sont-ils entiers sur $\mathbb{Z}$: $\frac{1+3i}{3}$, $\frac{1+\sqrt{5}}{2}$, $\frac{1+\sqrt{-5}}{2}$?

(3). Déterminer la clôture intégrale des anneaux suivants: $\mathbb{Z}[i]$ où $i^2 = -1$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Z}[\sqrt{5}]$, $\mathbb{Z}[j]$ où j est racine primitive cubique de 1.

(4). Soit p un nombre premier. Démontrer que l'anneau local $\mathbb{Z}_{(p)}$ est un sous-anneau de $\mathbb{Q}$ maximal dans l'ensemble des sous-anneaux de $\mathbb{Q}$ distincts de $\mathbb{Q}$.

Analogue à partir de l'anneau k[X] des polynômes à une indéterminée à coefficients dans un corps k.

(5). Soient B un anneau intègre, A un sous-anneau de B tel que B soit entier sur A, b un idéal non nul de B. Que peut-on dire de l'idéal $b \cap A$ de A ?

(6). Soient B un anneau, A un sous-anneau tel que B soit entier sur A, $q_1 \subset \ldots \subset q_r$ une suite strictement croissante d'idéaux premiers de B. Que peut-on dire de la suite $q_1 \cap A \subset \ldots \subset q_r \cap A$ d'idéaux de A ?

(7). Démontrer que, pour prouver la conjecture de Fermat, il suffit de démontrer que pour $n = 4$ ou n premier impair l'équation $x^n+y^n = z^n$ n'a pas de solution (x,y,z) dans $\mathbb{Z}$ telle que $xyz \neq 0$.

(8). 1. Démontrer, suivant les indications de l'introduction du chapitre 4, qu'une représentation paramétrique des solutions en nombres entiers de l'équation diophantienne $x^2+y^2 = z^2$ est donnée par

$x = d(u^2-v^2)$ $y = 2duv$ $z = d(u^2+v^2)$, où u, v sont des entiers positifs premiers entre eux, et l'analogue obtenue en échangeant les rôles de x et y.

2. On veut démontrer (par la *méthode de la descente infinie* de P. de Fermat)

l'inexistence de solution en nombres entiers *non nuls* de l'équation diophantienne $x^4+y^4 = z^2$. *On raisonne par l'absurde.*

Soit (x,y,z) *une solution avec* $x > 0$, $y > 0$, $z > 0$ *et* z *minimal.* On remarquera qu'alors $(x,y) = 1$. *On supposera* x *impair,* y *pair.* Il existe donc des entiers premiers entre eux u et v tels que: $x^2 = u^2-v^2$, $y^2 = 2uv$, $z = u^2+v^2$.

a. Démontrer que u est impair et v pair.

b. On pose $\bar{v} = 2v'$. Démontrer que $v' = v''^2$, $u = u''^2$ où u'' et v'' sont des entiers premiers entre eux.

Remarquer l'égalité $(2v''^2)^2 + x^2 = (u''^2)^2$.

c. Justifier l'existence d'entiers positifs a et b premiers entre eux et tels que $u''^2 = a^2+b^2$, $v''^2 = ab$ puis d'entiers a' et b' positifs tels que $a = a'^2$, $b = b'^2$.

d. Vérifier l'égalité $a'^4+b'^4 = u''^2$. Comparant u et u'', trouver une contradiction.

3. Démontrer que l'équation diophantienne $x^4+y^4 = z^4$ n'a pas de solution en nombres entiers *non nuls*.

(9). *Soit* A *un anneau intègre.*

Un *stathme euclidien* sur A est une application: $x \longmapsto |x|$ de $A-\{0\}$ dans $\mathbb{N}$ possédant les propriétés suivantes:

1. si $a,b \in A-\{0\}$ $\quad |ab| \geqslant |a|$
2. $a,b \in A$, il existe q et $r \in A$ tels que
   $b = qa + r$ où $r = 0$ ou $|r| < |a|$

Un anneau euclidien est un anneau intègre muni d'un stathme euclidien.

1. Démontrer que $\mathbb{Z}$ est euclidien et que l'anneau $k[X]$ des polynômes à une indéterminée X à coefficients dans un corps k est euclidien.

2. Démontrer qu'un anneau euclidien est principal (même démonstration que pour $\mathbb{Z}$). Donner des exemples d'anneaux ne possédant pas de stathme euclidien.

3. Soit $A = \mathbb{Z}[i]$ l'anneau des entiers de Gauss ($i^2 = -1$).

Démontrer que l'application: $a+ib \longmapsto (a+ib)(a-ib) = a^2+b^2 (a,b \in \mathbb{R})$ est un stathme euclidien sur A (Soient α, $\beta \in A$, $\alpha \neq 0$, $\gamma = \beta\alpha^{-1} \in \mathbb{Q}(i)$, $= c'+id'$, c et d les entiers tels que $|c'-c| < 1/2$ et $|d'-d| < 1/2$. Démontrer que $|\beta - (c+id)\alpha| < |\alpha|$.

4. Expliciter le groupe multiplicatif des éléments inversibles de $\mathbf{Z}[i]$.

Démontrer que si $\alpha \in \mathbf{Z}[i]$ est tel que $|\alpha|$ soit un nombre premier, α est un élément premier de $\mathbf{Z}[i]$; Etudier la réciproque.

5. Soit $j = \cos(2\pi/3) + \sin(2\pi/3)$ (racine primitive cubique de l'unité, $A = \mathbf{Z}[j]$.

Le nombre j est racine du polynôme X^2+X+1 dont l'autre racine est j^2 et qui est irréductible dans $\mathbf{Q}[X]$. Un élément de A s'écrit de manière unique $a+bj$ $(a,b \in \mathbf{Z})$.

Démontrer que l'application: $a+bj \longmapsto a^2-ab+b^2$ est un stathme euclidien de A. (même procédé que pour l'anneau des entiers de Gauss)

6. Expliciter le groupe multiplicatif des éléments inversible de $\mathbf{Z}[j]$.

Démontrer qu'un élément α de $\mathbf{Z}[j]$ tel que $|\alpha|$ soit un nombre premier est premier. En déduire que 1-j est premier. Quel est le quotient $\mathbf{Z}[j]/(1-j)$?

(10). Démontrer que l'anneau des entiers du corps quadratique $\mathbf{Q}(\sqrt{-5})$ n'est pas factoriel. (Utiliser les égalités $21 = 3.7 = (4+\sqrt{-5})(4-\sqrt{-5})$

On sait démontrer que les seuls corps quadratiques $\mathbf{Q}(\sqrt{-d})$, où d est entier positif sans facteur carré, dont l'anneau des entiers est principal (ou ce qui est équivalent pour les anneaux de ce type factoriel) sont obtenus pour d = 1,2,3,7,11,19,43,67,163.

On savait depuis les travaux de Heilbronn et Linfoot (*Quaterly Journ. of math. Oxford, 5, 1934, 150-160 et 293-301)* qu'il ne pouvait exister en plus des corps mentionnés qu'un seul autre. Dans: *A complete determination of the complex quadratic Fields of class number one. Michigan Math. j., 14, 1967,1-27,* H.M. Stark a démontré que cet éventuel corps supplémentaire n'existait pas.

On trouvera dans l'article: *About euclidean Rings. Journal of algebra. 19, 1971, 282-301* de P.Samuel la démonstration du fait que seuls les anneaux obtenus pour d = 1,2,3,7,11 sont euclidiens pour la norme ou n'importe quel stathme euclidien. Les anneaux obtenus pour d = 19,43,67, 163 sont donc principaux mais ne sont pas euclidiens.

(11). Soient d un entier (positif ou négatif) sans facteur carré, K le sous-corps de $\mathbb{C}$ des nombres de la forme $a+b\sqrt{d}$ $(a,b \in \mathbf{Q})$, A la fermeture intégrale de $\mathbf{Z}$ dans K.

Il existe deux $\mathbf{Q}$-automorphismes de K (isomorphisme de K sur K lais-

sant invariant tout élément de $\mathbb{Q}$: l'application identique et la conjugaison $s : a+b\sqrt{d} \longmapsto a-b\sqrt{d}$.

On appelle *trace* (resp. *norme*) de l'élément x de K le nombre $x+s(x)$ (resp. $xs(x)$). C'est un élément de $\mathbb{Q}$.

1. Démontrer les équivalences : (i) x appartient à A
(ii) la trace et la norme de x appartiennent à $\mathbb{Z}$

2. Soit $x = a+b\sqrt{d}$ $(a,b \in \mathbb{Q})$ un élément de A.

Démontrer que 2a et 2b appartiennent à $\mathbb{Z}$ (On utilisera le fait que $(2a)^2-d(2b)^2$ appartient à $\mathbb{Z}$).

On pose $a = a'/2$, $b = b'/2$. Démontrer que b' ne peut être impair que si $d = 1 \bmod.4$.

3. En déduire que A est un $\mathbb{Z}$-module libre de base

$1, \sqrt{d}$ si $d = 2$ ou $3 \bmod.4$

$1, \frac{1+\sqrt{d}}{2}$ si $d = 1 \bmod.4$

Examiner le cas $d = -1$. (Anneaux des entiers de Gauss)

(12). Démontrer que l'ensemble des idéaux fractionnaires non nuls d'un anneau de Dedekind ((FFAC.)chap.5.11.§2) est un groupe multiplicatif dont l'ensemble des idéaux principaux non nuls est un sous-groupe.

Le groupe quotient est appelé le groupe de classes d'idéaux de l'anneau de Dedekind. S'il est fini, on note h son ordre et on l'appelle le nombre de classes de l'anneau.

L'anneau des entiers d'un corps de nombres algébriques (extension de degré fini de $\mathbb{Q}$) est un anneau de Dedekind (chap.12.théorème IV.5). Le groupe des classes d'idéaux d'un tel anneau est fini (théorème de Dirichlet). Dire qu'un tel anneau est principal (ou factoriel, ce qui est équivalent pour ce type d'anneaux) c'est dire que $h = 1$.

Le calcul de h indique que l'anneau des entiers du corps cyclotomique $\mathbb{Q}(z)$ où z est racine primitive 23-ème de l'unité n'est pas principal (confer. Borevitch-Shafarevich. Number Theory. Pure and Applied Mathematics. table 8. p. 429).

Démontrer, de manière élémentaire, que cet anneau n'est pas principal.

(L'auteur ne connaît pas la solution de cet exercice et ignore s'il en existe une abordable)

(13). Soient A un anneau intègre, K son corps des fractions. On note K^* (resp. A^*) le groupe multiplicatif des éléments non nuls de K (resp. inversibles de A).

On définit une relation $\leqslant$ dans K^* par $x \leqslant y$ si et seulement si il existe $a \in A$ tel que $x = ay$.

1. Démontrer que $\leqslant$ est une relation de préordre dans K^*.

2. Démontrer que $\leqslant$ définit par passage au quotient une relation d'ordre sur le groupe quotient $\Gamma = K^*/A^*$ qui munit Γ d'une structure de *groupe ordonné*. On note encore $\leqslant$ cette relation d'ordre dans Γ.

3. Démontrer que Γ est totalement ordonné si et seulement si A est un anneau de valuation de K. Le groupe K^*/A^* est alors appelé le *groupe de la valuation* définie par A.

4. Soit alors v l'application de K dans Γ définie comme suit:

$v(0) = \infty$; si $x \in K^*$, $v(x)$ est la classe de x modulo A^* (valuation de A)

Démontrer les propriétés: (1) $v(xy) = v(x) + v(y)$

(2) $v(x+y) \geqslant \inf(v(x), v(y))$

5. Soit, réciproquement, v une application de K^* dans un groupe totalement ordonné satisfaisant à (1) et (2). On pose $v(0) = \infty$.

Démontrer que le sous-anneau $\{x \in K / v(x) \geqslant 0\}$ de K est un anneau de valuation de K. Que peut-on dire de $\mathrm{im}(v)$?

6. Soient A un anneau de valuation, p un idéal premier de A.

Démontrer que A_p est un anneau de valuation du corps K des fractions de A et que A/p est un anneau de valuation du corps résiduel de A.

Soit v la valuation associée à A. Etudier $v(A-p)$. Démontrer que c'est l'ensemble des éléments $\geqslant 0$ d'un sous-groupe Δ de Γ tel que $0 \leqslant b \leqslant a$ et $a \in \Delta$ implique $b \in \Delta$. (Un tel sous-groupe est dit *isolé*).

Quels sont les groupes de valeurs de A_p et A/p ?

(14). Soient k un corps, Γ un groupe abélien totalement ordonné, $R = k[\Gamma]$ l'algèbre du groupe Γ sur k. (On rappelle que $k[\Gamma]$ est le groupe additif $k^{(\Gamma)}$ de base $(e_\gamma)_{\gamma \in \Gamma}$, où e_γ est l'application de Γ dans k telle que $e_\gamma(\gamma) = 1$ et $e_\gamma(\gamma') = 0$ si $\gamma' \neq \gamma$, la multiplication étant donnée par $e_\gamma e_{\gamma'} = e_{\gamma+\gamma'}$). Comme le groupe Γ est abélien, R est un anneau *commutatif*.

Démontrer que R est intègre.

Un élément non nul x de R s'écrit de manière unique $\lambda_1 e^{\gamma_1}+\ldots+\lambda_n e^{\gamma_n}$ où $\lambda_i \neq 0$ et $\gamma_1 < \ldots < \gamma_n$. On pose $v(x) = \gamma_1$. Démontrer que l'application $v: x \longmapsto v(x)$ de $R-\{0\}$ dans Γ se prolonge, de manière unique, en une valuation du corps K des fractions de A de groupe de valuation Γ.

(15). On dit que l'anneau A est *semi-héréditaire* si tout idéal de *type fini* de A est projectif. Par exemple, un anneau héréditaire ((FFAC.chap. 5.II.2) est semi-héréditaire.

1. Démontrer qu'un anneau de valuation est semi-héréditaire.

2. Démontrer que, si l'anneau A est semi-héréditaire, tout sous-module de *type fini* d'un A-module *libre* est somme directe d'un nombre fini de modules isomorphes à des idéaux de type fini de A.

(Se ramener au cas où le A-module libre L est de type fini et faire une démonstration par récurrence sur le cardinal d'une base de L).

En déduire les équivalences pour un anneau A:

(i) A est semi-héréditaire

(ii) tout sous-module de *type fini* d'un module projectif est projectif

3. Démontrer qu'un sous-module de *type fini* d'un module libre sur un anneau de valuation A est libre.

Démontrer qu'un anneau de valuation est cohérent. Est-il absolument plat ?

(16). (Démonstration de la transcendance de e - Hermite.1873)

On suppose le nombre $e = 1+\frac{1}{1!}+\frac{1}{2!}+\ldots$ *algébrique sur* $\mathbb{Q}$. Soit $a_m e^m+\ldots+a_1 e+a_0 = 0$ une équation de dépendance de e sur $\mathbb{Q}$, avec $a_i \in \mathbb{Z}$ et $a_0 \neq 0$.

Soit p un nombre premier (que l'on fera tendre vers ∞ en fin de démonstration.)

On pose $f(X) = \dfrac{X^{p-1}(X-1)^p\ldots(X-m)^p}{(p-1)!}$ et

$F(X) = f(X) + f'(X) +\ldots+ f^{(mp+p-1)}(X)$ où $f^{(i)}(X)$ désigne la dérivée i-ème de f(X).

Déduire de l'égalité $\frac{d}{dX}(e^{-X}F(X)) = e^{-X}f(X)$, pour tout $i\in\{0,\ldots,m\}$, l'égalité

$$a_i\int_0^i e^{-X}f(X)dX = a_iF(0)-a_ie^{-i}F(i)$$

puis

$$(1)_{i\overset{\Sigma}{=}0}^{m}(a_ie^i\int_0^i e^{-X}f(X)dX) = -_{i\overset{\Sigma}{=}0}^{m}\ _{j\overset{\Sigma}{=}0}^{mp+p-1}\ a_if^{(j)}(i)$$

Démontrer que $f^{(j)}(i)$ est un entier. En déduire l'égalité

$$(2)_{i\overset{\Sigma}{=}0}^{m}(a_ie^i\int_0^i e^{-X}f(X)dX) = Kp + a_0(-1)^p\ldots(-m)^p$$

où $K \in \mathbb{Z}$ puis que ,pour p assez grand, le second membre de (2) n'est pas nul.

Démontrer enfin, que quand p tend vers ∞, le premier membre de (2) tend vers 0, obtenant ainsi une contradiction.

(17). (Démonstration de la transcendance de π. Lindemann.1882)

On suppose le nombre π algébrique sur $\mathbb{Q}$ ou ce qui revient au même le nombre $i\pi$, où $i^2=-1$, algébrique sur $\mathbb{Q}$.

Soit alors $\theta_1(X) = \mathrm{irr}(X,i\pi,\mathbb{Q})$ polynôme unitaire de plus petit degré à coefficients dans $\mathbb{Q}$ admettant $i\pi$ pour racine, $a_1 = i\pi,\ldots,a_n$ les racines dans $\mathbb{C}$ de $\theta_1(X)$.

Utilisant les fonctions symétriques élémentaires de $a_1,\ldots,a_n$ démontrer l'existence de $\theta(X) \in \mathbb{Z}[X]$ dont les racines soient les exposants non nuls $b_1,\ldots,b_r$ de e dans le développement de

$$(e^{a_1}+1)\ \ldots\ (e^{a_n}+1) = e^{b_1}+\ \ldots\ +e^{b_r}+k, \text{ où } k \in \mathbb{Z}.$$

Soit $\theta(X) = cX^r+c_1X^{r-1} + \ldots + c_r$. Soit p un nombre premier (que l'on fera tendre vers ∞ en fin de démonstration). On pose

$$f(X) = \frac{c^sX^{p-1}\theta(X)^p}{(p-1)!} \quad \text{où } s = rp-1 \quad \text{et } F(X) = f(X) + f'(X)+\ldots\ldots$$

$\ldots+ f^{(s+p)}(X)$.

Démontrer l'égalité $\frac{d}{dX}(e^{-X}F(X)) = e^{-X}f(X)$. En déduire l'égalité

$e^{-X}F(X) - F(0) = -\int_0^X e^{-Y}f(Y)dY$ puis, par changement de variables,

$F(X) - e^XF(0) = -X\int_0^1 e^{(1-t)X}f(tX)dt$ et enfin l'égalité

$$_{i\overset{\Sigma}{=}1}^{r}F(b_i) + kF(0) = -_{i\overset{\Sigma}{=}1}^{r}b_i\int_0^1 e^{(1-t)b_i}f(tb_i)dt$$

(où l'entier k a été défini plus haut).

Démontrer que pour p assez grand, le prmeier membre de cette égalité est un entier non divisible par p et donc non nul et que, quand p tend vers ∞, le second membre tend vers 0, obtenant ainsi une contradiction.

(18) *Nombres de* Liouville

1. On va démontrer qu'un nombre complexe non rationnel x est algébrique sur $\mathbb{Q}$ si et seulement si il se laisse mal approcher en un sens convenable par les nombres rationnels.

Si q est un entier naturel, p/q, où $p \in \mathbb{Z}$, désigne dans la suite un nombre rationnel valeur approchée à 1/q près par défaut ou excés de x.

Si $f(X) \in \mathbb{Q}[X]$, on désigne par K_f un entier $> \sup|f'(y)|$ où y parcourt la boule fermée de centre x et de rayon 1 .

a) On suppose dans cette question que x est racine de

$$f(X) = a_o X^n + a_1 X^{n-1} + \ldots + a_n \in \mathbb{Z}[X]$$

avec $a_o \neq 0$ et que p/q est distinct d'une racine rationnelle de f(X), condition sûrement réalisée pour q grand.

Déduire de l'inégalité de la moyenne

$$|f(x)-f(p/q)| < K_f|x-p/q|$$

l'inégalité $|x-p/q| > 1/(K_f q^n)$ et donc $|x-p/q| > 1/q^{n+1}$ Si $q \geqslant K_f$.

b) En déduire que s'il existe une infinité d'entiers naturels q tels que $|x-p/q| \leqslant 1/q^{n+1}$, le nombre x est transcendant sur $\mathbb{Q}$.

2. Un *nombre de* Liouville est un nombre réel de la forme

$$x = \sum_{n=1}^{\infty} \frac{a_n}{10^{n!}}$$

où les a_n sont des entiers compris entre 0 et 9 pas tous nuls à partir d'un certain rang.

Déduire de 2., en considérant les valeurs de q égales à $10^{n!}$, qu'un nombre de Liouville est transcendant sur $\mathbb{Q}$.

Associant au nombre de Liouville x écrit ci dessus le nombre réel $\sum_{n=1}^{\infty} \frac{a_n}{10^n}$, démontrer que l'ensemble des nombres de Liouville a la puissance du continu.

Le lecteur intéressé par des résultats de transcendance plus fins et plus complets pourra se référer, par exemple, au livre suivant: Introduction aux nombres transcendants. T. Schneider. Gauthier Villars - 1959.

CHAPITRE 5

Éléments de théorie des corps commutatifs

Le lecteur connaît sans doute le corps non commutatif $\mathbb{H}$ des quaternions, inventé par Hamilton en 1853 pour permettre un calcul algébrique des vecteurs libres de l'espace $\mathbb{R}^3$ et une interprétation des rotations de cet espace. (exercice 8)

Il existe donc des corps non commutatifs et leur étude est important. Toutefois, conformément au propos général de ce livre, on se limitera ici à l'étude des seuls corps commutatifs. Sauf au début de I.4 *les corps considérés seront donc toujours commutatifs.*

Deux raisons fondamentales sont à la base du développement de cette théorie des corps commutatifs. La première, historiquement, est son lien avec la théorie des équations algébriques. La seconde est le fait que l'étude de certaines extensions dites de type fini d'un corps coincide avec celle de la partie de la géométrie algébrique qui traite des problèmes dits birationnels.

Dans la théorie des équations algébriques, on associe à un polynôme non constant, à une indéterminée, à coefficients (pour fixer les idées) dans $\mathbb{Q}$, un sous-corps de $\mathbb{C}$, appelé *corps de décomposition du polynôme,* qui est le plus petit sous-corps contenant $\mathbb{Q}$ et les racines du polynôme.

Le groupe des automorphismes de ce corps de décomposition laissant invariant tous les éléments de $\mathbb{Q}$ est appelé le *groupe* de Galois du polynôme.

Les études du polynôme, de son corps de décomposition et de son groupe de Galois sont liées. Des théorèmes de théorie des groupes s'interprètent ainsi en théorie des équations. Le théorème d'Abel affirmant la simplicité du groupe alterné A_n pour $n \geqslant 5$, a, par exemple, pour conséquence que l'équation "générique" de degré $n \geqslant 5$ ne peut être résolue par radicaux (comme les équations de degrés 2, 3 ou 4).

En géométrie algébrique sur un corps k, on associe à certains êtres géométriques, les *variétés algébriques définies sur* k, un corps de fonctions admettant k comme sous-corps. Deux variétés définies sur k sont dites *birationnellement équivalentes* si elles admettent même corps de fonctions. La géométrie algébrique birationnelle s'intéresse aux invariants des classes de variétés birationnellement équivalentes.

Par définition même, elle étudie donc certaines extensions, les extensions dites de *type fini*, du corps k.

Dans I, nous avons donné les définitions d'une extension, démontré l'existence des bases de transcendance.

Dans II, on obtient des extensions d'un corps donné soit par adjonction d'une racine d'un polynôme soit par adjonction de toutes les racines. On construit également la clôture algébrique d'un corps.

Le paragraphe III est consacré à la théorie de Galois des extensions finies et aux notions qui s'y rattachent de normalité et séparabilité.

Enfin, dans IV, nous donnons quelques indications sur les extensions radicielles et démontrons l'existence des p bases.

I. Extensions algébriques et transcendantes

1. Définitions et rappels

Définition

Un corps k *est un anneau commutatif non nul vérifiant les assertions équivalentes*

(i) tout élément non nul de k *est inversible*

(ii) l'ensemble $k^* = k - \{0\}$ *muni de la multiplication est un groupe, le groupe multiplicatif de* k.

Voici quelques résultats simples sur cette structure. *Soit* k *un corps*.

1. Les seuls idéaux de k sont (0) et k. L'idéal (0) est l'unique idéal maximal de k. Il est premier. En conséquence, *le corps* k *est un anneau intègre*.

2. Un homomorphisme f de k dans un anneau *non nul* K, par exemple un corps, est *injectif* car, puisque $f(1) \neq 0$, ker(f) est différent de k et donc égal à (0).

Définition

1. *Un sous-corps de* k *est un sous-anneau* k' *de* k *muni par les lois de composition induites par celles de* k *d'une structure de corps.*

Le groupe multiplicatif $k'^* = k' - \{0\}$ est alors un sous-groupe du groupe multiplicatif $k^* = k - \{0\}$.

2. *Une extension d'un corps* k' *est la donnée d'une* k'- *algèbre* k *où l'anneau* k *est un corps.*

L'homomorphisme structural, nécéssairement injectif, de k' dans k permet alors d'identifier k' à un sous-corps de k.

On aura souvent dans la suite à contruire des extensions d'un corps donné k'.

On identifiera le plus souvent k' *à des sous-corps de telles extensions.*

Caractéristique

On rappelle, d'autre part, que la *caractéristique* d'un anneau A est l'entier naturel n tel que $\ker(\phi) = (n)$ où ϕ est l'homomorphisme naturel de $\mathbb{Z}$ dans A ((FFAC).chap.2.I.4). Comme $\mathbb{Z}/\ker(\phi)$ est isomorphe à un sous-anneau de A, *si l'anneau* A *est intègre* et, en particulier, s'il est un corps, l'idéal $\ker(\phi)$ de $\mathbb{Z}$ est premier et donc *la caractéristique de* A *est soit* 0 *soit un nombre premier* p.

Corps de caractéristique 0. Exemples: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

L'homomorphisme ϕ de $\mathbb{Z}$ dans le corps k de caractéristique 0 se prolonge en un homomorphisme, nécessairement injectif du corps $\mathbb{Q}$ dans k qui permet d'identifier $\mathbb{Q}$ à un sous-corps de k, *le corps premier de* k.

Réciproquement, si k contient un sous-anneau isomorphe à $\mathbb{Q}$, il est de caractéristique 0.

Corps de caractéristique un nombre premier p. Exemple: $\mathbb{F}_p = \mathbb{Z}/(p)$

L'homomorphisme ϕ de $\mathbb{Z}$ dans le corps k de caractéristique p définit un homomorphisme, nécessairement injectif, du corps $\mathbb{F}_p = \mathbb{Z}/(p)$ dans k qui permet d'identifier $\mathbb{F}_p$ à un sous-corps de k, *le corps premier de* k.

Réciproquement, si k contient un sous-corps isomorphe à $\mathbb{F}_p$, il est de caractéristique p.

Degré d'une extension

La donnée d'une extension K/k *du corps* k *est, en particulier,* par oubli de la structure multiplicative de K, *celle d'un* k*-espace vectoriel.*

La dimension $[K:k]$ *de cet espace vectoriel est appelé le degré de l'extension.*

Ce degré peut être *fini*: c'est ainsi que $[\mathbb{C}:\mathbb{R}] = 2$, ou *infini*: c'est le cas de l'extension $\mathbb{R}/\mathbb{Q}$ car $\mathbb{Q}$ est dénombrable mais $\mathbb{R}$ ne l'est pas.

Le degré est invariant par isomorphisme, deux extensions de k étant dites isomorphes si les k-algèbres le sont.

Le degré jouit d'une importante propriété de multiplicativité qui permet déjà de démontrer des résultats non évidents.

Proposition I.1 (multiplicativité du degré)

Soient k *un corps,* K/k *une extension de* k, L/K *une extension de* K.

Alors L *est de manière naturelle* (par exemple, par composition des homomorphismes structuraux) *une extension de* k.

On a l'égalité

$$[L:k] = [L:K][K:k]$$

Démonstration

Si $(x_i)_{i\in I}$ (resp. $(y_j)_{j\in J}$) est une base du k-espace vectoriel K (resp. du K-espace vectoriel L) en sorte que

$[K:k] = \mathrm{card}(I)$ et $[L:K] = \mathrm{card}(J)$, $(x_i y_j)_{(i,j)\in I\times J}$ est une base du k-espace vectoriel L. Donc, $[L:k] = \mathrm{card}(I\times J) = \mathrm{card}(I)\times \mathrm{card}(J) = [K:k]\,[L:K]$.

Exemples d'extensions

1. *Soient* k *un corps,* $(X_i)_{i\in I}$ *une famille d'indéterminées.*

Le corps des fractions de l'anneau $k[X_i]_{i\in I}$ des polynômes est noté $k(X_i)_{i\in I}$ et appelé le *corps de fractions rationnelles en les indéterminées* $(X_i)_{i\in I}$ à coefficients dans k.

C'est de manière naturelle une extension de k. Une extension de k isomorphe à une telle extension est dite *transcendante pure.*

2. *Une extension* K/k *de* k *est dite algébrique si* K *est algébrique sur* k.

Par exemple, l'extension $\mathbb{C}/\mathbb{R}$ de $\mathbb{R}$ est algébrique.

L'étude des extensions algébriques est importante en particulier dans la théorie des équations. Elle est évidemment insuffisante: l'extension $\mathbb{R}/\mathbb{Q}$ par exemple n'est pas algébrique: l'ensemble des nombres algébriques est dénombrable et $\mathbb{R}$ n'est pas dénombrable; la géométrie algébrique conduit aussi à des extensions qui ne sont pas algébriques.

On va démontrer dans les paragraphes suivants qu'étant donnée une extension K/k de k il existe une extension transcendante pure L/k d'ailleurs unique à isomorphisme près, telle que K soit extension algébrique de L.

L'étude d'une extension de corps se ramène donc à celle d'une extension transcendante pure (c'est souvent la partie la plus facile) *puis à celle d'une extension algébrique.*

Polynôme irréductible d'un élément algébrique

Soient K *un corps,* k *un sous-corps de* K, x *un élément de* K.

L'élément x est algébrique sur k si et seulement si $k[x]$ est un k-espace vectoriel de dimension finie.

Si x *est algébrique sur* k, l'idéal $\{g(X) \in k[X] / g(x) = 0\}$ est non nul. Il existe alors un polynôme unitaire et un seul f(X) engendrant cet idéal principal. C'est le polynôme unitaire $k[K]$ de degré minimal admettant x pour racine.

On l'appelle le *polynôme irréductible de* x sur k et *on le note* irr(X,x,k).

Proposition I.2

Soient K/k *une extension de* k, $x \in K$ *algébrique sur* k, n *le degré de* irr(X,x,k).

Alors, $\{1,x,\ldots,x^{n-1}\}$ *est une base du* k*-espace vectoriel* $k[x]$ *et donc* $[k[x]:k] = n$.

Démonstration

On sait que $\{1,x,\ldots,x^{n-1}\}$ est un système de générateurs du k-espace vectoriel $k[x]$.

(Chap.4.Théorème I.3). Il est libre car sinon il existerait g(X) non nul $\in k[X]$ de degré n-1 tel que $g(x) = 0$

Fermeture algébrique d'un sous-corps dans un corps

Soient K *un corps,* k *un sous-corps de* K.

Si x *est un élément de* K *non nul et algébrique sur* k, x^{-1} *est algébrique sur* k:

Soit, en effet, $f(X) = \text{irr}(X,x,k) = X^n + a_1X^{n-1}+\ldots+a_n$. Par minimalité de $d^\circ(f)$, $a_n \neq 0$. Donc, $-(a_n)^{-1}(x^{n-1}+\ldots+a_{n-1})$ est l'inverse de x dans K.

Ainsi, *la fermeture algébrique de* k *dans* K *est un sous-corps de* K *contenant* k.

Norme et trace d'un élément d'une extension de degré fini

Soient k *un corps,* K/k *une extension de degré fini de* k, $\{e_1,\ldots,e_n\}$ *une base du* k*-espace vectoriel* K, $x \in K$.

Si $xe_i = \sum_{j=1}^{n} a_{ij}e_j (i = 1,\ldots,n)$, la méthode indiquée dans la démonstration du théorème I.3 du chapitre 4 montre que x est racine du polynôme unitaire $f(X) = \det(X\delta_{ij} - a_{ij})$ de $k[X]$. Soit $f(X) = X^n+b_1X^{n-1}+\ldots+b_n$.

On laisse au lecteur le soin de vérifier que $f(X)$ est indépendant de la base choisie.

On appelle *trace de* x *dans* K/k l'élément $\sum_{i=1}^{n} a_{ii}$. C'est donc au signe près la trace de la matrice (a_{ij}). C'est aussi $-b_1$. *On note* $Tr_{K/k}(x)$ la trace.

On appelle *norme de* x *dans* K/k l'élément $(-1)^n \det(a_{ij})$ de k. C'est $(-1)^n b_n$. *On note* $N_{K/k}(x)$.

Les égalités $Tr_{K/k}(x+x') = Tr_{K/k}(x)+Tr_{K/k}(x')$ $(x,x' \in K)$

$Tr_{K/k}(ax) = a\, Tr_{K/k}(x)$ $(x \in K,\ a \in k)$

sont claires.

Donc, *l'application* $x \longmapsto Tr_{K/k}(x)$ *est une forme linéaire sur* K *et l'application* $(x,y) \longmapsto Tr_{K/k}(xy)$, utilisée dans certaines questions, *est une forme bilinéaire sur* $K\times K$.

La norme possède, elle, une *propriété de multiplicativité*: soient $x, y \in K$, $xe_i = \sum_{j=1}^{n} a_{ij}e_j$, $ye_j = \sum_{j=1}^{n} b_{jk}e_k$. Il est clair que

$xye_i = \sum_{k=1}^{n} (\sum_{j=1}^{n} a_{ij}b_{jk})e_k$.

On en déduit l'égalité $N_{K/k}(xy) = N_{K/k}(x)N_{K/k}(y)$. De plus, si $a \in k$ $N_{K/k}(ax) = a^n N_{K/k}(x)$.

Soit enfin L *un sous-corps de* K *contenant* k *et soit* $x \in L$.

On a l'égalité $Tr_{K/k}(x) = [K:L]\ Tr_{L/k}(x)$

$$N_{K/k}(x) = N_{L/k}(x)^{[K:L]}$$

Soit, en effet, $\{e_1,\ldots,e_r\}$ une base de L/k, $\{f_1,\ldots,f_s\}$ une base de K/L.

Alors, $\{e_i f_j\}_{i=1,\ldots,r;j=1,\ldots,s}$ est une base de K/k que l'on peut utiliser pour calculer $Tr_{K/k}(x)$ et $N_{K/k}(x)$. On remarque en effet que la matrice de x par rapport à cette base est formée de blocs diagonaux égaux à la matrice de x par rapport à la base $\{e_i\}$ en nombre $m = [L:K]$ les autres éléments étant nuls.

Corollaire de la proposition I.2

Avec les notations de la proposition I.2, soit $f(X) = irr(X,x,k) = X^n+b_1X^{n-1}+\ldots+b_n$.

Alors, $Tr_{k(x)/k} = -b_1$ *et* $N_{k(x)/k}(x) = (-1)^n b_n$.

Démonstration

On prend pour base du k-espace vectoriel $k(x)$ la base (e_i) où

$e_i = x^{i-1}$, $(i = 1,\ldots,n)$.

Compte tenu des égalités $xe_i = e_{i+1}$ si $i < n-1$, $xe_n = x^n = -b_n - \ldots - b_1 x^{n-1}$, on voit que la matrice (a_{ij}) telle que $xe_i = \sum_{j=1}^{n} a_{ij} e_j$ a tous ses éléments nuls sauf ceux de la n-ème colonne qui sont $-b_n, -b_{n-1},\ldots,-b_1$ et ceux de la diagonale immédiatement sous la diagonale principale qui sont tous égaux à 1.

Il suffit alors de revenir à la définition de la trace et de la norme.

2. Sous-extensions d'une extension de corps

Soient K *un corps,* k *un sous-corps de* K, X *une partie de* K.

L'ensemble Φ des sous-corps de K contenant k et X est non vide puisque il contient K. Il admet un plus petit élément: l'intersection des éléments de Φ. Ce plus petit élement est noté $k(X)$ et appelé *le sous-corps de* K *engendré par* X *sur* k.

L'application $X \longmapsto k(X)$ de l'ensemble des parties de K dans l'ensemble des sous-corps de K contenant k est surjective et possède les propriétés évidentes suivantes:

$X \subset k(X)$

$X_1 \subset X_2 \Longrightarrow k(X_1) \subset k(X_2)$

$k(k(X)) = k(X)$

$k(X_1)(X_2) = k(X_1 \cup X_2) = k(X_2)(X_1)$

On peut obtenir le corps $k(X)$ *engendré par* X *sur* k *d'une autre manière.*

L'intersection $k[X]$ des sous-anneaux de K contenant k et X est évidemment contenu dans $k(X)$. Le sous-ensemble $\{ab^{-1}; a,b \in k[X],\ b \neq 0\}$ de K est un sous-corps de K contenant k et X. Il s'identifie au corps des fractions de l'anneau intègre $k[X]$. Il contient $k(X)$, en vertu de la minimalité de $k(X)$. Comme $k[X] \subset k(X)$ il est clair qu'il lui est égal.

Ainsi, *le corps* $k(X)$ *est le corps des fractions de l'anneau* $k[X]$.

Il se peut que $k(X)$ soit égal à $k[X]$, i.e. que l'anneau $k[X]$ soit un corps, mais il n'en est pas ainsi en général.

Proposition I.3

1. *Avec les notations ci dessus, si tout élément de* X *est algébrique sur* k, $k(X) = k[X]$.

2. *Réciproquement, si X est fini et si $k(X) = k[X]$, tout élément de X est algébrique sur* k.

Démonstration

1. La première assertion résulte de l'application du lemme suivant avec $B = k[X]$.

Lemme

Soient B *un anneau INTEGRE,* k *un sous-corps de* B.

Si B *est entier sur* k, B *est un corps.*

Démonstration du lemme

Soient x un élément non nul de B, $f(x) = 0$, où

$$f(X) = X^n + \sum_{i=0}^{n-1} a_{n-i} X^i,$$

une équation de dépendance intégrale de degré n minimal de x sur k.

L'élément a_n est non nul car sinon, par intégrité de B,

$$x^{n-1} + \ldots + a_{n-1} = 0$$

serait une équation de dépendance intégrale de degré $< n$ de x sur k.

L'élément $-(a_n)^{-1}(x^{n-1}+\ldots+a_{n-1})$ est l'inverse de x.

2. L'assertion 2. peut s'énoncer:

Si une k*-algèbre de type fini sur un corps* k *est un corps, ce corps est algébrique sur* k.

Elle se démontre par récurrence sur $n = \mathrm{card}(X)$.

Cas $n = 1$: $X = \{x_1\}$

On peut supposer $x_1 \neq 0$. Il existe $f(X) \in k[X]$ tel que $x_1^{-1} = f(x_1)$ et x_1 est racine du polynôme *non nul* $Xf(X)-1$.

On suppose $n > 1$ *et l'assertion démontrée pour tous les corps* k *et tous les ensembles* X *de cardinal* $n-1$.

Soit $X = \{x_1,\ldots,x_n\}$. L'anneau $k[x_1,\ldots,x_n]$ est un corps contenant k et x_1 et donc le corps $k(x_1)$. Il est donc égal à $k(x_1)[x_2,\ldots,x_n]$.

Par hypothèse de récurrence, $x_2,\ldots,x_n$ sont algébriques sur $k(x_1)$.

Soit $a_{n_i,i}(x_1)x_i^{n_i} + \ldots + a_{0,i}(x_1) = 0$ une équation de dépendance algébrique de x_i sur $k(x_1)$ où $a_{j,i}(X) \in k[X]$ et $a_{n,i}(x_1) \neq 0$.

Si $\phi(X) = \prod_{i=2}^{n} a_{n_i,i}(X)$, il est aisé de vérifier que $\phi(x_1)x_i$ est entier sur $k[x_1]$ $(i = 2,\ldots,n)$ et donc que, pour tout élément ξ de $k[x_1,\ldots,x_n]$, il existe un entier naturel s tel que $\phi(x_1)^s\xi$ soit entier sur $k[x_1]$.

On va démontrer par l'absurde que x_1 *est algébrique sur* k.

Supposons *le transcendant* sur k. Alors l'anneau $k[x_1]$ est intégralement clos car isomorphe à un anneau de polynômes et donc tout élément de $k(x_1)$ s'écrit sous la forme $f(x_1)/\phi(x_1)^s$ avec $f(X) \in k[X]$.

Ceci est impossible:si, par exemple, $\psi(X)$ est un polynôme non divisible par $\phi(X)$, l'élément $1/\psi(x_1)$ ne peut-être de cette forme.

Remarques

1. On a vu dans la démonstration de l'assertion 1. le résultat souvent utile suivant: si l'élément x d'un anneau intègre B est algébrique sur un corps k il est inversible et *son inverse est un polynôme en* x *à coefficients dans* k.

2. Une forme équivalente de l'assertion 2. est connue sous le nom de *forme faible du théorème des zéros de* Hilbert:

Soient k *un corps*, m *un idéal MAXIMAL de l'anneau* $k[X_1,\ldots X_n]$ *où* $X_1,\ldots,X_n$ *sont des indéterminées. Le corps* $k[X_1,\ldots,X_n]/m$ *est algébrique sur* k. (chapitre 6).

3. Soit K un corps contenant k comme sous corps. Alors $k[K] = k(K)$.

L'hypothèse de finitude est donc essentielle dans la proposition I.2.2.

Extensions de type fini

Soit K/k *une extension du corps* k. On identifie k à un sous-corps de K.

On dit que l'extension K/k *est de type fini s'il existe une partie finie* X *de* K *telle que* $K = k(X)$.

Exemple

Une extension de degré fini est de type fini: si, avec les notations ci dessus, $K \neq k$, soit $a_1 \in K - k$; si $K \neq k(a_1)$, soit $a_2 \in K-k(a_1)$. Procédant ainsi de proche en proche, on obtient une suite croissante $k \subset k(a_1) \subset k(a_1,a_2) \subset \ldots$ qui aboutit à K au bout d'un nombre fini d'opérations en raison de la finitude de $[K:k]$ et de l'impossibilité d'existence d'une suite strictement croissante infinie de sous-espaces vectoriels.

L'extension k(X)/k, *où* X *est une indéterminée, est de type fini mais n'est pas de degré fini.*

Les extensions de type fini s'introduisent naturellement en géomé-

trie algébrique (chapitre 6: corps des fonctions rationnelles d'un ensemble algébrique irréductible).

Remarque importante

Dire que l'extension K/k *est de type fini n'est pas dire que l'algèbre* K *sur* k *est de type fini*, i.e. quotient d'un anneau de polynôme à un nombre *fini* d'indéterminée à coefficients dans k.

Comme $k(X)$ est le corps des fractions de l'anneau intègre $k[X]$, *dire que* K/k *est de type fini c'est dire que* K *est localisé en l'idéal* (0) *d'une* k-*algèbre de type fini intègre*. (C'est un cas particulier de ce qui est quelquefois appelé *algèbre essentiellement de type fini*).

3. Bases de transcendance

La lecture de ce paragraphe n'est pas utile pour la lecture de la suite du chapitre.

Soient K *un corps*, k *un sous-corps de* K.

On démontre ici l'existence d'un sous-ensemble X *de* K *algébriquement indépendant sur* k *tel que* K *soit algébrique sur* $k(X)$. Un tel sous-ensemble est appelé une *base de transcendance de* K/k.

Le cardinal d'une telle base est un invariant de l'extension, indépendant de la base. On le démontrera ici dans le cas où K/k admet une base de transcendance finie. Ce cardinal est appelé le *degré de transcendance de* K/k.

On verra ultérieurement que, pour les extensions de type fini K/k, il s'interprète géométriquement comme la *dimension d'un modèle de l'extension*.

L'étude d'une extension K/k se ramène à celle d'une extension transcendante pure $k(X)$, où X est une base de transcendance, puis à celle d'une extension algébrique de $k(X)$.

La démonstration de l'existence d'une base de transcendance se fait de manière purement formelle à partir de certaines propriétés explicitées ci dessous. Le lecteur pourra remarquer qu'une démonstration analogue fournit l'existence d'une base d'un espace vectoriel. Dans le §IV, on démontrera de la même manière l'existence de p-bases.

Soit X *un sous-ensemble de* K.

On note $s(X)$ le sous-corps de K contenant k, *fermeture algébrique de* $k(X)$ *dans* K.

L'application: $X \longmapsto s(X)$ *de l'ensemble des parties de* K *dans l'ensemble des sous-corps de* K *contenant* k *possède les cinq propriétés ci dessous dont se déduiront formellement les théorèmes d'existence annoncés.*

Lemme

1. $\boxed{X \subset s(X)}$

C'est clair car X $k(X)$

Lemme

2. $\boxed{X_2 \subset X_1 \quad s(X_2) \subset s(X_1)}$

Un élément de K algébrique sur $k(X_2)$ l'est, a fortiori , sur $k(X_1)$

Lemme

3. $\boxed{s(s(X)) = s(X)}$

D'après 1., $s(X) \subset s(s(X))$. Un élément x de $s(s(X))$ est algébrique sur $k(s(X))$ qui est $s(X)$. Comme $s(X)$ est algébrique sur $k(X)$, x est algébrique sur $k(X)$.

Il appartient donc à $s(X)$.

Si $x \in s(X)$, *on dira que* x *dépend algébriquement de* X *sur* k.

Lemme

4. $\boxed{x \in s(X) \Longrightarrow \exists\ Y \text{ fini} \subset X / x \in s(Y)}$

(Si x dépend algébriquement de X sur k il dépend algébriquement d'une partie finie de X sur k).

Il est clair que $k(X) = \bigcup_Y k(Y)$ où Y parcourt l'ensemble des parties finies de X.

Dire qu'un élément x appartient à $s(X)$ c'est dire que x satisfait à une équation $a_r x^r + \ldots + a_o = 0$ où a_i appartient à $k(X)$, $a_r \neq 0$.

Il existe une partie finie $Y = \{x_1, \ldots, x_n\}$ telle que a_i appartienne à $k(Y)$ $(i = 1, \ldots, r)$. Alors, x appartient à $s(Y)$.

Lemme

5. (Propriété d'échange)

Soient x, y *des éléments de* K, X *une partie de* K.

Si $y \in s(X \cup \{x\})$ *et* $y \notin s(X)$, $x \in s(X \cup \{y\})$

Cette propriété s'énonce en termes plus concrets; *si* y *dépend algébriquement de* $X \cup \{x\}$ *sur* k *mais ne dépend pas algébriquement de* X, x *dépend algébriquement de* $X \cup \{y\}$.

Démonstration

Il résulte de la propriété 4) que l'on peut supposer X fini, $X = \{x_1,\ldots,x_n\}$.

Dans la suite, les majuscules désignent des indéterminées.

Il existe, par hypothèse, $F(X_1,\ldots,X_n,X,Y) \in k[X_1,\ldots,X_n,X,Y]$ tel que

$$F(x_1,\ldots,x_n,x,y) = 0$$

$$F(x_1,\ldots,x_n,x,Y) \neq 0$$

En effet, dire que $y \in s(\{x_1,\ldots,x_n,x\})$ c'est dire qu'il existe un élément non nul $a_r(x_1,\ldots,x_n,r)Y^r+\ldots+a_o(x_1,\ldots,x_n,x)$ de $k(x_1,.,x_n,x)[Y]$ admettant y pour racine.

Il est loisible de supposer que les éléments $a_i(x_1,\ldots,x_n,x)$ appartiennent à $k[x_1,\ldots,x_n,x]$.

On prend alors $F(X_1,\ldots,X_n,X,Y) = a_r(X_1,\ldots,X_n,X)Y^r+ \ldots + a_o(X_1,\ldots,X_n,X)$.

On ordonne F par rapport à X:

$$F = \sum_{i=0}^{p} A_i(X_1,\ldots,X_n,Y)X^i$$

on a donc

$$0 = F(x_1,\ldots,x_n,x,y) = \sum_{i=0}^{p} A_i(x_1,\ldots,x_n,y)x^i$$

et $A_i(x_1,\ldots,x_n,y)$ appartient à $k[x_1,\ldots,x_n,y]$.

Un au moins des polynômes $A_i(x_1,\ldots,x_n,Y)$ est non nul puisque $F(x_1,\ldots,x_n,x,Y)$ est non nul.

Soit i_o tel que $A_{i_o}(x_1,\ldots,x_n,Y) \neq 0$. Alors, $A_{i_o}(x_1,\ldots,x_n,y)$ est non nul car sinon y dépendrait algébriquement de $x_1,\ldots,x_n$ sur k, i.e. appartiendrait à $s(X)$.

L'équation (1) est donc une équation de dépendance algébrique pour x sur $k(x_1,\ldots,x_n,y)$ i.e., x appartient à $s(X \cup \{y\})$.

Définitions

Soit K/k *une extension du corps* k, X *un sous-ensemble de* K.

1. *On dit que* X *est un système de* t-*générateurs de* K/k *si* $s(X) = K$
2. *On dit que* X *est un système* t-*libre si* $X = \emptyset$ *ou si* $X \neq \emptyset$ *et pour tout* x *de* X $x \notin s(X-\{x\})$ (i.e. si x de X ne dépend pas algébriquement sur k des autres éléments de X). *Ceci revient à dire que* X *est algébriquement indépendant sur* k. On remarque que $\emptyset$ est t-libre.
3. *On dit que* X *est une base de transcendance de* K/k *si c'est un système de* t-*générateurs qui est* t-*libre.*

On remarque que dire que X est un système de t-géénrateurs de K/k c'est dire que K est algébrique sur k.

Théorème I.4 (théorème de la base incomplète)

Soient K/k *une extension de* k, X *un système de* t-*générateurs de* K/k, L *un système* t-*libre.*

Il existe une partie X' *de* X *telle que* $L \cup X'$ *soit une base de transcendance de* K/k *et* $L \cap X' = \emptyset$

Démonstration

Soit F *l'ensemble des sous-ensembles* S *de* X *tels que* $L \cup S$ *soit* t-*libre et* $L \cap S = \emptyset$

Il est *non vide* car il contient $\emptyset$.

Ordonné par inclusion, *il est inductif*: en effet, soit $(S_i)_{i\in I}$ une famille totalement ordonnée de F. La réunion $\bigcup_{i\in I} S_i$ est une borne supérieure car si $L \cup \bigcup_{i\in I} S_i = \bigcup_{i\in I}(L \cup S_i)$ n'était pas t-libre, il existerait x de cet ensemble appartenant à $s(L \cup \bigcup_{i\in I} S_i - \{x\})$. Il existerait donc des éléments $x_1,\ldots,x_n$ de $L \cup \bigcup_{i\in I} S_i$ tels que x appartienne à $s(\{x_1,\ldots,x_n\})$.

Il existerait donc i de I tel que les éléments x_j appartiennent à $L \cup S_i$ $(j = 1,\ldots,n)$ ainsi que x et que x appartienne à $s(L \cup S_i - \{x\})$. Ceci contredirait le fait que $L \cup S_i$ est t-libre.

Soit alors X' *un élément maximal de* F dont l'existence est assurée par le théorème de Zorn. On va démontrer que $L \cup X'$ est une base de transcendance de K/k.

Comme on sait que $L \cup X'$ est t-libre, il suffit de démontrer que $L \cup X'$ est un système de t-générateurs, i.e. que $K = s(L \cup X')$.

Comme $K = s(X)$ par hypothèse, il suffit de démontrer que X est contenu dans $s(L \cup X')$ (propriété 2)).

On raisonne par l'absurde, supposant que X n'est pas contenu dans $s(L \cup X')$.

Soit alors x de X n'appartenant pas à $s(L \cup X')$ et soit $X'' = X' \cup \{x\}$.

On va vérifier que $X'' \in F$, ce qui contredira la maximalité de X' puisque x n'appartient pas à X' (propriété 1)).

Soit $y \in L \cup X''$ Si $y = x$, $L \cup X'' - \{y\} = L \cup X'$ et, par hypothèse x n'appartient pas à $s(L \cup X'')$. Si $y \neq x$, y appartient à $L \cup X'$. Il ne peut appartenir à $s(L \cup X'' - \{y\}) = s((L \cup X' - \{y\} \cup \{x\})$: en effet, y n'appartient pas à $s(L \cup X' - \{y\})$ et, en vertu de la propriété 4) (propriété d'échange), x appartiendrait alors à $s((L \cup X' - \{y\} \cup \{y\})$ i.e. à $s(L \cup X')$.

Corollaire

L'extension K/k *de* k *a une base de transcendance.*

De plus, de tout système de t*-générateurs, on peut extraire une base de transcendance.*

Démonstration

Il suffit d'appliquer le théorème au cas $L \neq \emptyset$ et au système $X = K$ de t-générateurs de K/k.

On va se contenter ici de prouver l'invariance du cardinal d'une base de transcendance de K/k dans le cas où ce cardinal est fini ou si l'on préfère dans le cas où l'extension K/k a un système fini de t-générateurs.

La preuve du cas général est reportée en exercice.

Théorème I.5

Soit K/k *une extension du corps* k.

On suppose que K/k *a une base de transcendance finie. Alors, toutes les bases de transcendance de* K/k *sont finies et ont le même nombre d'éléments.*

Démonstration

On procède par récurrence sur le nombre n *d'éléments d'une base* B *ayant le nombre minimal d'éléments.*

Cas n = 0. Alors $B = \emptyset$ et donc $k(B) = k$. Par conséquent, $K = s(B)$ est la fermeture algébrique de $k(B) = k$ dans K et K est algébrique sur k. Si B' est une base de transcendance de K/k, $B' = \emptyset$ car sinon un élément x de B' ne serait pas algébrique sur k.

On suppose l'assertion vraie pour les extensions K/k *de base minimale à* n *éléments.*

Soit K/k une extension telle que le nombre d'éléments d'une base minimale B soit n+1. Soit B' une base de transcendance de K/k et soit x un élément de B'.

L'ensemble $L = \{x\}$ est t-libre car sinon x appartiendrait à $s(L-\{x\})$ et a fortiori à $s(B'-\{x\})$.

On applique le théorème d'échange à L et B. Il existe un sous-ensemble C de B tel que $C \cap L = \emptyset$ et que $C \cup L$ soit une base de transcendance de K/k.

Comme, par minimalité de B, $\text{card}(C \cup \{x\}) \geqslant n+1$, $\text{card}(C) \geqslant n$. Comme C est strictement contenu dans B, $\text{card}(C) < n+1$ et donc $\text{card}(C) = n$.

Soit $k' = k(x)$. On va démontrer que C et $C' = B' - \{x\}$ sont des bases de transcendance de l'extension K/k'. Il suffit de le faire pour C.

L'ensemble C *est un système de* t*-générateurs de* K/k' car $k'(C) = k(x)(C) = k(\{x\} \cup C) = k(B)$ et K est algébrique sur $k(B)$ puisque B est un système de t-générateurs de K/k.

L'ensemble C *est* t*-libre sur* k'. Soit, en effet, $z \in C$. Si z appartenait à $s(C-\{z\})$, z serait algébrique sur $k'(C-\{z\}) = k(x)(C-\{z\}) = k(C \cup \{x\} - \{z\}) = k(B-\{z\})$, ce qui contredirait le fait que B est t-libre.

On vérifie aisément que C est une base de transcendance minimale de K/k'. Par hypothèse de récurrence, $\text{card}(C') = \text{card}(C) = n$ et donc $\text{card}(B) = n+1$.

Définition

Sous les hypothèses de la proposition, le nombre d'éléments d'une base de transcendance de K/k *est appelé le degré de transcendance de* K/k *et noté* $d^\circ tr(K/k)$.

Proposition I.6

Soient $k \subset K \subset L$ *une tour d'extensions,* X *une base de transcendance de* K/k, Y *une base de transcendance de* L/K. *Alors,* $x \cap y = \emptyset$ *et* $X \cup Y$ *est une base de transcendance de* L/k.

Démonstration

Comme K est algébrique sur $k(X)$ et L est algébrique sur $K(Y)$, L est algébrique sur $k(X)(Y) = k(X \cup Y)$. (corollaire 2 de proposition I.4)

Il suffit donc de démontrer que $X \cup Y$ est algébriquement indépendant sur k.

Soient $x_1,\dots,x_n$ (resp. $y_1,\dots,y_m$) des éléments de X (resp. Y) distincts, $f(T_1,\dots,T_n, U_1,\dots,U_m) \in [T_1,\dots,T_n, U_1,\dots,U_m]$ tel que

$f(x_1,\dots,x_n, y_1,\dots,y_m) = 0$

On ordonne f par rapport aux indéterminées $U_1,\dots,U_m$,

$$f = \sum_{(a_1,\dots,a_m)} f_{a_1\dots a_m}(T_1,\dots,T_n)U_1^{a_1}\dots U_m^{a_m}$$

Comme les éléments $y_1,\dots,y_m$ sont algébriquement indépendants sur K, $f_{a_1\dots a_m}(x_1,\dots,x_n) = 0$ pour tout $(a_1,\dots,a_m) \in N^m$. Comme les éléments $x_1,\dots,x_n$ sont algébriquement indépendants sur k, $f_{a_1\dots a_m}(T_1..T_n) = 0$ pour tout $(a_1,\dots,a_m) \in N^m$ et donc $f(T_1,\dots,T_n, U_1,\dots,U_m) = 0$.

Corollaire (additivité du degré de transcendance)

Si $d^\circ tr(K/k)$ *et* $d^\circ tr(L/K)$ *sont finis, il en est de même de* $d^\circ tr(L/k)$ *et* $d^\circ tr(L/k) = d^\circ tr(L/K) + d^\circ tr(K/k)$.

4. Le théorème de Lüroth

Le problème suivant se pose naturellement:

Un sous-extension d'une extension transcendante pure d'un corps k *est-elle transcendante pure ?*

On a une *réponse affirmative* dans le cas où l'extension transcendante pure K/k est de degré *de transcendance* 1, i.e. où K est isomorphe à l'algèbre K(T) des fractions rationnelles à une indéterminée dans k. C'est le théorème de Lüroth exposé ci dessous.

La réponse est également *affirmative* pour les extensions transcendantes pures de $\mathbb{C}$ de *degré de transcendance* 2. C'est un théorème de Castelnuovo qu'il n'est pas question d'exposer ici.

Il existe des *contre-exemples* dus à Enriques pour les extensions transcendantes pures de $\mathbb{C}$ *de degré de transcendance* 3.

Proposition I.7

Soient k *un corps,* X *une indéterminée,* $K = k(X)$, $\alpha = f(X)/g(X)$, *où* $f(X)$ *et* $g(X)$ *sont premiers entre eux dans* $k[X]$, *un élément non constant de* K.

Alors, K *est algébrique sur* $k(\alpha)$ *de degré égal à* $\sup(d^\circ f, d^\circ g)$ *et* α *est transcendant sur* k.

Démonstration

Soit T une indéterminée. L'élément X est racine du polynôme $\phi(T) = \alpha g(T) - f(T)$.

On va démontrer que $\phi(T)$ *est irréductible dans* $k(\alpha)[T]$.

D'abord, $\phi(T)$ *est non nul*: sinon, il existerait $i \in N$ tel que le coefficient b_i de T^i dans $g(T)$ soit non nul et, si a_i est le coefficient de T^i dans $f(T)$, α soit égal à a_i/b_i et appartienne donc à k.

Donc, X est algébrique sur $k(\alpha)$. Il en résulte que α est transcendant sur k (transitivité de la dépendance algébrique) et que K est algébrique sur $k(\alpha)$.

On suppose $\phi(T)$ *réductible dans* $k(\alpha)[T]$. On a donc une égalité $c(\alpha)(\alpha g(T) - f(T)) = r(T)s(T)$ avec $d^\circ r(T) \geqslant 1$ et $d^\circ s(T) \geqslant 1$, où $r(T)$, $s(T)$ appartiennent à $k[\alpha,T]$ et $c(\alpha)$ à $k[\alpha]$. Un facteur irréductible de $c(\alpha)$ divise $r(T)$ ou $s(T)$ (lemme de Gauss). On peut donc supposer $c(\alpha) = 1$.

Alors $d^\circ_\alpha (\alpha g(T) - f(T)) = 1 = d^\circ_\alpha(r(T)) + d^\circ_\alpha (s(T))$ et donc un des polynômes $r(T)$ et $s(T)$ appartient à $k[T]$. Comme $f(T)$ et $g(T)$ sont premiers entre eux, ce polynôme est une constante non nulle. Ceci contredit l'hypothèse $d^\circ(r) \geqslant 1$ et $d^\circ(s) \geqslant 1$.

Théorème I.8 (Lüroth)

Soient k *un corps,* $K = k(X)$ *une extension monogène transcendante pure de* k, L *un sous-corps de* K *contenant strictement* k.

Il existe alors $y \in L$ *transcendant sur* k *tel que* $L = k(y)$.

Démonstration

D'abord, K est algébrique sur L: en effet, si $\alpha \in L-k$, K est algébrique sur $k(\alpha)$.

On va démontrer l'existence d'un élément y *de* L *tel que* $[K:L] = [K:k(y)]$.

Comme $K = L(X)$, $[K:L]$ est le degré du polynôme $\phi(T) = \mathrm{irr}(T,X,L) = T^n + a_1(X)T^{n-1} + \ldots + a_n(X)$ où $a_i(X) \in L$.

On écrit $a_i(X)$ sous la forme $b_i(X)/b_o(X)$ où $b_i(X)$ appartient à $k[X]$ $(i = 0,\ldots,n-1)$ et où $b_o(X)$ a été choisi *de degré minimal*.

Le polynôme $f(X,T) = b_o(X)T^n + b_1(X)T^{n-1} + \ldots + b_n(X) \in k[X,T]$ est irréductible en tant que polynôme en T, *primitif* en tant que polynôme en X et tel que $f(X,X) = 0$.

On va désigner par m (resp. n) *le degré de* f *en* X (resp. T).

Un au moins des éléments $a_i(X)$ est non nul (car sinon X serait nul). Soit y un tel élément. Il s'écrit $y = g(X)/h(X)$ où $g(X)$ et $h(X)$ sont premiers entre eux dans $k[X]$ et où donc $d^\circ(g) \leqslant d^\circ(b_i) \leqslant m$ et $d^\circ(h) \leqslant d^\circ(b_o) \leqslant m$.

Le polynôme $g(T) - yh(T) \in L[T]$ admet X pour racine. Il est donc divisible par $\phi(T)$ dans $L[T]$. Comme $g(T) - yh(T) = g(T)-(g(X)/h(X))h(T)$, on a une égalité

$u(X)(h(X)g(T) - g(X)h(T)) = q(X,T)f(X,T)$ où $u(X) \in k[X]$ et $q(X,T) \in k[X,T]$.

Comme $h(X)g(T) - g(X)h(T)$ et $f(X,T)$ sont primitifs en X, $u(X)$ divise $q(X,T)$. On peut donc supposer $u(X) = 1$. Ainsi on a l'égalité

(1) $h(X)g(T) - g(X)h(T) = q(X,T)f(X,T)$

On va démontrer que $q(X,T)$ *appartient à* k, i.e. est de degré 0 en X et en T.

D'abord, le degré en X du premier membre de (1) est $\leqslant m$, celui du second membre est $m + d^\circ_X(q(X,T))$. Donc, $d^\circ_X(q(X,T)) = 0$. On voit de plus que $d^\circ_X(h(X)g(T) - g(X)h(T)) = m$.

Par symétrie, $d^\circ_T(h(X)g(T) - g(X)h(T) = m$.

Il résulte d'autre part, de la proposition I.6 que n, qui est $\sup(d^\circ g, d^\circ h)$, est $[K:k(y)]$. Comme $[K:k(y)] \geqslant [K:L]$, $n \geqslant m$. Ceci implique que q est constant en T et que $m = n$.

Le théorème de Lüroth a une interprétation géométrique suggérée ci dessous (confer. chap. 6 exercice 14).

A une courbe algébrique irréductible, par exemple, une courbe algébrique plane irréductible $\{(x,y) \in \mathbb{C}^2 / f(x,y) = 0$ où $f(X,Y)$ est un polynôme irréductible $\in \mathbb{C}[X,Y]\}$, on peut associer une extension $K/\mathbb{C}$ de degré de transcendance 1.

On dit que la courbe est *unirationnelle* (resp. *rationnelle* ou *unicursale*) si K est une sous-extension d'une extension transcendante pure, de degré de transcendance 1, de $\mathbb{C}$ (resp. une extension transcendante pure de $\mathbb{C}$).

Le théorème de Lüroth implique alors qu'une courbe unirationnelle est rationnelle.

Corollaire de la proposition I.7 (automorphismes d'un corps de fonctions rationnelles)

Soient k *un corps,* X *une indéterminée.*

Un automorphisme du corps k(X) *prolongeant* 1_k *est de la forme:* $f(X) \longmapsto f(\frac{aX+b}{cX+d})$, *où* a,b,c,d ∈ k *et* ad-bc ≠ 0.

Démonstration

Un homomorphisme ϕ prolongeant 1_k de k(X) dans k(X) est de la forme: $f(X) \longmapsto f(\phi(X))$.

Dire qu'il est un automorphisme c'est dire qu'il est surjectif, i.e. que $[k(X):k(\phi(X))] = 1$ i.e. que le degré de $\phi(X)$ est 1.

II. Construction de quelques extensions remarquables

1. Corps de rupture d'un polynôme

Problème: soient k *un corps,* X *une indéterminée,* f(X) *un polynôme non constant* ∈ k[X].

Trouver une extension K/k *telle que: 1)* f(X) *ait une racine* x *dans* K

2) K = k(x)

Un tel corps K *est appelé corps de rupture de* f(X) *sur* k.

Quitte à remplacer f(X) par un de ses facteurs irréductibles dans k[X], *on peut supposer,* de plus, f(X) *irréductible.*

On suppose le problème résolu.

Il existe un homomorphisme et un seul θ de k-algèbres de k[X] dans k[x] = k(x) = K tel que θ(X) = x.

Il est surjectif. Son noyau ker(θ) contient (f(X)) et, comme (f(X)) est un idéal maximal de k[X], parce que f(X) est irréductible, ker(θ) = (f(X)).

L'homomorphisme θ définit donc un isomorphisme $\overline{\theta}$ de la k-algèbre k[X]/(f(X)) sur K tel que $\overline{\theta}$ (classe de X modulo (f(X)) = x.

D'où la construction. On pose K = k[X]/(f(X)).

On identifie k à un sous-corps de K, au moyen de l'homomorphisme injectif composé de l'injection naturelle de k dans k[X] et de la surjection canonique de k[X] sur K. Soit x la classe de X modulo (f(X)). Alors, K = k(x) et f(x) = 0.

Ce procédé, du à Cauchy et à Kronecker, est appelé le *procédé d'adjonction symbolique.*

Exemples

1. k = ℚ, $f(X) = X^2 - 2$. Alors K = ℚ($\sqrt{2}$).

2. k = ℝ, $f(X) = X^2 + 1$. Alors K = ℝ(i), où $i^2 = -1$, est le corps ℂ des nombres complexes.

Remarque

Il est indispensable, pour la construction précédente, de supposer f(X) irréductible.

Sinon, l'anneau quotient $k[X]/(f(X))$ n'est pas un corps: exemple, $f(X) = (X-1)(X+1)$; Il résulte du théorème chinois que $k[X]/(f(X))$ est isomorphe à $(k[X]/(X-1)) \times (k[X]/(X+1)) = k^2$.

Proposition II.1 (prolongement des isomorphismes)

Soient k *et* k' *des corps,* X *une indéterminée.*

On suppose qu'il existe un isomorphisme s *de* k *sur* k'. *On note* $\bar{s}$ *l'isomorphisme:* $\Sigma a_i X^i \longrightarrow \Sigma s(a_i) X^i$ *de* $k[X]$ *sur* $k'[X]$ *prolongeant* s.

1. *Soit* f(X) *un polynôme irréductible de* $k[X]$.

Alors, $\bar{s}(f(X))$ *est un polynôme irréductible de* $k'[X]$

2. *Soient* K *et* K' *des extensions respectives de* k *et* k', x *et* x' *des racines respectives de* f(X) *et* $f'(X) = \bar{s}(f(X))$ *dans* K *et* K'.

Il existe un isomorphisme t et un seul de k(x) dans k'(x') prolongeant s et tel que t(x) = x'.

Démonstration

1. est clair.

2. *Unicité:* un élément y de k(x) s'écrit de manière unique,

$$a_o + \ldots + a_{n-1} x^{n-1},$$

où $a_i \in k$, $n = d^\circ f$. On doit donc avoir $t(y) = s(a_o) + \ldots + s(a_{n-1}) x'^{n-1}$.

Existence. On a un diagramme

$$\begin{array}{ccc} k[X]/(f(X)) & \xrightarrow{s_1} & k'[X]/f'(X)) \\ \Big\downarrow \bar{\theta} & & \Big\downarrow \bar{\theta}' \\ k(x) & & k'(x) \end{array}$$

où s_1 est déduit de $\bar{s}$ par passage au quotient, $\bar{\theta}$ et $\bar{\theta}'$ sont les isomorphismes canoniques appliquant respectivement les classes de X modulo (f(X)) et (f'(X)) sur x et x'. L'isomorphisme $t = \bar{\theta}' \circ s_1 \circ \theta^{-1}$ répond à la question.

Cette proposition, en dépit de sa simplicité, est d'une importance capitale pour la suite.

Corollaire 1

Soient K *un corps,* k *un sous-corps de* K, x *et* x' *des éléments de* K, *algébriques sur* k.

Les assertions suivantes sont équivalentes:

(i) irr(X,x,k) = irr(X,x',k)

(ii) *il existe un isomorphisme de* k(x) *sur* k(x') *prolongeant* 1_K *et appliquant* x *sur* x'. (Cet isomorphisme est alors unique).

Démonstration

(i) $\Longrightarrow$ (ii): c'est un cas particulier de la proposition 1 avec k = k', s = 1_K, f(X) = irr(X,x,k)

(ii) $\Longrightarrow$ (i): évident.

Définition

Si les conditions équivalentes (i) et (ii) du corollaire sont satisfaites, on dit que x *et* x' *sont conjugués sur* k.

Exemples:

1. k = $\mathbb{Q}$, K = $\mathbb{R}$, $\sqrt{2}$ et $-\sqrt{2}$ sont conjugués sur $\mathbb{Q}$

2. k = $\mathbb{Q}$, K = $\mathbb{C}$, i et -i, où $i^2 = -1$ sont conjugués sur $\mathbb{R}$.

Corollaire 2

Deux corps de rupture d'un polynôme irréductible de k[X] *sont isomorphes dans un isomorphisme de* k*-algèbre.*

Remarque

Le résultat du début de ce paragraphe peut être généralisé comme suit:

Soient A *un anneau intégralement clos,* K *son corps des fractions,* f(X) *un polynôme unitaire irréductible de* A[X], B *un anneau contenant* A *comme sous-anneau,* x *un élément de* B *tel que* f(x) = 0.

1. f(X) *est irréductible dans* K[X].

2. *L'homomorphisme surjectif de* A*-algèbres de* A[X] *sur* A[x] *appliquant* X *sur* x *définit un isomorphisme de* A*-algèbres de* A[X]/(f(X)) *sur* A[x].

L'anneau A[x] *est intègre et le* A*-module* A[x] *est libre de base* $\{1, x, \ldots, x^{n-1}\}$

Démonstration

1. Soit f(X) = g(X)h(X) une décomposition de f(X) dans K[X]. Les coefficients de g(X) et h(X) sont des fonctions symétriques élémentaires de racines de f(X) dans un anneau convenable contenant A (qui sera construit dans le paragraphe suivant).

Ce sont donc des éléments de K entiers sur A. Ils appartiennent à A.

L'irréductibilité de f(X) dans A[X] implique que g(X) ou h(X) est un élément inversible de A[X], i.e. de A et, a fortiori, de K.

2. *L'idéal* f(X)A[X] *est premier.*

En effet, f(X)A[X] = f(X)K[X] ∩ A[X]: soient $f(X) = X^n+a_1X^{n-1}+\ldots+a_n$ et $g(X) = b_oX^m+\ldots+b_m$, où $b_i \in K$; la condition $f(X)g(X) \in A[X]$ implique successivement $b_o \in A$, $b_1 \in A, \ldots, b_m \in A$.

Soit alors $g(X) \in A[X]$ tel que g(x) = 0. Il appartient à f(X)K[X] ∩ A[X] = f(X)A[X].

Le noyau de l'homomorphisme surjectif de A[X] sur A[x] est f(X)A[X].

La démonstration devient alors immédiate.

2. Corps de décomposition d'un polynôme

Définition

Soient k *un corps,* X *une indéterminée,* f(X) *un polynôme non constant* ∈ k[X].

On appelle corps de décomposition de f(X) *sur* k *une extension* K/k *telle que*

1. *dans* K[X], $f(X) = c(X-x_1)\ldots(X-x_n)$
2. $K = k(x_1,\ldots,x_n)$

Exemples

1. $\mathbb{Q}(\sqrt{2})$ est un corps de décomposition sur $\mathbb{Q}$ de X^2-2.
2. $\mathbb{C} = \mathbb{R}(i)$ est un corps de décomposition sur $\mathbb{R}$ de X^2+1.
3. K est un corps de décomposition sur k de tout polynôme de degré 1.

Proposition II.2 (existence et unicité, à isomorphisme près, du corps de décomposition)

Soient k *un corps,* X *une indéterminée,* f(X) *un polynôme non constant de* k[X].

1. *Il existe un corps de décomposition de* f(X)
2. *Deux corps de décomposition de* f(X) *sont isomorphes dans un isomorphisme* (en général, non unique) *de* k*-algèbres.*

(On dit qu'ils sont k-isomorphes)

Démonstration

1. Existence

Démonstration par récurrence sur d°f. L'assertion est claire si d°f = 1.

On suppose donc l'assertion vraie pour tous les corps k et tous les

polynômes de degré n-1 avec $n > 1$. Soit $f(X)$ un polynôme de degré n.

On considère un facteur irréductible $g(X)$ de $f(X)$ et un corps de rupture $k(x_1)$ de $g(x)$. Alors, $f(X)/(X-x_1) \in k(x_1)[X]$ admet un corps de décomposition $K = k(x_1)(x_2,\ldots,x_n)$ sur $k(x_1)$ (hypothèse de récurrence). Il est clair que K est corps de décomposition de $f(X)$ sur k.

2. Unicité

On démontre, par récurrence sur $d^\circ f$, *un résultat plus général.*

Soient k *et* k' *deux corps,* $f(X)$ *un polynôme non constant de* $k[X]$.

On suppose qu'il existe un isomorphisme s *de* k *sur* k'. *On désigne par* $\bar{s}$ *l'isomorphisme de* $k[X]$ *sur* $k'[X]$ *prolongeant* s, *par* $f'(X)$ *le polynôme* $\bar{s}(f(X)) \in k'[X]$.

Soient K *et* K' *des corps de décomposition de* $f(X)$ *et* $f'(X)$ *respectivement sur* k *et* k'.

Il existe un isomoprhisme t *de* K *sur* K' *prolongeant* s.

L'assertion est claire si $d^\circ f = 1$ auquel cas $K = k$, $K' = k'$. On la suppose vraie pour $d^\circ f = n-1$.

Soit f de degré n. Alors $K = k(x_1,\ldots,x_n)$ où $f(X) = c(X-x_1)\ldots(X-x_n)$ et $K' = k'(x'_1,\ldots,x'_n)$ où $f'(X) = c(X-x'_1)\ldots(X-x'_n)$. Soit $g(X)$ un facteur irréductible de $f(X)$ admettant x_1 pour racine dans K. Quitte à renuméroter $x'_1,\ldots,x'_n$, on peut supposer que x'_1 est racine dans K' de $\bar{s}(g(X))$.

On déduit de la proposition 1 l'existence d'un isomorphisme t' de $k(x_1)$ sur $k'(x'_1)$ prolongeant s. Par hypothèse de récurrence, il existe un isomorphisme t de K (qui est corps de décomposition sur $k(x_1)$ de $f(X)/(X-x_1)$) sur K' (qui est corps de décomposition sur $k'(x'_1)$ de $f'(X)/(X-x'_1)$) prolongeant t' et donc s.

3. Clôture algébrique d'un corps

Définition

Un corps k *est dit algébriquement clos s'il satisfait aux conditions équivalentes suivantes:*

(i) tout polynôme non constant $\in k[X]$, *où* X *est une indéterminée, a une racine dans* k

(ii) tout polynôme non constant $\in k[X]$ *se décompose dans* $k[X]$ *en facteurs du premier degré.*

Exemples:

1. $\mathbb{Q}$ n'est pas algébriquement clos; par exemple, X^2-2 et X^2+1 n'ont pas de racine dans $\mathbb{Q}$

2. $\mathbb{R}$ n'est pas algébriquement clos: X^2+1 n'a pas de racine dans $\mathbb{R}$.

Théorème II.3 (théorème de d'Alembert)

Le corps $\mathbb{C}$ des complexes est algébriquement clos

Démonstration

Il existe de nombreuses démonstrations, fort différentes, de ce théorème, appelé quelquefois théorème fondamental de l'algèbre. Gauss en a donné cinq preuves.

Soit $f(X)$ un polynôme non constant $\in \mathbb{C}[X]$. Supposons qu'il n'ait pas de racine dans $\mathbb{C}$. La fonction : $z \longmapsto g(z) = \frac{1}{f(z)}$ est holomorphe dans tout le plan complexe. Comme elle tend vers 0 quand z tend vers l'infini, elle est bornée.

Il résulte alors du théorème de Liouville que cette fonction est constante. Il en est de même de la fonction: $z \longmapsto f(z)$. C'est absurde.

Proposition II.4

Un corps algébriquement clos est infini

Démonstration

Soit k un corps fini, $k = \{a_1 = 0, a_2 = 1, \ldots, a_n\}$. Le polynôme $\prod_{i=1}^{n}(X-a_i)+1$ n'a pas de racine dans k.

Définition

Soit k un corps. Une extension K/k de k est appelée une clôture algébrique de k si 1. *K est algébriquement clos.*
2. *K est algébrique sur k*

Exemples:

1. *$\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$*
2. *Soient K un corps algébriquement clos, k un sous-corps de K.*

La fermeture algébrique L de k dans K est une clôture algébrique de k.

En effet, soit $f(X)$ un polynôme non constant $\in L[X]$. Il admet une racine x dans K, qui est algébriquement clos. L'élément x est algébrique sur L et, par transitivité, sur k. Il appartient donc à L. Ainsi, L est algébriquement clos. Par exemple, *le corps des nombres algébriques* (fermeture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$) est une *clôture algébrique de $\mathbb{Q}$. C'est un corps algébriquement clos dénombrable.*

3. *Soient* k *un corps algébriquement clos,* X *une indéterminée.* Le corps des fractions de l'anneau intègre $k[\![X]\!]$ des séries formelles (FFAC) chapitre 2.II.1) est appelé le corps des séries formelles, et noté k((X)). Un théorème du à Puiseux affirme que, si la caractéristique de k est 0, une clôture algébrique de k((X)) est $\bigcup_{n\in N} k((X^{1/n}))$.

Théorème II.5 (existence et unicité, à isomorphisme près, de la clôture algébrique)

Soit k *un corps.*

1. *Il existe une clôture algébrique de* k

2. *Soient* K *et* K' *deux clôtures algébriques de* k. *Il existe un isomorphisme* t (non unique en général) *de* K *sur* K' *prolongeant* 1_K.

Démonstration

1. Existence

Soit F l'ensemble des polynômes non constants de $k[X]$. On considère une famille $(X_f)_{f\in F}$ d'indéterminées indexée par une application: $f \longmapsto X_f$ *injective.*

L'idéal $a = (f(X_f))_{f\in F}$ *de l'anneau* $k[X_f]_{f\in F}$ *est distinct de* $k[X_f]_{f\in F}$ sinon, on aurait une égalité

$$(*)\quad 1 = \sum_{i=1}^{n} g_i(\ldots)f_i(X_{f_i})$$

Considérant alors un corps Ω de décomposition du polynôme $\prod_{i=1}^{n} f_i(X)$ et spécialisant X_{f_i} en une racine du polynôme $f_i(X)$, on déduirait de (*) l'égalité absurde 1 = 0.

Soit m un idéal maximal de $k[X_f]_{f\in F}$ contenant a. On pose $k_1 = k[X_f]_{f\in F}/m$ et on identifie k à un sous-corps de k_1. La classe x_f de X_f modulo m est une racine dans le corps k_1 du polynôme f(X).

Le corps $k_1 = k(x_f)_{f\in F}$ *est algébrique sur* k *et tout polynôme non constant* $\in k[X]$ *a une racine dans* k_1.

On construit k_2 à partir de k_1 et, plus généralement, k_{n+1} à partir de k_n, comme on a construit k_1 à partir de k. *On pose* $K = \bigcup_{n\in N^*} k_n$.

Il est clair que K est un corps, *extension algébrique de* k.

Il est algébriquement clos: un polynôme f(X) non constant $\in K[X]$ appartient, en fait, à $k_n[X]$ pour un entier n convenable: Il a donc une racine dans k_{n+1} et, a fortiori, dans K.

Par conséquent, K *est une clôture algébrique de* k.

2. Unicité

On va démontrer le résultat plus fort ci dessous

Soient k *un corps,* k'/k *une extension algébrique de* k, K *un corps algébriquement clos,* s *un homomorphisme (injectif) de* k *dans* K.

Il existe un homomorphisme t *de* k' *dans* K *prolongeant* s.

Démonstration

L'ensemble F des couples (k",s") d'une extension k" de k contenue dans k' et d'un homomorphisme s" de k" dans K prolongeant s, ordonné par inclusion des corps et prolongement des homomorphismes, est inductif.

Il admet donc un élement maximal (k'_1,s'_1).

On a l'égalité $k'_1 = k'$: sinon, soit $a \in k'$, $a \notin k'_1$. Si $f(X) = \mathrm{irr}(X,a,k'_1)$, le polynôme $f'(X) \in K[X]$, obtenu en appliquant s'_1 aux coefficients de f(X), a une racine a' dans K.

Il existe donc un homomorphisme s" de $k'_1(a)$ sur $(s'_1(k'_1))(a')$ prolongeant s'_1.

Le couple $(k'_1(a),s")$ appartient à F et est strictement supérieur à (k'_1,s'_1), contrairement à l'hypothèse de maximalité de (k'_1,s'_1).

Un corollaire de ce résultat est la proposition suivante dont un cas particulier est la partie 2. du théorème.

Soient k *et* k' *deux corps,* K *et* K' *des clôtures algébriques respectives de* k *et* k'.

On suppose qu'il existe un isomorphisme s *de* k *sur* k'.

Il existe alors un isomorphisme (en général non unique) t *de* K *sur* K' *prolongeant* s.

Démonstration

Le composé de s et de l'injection de k' dans K' se prolonge en un homomorphisme t de K dans K'.

Le corps t(K), isomorphe à K, est algébriquement clos. Le corps K' est algébrique sur t(K). Il lui est donc égal. Par conséquent, t qui est injectif et surjectif est un isomorphisme.

4. Corps finis

Contrairement à nos conventions générales, on va supposer au début de ce paragraphe, le corps k *non nécessairement commutatif.*

Le centre $Z = \{x \in k / \forall y \in k,\ xy = yx\}$ de k est un sous-corps commutatif de k.

Si k est fini, il en est de même de Z.

La caractéristique de Z ne peut être 0 car sinon Z contiendrait le corps infini $\mathbb{Q}$.

La caractéristique de Z est donc un nombre premier p.

Le théorème suivant, du à Wedderburn, va nous ramener à l'étude des corps finis commutatifs.

Théorème II.6 (théorème de Wedderburn)

Un corps, non nécessairement commutatif, fini est commutatif

Démonstration

La démonstration donnée ci dessous utilise la théorie des *polynômes cyclotomiques*.

Le corps de base est le corps $\mathbb{Q}$. On appelle *n-ième polynôme cyclotomique le polynôme* $\Phi_n(X) = \prod_{(r,n)=1}^{n}(X-z^r)$, où z est une racine primitive n-ième de l'unité, par exemple, $\cos(2\pi/n) + i \sin(2\pi/n)$. En fait, $\Phi_n(X)$ est aussi égal à $\prod(X-\zeta_i)$ où ζ_i parcourt l'ensemble des racines primitives n-ièmes de l'unité.

Lemme 1

Le polynôme $\Phi_n(X)$ *est à coefficients entiers.*

Démonstration

On procède par récurrence sur n, à partir de l'égalité $X^n-1 = \prod_{d/n}\Phi_d(X)$ (où la notation d/n signifie que d divise n) qui montre que $\Phi_n(X)$ est le quotient du polynôme X^n-1, à coefficients entiers, par un polynôme unitaire à coefficients entier $\prod_{\substack{d\neq n \\ d/n}}\Phi_d(X)$.

Lemme 2

Soit n > 1. *Pour tout diviseur* d *de* n *distinct de* n, *le polynôme* $\Phi_n(X)$ *divise, dans* $\mathbb{Z}[X]$, *le polynôme* $\dfrac{X^n-1}{X^d-1}$

Démonstration

C'est une conséquence immédiate des égalités $X^n-1 = \prod_{d'/n}\Phi_{d'}(X)$ et $X^d-1 = \prod_{d'/d}\Phi_{d'}(X)$.

Ces lemmes étant établis, on peut passer à la démonstration du théorème.

Soit k *un corps fini, non nécessairement commutatif.*

Son *centre* $Z = \{x \in k / \forall y \in k,\ xy = yx\}$ est un sous-corps commutatif de k.

Soient p la caractéristique de Z, $f = [Z:F_p]$, en sorte que $q = p^f$ est le nombre d'éléments de Z, $n = [k:Z]$, en sorte que q^n est le nombre d'éléments de k.

Si $x \in k^* = k - \{0\}$, soit $Z(x) = \{y \in k / yx = xy\}$. Alors, $Z(x)$ est un sous-corps de k contenant Z et le nombre d'éléments de $Z(x)$ est $q^{d(x)}$ où $d(x) = [Z(x):Z]$.

On fait opérer le groupe multiplicatif k^* *sur l'ensemble* k^* *par conjugaison intérieure* : $(y,x) \longmapsto yxy^{-1}$.

On obtient ainsi une partition de k^* en un nombre fini d'orbites.

L'orbite de x est réduite à x si et seulement si x appartient à Z.

Il existe donc $q-1$ telles orbites.

L'orbite de x a, de toutes façon, $\dfrac{q^n-1}{q^{d(x)}-1}$ éléments car, on sait que son cardinal est égal à l'indice dans k^* du groupe de stabilité de x, groupe qui n'est autre que $(Z(x))^*$, et donc au quotient de l'ordre q^n-1 du groupe k^* par l'ordre $q^{d(x)}-1$ du groupe $(Z(x))^*$.

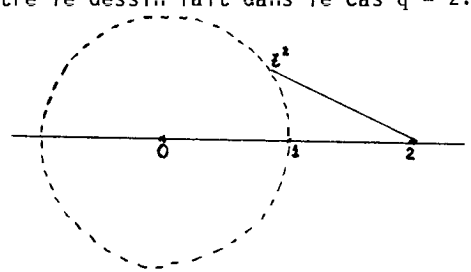
On a ainsi une égalité

$$(1)\quad q^n-1 = q-1 + \Sigma_x \frac{q^n-1}{q^{d(x)}-1}$$

où, dans la sommation, x parcourt un ensemble de représentants dans k^* de l'ensemble des orbites non réduites à un point. Cet ensemble n'est vide que si $k = Z$, i.e. si $n = 1$.

On suppose $n > 1$. Il résulte du lemme 2 que $\Phi_n(q)$ divise tous les termes de l'égalité (1) autres que $q-1$. Il divise donc $q-1$. Ceci est impossible.

En effet, $\Phi_n(q) = \prod(q-z^r)$ est un produit de facteurs de module $> q-1$ comme le montre le dessin fait dans le cas $q = 2$.



Donc, $n = 1$ et $k = \mathbb{Z}$ est commutatif.

Il suffit donc d'étudier les corps finis commutatifs. Ils sont connus depuis Galois. On les appelle quelquefois corps de Galois.

Théorème II.7 (structure des corps finis)

1. *Un corps fini* k *est de caractéristique un nombre premier* p. *Si* $[k:\mathbb{F}_p] = n$, *il a* p^n *éléments.*

2. *Réciproquement, pour tout nombre premier* p *et tout entier* $n > 1$, *il existe un corps à* p^n *éléments. Il est corps de décomposition sur* $\mathbb{F}_p$ *du polynôme* $X^{p^n}-X$.

3. *Deux corps finis ayant le même nombre d'éléments sont isomorphes.*

Démonstration

1. Evident

2 et 3. Soit k un corps à p^n éléments. Le groupe multiplicatif $k^* = k-\{0\}$ est d'ordre p^n-1. Donc, pour tout élément x de k^*, $x^{p^n-1}-1 = 0$ et, pour tout élément x de k, $x^{p^n}-x = 0$.

Le polynôme $X^{p^n}-X \in \mathbb{F}_p[X]$, qui est de degré n, a, au plus p^n racines distinctes dans k. Comme tout élément de k est racine de ce polynôme, on voit que ce polynôme a toutes ses racines distinctes et que k est corps de décomposition de ce polynôme. Ceci prouve 3.

Soit, réciproquement, k un corps de décomposition de $X^{p^n}-X$ sur $\mathbb{F}_p$.

L'ensemble k_1 des racines de $X^{p^n}-X$ dans k a p^n éléments. Il contient $\mathbb{F}_p$ car un élément a de $\mathbb{F}_p$ est tel que $a^p = a$ et, donc, $a^{p^n} = a$.

C'est un sous-corps de k. En effet, soient $a, b \in k_1$. Alors ab appartient à k_1 car $(ab)^{p^n} = a^{p^n}b^{p^n} = ab$, si a est non nul, a^{-1} appartient à k_1 car $(a^{-1})^{p^n} = (a^{p^n})^{-1} = a^{-1}$; et, enfin, $a-b$ appartient à k_1, en vertu du lemme suivant.

Lemme

Soient A *un anneau de caractéristique le nombre premier* p, $n \in \mathbb{N}^*$, $a,b \in A$.

Alors, $(a-b)^{p^n} = a^{p^n}-b^{p^n}$

Démonstration

Il suffit de traiter le cas $n = 1$. Alors, $(a-b)^p = a^p-pa^{p-1}b+\ldots+(-1)^i\binom{p}{i}a^{p-i}b^i+\ldots+(-1)^pb^p$. Le résultat provient de ce que $\binom{p}{i}$ est divisible par p, pour $i = 1,\ldots,p-1$ et de ce que $(-1)^p = -1$, si p est impair de manière évidente, et, si $p = 2$, parce que $1 = -1$ dans A.

Comme les racines de $X^{p^n}-X$ dans k sont distinctes, $k_1 = k$ et k a p^n éléments.

Théorème II.8

Le groupe multiplicatif d'un corps fini est cyclique

Démonstration

On va démontrer le résultat plus général suivant:

Un sous-groupe fini G *du groupe multiplicatif* k^* *d'un corps* k *est cyclique.*

Soient n *l'ordre de* G, r *la borne supérieure des ordres des éléments de* G.

On sait, alors, que, pour tout $x \in G$, $x^n = 1$, i.e. que G est l'ensemble des racines n-ièmes de l'unité dans k^* et, comme l'ordre de G est n, que le polynôme X^n-1 a n racines distinctes dans k. On va démontrer que l'ordre de tout élément de G divise r.

Il en résultera que G est un ensemble de racines de X^r-1 dans k et donc que r est égal à n. *Le groupe* G *sera donc cyclique engendré par un élément* x *d'ordre* r.

Soit $y \in G$ un élément d'ordre s ne divisant pas r. Il existe un nombre premier q et un entier m tel que $s = q^m s'$ et q^m ne divise pas r. Donc, $r = q^u r'$ avec $0 \leqslant u < m$ et r' non multiple de q. L'élément $x' = x^{q^u}$ a pour ordre r' et l'élément $y' = y^{s'}$ pour ordre q^m. L'élément x'y' a pour ordre $q^m r'$, strictement supérieur à r, ce qui est absurde, en vertu du lemme suivant de théorie des groupes.

Lemme

Soient G *un groupe,* x *(resp.* y*) un élément d'ordre* m *(resp.* n*)* tels que $xy = yx$ et $(m,n) = 1$. *L'ordre de* xy *est* mn.

Démonstration

D'une part, $(xy)^{mn} = (x^m)^n (y^n)^m = 1$. Si d'autre part, $(xy)^q = 1$, $x^q = y^{-q}$; donc $1 = x^{mq} = y^{-mq}$ et n divise mq; par conséquent, n divise q. De même, m divise q et par suite, mn divise q.

5. Anneau de décomposition d'un polynôme unitaire

Il peut être utile d'avoir pour les anneaux, à condition de considérer des polynômes *unitaires*, l'analogue de certains résultats précédents.

Proposition II,9

Soient A *un anneau,* X *une indéterminée,* f(X) *un polynôme unitaire* $\in A[X]$.

Il existe un anneau B *contenant* A *comme sous-anneau tel que*

1. *Dans* $B[X]$, $f(X) = \prod_{i=1}^{n} (X-x_i)$
2. $B = A[x_1,\ldots,x_n]$

Démonstration

On va donner deux constructions différentes d'un tel annneau B.

1ère construction

Soient $A_1 = A[X]/(f(X))$, x_1 la classe de X modulo (f(X)). Comme f(X) est unitaire, $A \cap (f(X)) = (0)$ et on peut identifier A à un sous-anneau de A_1 en sorte que $A_1 = A[x_1]$. Remplaçant A par A_1, f(X) par le polynôme unitaire $f(X)/(X-x_1)$ à coefficients dans A_1, on obtient A_2, x_2. Procédant ainsi, de proche en proche, on obtient un anneau A_n et des éléments $x_1,\ldots,x_n$ tels que $A_n = A[x_1,\ldots,x_n]$ et $f(X) = \prod_{i=1}^{n}(X-x_i)$.

2-ième construction

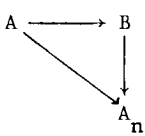
Soit $f(X) = X^n + \sum_{i=1}^{n} a_i X^{n-i}$. *On introduit des indéterminées* $T_1,\ldots,T_n$ *et on désigne par* $s_i(T_1,\ldots,T_n)$ *la i-ème fonction symétrique élémentaire de* $T_1,\ldots,T_n$, $s_i(T_1,\ldots,T_n) = \Sigma\, T_{j_1}\ldots T_{j_i}$, la sommation étant étendue aux suites $j_1,\ldots,j_i$ strictement croissantes d'éléments de $\{1,\ldots,n\}$.

Soient B *l'anneau quotient* $A[T_1,\ldots,T_n]/(s_i(T_1,\ldots,T_n) - (-1)^i a_i)$, x_i *la classe de* T_i $(i = 1,\ldots,n)$.

Si C est une A-algèbre, d'homomorphisme structural ρ, tel que, dans $C[X]$, le polynôme ${}^{\rho}f(X)$, obtenu en appliquant ρ aux coefficients de f(X), soit de la forme $\prod_{i=1}^{n}(X-x_i)$, il existe un homomorphisme ϕ et un seul de A-algèbres de $A[T_1,\ldots,T_n]$ dans B tel que $\phi(T_i) = y_i$ $(i = 1,\ldots,n)$.

Un calcul classique montre que $\phi(s_i(T_1,\ldots,T_n)) = (-1)^i \rho(a_i)$ $(i = 1,\ldots,n)$ et par conséquent, ϕ définit, par passage au quotient, un homomorphisme ψ de A-algèbres de B dans C tel que $\psi(x_i) = y_i$.

On déduit de l'existence, qui en résulte, d'un diagramme commutatif



où $A \longrightarrow B$ et $A \longrightarrow A_n$ sont les homomorphismes de structure et de l'injectivité de $A \longrightarrow A_n$, que l'homomorphisme: $A \longrightarrow B$ est injectif.

Il en résulte que l'anneau B répond à la question.

Remarque

Si A est un corps, en remplaçant B par son quotient par un idéal maximal, on obtient un corps de décomposition de f(X) sur A.

III. Eléments de théorie de Galois des extensions finies

L'origine historique de la théorie de Galois est la théorie des équations algébriques.

Soient k un corps, K/k une extension de k.

Un k-*automorphisme de* K est un isomorphisme de K sur K prolongeant 1_k. Le groupe des k-automorphismes de K, pour la composition, est appelé le *groupe de* Galois *de l'extension* K/k. Il est noté *Gal*(K/k), ou $G_{K/k}$.

Soit f(X) *un polynôme non constant* $\in k[X]$. *Le groupe de* Galois *de* f(X) *est le groupe Gal*(K/k) *où* K *est un corps de décomposition de* f(x) *sur* k.

L'étude du groupe de Galois du polynôme f(X) fournit des renseignements sur les racines du polynôme.

La théorie de Galois *est souvent utilisée en algèbre commutative ou géométrie algébrique de manière un peu différente.*

Supposons, par exemple, qu'à *partir de données définies sur un corps* k, on ait obtenu un élément x d'une extension K/k et que l'on veuille vérifier que x appartient en fait à k. Une condition nécéssaire évidente pour qu'il en soit ainsi est que x soit invariant par tout k-automorphisme de K. *La théorie de* Galois *affirme que, sous certaines hypothèses, cette condition est aussi suffisante.*

Un problème analogue se pose en géométrie algébrique: ayant obtenu, à partir d'ensembles algébriques définis sur k, un ensemble algébrique défini sur une extension K/k de k (le plus souvent, K est une clôture algébrique de k), on veut vérifier que cet ensemble est, en fait, défini sur k. Il se traite de la même manière.

C'est sans doute cette deuxième utilisation de la théorie de Galois *qui justifie sa présentation actuelle.*

On va se limiter ici à la théorie de Galois des extensions *finies*,

laissant en exercices celle des extensions algébriques quelconques, importante si l'on remarque qu'en général la clôture algébrique d'un corps n'est pas une extension finie de celui ci, mais dont l'étude se ramène facilement à celle des extensions finies. |confer. exercice 28|

Il existe maintenant une *théorie* de Galois *des anneaux commutatifs* parfaitement au point et redonnant dans le cas des corps les résultats usuels. Le lecteur pourra se reporter aux exercices 5, 6, 7, 8, 9, 10 du chapitre 9 où à l'exposé très clair de (42).

Problème

Soient K/k *une extension du corps* k, G *un groupe d'automorphisme de* K.

L'ensemble $\{x \in K/ \quad s \in G, s(x) = x\}$ *est un sous-corps de* K *appelé corps des invariants de* G *est noté* $Inv(G)$ *ou* K^G. *Si* G *est un sous-groupe de* $Gal(K/k)$, $Inv(G)$ *contient* k.

Le problème posé est le suivant:

A-*t-on l'égalité* $k = Inv(Gal(K/k))$ (ou avec les autres notations $k = K^{G}_{K/k}$) ?

Le théorème fondamental de la théorie de Galois *affirme qu'il en est bien ainsi, sous certaines hypothèses, pour des extensions algébriques finies.*

On va examiner ici quelques cas particuliers simples qui mettent en évidences les faits essentiels.

Une idée naturelle est la suivante: l'égalité $k = Inv(Gal(K/k))$ est vraie si K/k a "suffisamment" d'automorphismes.On verra qu'un manque d'automorphisme peut être du à deux causes différentes: non normalité ou non séparabilité.

1. $K = k$. Alors $Gal(K/k) = \{1_K\}$ et $Inv(Gal(K/k)) = k$
2. $k = \mathbb{R}$, $K = \mathbb{C} = \mathbb{R}(i)$ où $i^2 = -1$.

Alors $Gal(K/k) = \{1_K, s\}$ où s est la conjugaison: $a+bi \longrightarrow a-bi$ $(a, b \in \mathbb{R})$.

L'élément a+bi appartient à $Inv(Gal(K/k))$ si et seulement si a+bi = a-bi, i.e. si b = 0. Donc, $Inv(Gal(K/k)) = k$.

3. Un exemple analogue est fourni par $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$
4. $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$.

Il est clair que $irr(X, \sqrt[3]{2}, \mathbb{Q}) = X^3 - 2 = (X - \sqrt[3]{2})(X - j\sqrt[3]{2})(X - j^2\sqrt[3]{2})$ où $j = \cos(2\pi/3) + i \sin(2\pi/3)$.

Si $s \in Gal(K/k)$, $s(\sqrt[3]{2})$ est forcément un conjugué de $\sqrt[3]{2}$ dans K, i.e. est $\sqrt[3]{2}$. Il en résulte que $s = 1_K$.

Par conséquent, $Inv(Gal(K/k)) = K \neq k$.

L'inégalité $Inv(Gal(K/k)) \neq k$ *résulte du fait suivant:* le polynôme irréductible X^3-2 de $k[X]$ a une racine dans K mais ne se décompose pas dans $K[X]$ en facteurs du premier degré.

On dit que l'extension K/k n'est pas *normale* (ou *quasi-galoisienne*)

On laisse au lecteur afin de se persuader que la raison invoquée est effective le soin de traiter l'exemple où $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2})$ Il existe alors un k-automorphisme s (resp. t) tel que $s(\sqrt[3]{2}) = j\sqrt[3]{2}$ (resp. $t(\sqrt[3]{2}) = j^2\sqrt[3]{2}$).

On vérifie $Inv(Gal(K/k)) = k$.

5. *Soient* Y *une indéterminée,* $k = \mathbb{F}_2(Y)$, $k = k(x)$ *où* $irr(X,x,k) = X^2-Y$.

Alors $irr(X,x,k) = (X-x)^2$. Il en résulte que si $s \in Gal(K/k)$, $s(x) = x$ et donc $Gal(K/k) = \{1_K\}$. Par conséquent $Inv(Gal(K/k) = K \neq k$.

L'inégalité $Inv(Gal(K/k)) \neq k$ *résulte du fait suivant:* le polynôme irréductible X^2-Y de $k[X]$ a une racine multiple.

On dit que l'extension K/k n'est pas *séparable*.

On verra que ce phénomène ne se produit pas en caractéristique 0;

On va étudier de manière plus approfondie les notions d'extensions normale et séparable puis la théorie de Galois des extensions algébriques finies.

On étudiera plus en détail des exemples numériques (§9)

1. Extensions normales ou quasi-galoisiennes

Proposition III.1

Soient k *un corps,* K *une extension algébrique de* k, $\overline{K}$ *une clôture algébrique de* K.

Les assertions suivantes sont équivalentes:

(i) tout polynôme irréductible de $k[X]$ *qui a une racine dans* K *se décompose dans* $K[X]$ *en facteurs du premier degré.*

(ii) tout homomorphisme t *de* K *dans* $\overline{K}$ *prolongeant* 1_k *est un isomorphisme de* K *sur* K *i.e. ce qu'on appelle un* k*-automorphisme de* K

Démonstration

(i) $\Longrightarrow$ (ii) - *On démontre d'abord* $t(K) \subset K$.

Soient $a \in K$, $f(X) = \mathrm{irr}(X,a,k)$. L'homomorphisme t applique a sur un conjugué de a sur k, i.e. une racine de $f(X)$. Comme $f(X)$ se décompose en facteurs du premier degré dans $K[X]$, $t(a)$ appartient à K.

On démontre ensuite $t(K) = K$.

C'est clair si $[K:k] < \infty$ car alors $[t(K):k]$ étant égal à $[K:k]$, $[K:t(K)] = 1$ et $K = t(K)$.

Dans le cas général, soient $a \in K$, $f(X) = \mathrm{irr}(X,a,k) = (X-a_1)\ldots(X-a_n)$ avec $a_1 = a$, $a_i \in K$, $K' = k(a_1,\ldots,a_n)$, t' la restriction de t à K'

Alors, $[K':k] < \infty$. Comme pour $i = 1,\ldots,n, t'(a_i)$ est conjugué de a_i sur k, il existe $j \in \{1,\ldots,n\}$ tel que $t'(a_i) = a_j$. Par conséquent, $t'(K')$ est contenu dans K' et il résulte du premier cas envisagé que $t'(K') = K'$. Il existe donc $a_r \in K'$ tel que $a = t'(a_r) = t(a_r)$ et donc t est surjectif.

(ii) $\Longrightarrow$ (i). Soit $f(X)$ un polynôme irréductible de $k[X]$ admettant une racine a dans K. Soit $f(X) = c(X-a_1)\ldots(X-a_n)$ avec $a_1 = a$ la décomposition de $f(X)$ en facteurs du premier degré dans $\overline{K}[X]$.

Le composé de l'injection de $k(a_i)$ dans $\overline{K}$ et de l'isomorphisme de $k(a_1)$ sur $k(a_i)$ prolongeant 1_k et appliquant a_1 sur a_i se prolonge en un homomorphisme t de K dans $\overline{K}$. Par hypothèse, $t(K)$ est contenu dans K. Donc, $t(a_1) = a_i$ appartient à K et $f(X)$ se décompose en facteurs du premier degré dans $K[X]$.

Définition

Une extension K/k *satisfaisant aux conditions équivalentes de la proposition* III.1 *est dite quasi-galoisienne ou normale .*

Exemples

1. *Soient* k *un corps,* $f(X)$ *un polynôme irréductible de* $k[X]$, K *le corps de décomposition de* $f(X)$ *sur* k.

L'extension K/k *est normale*: soient, en effet, $f(X)=(X-a_1),..(X-a_n)$ $K = k(a_1,\ldots,a_n)$, t un homomorphisme de K dans $\overline{K}$ prolongeant 1_k. Il est clair que $t(a_i) = a_j$ pour un indice j convenable. Donc, $t(K)$ est contenu dans K.

Par exemple, l'extension $\mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2})$ (où j est une racine primitive cubique de l'unité) de $\mathbb{Q}$ est normale car elle est le corps de décomposition sur $\mathbb{Q}$ du polynôme irréductible X^3-2.

2. L'extension $\mathbb{Q}(\sqrt[3]{2})$ n'est pas normale car $\mathrm{irr}(X,\sqrt[3]{2},\mathbb{Q}) = X^3-2$ a une ra-

cine dans $\mathbb{Q}(\sqrt[3]{2})$ mais ne se décompose pas en facteurs du premier degré dans $\mathbb{Q}(\sqrt[3]{2})[X]$.

3. *Soit* $k \subset L \subset K$ *une tour d'extensions algébriques.*

Si K/k *est normale, il en est de même de* K/L: en effet, un homomorphisme de K dans $\overline{K}$ prolongeant 1_L prolonge, a fortiori, 1_k et est donc un automorphisme de K.

Par contre, *l'extension* L/k *n'est pas forcément normale*: ainsi $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ est une sous-extension non normale de l'extension normale $\mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2})/\mathbb{Q}$.

On remarque les équivalences:

(i) L/k *est normale*

(ii) *pour tout* $s \in Gal(K/k)$, $s(L) = L$.

Démonstration

(i) $\Longrightarrow$ (ii): $s \in Gal(K/k)$ définit par restriction un homomorphisme de L dans $\overline{K}$. Comme L/k est normale, cet homomorphisme est un automorphisme de L. Donc, $s(L) = L$.

(ii) $\Longrightarrow$ (i): un homomorphisme t de L dans $\overline{K} = \overline{L}$ prolongeant 1_k se prolonge en un homomorphisme de K dans $\overline{K}$, et donc, puisque K/k est normale, en un automorphisme s de K. Donc, $s(L) = L$ et l'homomorphisme t est un automorphisme de L.

2. Extensions séparables

Définitions

1. *Soient* k *un corps,* X *une indéterminée,* f(X) *un polynôme non constant de* k[X], K *un corps de décomposition de* f(X) *sur* k.

On dit que f(X) *est séparable sur* k *s'il n'a que des racines simples dans* K.

Si le corps k *est de caractéristique* 0 *et si* f(X) *est irréductible dans* k[X], f(X) *est séparable:* il ne peut, en effet, avoir de racine commune avec son polynôme dérivé qui est de degré $d^\circ(f)-1$.

Il n'en est pas toujours de même en caractéristique $p > 0$: si, par exemple, $a \in k$ n'a pas de racine p-ème dans k, le polynôme $f(X) = X^p - a$ est irréductible dans k[X] mais n'est pas séparable car, b désignant une racine dans K, $f(X) = (X-b)^p$. On remarque que dans ce cas $f'(X) = pX^{p-1} = 0$.

2. *Soient* K/k *une extension de* k, $a \in K$ *algébrique sur* k.

On dit que a *est séparable sur* k *si* irr(X,a,k) *est un polynôme séparable sur* k.

Dire que a est séparable sur k c'est dire que le nombre de conjugués distincts de a dans un corps de décomposition de irr(X,a,k) sur k est égal au degré de ce polynôme.

3. *Une extension algébrique* K/k *de* k *est dite séparable si tout élément de* K *est séparable sur* k.

On introduira plus loin (chapitre 9) une notion plus générale d'extension séparable.

On va traduire d'une autre manière la notion de séparabilité.

Proposition III.2

Soient K/k *une extension algébrique du corps* k, s *un homomorphisme de* k *dans un corps algébriquement clos* Ω *algébrique sur* s(k).

1. *Le cardinal de l'ensemble* $\Phi_{s,\Omega}$ *des homomorphisme de* K *dans* Ω *prolongeant* s *ne dépend pas du couple* (Ω,s). *On note ce cardinal* $[K:k]_s$. *On l'appelle le degré séparable de* K/k.

2. *Si* K *est une extension algébrique monogène* k(a) *de* k, $[K:k]_s$ *est égal au nombre de racines distinctes de* f(X) = irr(X,a,k) *dans un corps de décomposition de* f(X) *sur* k.

Démonstration

1. Soit s' un homomorphisme de k dans un corps Ω' algébriquement clos algébrique sur s'(k'). Il existe un isomorphisme u de Ω dans Ω' prolongeant l'isomorphisme $s' \circ (s_1)^{-1}$ de s(k) dans s'(k') où s_1 est l'isomorphisme de k sur s(k) induit par s.

L'application: $t \longrightarrow u \circ t$ est une bijection de l'ensemble $\Phi_{s,\Omega}$ sur l'ensemble $\Phi_{s',\Omega'}$.

2. Soit Ω une clôture algébrique de K et donc de k. Alors, $[K:k]_s$ est le cardinal de l'ensemble $\Phi_{s,\Omega}$ où s est l'injection de k dans Ω.

L'application: $t \longrightarrow t(a)$ est une bijection de l'ensemble $\Phi_{s,\Omega}$ sur l'ensemble des racines (distinctes) de f(X).

Définition

Le cardinal $[K:k]_s$ *est appelé le degré séparable de l'extension algébrique* K/k.

Proposition III.3 (multiplicativité du degré séparable)

1. *Soient* L *un corps,* K *un sous-corps de* L, k *un sous-corps de* K,

On suppose L/k *algébrique.*

Alors, $[L:k]_s = [L:K]_s [K:k]_s$

2. *Soit* K/k *une extension finie* (et donc algébrique)

Alors $[K:k]_s \leqslant [K:k]$

Démonstration

1. Soit s un homomorphisme injectif de k dans un corps algébriquement clos Ω algébrique sur k.

Soit $(s_i)_{i\in I}$ la famille des homomorphismes distincts de K dans Ω prolongeant s en sorte que $[K:k]_s = \mathrm{card}(I)$. Si $i \in I$, soit $(t_{ij})_{j\in J(i)}$ la famille des homomorphismes distincts de L dans Ω prolongeant s_i en sorte que $[L:K]_s = \mathrm{card}(J(i))$.

Il est clair que $(t_{ij})_{i\in I, j\in J(i)}$ est la famille des homomorphismes distincts de L dans Ω prolongeant s. Donc, $[L:k]_s = \mathrm{card}((t_{ij})_{i\in I, j\in J(i)}) = [K:k]_s [L:K]_s$

2. Le corps K est de la forme $k(a_1,\ldots,a_n)$. On considère la tour

$$k \subset k(a_1) \subset k(a_1)(a_2) \subset \ldots \subset k(a_1,\ldots,a_{n-1})(a_n) = K$$

On utilise la propriété de multiplicativité du degré et du degré séparable et on remarque que l'inégalité $[K:k]_s \leqslant [K:k]$ est une conséquence immédiate de la proposition III.2.2 dans le cas où K est monogène = k(a) car $[K:k]$ est le degré de irr(X,a,k) et $[K:k]_s$ le nombre de racines distinctes de ce polynôme.

Proposition III.4

Soit K/k *une extension algébrique de* k.

Si K/k *est finie, les assertions suivantes sont équivalentes:*

(i) K/k *est séparable*

(ii) $[K:k] = [K:k]_s$

Démonstration

Cas monogène. On remarque les équivalences pour $a \in K$ *algébrique sur* k:

1. a *est séparable sur* k
2. $[k(a):k] = [k(a):k]_s$
3. k(a) *est séparable sur* k

L'équivalence de 1. et 2. est conséquence de la proposition III.2. L'implication 3 $\Rightarrow$ 1 est clair. L'implication 2 $\Rightarrow$ 3 résulte de ce que si $b \in k(a)$, $[k(b):k]_s = [k(a):k]_s / [k(a):k(b)]_s$, de ce que a est séparable sur k(b) car le polynôme irr(X,a,k(b)) divise irr(X,a,k) et donc de l'é

galité $[k(b):k]_s = [k(a):k]/[k(a):k(b)] = [k(b):k]$.

Cas général. On utilise la tour d'extensions:

$$k_o = k \subset k(a_1) \subset \ldots \subset k_{n-1} \subset k_n = k(a_1,\ldots,a_n) = K$$

où $k_i = k_{i-1}(a_i)$. L'égalité $[K:k] = [K:k]_s$ équivaut, compte tenu de la multiplicativité du degré et du degré séparable, aux égalités

$[k_i:k_{i-1}] = [k_i:k_{i-1}]_s$, i.e. à la séparabilité de a_i sur k_{i-1}.

Comme si a_i est séparable sur k, il l'est, a fortiori, sur k_{i-1}, on voit que (i) $\Longrightarrow$ (ii).

non(i) $\Longrightarrow$ non(ii). Soit, en effet, $a_1 \in K$ non séparable sur k. Alors $[k(a_1):k]$ est $> [k(a_1):k]_s$. La considération de la tour $k \subset k(a_1) \subset K$ montre alors l'inégalité $[K:k] > [K:k]_s$.

Remarque

Si a_i est algébrique sur k, $(i = 1,\ldots,n)$, l'extension $k(a_1,\ldots,a_n)/k$ est séparable.

Corollaire 1

Soit K/k *une extension algébrique du corps* k.

Les assertions suivantes sont équivalentes:

(i) K/k *est séparable*

(ii) pour toute sous-extension finie L/k *de* K/k, $[L:k] = [L:k]_s$

Corollaire 2

Soient K/k *une extension algébrique du corps* k, L *un sous-corps de* $\bar{K}$ *contenant* k.

Les assertions suivantes sont équivalentes:

(i) K/k *est séparable*

(ii) K/L *et* L/k *sont séparables*

Démonstration

Elle résulte si l'extension K/k est finie des égalités $[K:k] = [K:L][L:k]$ et $[K:k]_s = [K:L]_s[L:k]_s$ et des inégalités $[K:L] \geq [K:L]_s$ et $[L:k] \geq [L:k]_s$ qui montrent que $[K:k] = [K:k]_s$ si et seulement si $[K:L] = [K:L]_s$ et $[L:k] = [L:k]_s$.

Dans le cas général, il est clair que (i) $\Longrightarrow$ (ii).

(ii) $\Longrightarrow$ (i)

Soit $a \in K$. Il existe une sous-extension *finie* L'/k de L/k telle que irr(X,a,L) appartienne à L'[X]. Soit K' = L'(a). Les extensions K'/L' et L'/k sont séparables.

On déduit de ce qui précède que l'extension K'/k est séparable et donc que a est séparable sur k.

3. Elément primitif

Définition

Soient K/k *une extension du corps* k, $a \in K$.

On dit que a *est élément primitif de l'extension* K/k *si* $K = k(a)$.

1. Une condition nécessaire pour l'existence d'un élément primitif de l'extension K/k est, évidemment, que $d^\circ tr(K/k)$ soit inférieur ou égal à 1.

Il existe donc des extensions ne possédant pas d'élément primitif.

2. Le théorème de Lurŏth affirme l'exsitence d'un élément primitif pour une sous-extension, distincte de k, d'une extension transcendante pure K/k de degré de transcendance 1.

On s'intéresse ici à la question de l'existence d'éléments primitifs pour une extension algébrique finie K/k. *Le résultat essentiel est qu'il existe un tel élément si* K/k *est séparable.*

Si $n = [K:k]$ et si a est élément primitif de K/k, $irr(X,a,k)$ est de degré n.

Réciproquement, s'il existe $a \in K$ tel que $d^\circ(irr(X,a,k)) = [K:k]$, $K = k(a)$ et a est élément primitif de l'extension K/k.

Théorème III.5

Soit K/k *une extension finie séparable du corps* k.

Il existe un élément primitif de K/k.

Démonstration

Le résultat a déjà été établi si le corps k est fini (proposition II.6).

On suppose donc le corps k *infini.*

On va donner deux démonstrations du théorème, l'une utilisant la notion de degré séparable, l'autre ne l'utilisant pas.

1ère démonstration

On se ramène par récurrence au cas où $K = k(a_1,a_2)$ avec a_1, a_2 non nuls.

Soient $s_1,\ldots,s_n$ les homomorphismes distincts de K dans une clôture algébrique $\overline{K}$ de K prolongeant l'injection de k dans $\overline{K}$ en sorte que $[K:k]_s = n$ et donc puisque K/k est séparable, $[K:k] = n$.

Le polynôme $f(X) = \prod_{1\leqslant i<j\leqslant n}(s_i-s_j)(a_2X+a_1)$ est non nul : des égalités $s_i(a_1) = s_j(a_1)$ et $s_i(a_2) = s_j(a_2)$ impliqueraient l'égalité $s_i = s_j$.

Comme le corps k est *infini*, il existe $c \in k$ tel que $f(c) \neq 0$ et donc tel que, si $i \neq j$, $s_i(a_2c+a_1) \neq s_j(a_2c+a_1)$. Les restrictions au corps $k(a_2+ca_1)$ des homomorphismes $s_1,\ldots,s_n$ sont donc des homomorphismes *distincts* de $k(a_2+ca_1)$ dans $\overline{K}$ prolongeant l'inclusion de k dans $\overline{K}$. Par conséquent,

$$n \leqslant [k(a_2c+a_1):k]_s = [k(a_2c+a_1):k] \leqslant [K:k] = n$$

d'où $[K:k(a_2c+a_1)] = 1$ et $K = k(a_2c+a_1)$. L'élément a_2c+a_1 est donc primitif.

2ème démonstration

Soient $f(X) = \mathrm{irr}(X,a_1,k)$ et $g(X) = \mathrm{irr}(X,a_2,k)$, L un corps de décomposition de $f(X)g(X)$ sur k, $x_1 = a_1,\ldots,x_r$, $y_1 = a_2,\ldots,y_s$ les racines respectives de f(X) et g(X) dans L. L'équation $y_1X+x_1 = y_jX+x_k$ a, pour $j \neq 1$, au plus une racine dans k.

Soit $c \in k$ distinct de toutes les racines de ces équations en sorte que y_jc+x_k est distinct de y_1c+x_1 pour tout k et tout $j \neq 1$. Soit $\theta = y_1c+x_1 = a_2c+a_1$.

L'élément a_2 est la seule racine commune des polynômes g(X) et $f(\theta-cX) = 0$ et elle est *simple*. Le p.g.c.d. de ces deux polynômes est donc $X-a_2$. Il appartient à $k(\theta)[X]$ comme g(X) et $f(\theta-cX)$. Donc, a_2 appartient à $k(\theta)$. Il en est alors de même de $a_1 = \theta-a_2c$.

Le résultat suivant donne une condition nécéssaire et suffisante pour qu'une extension finie admette un élément primitif.

Théorème III.6

Soit K/k *une extension finie du corps* k.

Les assertions suivantes sont équivalentes:

(i) K/k *a un élément primitif.*

(ii) l'ensemble des sous-corps de K *contenant* k *est fini*

Démonstration

Les équivalences sont claires si k *est fini ou ce qui est équivalent si* K *est fini,* car alors (ii) est satisfaite et il en est de même de (i) puisque le groupe multiplicatif K^* de K est cyclique engendré par un élément a et que par conséquent $K = k(a)$.

On peut donc supposer k *infini*

(ii) $\Longrightarrow$ (i). La démonstration se fait par récurrence sur l'entier n tel que $K = k(a_1,\ldots,a_n)$. Le seul point délicat est celui où $n = 2$.

L'ensemble des sous-corps de K contenant k de la forme $k(a_1+ca_2)$, où c parcourt k, est fini par hypothèse. Comme k est infini, il existe deux éléments distincts c_1 et c_2 de k tels que $k(a_1+c_1a_2) = k(a_1+c_2a_2)$.

Soit $a = a_1+c_1a_2$. L'élément $(c_2-c_1)a_2$ appartient à k(a) et il en est donc de même de a_2 et a_1. Par conséquent, $k(a_1,a_2) = k(a)$ et a est élément primitif de l'extension K/k.

(i) $\Longrightarrow$ (ii). On suppose donc $K = k(a)$. Soit F un sous-corps de K contenant k.

Le polynôme $f_F(X) = \mathrm{irr}(X,a,F)$ divise $f_k(X) = \mathrm{irr}(X,a,k)$. Le polynôme $f_k(X)$ n'a qu'un nombre fini de diviseurs dans $K[X]$.

Il suffit de démontrer que l'application $F \longmapsto f_F(X)$ de l'ensemble des sous-corps de K contenant k dans l'ensemble des diviseurs de $f_k(X)$ dans $K[X]$ est injective.

Soit F_o le sous-corps de K engendré sur k par les coefficients de $f_F(X)$.

Le polynôme $f_F(X)$ qui est irréductible dans $F[X]$ l'est a fortiori dans $F_o[X]$ car F_o est contenu dans F.

Il est clair que $K = F_o(a) = F(a)$. Or, $[K:F_o] = d^\circ f_{F_o}(X)$ et $[K:F] = d^\circ f_F(X)$.

Donc, $[K:F_o] = [K:F]$ soit $F = F_o$.

4. Le théorème fondamental de la théorie de Galois des extensions finies

La proposition suivante précise les conclusions suggérées par les exemples de l'introduction de III.

Proposition III.7 (première partie du théorème fondamental)

Soient k un corps, K/k une extension algébrique de k.

Les assertions suivantes sont équivalentes:

(i) $Inv(Gal(K/k)) = k$

(ii) l'extension K/k est normale et séparable

Démonstration

L'assertion (ii) peut s'énoncer:

pour tout $x \in K$, $\mathrm{irr}(X,x,k)$ *a toutes ses racines simples et contenues dans* K (prop. III.1 et III.2).

(i) $\Longrightarrow$ (ii)

Soient $x \in K$, $x_1 = x, \ldots, x_n$ les racines distinctes de $irr(X,x,k)$ dans K.

Tout élément s de $Gal(K/k)$ permute $x_1, \ldots, x_n$. Il laisse donc invariant les coefficients du polynôme $g(X) = \prod_{i=1}^{n} (X - x_i)$ qui sont les fonctions symétriques élémentaires de $x_1, \ldots, x_n$.

Par hypothèse, g(X) qui est, a priori, un élément de $K[X]$, appartient, en fait, à $k[X]$. Il est donc nécessairement égal à $irr(X,x,k)$ qui a ainsi toutes ses racines simples et contenues dans K.

(ii) $\Longrightarrow$ (i)

Soit $x \in K$ n'appartenant pas à k, en sorte que $d^\circ(irr(X,x,k)) > 1$.

Par hypothèse, il existe $y \in K$ distinct de x et racine de $irr(X,x,k)$.

On sait alors qu'il existe un homomorphisme de k(x) dans une clôture algébrique $\overline{K}$ de K prolongeant 1_k et appliquant x sur y et qu'il se prolonge en un homomorphisme de K dans $\overline{K}$. Cet homomorphisme applique K dans K. C'est un k-automorphisme de K, i.e. un élément de $Gal(K/k)$, qui ne laisse pas invariant x.

Par conséquent, x n'appartient pas à $Inv(Gal(K/k))$.

Proposition III.8 (deuxième partie du théorème fondamental)

Soient K *un corps,* G *un groupe fini d'automorphismes de* K, $k = Inv(G)$.

1. *L'extension* K/k *est algébrique, normale et séparable.*
2. $[K:k] = card(G)$ *et* $G = Gal(K/k)$.

Démonstration

1. Soient $x \in K$, $\{x_1 = x, \ldots, x_r\} = \{s(x)/x \in G\}$ où $x_i \neq x_j$ si $i \neq j$, $g(X) = \prod_{i=1}^{r} (X - x_i)$.

Pour tout $s \in G$, il existe une permutation π de $\{1,\ldots,r\}$ telle que $s(x_i) = x_{\pi(i)}$.

Il en résulte que les coefficients de g(X), qui sont fonctions symétriques des éléments $x_1, \ldots, x_r$, sont invariants par G et donc appartiennent à k.

Comme $g(x) = 0$, x est algébrique sur k. De plus le polynôme $irr(X,x,k)$ divise g(X) et a donc toutes ses racines simples dans K.

2. On déduit de ce qui précède que, pour tout $x \in K$ $[k(x):k] \leqslant r \leqslant n = card(G)$.

Si on savait que K/k est finie, on pourrait conclure que $[K:k] \leqslant n$ au moyen du théorème de l'élément primitif. Il faut procéder autrement: soit $x \in K$ tel que $[k(x):k]$ soit maximal. Si $y \in k$, $k(x,y)$ est de la forme $k(z)$ (théorème de l'élément primitif).

Donc, par maximalité de $[k(x):k]$, $[k(x,y):k] = [k(x):k]$ et $k(x,y) = k(x)$. Par conséquent, y appartient à $k(x)$ et $K = k(x)$. Ainsi, $[K:k] \leqslant n$.

L'extension K/k est finie et normale; donc, $\mathrm{card}(Gal(K/k)) = [K:k]_s$ Elle est séparable; donc, $[K:k]_s = [K:k]$. Par suite, $\mathrm{card}(Gal(K/k)) = [K:k] \leqslant \mathrm{card}(G) = n$. Comme G est contenu dans $Gal(K/k)$, on voit que $G = Gal(K/k)$ et $\mathrm{card}(G) = [K:k]$.

Définition

Une extension algébrique K/k *du corps* k *est dite galoisienne si elle est normale et séparable.*

Théorème III.9 (théorème fondamental de la théorie de Galois)

Soit K/k *une extension galoisienne de degré fini du corps* k.

L'application: $L \longmapsto Gal(K/L)$ *est une bijection décroissante de l'ensemble* (ordonné par inclusion) *des sous-corps de* K *contenant* k *sur l'ensemble* (ordonné par inclusion) *des sous-groupes du groupe de Galois* $Gal(K/k)$.

La bijection réciproque fait correspondre au sous-groupe H *de* $Gal(K/k)$ *le sous-groupe* $Inv(H)$ (noté aussi K^H) *de* K.

Démonstration

Soit L *un sous-corps de* K *contenant* k.

Alors, $Gal(K/L)$ est un sous-groupe de $Gal(K/k)$.

De plus, comme K/L est galoisienne comme K/k, il résulte de la proposition III.9 que $L = Inv(Gal(K/L))$.

Soit H *un sous-groupe de* $Gal(K/k)$.

Alors, $Inv(H)$ est un sous-corps de K contenant k. Il résulte de la proposition III.10 que $H = Gal(K/Inv(H))$.

On verra dans le paragraphe 5 (exemple 1) que, avec les notations et hypothèses du théorème III.9, si L est un sous-corps de K contenant k, l'extension L/k est séparable mais n'est pas forcément normale.

On va préciser maintenant ce point.

Définition

Des sous-corps L *et* L' *de* K *contenant* k *sont dits conjugués sur* k

s'il existe $s \in Gal(K/k)$ *tel que* $s(L) = L'$.

Proposition III.10 (sous-corps et sous-groupes conjugués)

Soit K/k *une extension galoisienne de degré fini du corps* k.

Soient L *et* L' *deux sous-corps de* K *contenant* k.

Les assertions suivantes sont équivalentes:

(i) L *et* L' *sont conjugués sur* k

(ii) $Gal(K/L)$ *et* $Gal(K/L')$ *sont des sous-groupes conjugués de* $Gal(K/k)$

Démonstration

(i) $\Longrightarrow$ (ii)

Soit $s \in Gal(K/k)$ tel que $s(L) = L'$. Si $t \in Gal(K/L)$ $s \circ t \circ s^{-1}$ appartient à $Gal(K/L')$: en effet, pour $x \in L'$, $t(s^{-1}(x)) = s^{-1}(x)$ et donc $(s \circ t \circ s^{-1})(x) = x$. On en déduit l'égalité $Gal(K/L') = s \circ Gal(K/L) \circ s^{-1}$, i.e. le fait que $Gal(K/L)$ et $Gal(K/L')$ sont conjugués.

(ii) $\Longrightarrow$ (i)

Soient H et $H' = s \circ H \circ s^{-1}$, où $s \in Gal(K/k)$, deux sous-groupes conjugués de $Gal(K/k)$.

Il est clair que $Inv(H') = s(Inv(L))$: si $x \in Inv(H)$ et $s \circ t \circ s^{-1}$ est un élément de H' (où $t \in H$), $s \circ t \circ s^{-1}(s(x)) = s(t(x)) = s(x)$ et donc $s(x)$ appartient à $Inv(H')$.

Ainsi, $s(Inv(H)) \subset Inv(H')$. On obtient de même $s^{-1}(Inv(H')) \subset Inv(H)$ d'où $Inv(H') \subset s(Inv(H))$ et $Inv(H') = s(Inv(H))$.

On déduit de la remarque du paragraphe 1 que dire que l'extension L/k est normale c'est dire qu'il n'existe pas de conjugué de L sur k distinct de L.

Corollaire

Soit K/k *une extension galoisienne de degré fini du corps* k, L *un sous-corps de* K *contenant* k.

1. Les assertions suivantes sont équivalentes:

(i) L'*extension* L/k *est galoisienne* (i.e. est normale)

(ii) $Gal(K/L)$ *est un sous-groupe distingué* (ou normal) *de* $Gal(K/k)$

2. Si elles sont vérifiées, l'application qui à un élément de $Gal(K/k)$ *fait correspondre sa restriction à* L *définit un isomorphisme de groupes de* $Gal(K/k)/Gal(K/L)$ *sur* $Gal(L/k)$.

Démonstration

1. est une conséquence immédiate de la proposition III.10: un sous-grou-

pe est distingué s'il est égal à ses conjugués.

2. si $s \in Gal(K/k)$, comme L/k est normale, $s(L) = L$ et donc la restriction s/L de s à L est un élément de $Gal(L/k)$.

L'application: $s \longmapsto s/L$ est un homomorphisme de $Gal(K/k)$ dans $Gal(L/k)$. Il résulte du théorème de prolongement et de la normalité de K/k qu'elle est surjective.

Son noyau est $Gal(K/L)$, d'où le résultat.

5. Etudes d'exemples

1. Théorie de Galois des corps finis

Soient K un corps fini à p^n éléments, $k = \mathbb{F}_p$ son corps premier.

Comme la caractéristique est p, l'application: $x \longmapsto x^p$ est un automorphisme de K.

Cet automorphisme laisse invariant tout élément de k. C'est donc un élément s de $Gal(K/k)$ (substitution de Frobenius).

L'application $\theta: r \longmapsto s^r$ est un homomorphisme du groupe additif $\mathbb{Z}$ dans le groupe $Gal(K/k)$. Son noyau est (n): en effet, si $m < n$, il existe $x \in K$ tel que $x^{p^m} \neq x$.

L'extension K/k est galoisienne: elle est normale car K est le corps de décomposition sur k du polynôme $X^{p^n} - X$; elle est séparable comme ce polynôme.

Donc, l'ordre de $Gal(K/k)$ est égal au degré n de l'extension K/k. L'application θ est donc surjective et $Gal(K/k)$ *est cyclique d'ordre* n *engendré par* s.

Un sous-groupe de $Gal(K/k)$ est un groupe cyclique H engendré par s^m, où m est un diviseur de n. Le groupe H est d'ordre m/n. Le corps des invariants de H est le corps $\mathbb{F}_{p^{m/n}}$ et H en est le groupe de Galois sur k.

2. Extension galoisienne de groupe de Galois le groupe symétrique S_n

Soient k un corps, f(X) un polynôme non constant séparable de $k[X]$, *K le corps de décomposition de f(X) sur k,* $K = k(a_1, \ldots, a_n)$ *où* $f(X) = c\prod_{i=1}^{n}(X - a_i)$.

Si $s \in Gal(K/k)$ (groupe de Galois de f(X) sur k), il existe un unique élément σ_s du groupe symétrique S_n tel que, pour tout $i \in \{1, \ldots, n\}$ $s(a_i) = a_{\sigma_s(i)}$.

L'application: $s \longmapsto \sigma_s$ *de* $Gal(K/k)$ *dans* S_n *est un homomorphisme de groupe.*

Cet homomorphisme est injectif et permet donc *d'identifier* $Gal(K/k)$ *à un sous-groupe de* S_n.

On verra dans l'exemple 3 que $Gal(K/k)$ n'est pas toujours égal à S_n. Il est toutefois des cas importants où il en est ainsi, notamment le cas suivant:

Soient $c_1,\ldots,c_n$ des nombres complexes algébriquement indépendants sur $\mathbb{Q}$, $f(X) = X^n - c_1X^{n-1} + \ldots + (-1)^i c_i X^{n-i} + \ldots + (-1)c_n$.

On considère $f(X)$ comme un polynôme à coefficients dans $k=\mathbb{Q}(c_1,.c_n)$. On va démontrer que le groupe de Galois de $f(X)$ sur k est S_n.

On pourra en déduire, par exemple, que si $n \geqslant 5$, on ne peut résoudre l'équation $f(X) = 0$ par radicaux comme c'est la cas pour $n = 1,2$ (formule usuelle), 3 (formule de Cardan), 4 (formule de Ferrari). (exercice 26).

Soient, plus généralement, k' *un corps,* $c_1,\ldots,c_n$ *des éléments d'une extension de* k' *algébriquement indépendants sur* k', $k = k'(c_1,..,c_n)$, $f(X)$ *le polynôme*

$$(*)\quad X^n - c_1X^{n-1} + \ldots + (-1)^i c_i X^{n-i} + \ldots + (-1)^n c_n$$

$K = k(a_1,\ldots,a_n)$ *où* $f(X) = \prod_{i=1}^{n} (X-a_i)$ *le corps de décomposition de* $f(X)$ *sur* k.

Alors, le groupe de Galois *de* $f(X)$ *sur* k *est isomorphe au groupe symétrique* S_n.

On va démontrer le lemme suivant:

Lemme 1

Les éléments $a_1,\ldots,a_n$ *sont algébriquement indépendants sur* k'.

Démonstration

Soit $g(X_1,\ldots,X_n) \in k'[X_1,\ldots,X_n]$ tel que $g(a_1,\ldots,a_n) = 0$.

Si $\sigma \in S_n$, on note ${}^{\sigma}g$ le polynôme $g(X_{\sigma(1)},\ldots,X_{\sigma(n)})$. Le polynôme $h(X_1,\ldots,X_n) = \prod_{\sigma \in S_n} ({}^{\sigma}g)$ est symétrique et, en vertu d'un théorème classique, il est de la forme $\phi(S_1(X_1,\ldots,X_n),\ldots,S_n(X_1,\ldots,X_n))$ où $S_1,\ldots,S_n$ sont les fonctions symétriques élémentaires.

Comme $S_i(a_1,\ldots,a_n) = c_i$, on voit que $\phi(c_1,\ldots,c_n) = 0$. Puisque $c_1,\ldots,c_n$ sont algébriquement indépendants sur k', $\phi(S_1,\ldots,S_n) = 0$.

Donc, $h(X_1,\ldots,X_n) = 0$ et $g(X_1,\ldots,X_n) = 0$.

On en déduit l'existence, pour tout $\sigma \in S_n$ d'un k'-automorphisme s de K tel que $\sigma = \sigma_s$, i.e. $s(a_i) = a_{\sigma(i)}$. En effet, $K = k'(a_1,\ldots,a_n)$

L'automorphisme s, qui laisse invariantes les fonctions symétriques élémentaires $c_1,\ldots,c_n$ de $a_1,\ldots,a_n$, est un k-automorphisme.

Ainsi l'application $\cdot\ s \longmapsto \sigma_s$ de $Gal(K/k)$ dans S_n est surjective et donc bijective.

Remarques

1. On peut prendre pour $c_1,\ldots,c_n$ des indéterminées. Tout polynôme unitaire de degré n à coefficients dans k' s'obtient en donnant alors à $c_1,\ldots,c_n$ des valeurs convenables dans k'. Pour cette raison, le polynôme f(X) est appelé le *polynôme générique de degré* n, conformément à la terminologie de la géométrie algébrique (chapitre 6).

2. Le problème de la recherche d'extensions finies galoisiennes de $\mathbb{Q}$, de groupe de Galois un groupe fini donné, n'est encore résolu que dans des cas particuliers.

Le lecteur pourra trouver des renseignements sur les polynômes à coefficients rationnels de groupe de Galois S_n, avec n égal au degré du polynôme, dans le livre de Van Der Waerden. Modern Algebra ((20).61).

Groupes Résolubles

On va rappeler ici, sans démonstration, un certain nombre de résultats de théorie des groupes et notamment de théorie des groupes résolubles. Pour les démonstrations, on pourra, par exemple, se reporter à (20).

Soit G *un groupe noté multiplicativement d'élément neutre* e.

1. Une *suite de composition* de G est une suite strictement décroissante:

(1) $G_o = G \supset G_1 \supset \ldots \supset G_n = \{e\}$

de sous-groupes de G tels que, pour tout $i = 0,\ldots,n-1, G_{i+1}$ soit un sous-groupe *normal* de G_i.

2. L'entier n est alors appelé la *longueur* de la suite de composition (1).

3. Les quotients G_i/G_{i+1} sont appelés les *facteurs* de la suite de composition.

4. Un *raffinement* de la suite de composition (1) est une suite de composition.

(2) $G'_o = G \supset G'_1 \supset \ldots \supset G'_m = \{e\}$

telle que $\{G_o,\ldots,G_n\}$ soit contenu dans $\{G'_o,\ldots,G'_m\}$

5. Une suite de composition de G n'admettant pas de raffinement strictement plus fin (i.e. contenant strictement plus de sous-groupes) est appelée une *suite de Jordan-Hölder de* G.

L'exemple d'un *groupe cyclique infini* montre qu'un groupe peut ne pas avoir de suite de Jordan-Hölder.

6. On dit que deux *suites de composition* de G sont *isomorphes* si elles ont même longueur et si elles ont des facteurs isomorphes (dans des ordres éventuellement différents. *Exemple*: si G est un groupe cyclique d'ordre 6 engendré par un élément a, les deux séries de composition : $G \supset (a^2) \supset (e)$ et $G \supset (a^3) \supset (e)$, où ( ) désigne le sous-groupe engendré, qui sont isomorphes.)

Voici les principaux résultats de la théorie.

7. (Théorème de Schreier)

Deux suites de composition d'un groupe G *ont des raffinements isomorphes.*

8. (Théorème de Jordan-Hölder)

1. *Deux suites de* Jordan-Hölder *d'un groupe sont isomorphes*

2. *Si* G *possède une suite de Jordan-Hölder, toute suite de composition peut être raffinée en une suite de* Jordan-Hölder.

Si un groupe G admet une suite de Jordan-Hölder, la longueur d'une telle suite est aussi la longueur de toute suite de Jordan-Hölder de G.

On l'appelle la *longueur du groupe* G.

9. *Un groupe* G *est dit résoluble s'il admet une suite de composition dont tous les facteurs sont abéliens.*

Si un tel groupe admet une suite de Jordan-Hölder, ses facteurs sont des *groupes abéliens simples*, i.e. des groupes cycliques d'ordre premier.

(On rappelle qu'un groupe G est dit simple si ses seuls sous-groupes distingués sont G et {e}. Dire qu'une suite de composition (1) du groupe G est de Jordan-Hölder c'est évidemment dire que ses facteurs sont simples).

10. *Si* $n \geqslant 5$, *le gorupe symétrique* S_n *n'est pas résoluble.*

On a, en effet, une suite de composition $S_n \supset A_n \supset \{e\}$. Or on démontre (théorème d'Abel) que pour $n \geqslant 5$, le groupe A_n est simple non abélien. (chap. 2, ex. 11). Cette suite de composition ne peut donc être raffinée en une suite de Jordan-Hölder à facteurs abéliens. Or, comme S_n est fini,

il admet des suites de Jordan-Hölder. S'il était résoluble, il admettrait une telle suite à facteurs abéliens et toute suite de Jodan-Hölder serait à facteurs abéliens ce qui n'est pas le cas.

11. *Soient* G *un groupe,* H *un sous-groupe distingué de* G.

Les assertions suivantes sont équivalentes:

(i) G *est résoluble*

(ii) H *et* G/H *sont résolubles*

Démonstration

(i) $\Longrightarrow$ (ii).

On raffine la suite de composition $G \supset H \supset \{e\}$ en une suite de Jordan-Hölder. Les facteurs de cette suite sont abéliens. On obtient ainsi une suite de Jordan-Hölder à facteurs abéliens de H qui est donc résoluble et aussi, par passage au quotient par H, une suite de Jordan-Hölder de G/H à facteurs abéliens et G/H est résoluble.

(ii) $\Longrightarrow$ (i). Même type de démonstration.

Définition

Soit k *un corps. Un polynôme* $f(X) \in k[X]$ *est dit résoluble par radicaux* (ou simplement résoluble sur k) *s'il existe une tour:* $k_o = k \subset k_1 \subset \ldots \subset k_r$ *de corps et une suite finie* $n_o, \ldots, n_{r-1}$ *d'entiers* ≥ 1 *telles que:*

1) pour $i = 0, \ldots, r-1$, $k_{i+1} = k_i(\gamma_i)$ *où* $\gamma_i^{n_i}$ *appartient à* k_i

2) k_r *contienne le corps de décomposition de* f(X) *sur* k

Exemples

1. Soient k un corps de caractéristique 0, $f(X) = X^2+2aX+b \in k[X]$.

Ce polynôme est résoluble par radicaux. Il suffit, en effet, de considérer la tour: $k_o = k$, $k_1 = k(c)$ où $c^2 = a^2-b$.

2. On vérifiera, par contre, que le polynôme $X^2+X+1 \in \mathbb{F}_2[X]$ n'est pas résoluble par radicaux.

Lemme 2

Soient k *un corps,* n *un entier* ≥ 1 *non divisible par la caractéristique de* k, z *un élément d'une extension de* k *racine primitive* n*-ième de l'unité.*

Alors, l'extension k(z)/k *est galoisienne de groupe de Galois abélien. Si, de plus,* z *n'appartient pas à* k, *ce groupe de Galois est isomorphe au groupe multiplicatif des classes modulo* n *d'entiers premiers à* n.

Démonstration

Elle est claire si z appartient à k. On suppose donc que z n'appartient pas à k.

Le polynôme X^n-1 est alors *irréductible* sur k car, sinon, z serait racine d'un polynôme à coefficients dans k de degré $< n$ et ne serait pas racine primitive n-ième de 1.

L'extension $k(z)/k$ est *normale* car $k(z)$ est le corps de décomposition sur k du polynôme X^n-1. Elle est *séparable* car le polynôme X^n-1, de dérivé nX^{n-1} non nul en vertu de l'hypothèse faite sur la caractéristique, l'est. L'extension $k(z)/k$ est donc galoisienne.

Un élément s de $Gal(K/k)$ est déterminée par l'élément $s(z)$ qui doit être une racine primitive n-ième de 1, i.e. de la forme z^q, où $(q,n) = 1$.

L'application: $q \longmapsto s$, où $s(z) = z^q$, est un homomorphisme surjectif de l'ensemble, muni de la multiplication, des entiers q tels que $(q,n) = 1$ sur le groupe $Gal(k(z)/k)$.

Il définit un isomorphisme du groupe multiplicatif des classes modulo n d'entiers premiers à n sur $Gal(k(z)/k)$.

Lemme 3

Soient k un corps, n un entier $\geqslant 1$ non divisible par la caractéristique de k.

On suppose que k contient une racine primitive n-ième de l'unité z.

Une extension $k(c)/k$, où $c^n = a$ appartient à k, est galoisienne de groupe de Galois cyclique et donc abélien.

Démonstration

Soit z une racine primitive n-ième contenue dans k.

Si c appartient à k, l'assertion est claire. On suppose donc que c n'appartient pas à k. Alors, $k(c)/k$ est le corps de décomposition de $X^n-a = \prod_{i=0}^{n-1} (X-z^i c)$. L'extension $k(c)/k$ est donc *normale*. Elle est *séparable* comme le polynôme X^n-a. Elle est donc *galoisienne*.

Un élément s du groupe de Galois $Gal(k(c)/k)$ est déterminé par l'élément $s(c)$ qui est de la forme cz^i. Soient $s, t \in Gal(k(c)/k)$, $s(z) = z^i$, $t(z) = z^j$. Alors, $(s \circ t)(z) = s(cz^j) = s(c)z^j = cz^{i+j}$. L'application : $i \longmapsto s$, où $s(c) = cz^i$ définit un isomorphisme du groupe cyclique $\mathbf{Z}/(n)$ sur $Gal(k(c)/k)$.

Lemme 4

Soient k *un corps,* n *un entier* $\geqslant 1$ *non divisible par la caractéristique de* k, k(c)/k, *où* c^n *appartient à* k, *une extension, non nécessairement normale de* k, z *une racine primitive n-ième de l'unité dans une extension de* k(c). *Alors, les extensions successives de la tour*

$$k \subset k(z) \subset k(z,c_1)$$

sont galoisienne de groupe de Galois abéliens.

Démonstration

L'extension k(z)/k est galoisienne de groupe de Galois abélien (lemme 1). Il en est de même de l'extension k(z,c)/k(z).(lemme 2).

On va maintenant modifier la tour de la définition.

Proposition III.11

Soient k *un corps de caractéristique* 0, f(X) *un polynôme non constant de* k[X].

Les assertions suivantes sont équivalentes:

(i) f(X) *est résoluble par radicaux*

(ii) Il existe une tour comme dans la définition telle que, pour tout $i = 0,\ldots,r-1$, *l'extension* k_{i+1}/k_i *soit galoisienne de groupe de Galois abélien.*

Démonstration

(ii) $\Longrightarrow$ (i). Clair

(i) $\Longrightarrow$ (ii). Soit $k_o = k \subset k_1 \subset \ldots \subset k_r$ une tour comme dans la définition

On remplace l'extension k_1/k_o par la tour

$$k = k_o \subset k_o(z_1) \subset k_o(z_1,c_1)$$

où z_1 est une racine primitive n-ième de l'unité, $c_1,\ldots,c_s$ les conjugués de γ_1 sur $k_o(z_1)$ puis la tour $k_o = k \subset k_1 \subset \ldots \subset k_r$ par la tour

$$k_o = k \subset k_o(z_1) \subset \ldots \subset k_1' \subset k_2' = k_1'(\gamma_2) \ \ldots \ \ k_r' = k_{r-1}'(\gamma_r).$$

On procède de la même manière avec l'extension k_2'/k_1' et ainsi, de proche en proche, obtenant une tour d'extensions de k satisfaisant à la condition (ii).

Corollaire 1

Soient k *un corps de caractériqtique* 0, f(X) *un polynôme non constant de* k[X].

Si f(X) *est résoluble par radicaux sur* k, *le groupe de Galois de* f *sur* k *est résoluble.*

Démonstration

Soient K le corps de décomposition de f(X) sur k, $k = k_o \subset k_1 \subset \ldots \subset k_r$ une tour d'extensions de k telle que, pour tout i = 0,...,r-1, l'extension k_{i+1}/k_i soit galoisienne de groupe de Galois abélien et que k_r contienne K.

Alors, le groupe $Gal(k_r/k)$ est résoluble. Comme l'extension K/k est normale, le groupe $Gal(K/k)$ est une quotient de $Gal(k_r/k)$. Il est donc résoluble.

Corollaire 2 (théorème d'Abel)

Les notations sont celles du début de 2, concernant les corps k', k *et le polynôme générique de degré* n *sur* k'.

Si $n \geqslant 5$, *le polynôme générique de degré* n *sur* k' *n'est pas résoluble par radicaux sur* k.

Démonstration

Elle résulte de ce que le groupe de Galois de ce polynôme est S_n et que, pour $n \geqslant 5$, le groupe S_n n'est pas résoluble.

Remarque

La réciproque du corollaire 1 est exacte. Si le groupe de Galois de f sur k est résoluble, le polynôme f(X) est résoluble par radicaux sur k. La démonstration de ce fait repose sur l'étude des extensions cycliques, i.e. de groupes de Galois cycliques. (ex. 25).

3. Extension galoisienne de Groupe de Galois le groupe diédral d'ordre 8

Rappels sur le groupe diédral d'ordre 8

Le *groupe diédral d'ordre 8* est le groupe G des rotations de l'espace à trois dimensions laissant invariant un carré.

On note O le centre de ce carré, 1, 2, 3, 4 ces sommets.

On identifie le groupe G au sous-groupe $\{s_1,\ldots,s_8\}$ du groupe symétrique S_4 où s_1 est l'application identique, $s_2 = (1234)$ est la rotation d'angle $+\pi/2$, $s_3 = (13)(24)$ la rotation d'angle π, $s_4 = (1432)$ la rotation d'angle $-\pi/2$ autour de O, $s_5 = (24)$ la rotation d'angle π autour de l'axe 13, $s_7 = (13)$ la rotation d'angle π autour de l'axe 24, $s_6 = (12)(34)$ la rotation d'angle π autour de la bissectrice de l'angle $\widehat{102}$, $s_8 = (14)(32)$ la rotation d'angle π autour de la bissectrice de l'angle $\widehat{104}$.

Sous-groupes du groupe diédral d'ordre 8

sous-groupe d'ordre 1: $G_o = \{s_1\}$

sous-groupes d'ordre 2: G_3, G_5, G_7, G_6, G_8 engendrés par les permutations S_3, S_5, S_7, S_6, S_8 respectivement

sous-groupes d'ordre 4: $G_2 = \{s_1, s_2, s_3, s_4\}$ engendré par s_2

$G_4 = \{s_1, s_3, s_6, s_8\}$

$G_1 = \{s_1, s_5, s_7, s_3\}$

sous-groupe d'ordre 8: $G_9 = G$

On interprétera aisément ces sous-groupes de façon géométrique

Soit K *le corps de décomposition sur* $\mathbb{Q}$ *du polynôme* X^4-5.

Les racines de X^5-4 sont $a_1 = 5^{1/4}$, $a_2 = i5^{1/4}$, $a_3 = -5^{1/4}$, $a_4 = -i5^{1/4}$. Le corps K est donc $\mathbb{Q}(i,5^{1/4})$. Il résulte de la tour

$$\mathbb{Q} \subset \mathbb{Q}(5^{1/4}) \subset \mathbb{Q}(i,5^{1/4}) = \mathbb{Q}(5^{1/4})(i)$$

que $[K:\mathbb{Q}] = 2 \times 4 = 8$.

Il s'ensuit que *l'ordre du groupe de Galois* $Gal(K/\mathbb{Q})$ *est* 8.

Un élément s de $Gal(K/\mathbb{Q})$ permute les racines a_1, a_2, a_3, a_4 de X^5-4. Il est parfaitement déterminé par les valeurs de $s(a_1)$ et de $s(i)$. Comme $s(i)$ est $+i$ ou $-i$ puisque s laisse invariant le polynôme X^2+1, *on obtient* facilement *le tableau suivant qui permet d'identifier les éléments de* $Gal(K/\mathbb{Q})$ *aux éléments énumérés plus haut du groupe diédral*

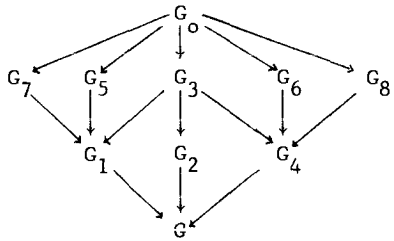
automorphismes de $K/\mathbb{Q}$	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
effet sur i	i	i	i	i	-i	-i	-i	-i
effet sur a_1	a_1	a_2	a_3	a_4	a_1	a_2	a_3	a_4
effet sur a_2	a_2	a_3	a_4	a_1	a_4	a_1	a_2	a_3
effet sur a_3	a_3	a_4	a_1	a_2	a_3	a_4	a_1	a_2
effet sur a_4	a_4	a_1	a_2	a_3	a_2	a_3	a_4	a_1

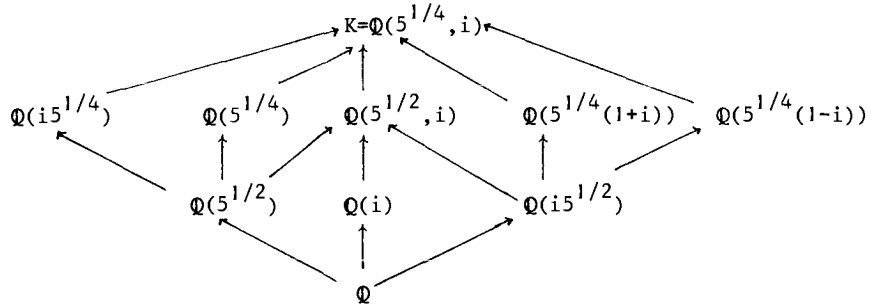
Un élément y *de* K *s'écrit de manière unique,*

$$x_o + x_1a_1 + x_2a_1^2 + x_3a_1^3 + x_4i + x_5ia_1 + x_6ia_1^2 + x_7ia_1^3 \quad (x_j \in \mathbb{Q}; j=0,.,7)$$

Le calcul des sous-corps invariants par les différents sous-groupes

de $Gal(K/\mathbb{Q})$ ne présente pas de difficulté. *La situation est schématisée par les deux diagrammes suivants dans lesquels les flèches sont des injections:*





On va se contenter ici de faire quelques unes des vérifications

On remarque que $s_3(y) = x_o - x_1a_1 + x_2a_1^2 - x_3a_1^3 + x_4i - x_5ia_1 + x_6ia_1^2 - x_7ia_1^3$

Ainsi le corps des invariants par s_3, ou ce qui est équivalent par G_3, est l'ensemble $\{x_o + x_2a_1^2 + x_4i + x_6ia_1^2/x_j \in \mathbb{Q}\}$. C'est donc $\mathbb{Q}(5^{1/2},i)$

On vérifie ensuite les égalités

$$s_6(x_o + x_2a_1^2 + x_4i + x_6ia_1^2) = x_o - x_2a_1^2 - x_4i + x_6ia_1^2$$

$$s_5(x_o + x_2a_1^2 + x_4i + x_6ia_1^2) = x_o + x_2a_1^2 - x_4i - x_6ia_1^2$$

Le corps des invariants par s_5, i.e. par G_1, (resp. s_6, i.e. G_4) est donc celui des éléments $x_o + x_1a_1^2$ (resp. $x_o + x_6ia_1^2$), i.e. $\mathbb{Q}(5^{1/2})$ (resp. $\mathbb{Q}(i5^{1/2})$

Remarques

1. Les éléments $s_j(i+5^{1/4})$ $(j = 1,\ldots,8)$ sont distincts.

Il en résulte que *l'élément* $i+5^{1/4}$ *est élément primitif de l'extension* $K/\mathbb{Q}$.

2. Comme $s_7 = s_2^{-1} s_5 s_2$, les sous-groupes G_5 et G_7 sont conjugués.

Les corps correspondants $\mathbb{Q}(5^{1/4})$ et $\mathbb{Q}(i5^{1/4}$ sont conjugués. Leurs éléments primitifs sont d'ailleurs racines du polynôme X^4-5. Les sous-groupes G_6 et G_8 sont conjugués ainsi que les corps correspondants $\mathbb{Q}(5^{1/4}(1+i))$ et $\mathbb{Q}(5^{1/4}(1-i))$ d'éléments primitifs racines de X^4+20.

6. Fermeture galoisienne d'une extension algébrique séparable

Définition

Soient k *un corps,* K/k *une extension algébrique de* k.

Une fermeture galoisienne de K/k *est la donnée d'une extension* L/K *telle que*

1. *L'extension* L/k *soit galoisienne*
2. *Pour toute extension* M/K *de* K *telle que l'extension* M/k *soit galoisienne il existe un homomorphisme* (non nécéssairement unique) *de* L *dans* M *prolongeant* 1_K.

Une condition nécessaire évidente d'existence d'une fermeture galoisienne de K/k est que l'extension K/k soit séparable (prop. III.5). La proposition ci dessous affirme que cette condition est aussi suffisante.

Proposition III.12

Soit K/k *une extension séparable de* k.

1. *Il existe une fermeture galoisienne de* K/k
2. *Deux fermetures galoisiennes de* K/k *sont* K*-isomorphes*

Démonstration

1. Si $x \in K$, soit S_x l'ensemble des conjugués de x dans la clôture algébrique $\overline{K}$ de K, i.e. l'ensemble des racines dans $\overline{K}$ de irr(X,x,k).

Soit $L = k(\bigcup_{x \in K} S_x)$. Il est clair que L contient K et que L/k est *séparable.*

En effet, tout élément y du système $\bigcup_{x \in K} S_x$ de générateurs de L/k est séparable puisque racine d'un polynôme irr(X,x,k) où $x \in K$.

L'extension L/k est normale: il suffit, en effet, de démontrer que tout k-homomorphisme t de L dans $\overline{K}$ (qui est une clôture algébrique de k) est un k-automorphisme de L dans L, i.e., compte tenu du lemme de la proposition III.1, est tel que $t(L) \subset L$. Il suffit, a cet effet, de vérifier si $y \in \bigcup_{x \in K} S_x$, t(y) appartient à L; or, si $y \in S_x$, y et t(y) sont racines du même polynôme irr(X,x,k) et donc $y \in S_x$.

On a donc démontré que l'extension L/k est galoisienne.

Si M/K est une extension de K telle que M/k soit galoisienne, on peut toujours supposer M contenu dans $\overline{K}$. Il est alors clair que M contient L.

2. Soient L/K et L'/K deux fermetures galoisiennes de K/k. Il existe un k-homomorphisme f(resp.g) de L dans L' (resp.L' dans L). Le k-homomorphisme $g \circ f$ de L dans L est un k-automorphisme de L et f est un k-isomorphisme

Complément

Si, de plus, l'extension K/k *est finie, une fermeture galoisienne de* K/k *est finie sur* k.

Démonstration

Soit x un élément primitif de K/k. On vérifie immédiatement que, avec les notations de la démonstration précédente, $k(S_x)$ est fermeture galoisienne de k.

Il suffit alors de remarquer que l'ensemble S_x est *fini*.

L'existence de la fermeture galoisienne d'une extension algébrique séparable permet, dans certaines démonstrations portant sur des *extensions séparables*, de se limiter aux seules *extensions galoisiennes*.

Voici, à titre d'application de cette méthode, la démonstration d'un important résultat de finitude.

Proposition III.13

Soient A *un anneau noethérien intégralement clos,* k *son corps des fractions,* K/k *une extension finie séparable de* k, B *la fermeture intégrale de* A *dans* K.

Le A*-module* B *est de type fini et l'anneau* B *est noethérien.*

Démonstration

Un idéal de l'anneau B est un sous-module du A-module B. *Il suffit donc de démontrer la finitude du* A*-module* B.

Soient L/K la fermeture galoisienne de K/k, C la fermeture intégrale de A dans L.

Si le A-module C est de type fini, il en est de même du A-module B qui en est un sous-module.

On peut donc supposer l'extension K/k *galoisienne.*

Soient alors $n = [K:k]$, $Gal(K/k) = \{s_1, \ldots, s_n\}$ (avec le même entier n).

Il existe un *élément* x *de* B *primitif* de K/k car, si $y \in K$ est un élément primitif, y s'écrit x/a où $x \in B$ et $a \in A$ et x est primitif comme y.

On pose $e_i = x^{i-1}$ $(i = 1,\ldots,n)$, obtenant la base $\{e_1,\ldots,e_n\}$ du k-espace vectoriel K.

On remarque que, pour tout $j = 1,\ldots,n$, tout $i = 1,\ldots,n$, $s_j(e_i)$ appartient à B car $s_j(e_i)$ est entier sur A comme e_i (appliquer s_j à une équation de dépendance intégrale de e_i sur A).

Le déterminant $\det((s_j(e_i))$ de la matrice $n \times n$ $(s_j(e_i))$ est non nul comme *déterminant de* Van der Monde puisque les éléments $s_1(x),\ldots,$ $s_n(x)$ sont distincts.

C'est un élément de B. Il en est de même de $d = \det((s_j(e_i))^2$. De plus, il est clair que d appartient à $Inv(Gal(K/k)) = k$. Comme A est *intégralement clos*, d appartient à A.

Un élément x de K s'écrit de manière unique $\sum_{i=1}^{n} b_i e_i$ où $b_i \in k$.

La *règle de* Cramer, donne, par résolution du système d'équations linéaires

$$\sum_{i=1}^{n} b_i s_j(e_i) = s_j(x) \quad (j = 1,\ldots,n)$$

des égalités $b_i = u_i/\det((s_j(e_i))$ où $u_i \in K$. *Si* x *appartient à* B, u_i appartient à B comme les éléments $s_j(x)$. On peut alors écrire $b_i = c_i/d$ où $c_i = u_i \det((s_j(e_i))$.

Par conséquent, c_i appartient à B comme u_i et $\det((s_j(e_i))$ et à k puisque $c_i = b_i d$.

Donc, c_i appartient à A (parce que A est intégralement clos).

En définitive, le A-module B est contenu dans le A-module de type fini $\sum_{i=1}^{n} A(e_i/d)$. Puisque A est *noethérien*, il est de type fini.

IV. Extensions inséparables

Les *phénomènes d'inséparabilité* créent des difficultés en théorie de Galois.

Ils jouent néammoins un rôle important dans des problèmes naturels car ils sont liés à la notion de *multiplicité*.

On vérifie, par exemple, que si l'élément a d'une extension du corps k, de caractéristique $p > 0$, est algébrique sur k mais non séparable sur k, toute racine du polynôme irr(X,a,k) est multiple d'ordre de multiplicité une puissance positive de p.

On pourra se reporter aussi à la théorie des multiplicités d'intersection d'A. Weil (34) pour trouver une situation analogue (mais plus difficile) en géométrie algébrique.

On aborde ici l'étude des extensions non séparables. On démontre en particulier, qu'une extension algébrique peut s'obtenir en considérant d'abord une extension séparable puis une extension dite radicielle (ou purement inséparable) de cette extension séparable, cette deuxième extension étant obtenue par extraction de racines d'ordres des puissances de la caractéristique.

L'étude des extensions radicielles n'est ici qu'esquissée. On n'aborde pas, par exemple, l'étude de l'analogue de la théorie de Galois, où interviennent d'autres structures que celles du groupe de Galois (qui est alors réduit à son élément neutre)) et, notamment, les *dérivations d'ordre supérieur.*

On se contente ici de démontrer l'existence d'une p-base pour des corps de caractéristique $p > 0$, i.e. de familles $(x_i)_{i\in I}$ d'éléments de k tels que les monômes

$$x_{i_1}^{n_{i_1}} \dots x_{i_r}^{n_{i_r}}$$

où les éléments $i_1,\dots,i_r$ de I sont distincts et $0 \leqslant n_{i_j} < p$, forment une base du k^p-espace vectoriel k.

Cette notion de p-base est utile, par exemple, dans certaines théorèmes de relévements (structures des anneaux complets). Elle peut être laissée en première lecture.

1. Extensions radicielles (ou purement inséparables)

Proposition IV.1 (caractérisation des éléments inséparables)

Soient k *un corps,* K/k *une extension de* k, a ε K *un élément algébrique sur* k, f(X) = irr(X,a,k).

Les assertions suivantes sont équivalentes:

(*i*) a *n'est pas séparable sur* k

(*ii*) f'(X) = 0 (où f'(X) est le polynôme dérivé de f(X))

(*iii*) *le corps* k *est de caractéristique* p *non nulle et* f(X) ε $k[X^p]$

Démonstration

(i) $\Longleftrightarrow$ (ii)

Dire que a n'est pas séparable sur k c'est dire que f(X)a (dans une clôture algébrique de k) des racines multiples. Une telle racine multiple b est aussi racine du polynôme dérivé f'(X). Par minimalité du degré de f, ceci implique f'(X) = 0.

(ii) $\Longleftrightarrow$ (iii)

Evident.

Exemple d'élément inséparable

Soit α un élément du corps k de caractéristique $p > 0$ n'admettant pas de racine p^n-ème dans k. Le polynôme $X^{p^n} - \alpha$ est alors irréductible dans $k[X]$.

Soit a une racine $X^{p^n} - \alpha$ dans une clôture algébrique de k.

Alors, $X^{p^n} - \alpha = \mathrm{irr}(X,a,k)$ admet a pour racine d'ordre de multiplicité p^n, car

$$X^{p^n} - \alpha = X^{p^n} - a^{p^n} = (X-a)^{p^n}.$$

Définition

Soient k un corps, K/k une extension de k, a $\in$ K.

On dit que a est radiciel (ou purement inséparable) sur k si l'une des conditions suivantes est satisfaite:

1. k est de caractéristique 0 et a appartient à k

2. k est de caractéristique $p > 0$ et il existe $n \in N$ tel que a^{p^n} appartienne à k (ceci n'exclut pas le cas $a \in k$ obtenu pour $n = 0$).

L'extension K/k est dite radicielle (ou purement inséparable) si tout élément de K est radiciel sur k.

En caractéristique 0, ceci implique *l'égalité* $K = k$.

On remarquera qu'un élément (resp. une extension) radiciel (resp. radicielle) sur k est *algébrique* sur k.

Remarque

Si l'extension K/k est radicielle, le groupe de Galois Gal(K/k) est réduit à l'automorphisme identique.

C'est clair en caractéristique 0 où $K = k$.

Si la caractéristique est $p > 0$, soient $x \in K$, $s \in Gal(K/k)$. Il existe $n \in N$ tel que X^{p^n} appartienne à k. Alors

$$s(x^{p^n}) = s(x)^{p^n} = x^{p^n},$$

d'où

$(s(x)-x)^{p^n} = 0$ et $s(x) = x$.

Proposition IV.2

Soient k *un corps de caractéristique* $p > 0$, $\overline{k}$ la clôture algébrique de k.

1. *Pour tout* $n \in N^*$, *l'ensemble* $\{a^{p^n} / a \in k\}$ *est un sous-corps de* k, *noté* k^{p^n}.

2. *Pour tout* $n \in N^*_{-\infty}$ *un élément* a *de* k *a une seule racine* p^n*-ème dans* $\overline{k}$. *On a la note* $a^{p^{-n}}$.

L'ensemble $\{a^{p^{-n}} / a \in k\}$ *est un sous-corps, noté* $k^{p^{-n}}$, *de* $\overline{k}$ *contenant* k.

Démonstration

Elle est facile et laissée au soin du lecteur.

Définition

Soient k *un corps,* $\overline{k}$ *une clôture algébrique de* k.

L'ensemble des éléments de $\overline{k}$ *radiciels sur* k *est appelé la clôture radicielle de* k. *On dit aussi clôture parfaite.*

Si k est de caractéristique 0, la clôture radicielle de k est k.

Si k est de caractéristique $p > 0$, la clôture radicielle de k est le sous-corps $\bigcup_{n \in N^*_{-\infty}} k^{p^{-n}}$ de $\overline{k}$.

On la note $k^{p^{-\infty}}$

Soit K *un sous-corps de* $\overline{k}$ *contenant* k.

L'ensemble des éléments de K *radiciels sur* k *est appelé la fermeture radicielle de* k.

Cette fermeture radicielle est k en caractéristique 0, $k^{p^{-\infty}} \cap K$ en caractéristique $p > 0$.

Remarque

On laisse au lecteur le soin de vérifier que la notion de clôture radicielle est indépendante, à isomorphisme près, de la clôture algébrique choisie $\overline{k}$ de k.

Définition

Un corps k *est dit parfait s'il est égal à sa clôture radicielle.*

1. Un corps de caractéristique 0 est donc parfait.

2. Un corps de caractéristique $p \neq 0$ est parfait si et seulement si, pour tout $n \in N^*$, tout $a \in k$, il existe dans k une racine p^n-ème de a.

Il suffit, évidemment, à cet effet, que tout élément de k admette dans k une racine p-ème.

Il en résulte qu'un corps fini est parfait: en effet, le cardinal d'un tel corps est de la forme p^r, et pour tout élément a du corps, $(a^{p^{r-1}})^p = a$.

3. Un corps algébriquement clos est parfait.

Proposition IV.3

Soit k *un corps.*

Les assertions suivantes sont équivalentes:

(i) k *est parfait*

(ii) toute extension algébrique de k *est séparable*

Démonstration

On peut se limiter au cas où la caractéristique p de k est > 0.

(i) $\Longrightarrow$ (ii)

Soit a un élément d'une extension de k algébrique sur k.

Dire qu'il n'est pas séparable c'est dire que f(X) = irr(X,a,k) est de la forme $g(X^p)$ où $g(Y) = Y^r + a_1 Y^{r-1} + \ldots + a_r \in k[Y]$. Soit $b_i \in k$ tel que $b_i^p = a_i$. Le polynôme f(X) s'écrit $(X^r + b_1 X^{r-1} + \ldots + b_r)^p$. Ceci contredit l'irréductibilité de f(X) dans $k[X]$.

(ii) $\Longrightarrow$ (i)

Si k n'est pas parfait, il existe $a \in k$ sans racine p-ème. Le polynôme $X^p - a$ n'est pas séparable. L'extension $k[X]/(X^p - a)$ n'est pas séparable

Proposition IV.4

Soient k *un corps,* K/k *une extension algébrique de* k.

1. Le sous-ensemble de K *des éléments séparables sur* k *est un sous-corps* K_s *(appelé fermeture algébrique séparable de* k *dans* K*) de* K *contenant* k.

L'extension K/K_s *est radicielle.*

2. Soit K_r *la fermeture radicielle de* k *dans* K. *L'extension* K/K_r *est séparable.*

Démonstration

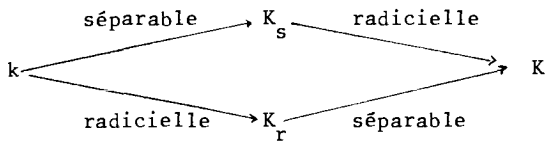
1. Si $x,y \in K_s$, le corps k(x,y) est séparable sur k. Donc, xy et x-y et x^{-1} (si $x \neq 0$) appartiennent à K_s qui est ainsi un sous-corps de K.

Soit $a \in K$. Il existe $n \in \mathbb{N}^*$ tel que irr(X,a,k) appartienne à $k[X^{p^n}]$ mais n'appartienne pas à $k[X^{p^{n+1}}]$. Si $irr(X,a,k) = g(X^{p^n})$, g(Y)

est irréductible dans $k[Y]$ et est donc $\mathrm{irr}(Y, a^{p^n}, k)$. Comme $g(Y)$ n'appartient pas à $k[X^p]$, a^{p^n} est séparable sur k, i.e. appartient à K_s et donc a est radiciel sur K_s.

2. Soit $a \in K$. Le polynôme $\mathrm{irr}(X, a, K_r)$ n'appartient pas à $K_r[X^p]$ car sinon il ne serait pas irréductible. Donc, a est séparable sur K_r.

La situation est résumée sur le diagramme.



Le degré $[K:K_s]$ est appelé *le degré inséparable* de l'extension K/k et noté $[K:k]_r$. On a les égalités $[K:k] = [K:K_s][K_s:k] = [K:K_r][K_r:k]$.

Proposition IV.5

Soit K/k une extension radicielle de k.

1. Le degré séparable $[K:k]_s$ de K/k est 1.

2. Si de plus, K/k est de degré fini, le degré $[K:k]$ de K/k (égal à son degré inséparable) *est de la forme p^m ($m \in \mathbb{N}$) si k est de caractéristique $p > 0$.*

Démonstration

1. Le seul k-homomorphisme de K dans une clôture algébrique $\bar{K}$ de K est l'injection de K dans $\bar{K}$: si s est un tel homomorphisme et $x \in K$, $x \notin k$, il existe $n \in \mathbb{N}^*$ tel que x^{p^n} appartienne à k; donc,

$$s(x)^{p^n} = s(x^{p^n}) = x^{p^n},$$

d'où $s(x) = x$

2. On remarque que si $k \subset K' \subset K$ est une tour d'extensions de k, K est radiciel sur k si et seulement si K est radiciel sur K' et K' est radiciel sur k.

Il résulte alors de la propriété de multiplicativité des degrés *qu'on peut se limiter aux extensions monogènes.*

Soit donc $K = k(a)$ où a est radiciel sur k. Soit m l'entier tel que a^{p^n} appartienne à k et $a^{p^{m-1}}$ n'appartienne pas à k. (On suppose $a \notin k$ car ce cas est évident).

Le polynôme $X^{p^m} - a^{p^m}$ est irréductible dans $k[X]$ car un facteur

devrait être de la forme $X^{p^r} - a^{p^r}$ où $r < m$. C'est donc irr(X,a,k). Par conséquent, $[K:k] = p^m$.

Corollaire

Soit k *un corps de caractéristique* $p > 0$.

Soit K/k *une extension algébrique de* k. Les notations sont comme ci dessus.

1. $[K_s:k] = [K:K_r] = [K:k]_s$ (degré séparable de K/k) *et* $[K:K_s] = [K_r:k]$.
2. $[K:k] = [K:k]_r[K:k]_s$

En particulier, si l'extension K/k *est finie,* $[K:k]$ *est de la forme* $p^m[K:k]_s$. (produit du degré séparable par une puissance de la caractéristique).

Démonstration

1. Les égalités $[K_s:k] = [K:K_r] = [K:k]_s$ résultent immédiatement de la multiplicativité du degré séparable et de la proposition IV.4.1.

Les égalités $[K:K_s] = [K_r:k] = [K:k]_s$ en résultent.

2. C'est une conséquence facile de 1. et de la proposition IV.4.2.

2. Notion de p-Base

Définition

Soient k *un corps de caractéristique* $p > 0$, k' *un sous-corps de* k *tel que* $k^p \subset k' \subset k$.

Des éléments $x_1,\ldots,x_n$ *de* k *sont dits* p*-indépendants sur* k' *si les monômes*

$$x_1^{i_1}\ldots x_n^{i_n} \quad (0 \leqslant i_q < p;\ q = 1,\ldots,n)$$

sont linéairement indépendants sur k'.

Un sous-ensemble X de k *est dit* p*-indépendant sur* k' *si tout sous-ensemble fini de X est formé d'éléments* p*-indépendants sur* k'

Lemme

Soit $X = \{x_1,\ldots,x_n\}$ *un sous-ensemble* (fini) *de* k.

Les assertions suivantes sont équivalentes;

(i) X est p*-indépendant sur* k'

(ii) pour tout $i = 1,\ldots,n$, x_i *n'appartient pas à* $k'(X-\{x_i\})$

Démonstration

(i) $\Longrightarrow$ (ii)

Un élément de $k'(x_1,\ldots,x_{n-1})$ s'écrit $g(x_1,\ldots,x_{n-1})$ où $g(X_1,..,X_{n-1})$

ε k' $[X_1,\ldots,X_{n-1}]$ est un polynôme de degré < p en chaque X_i.

Si x_n appartenait à $k'(x_1,\ldots,x_{n-1})$, on aurait donc une égalité

$$x_n = g(x_1,\ldots,x_{n-1})$$

avec un polynôme g comme c- dessus. Ceci contredirait le fait que *X* est p-indépendant sur k'.

(ii) $\Longrightarrow$ (i)

La démonstration se fait par récurrence sur n. Le cas n = 0 est évident.

On démontre que si (ii) est vérifiée et si $f(X_1,\ldots,X_n) \varepsilon k'[X_1,\ldots,X_n]$ est non nul de degré < p en chaque X_i, $f(x_1,\ldots,x_n)$ est non nul.

On peut supposer que l'indéterminée X_n apparait effectivement dans f. L'ensemble $\{x_1,\ldots,x_{n-1}\}$ satisfait à (ii). Il est donc, par hypothèse de récurrence p-indépendant sur k'. Le polynôme $f(x_1,\ldots,x_{n-1},X_n)$ n'est donc pas nul, et, comme il est de degré < p, il est séparable sur $k'(x_1,\ldots,x_{n-1})$.

Comme $k^p \subset k'$, x_n est radiciel sur k'. L'égalité $f(x_1,\ldots,x_{n-1},x_n) = 0$ impliquerait qu'il est séparable sur $k'(x_1,\ldots,x_{n-1})$. Etant radiciel et séparable, il appartiendrait à $k'(x_1,\ldots,x_{n-1})$ contrairement à l'hypothèse.

Remarque

Un critère analogue est valable pour un ensemble X non nécessairement fini.

La démonstration immédiate en est laissée au soin du lecteur.

Définition

Un sous-ensemble X de k *est appelé une* p*-base de* k *sur* k' *si il est* p*-indépendant sur* k' *et si* $k'(X) = k$.

Si $k' = k^p$, *on dit simplement* p*-base de* k.

Des arguments analogues à ceux qui ont permis de démontrer l'existence d'une base de transcendance d'une extension de corps vont permettre de démontrer l'existence de p-bases.

Théorème III.6

Soient k *un corps de caractéristique* p > 0, k' *un sous-corps de* k *tel que* $k^p \subset k' \subset k$.

Il existe des p*-bases de* k *sur* k'.

Démonstration

On commence par démontrer un théorème d'échange:

Avec les notations ci dessus, *soient X une partie de* k, x *et* y *des éléments de* k.

Si $x \in k'(X \cup \{y\})$ *et* $x \notin k'(X)$, *alors* $y \in k'(X \cup \{x\})$.

On peut, en effet, écrire, x sous la forme

$a_{p-1}y^{p-1} + \ldots + a_o$ où $a_i \in k'(X)$

Comme $x \notin k'(X)$, un des coefficients a_i n'est pas nul. Par conséquent, y qui est à la fois séparable et radiciel sur $k'(X \cup \{x\})$ appartient à $k'(X \cup \{x\})$.

Soit alors F l'ensemble des parties X de k p-*indépendantes sur* k'.

Il est non vide car $\emptyset \in F$. Ordonné par inclusion, il est inductif.

Soit X un élément maximal de F.

Alors $k'(X) = k$. Sinon, il existe $x \in k - k'(X)$. L'ensemble $X \cup \{x\}$ est p-indépendant sur k': soit, en effet, $y \in X \cup \{x\}$. L'élément y n'appartient pas à $k'((X \cup \{x\}) - \{y\})$: c'est clair si $y = x$ puisque $x \notin k'(X)$; si $y \neq x$, l'appartenance de y à $k'((X \cup \{x\} - \{y\}) = k'((X - \{y\}) \cup \{x\})$ impliquerait, puisque $y \notin k'(X)$, l'appartenance de x à $k'((X - \{y\}) \cup \{y\}) = k'(X)$ (propriété d'échange), contrairement à l'hypothèse.

L'ensemble $X \cup \{x\}$ contiendrait strictement X et appartiendrait à F. C'est impossible.

Exercices du chapitre 5

(1) Quelle est l'intersection de tous les sous-corps d'un corps ?

Quels sont les sous-corps de $\mathbb{Q}$? de $\mathbb{F}_p$?

(2) Les nombres complexes suivants sont-ils conjugués sur $\mathbb{R}$?

1. i et $\sqrt{2}$

2. $i + \sqrt{2}$ et $i - \sqrt{2}$

(3) Comparer les corps de décomposition sur $\mathbb{Q}$ des polynômes $X^2 + X + 1$ et $X^2 + 3$.

En déduire que le polynôme $X^2 + X + 1$ est résoluble par radicaux sur $\mathbb{Q}$.

Même question le corps de base étant $\mathbb{F}_2$.

(4) Quelle est la clôture algébrique du corps $\mathbb{F}_p$ à p éléments (p premier) ? du corps $\mathbb{F}_{p^n}$ à p^n éléments (p premier, $n \geqslant 1$) ?

(5) Soit K/k une extension galoisienne du corps k telle que $Gal(K/k)$ soit un groupe abélien (On dit alors que l'extension K/k est *abélienne*). Soient H un sous-groupe de $Gal(K/k)$, $L = Inv(H)$;

L'extension L/k est-elle galoisienne? abélienne ?

Démontrer que l'hypothèse $Gal(K/k)$ abélien est satisfaite si $k = \mathbb{Q}$ et si K est le corps de décomposition sur $\mathbb{Q}$ du polynôme

$(X^2-2)(X^2-5)(X^2-7)$.

Expliciter alors le groupe $Gal(K/k)$, ses sous-groupes et les sous-extensions de K/k.

(6) Quels sont les éléments primitifs de l'extension $\mathbb{F}_{p^n}/\mathbb{F}_p$?

(7) Soit k un corps de caractéristique $p > 0$. Si K/k est une extension finie de k, on appelle *degré d'inséparabilité* de l'extension K/k et on note $[K:k]_r$ le quotient $[K:k]/[K:k]_s$.

Démontrer que $[K:k]_r$ est une puissance de p.

Démontrer la multiplicativité de ce degré d'inséparabilité.

(8) Quaternions

Soient $\mathbb{H}$ le $\mathbb{R}$-espace vectoriel $\mathbb{R}^4$, $\{e,i,j,k\}$ sa base canonique.

On munit $\mathbb{H}$ d'une structure de $\mathbb{R}$-algèbre en définissant le produit dans $\mathbb{H}$ par linéarité à partir de la table de multiplication:

$ee = e \qquad ei = ie = i \qquad ej = je = j \qquad ek = ke = k$

$i^2 = j^2 = k^2 = -e$

$ij = -ji = k \qquad jk = -kj = i \qquad ki = -ik = j$

1. Vérifier l'associativité de la multiplication.

Un élément de $\mathbb{H}$ est appelé *un quaternion*. Il s'écrit de manière unique $ae + bi + cj + dk$ où $a,b,c,d \in \mathbb{R}$.

Un quaternion de la forme $xi + yj + zk$ est dit quaternion *pur*. Le vecteur libre (x,y,z) de $\mathbb{R}^3$ est dit *associé* à ce quaternion pur.

On appelle *conjugué* du quaternion $z = ae + bi + cj + dk$ le quaternion $\overline{z} = ae - bi - cj - dk$ et *norme* du quaternion z le nombre réel positif ou nul $N(z) = z\overline{z} = \overline{z}z = a^2 + b^2 + c^2 + d^2$.

2. a) Démontrer si $z, z' \in \mathbb{H}$ l'égalité $N(zz') = N(z)N(z')$

b) Démontrer que, si z est un élément non nul de $\mathbb{H}$, z admet pour inverse $N(z)^{-1}\,\overline{z}$.

En déduire que $\mathbb{H}$ est un corps non commutatif.

c) Démontrer les équivalences pour un quaternion *pur* z:

(i) $N(z) = 1$

(ii) $z^2 = -1$

Deux quaternions purs $z = xi + yj + zk$ et $z' = x'i + y'j + z'k$ sont dits *orthogonaux* si $xx' + yy' + zz' = 0$, i.e. si les vecteurs libres associés sont orthogonaux.

3. a) Démontrer que le produit de deux quaternions purs *orthogonaux* z et z' est un quaternion orthogonal pur à z et z'. Qelle est sa norme si $N(z) = N(z') = 1$?

b) Soit ε_1 un quaternion pur de norme 1. Justifier l'existence d'un quaternion pur ε_2 orthogonal à ε_1 et de norme 1. On pose $\varepsilon_3 = \varepsilon_1 \varepsilon_2$.

Calculer ε_1^2, ε_2^2, ε_3^2, $\varepsilon_1\varepsilon_2$, $\varepsilon_2\varepsilon_1$, $\varepsilon_2\varepsilon_3$, $\varepsilon_3\varepsilon_2$, $\varepsilon_3\varepsilon_1$, $\varepsilon_1\varepsilon_3$.

En déduire que $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$ est une base du $\mathbb{R}$-espace vectoriel $\mathbb{H}_p$ des quaternions purs.

c) Soit $\alpha \in \mathbb{R}$. On note u_α l'application $\mathbb{R}$-linéaire de $\mathbb{H}_p$ dans $\mathbb{H}_p$ définie par

$$u_\alpha(z) = (\cos \frac{\alpha}{2} + \varepsilon_1 \sin \frac{\alpha}{2})\, z (\cos \frac{\alpha}{2} - \varepsilon_1 \sin \frac{\alpha}{2})$$

Calculer les coordonnées de $u_\alpha(z)$ en fonction des coordonnées de z dans la base $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$.

Interpréter u_α comme la rotation d'angle α et de vecteur directeur ε_1.

4. Identifiant le quaternion pur $bi + cj + dk$ au vecteur libre associé $\underline{v} = (b,c,d)$, le quaternion $z = ae + bi + cj + dk$ s'écrit $ae + \underline{v}$.

Calculer le produit $(ae + \underline{v})(a'e + \underline{v}')$ en termes de $a, a', \underline{v}, \underline{v}'$ et des produits scalaires et vectoriel de $\underline{v}$ et $\underline{v}'$. Cas $a = a' = 0$.

Soient $\underline{v}$ et $\underline{v}'$ deux vecteurs libres de $\mathbb{R}^3$, $\underline{v}' \neq 0$. Calculer le quotient $\underline{v}/\underline{v}'$!

(9) Soient K/k une extension de k, X un système de t-générateurs de K/k, L un système libre de K/k.

1. Soit $y \in L$. Démontrer, en utilisant le propriété d'échange, qu'il existe $x \in X$ tel que $(X - \{x\}) \cup \{y\}$ soit un système de t-générateurs de K/k.

2. En déduire si X est *fini*, par itération de ce procédé, l'existence d'une partie X' de X en bijection avec L telle que $L \cup (X - X')$ soit un système de t-générateurs de K/k (théorème d'échange).

3. Généraliser par récurrence transfinie au cas général.

(10) Utiliser la notion de dimension d'un espace vectoriel pour démontrer l'analogue du théorème I.3 du chapitre 4 sans utiliser la *notion de déterminant*, à savoir:

Soient K un corps, k un sous-corps de K, $x \in K$.

Les assertions suivantes sont équivalentes:

(i) x est algébrique sur k

(ii) $[k[x]:k] < \infty$

(iii) il existe un sous-espace vectoriel de K contenant k et de dimension finie sur k.

(11) Soient k un corps, X une indéterminée, $K = k(X)$.

Utiliser le corollaire de la proposition I.7 pour calculer $Inv(Gal(K/k))$.

Démontrer que c'est k, si k est infini, et $\mathbb{F}_q\left(\frac{(X^{q^2} - X)^{q+1}}{(X^q - X)^{q^2+1}}\right)$, si k est le corps $\mathbb{F}_q$ à q éléments.

(12) Soient k un corps premier, n un entier $\geqslant 1$, non divisible par la caractéristique de k si elle est non nulle, K le corps de décomposition sur k du polynôme $X^n - 1$.

1. Démontrer que l'ensemble des racines de $X^n - 1$ dans K est un sous-groupe du groupe multiplicatif K^* et que ce sous-groupe est cyclique.

Un générateur de ce sous-groupe est appelé une *racine primitive n-ème de l'unité*.

2. Soit z une racine primitive n-ème de l'unité.

Démontrer les équivalences pour un entier $r \geqslant 1$:

(i) z^r est racine primitive n-ème de l'unité

(ii) $(r,n) = 1$

En déduire que le nombre de racines primitives n-èmes de l'unité est le nombre $\phi(n)$ nombre d'entiers r tels que $1 \leqslant r < n$ et $(r,n) = 1$ (indicateur d'Euler).

3. Démontrer que, si n et m sont premiers entre eux, $\phi(nm) = \phi(n)\phi(m)$.

Calculer $\phi(p^r)$, où p est un nombre premier et r un entier $\geqslant 1$.

En déduire l'expression générale de $\phi(n)$.

(13) Démontrer que le n-ième polynôme cyclotomique $\Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$.

[Soient z une racine primitive n-ième de l'unité, $f(X) = \mathrm{irr}(X,z,\mathbb{Q})$, $\Phi_n(X) = f(X)g(X)$.

Remarquer que $g(X) \in \mathbb{Z}[X]$. Soit p un nombre premier ne divisant pas n. Supposer $f(z^p) \neq 0$. Démontrer $g(z^p) = 0$. Posant $h(X) = g(X^p)$, démontrer une égalité $h(X) = f(X)q(X)$ pour un élément $q(X)$ de $\mathbb{Z}[X]$. Réduisant modulo p, démontrer que si $\psi(X) \in \mathbb{Z}[X]$ est modulo p un facteur irréductible dans $\mathbb{F}_p[X]$ de la classe de $f(X)$, $\psi(X)^2$ divise $\Phi_n(X)$. En déduire, que nécessairement, $f(z^p) = 0$ puis que toute racine de $\Phi_n(X)$ est racine de $f(X)$ et enfin que $\Phi_n(X) = f(X)$.]

(14) Soit k un corps fini ayant un nombre q impair d'éléments.

1. Démontrer que l'application $x \longmapsto x^2$ est un homomorphisme du groupe multiplicatif k^* dans lui même. Quel est son noyau ?

En déduire que les éléments de k^* qui sont des carrés forment un sous-groupe de k^* ayant $\frac{q-1}{2}$ éléments.

Calculer $x^{\frac{q-1}{2}}$ suivant que x est un carré ou n'est pas un carré dans k^*.

2. Soit p un nombre premier impair. Un entier n non divisible par p est appelé un *résidu quadratique modulo* p s'il existe $x \in \mathbb{Z}$ tel que

$$x^2 \equiv n \text{ modulo } p$$

Démontrer qu'il existe $\frac{p-1}{2}$ classes modulo p de résidus quadratiques modulo p et que, pour tout entier n non divisible par p on a

$$n^{\frac{p-1}{2}} \equiv \begin{cases} 1 \text{ modulo } p \text{ si } n \text{ est résidu quadratique modulo } p \\ -1 \text{ modulo } p \text{ si } n \text{ n'est pas résidu quadratique modulo } p \end{cases}$$

Les exercices suivants 15, 16, 17 sont consacrés à quelques démonstrations du théorème de d'Alembert: *le corps* $\mathbb{C}$ *est algébriquement clos.*

(15) (Utilisation de propriétés des fonctions continues)

Soit $f(X)$ *un polynôme non constant* $\in \mathbb{C}[X]$.

Démontrer l'existence de $m = \inf_{z \in \mathbb{C}} |f(z)|$ et de $z_o \in \mathbb{C}$ tel que $m = |f(z_o)|$.

Soit $f(X) = f(z_o) + c_k(X-z_o)^k + \ldots + c_n(X-z_o)^n$ avec $c_k \neq 0$ le développement de Taylor de $f(X)$.

Démontrer que pour tout $r \in \mathbb{R}^+$ suffisamment petit, on a une implication

$|z - z_o| = r \Longrightarrow |c_{k+1}(z - z_o)^{k+1} + \ldots + c_n(z - z_o)^n| < |c_k| r^k$

On suppose que f(X) *n'a pas de racine dans* $\mathbb{C}$, *i.e. que* m *est strictement positif.*

On choisit alors r *en sorte que* $|c_k| r^k < m$.

Démontrer l'existence de $z_1 \in \mathbb{C}$ que $|z_1 - z_o| = r$ et que le point $f(z_o) + c_k(z_1 - z_o)^k$ appartienne au segment joignant l'origine au point $f(z_o)$.

Calculer alors $|f(z_o) + c_k(z_1 - z_o)^k|$ et en déduire l'inégalité stricte $|f(z_1)| < m$, contredisant la définition de m.

(16) *Soit* f(X) *un polynôme non constant.* On suppose que f(X) n'a pas de racine dans $\mathbb{C}$.

1. Démontrer que la fonction: $z \longmapsto g(z) = \frac{1}{f(z)}$ est holomorphe dans $\mathbb{C}$ et bornée dans $\mathbb{C}$. Obtenir une contradiction par le théorème de Liouville.

2. On pose $h(z) = \frac{g(z) - g(0)}{z}$. Utiliser l'intégrale de Cauchy $\int_{C(R)} h(z)dz$ où C(R) est le cercle de centre l'origine et de rayon R pour démontrer (en faisant tendre R vers ∞) que $g(0) = 0$ et en déduire une contradiction.

(17) (Démonstration de Lagrange)

1. Démontrer que, pour prouver que $\mathbb{C}$ est algébriquement clos, il suffit de démontrer que tout polynôme non constant à coefficients *réels* a une racine dans $\mathbb{C}$.

(Associer à $f(X) \in \mathbb{C}[X]$, le produit de f(X) par son conjugué)

2. Démontrer, par récurrence sur l'entier m tel que $d^\circ(f) = 2^m n'$ avec n' impair, que le polynôme non constant $f(X) \in \mathbb{R}[X]$ a une racine dans $\mathbb{C}$.

Examiner le cas $m = 0$.

Supposer $m > 1$ et le théorème démontré pour $m - 1$.

Considerer un corps K de décomposition de f(X) sur $\mathbb{C}$, $z_1, \ldots, z_m$ les racines de f(X) dans $K[X]$.

Soient $c \in \mathbb{R}$, $y_{ij} = z_i + z_j + c z_i z_j$ $(1 \leqslant i < j \leqslant m)$.

Démontrer que le polynôme $g(X) = \prod_{1 \leqslant i < j \leqslant m} (X - y_{ij})$ appartient à $\mathbb{R}[X]$ et que son degré est de la forme $2^{m-1} n''$ où n'' est impair. Déduire de l'hypothèse de récurrence l'existence d'un couple (i,j) tel que y_{ij} appartienne à $\mathbb{C}$.

Démontrer l'existence de nombres réels c et c' distincts et d'un couple (r,s) tels que $z_r+z_s+cz_rz_s$ et $z_r+z_s+c'z_rz_s$ appartiennent à $\mathbb{C}$. En déduire que z_r et z_s appartiennent à $\mathbb{C}$.

(18) Soient k un corps, $\leqslant$ une relation d'ordre total sur l'ensemble k.

On dit que $(k,\leqslant)$, ou plus simplement k, est un corps totalement ordonné si les propriétés suivantes sont vérifiées:

$$\forall x,y,z \in k \qquad x \leqslant y \Longrightarrow x+z \leqslant y+z$$

$$0 \leqslant z \text{ et } x \leqslant y \Longrightarrow xz \leqslant yz$$

1. Démontrer que si le corps k est totalement ordonné, un carré de k est positif, que la caractéristique de k est 0, que si $x \in k$ est > 0, x^{-1} est > 0.

2. Soit $P = \{x \in k / x \geqslant 0\}$. Démontrer, avec les conventions d'écriture usuelle,

$$P + P \subset P \qquad PP \subset P \quad \text{et} \quad P \cap (-P) = \{0\}$$

Démontrer que, réciproquement, la donnée d'une partie P de k satisfaisant à ces propriétés munit k d'une structure de corps totalement ordonnée.

(19) Un corps k est dit *formellement réel* si -1 n'est pas une somme de carrés dans k.

Il est dit *réellement clos* s'il est formellement réel mais n'admet pas d'extension algébrique K/k distincte de k formellement réelle. *On suppose* k *réellement clos.*

1. Démontrer que, si $a \in k$ n'est pas un carré dans k, il n'est pas somme de carrés dans k. [Ecrire que le corps $k(\sqrt{a})$ n'est pas formellement réel; en déduire une égalité $-1 = (\sum_{r=1}^{n} \alpha_r^2)a + \sum_{r=1}^{n} \beta_r^2(1)$]

En déduire qu'une somme de carrés de k est un carré de k.

Démontrer que si a n'est pas un carré dans k, $-a$ est un carré dans k. [Utiliser l'égalité (1)].

En déduire que l'ensemble P des carrés de k satisfait aux conditions de l'exercice 18 et définit sur k une structure de corps totalement ordonné.

Existe-t-il sur k d'autres structures de corps totalement ordonné ?

2. Démontrer par récurrence sur le degré, que tout polynôme de degré *impair* à coefficients dans k (réellement clos) a une racine dans k. [Se ramener au cas où le polynôme $f(X)$ est irréductible; adjoindre à k

une racine a de f(X); écrire que k(a) n'est pas formellement réel; en déduire une égalité $-1 = \sum_{r=1}^{n} h_r(X)^2 + f(X)g(X)$ où $d^\circ h_r < d^\circ f-1, d^\circ g < d^\circ f-2$ puis une égalité $-1 = \sum_{r=1}^{n} h_r(b)^2$, où b est une racine de g(X).]

3. Reprenant la démonstration du fait que $\mathbb{C} = \mathbb{R}(i)$ est algébriquement clos donnée dans l'exercice 17, démontrer que si k est formellement réel k(i) est algébriquement clos. Démontrer que k n'est pas algébriquement clos.

(2D) (théorème de Puiseux) (clôture algébrique du corps k((X))).

Soient k un corps *algébriquement clos de caractéristique* 0, X une indéterminée, k((X)) le corps des fractions de l'anneau k[[X]] des séries formelles.

On veut démontrer que le corps $\Omega = \bigcup_{n\in N} k((X^{1/n}))$ *est une clôture algébrique de* k.

1. Démontrer que Ω est algébrique sur k.

2. Démontrer que, pour prouver que Ω est algébriquement clos, il suffit de démontrer qu'un polynôme f(X,Y) de la forme $Y^n + a_1(X)Y^{n-1} + \ldots + a_n(X)$, où $a_i(X)$ appartient à k[[X]], a une racine dans Ω.

Démontrer, ensuite, qu'il suffit de démontrer, *dans le cas* $a_n(0)=0$ qu'il existe $\phi(X) \in \Omega$ tel que $\phi(0) = 0$ et $f(X,\phi(X)) = 0$.

Démontrer ce résultat dans le cas où 0 est racine *simple* de f(0,Y).

3. *On va démontrer, par récurrence sur le degré* n *en* Y *du polynôme*

$$f(X,Y) = \sum_{i\in N} \sum_{j=0}^{n} c_{ij} X^i Y^j, \text{ où } c_{ij} \in k \text{ et } c_{oo} = 0,$$

l'existence d'une racine, dans Ω, *de ce polynôme de la forme*

$$tX^{\lambda} + t_1 X^{\lambda+\lambda_1} + \ldots,$$

où $t, t_1 \ldots$ *sont des éléments non nuls de* k *et où* $\lambda, \lambda_1 \ldots$ *sont des nombres rationnels positifs admettant un dénominateur commun.*

On considère, à cet effet, l'ensemble E_f des points M_{ab} du plan $\mathbb{R}^2$, de coordonnées (a, b) si $c_{ab} \neq 0$, et l'enveloppe convexe de cet ensemble, appelé *polygône* de Newton de f(X,Y).

Démontrer que ce polygône a au moins un côté de pente *négative*.

On choisit deux points M_{ab} et $M_{a_1 b_1}$ du polygône de Newton sur un tel côté. *On veut démontrer que l'on peut prendre pour* λ *le nombre* $-\frac{a-a_1}{b-b_1}$.

Soit p/q avec $p,q \in \mathbf{Z}$ et $(p,q) = 1$ ce nombre. Soient $M_{a_i b_i}$ les points situés sur le côté choisi du polygône de Newton, où les entiers b_i sont écrits dans l'ordre croissant.

Remarquer que $f(X,tX^{\lambda}) = X^{\gamma}(g(t)t^{b_o} + X^{m}h(X,t))$ où

$$g(t) = \Sigma c_{a_i b_i} t^{b_i - b_o}$$

est de la forme $g_1(t^q)$. Prendre pour t une racine de $g(X)$.

Calculer $X^{-\gamma q} f(X^q, X^{\lambda q}(t+Y_1)) = f_1(X,Y_1) = (t+Y_1)^{b_o} g(Y_1+t) + X^{mq}h(X^q, Y_1+t)$.

Remarquer que c'est une série *formelle* (et, non plus, nécessairement un polynôme en Y_1) mais qu'elle est régulière en Y_1 d'ordre celui de $g(Y_1+t)$ et donc inférieur à n si $g(Y_1+t)$ est différent de cY_1 avec $c \neq 0$.

Conclure, dans ce cas, à l'existence de la racine cherchée, en appliquant l'hypothèse de récurrence au *polynôme distingué* de la série régulière $f_1(X,Y_1)$.(analogue proposé dans l'exercice du chapitre 8 de l'exercice 16 du chapitre 2).

Traiter ensuite, le cas où $g(T) = c(T-t)^n$ avec c non nul de k. Démontrer que ce cas n'est possible que si n est un entier. Calculer alors γ_1 par le même procédé.

(21) (Corps cyclotomiques)

Soient n un entier > 1, ζ une racine primitive n-ème de l'unité (donc, $\zeta^n = 1$ et $\zeta^i \neq 1$ si $1 \leq i \leq n-1$), $\Phi_n(X) = \mathrm{irr}(X,\zeta,\mathbf{Q})$

1. Déduire de fait que $\Phi_n(X)$ divise $X^n - 1$ que le corps $K = \mathbf{Q}(\zeta)$est une extension galoisienne de $\mathbf{Q}$.(Dn l'appelle le *n-ème corps cyclotomique* car il est lié au polygône régulier convexe à n côtés ou à la partition du cercle en n arcs égaux).

Expliciter le groupe de Galois $Gal(K/k)$ en considérant si $s \in Gal(K/k$ l'élément $s(\zeta)$.

En déduire que le polynôme $\Phi_n(X)$ (appelé *n-ème polynôme cyclotomique*), qui est en fait à coefficients dans $\mathbf{Z}$, est égal à

$$\prod_{i\in\{1,\ldots,n-1\},\ (i,n)=1} (X-\zeta^i)$$

2. On suppose que n est un *nombre premier impair* p.

Démontrer que $1, \zeta, \ldots, \zeta^{p-2}$ est une base de K sur $\mathbb{Q}$.

On se propose de démontrer que l'anneau A *des entiers algébriques du corps* K *est* $\mathbb{Z}[\zeta]$ (*). Il est d'abord clair que $\mathbb{Z}[\zeta] \subset A$.

Calculer $Tr_{K/\mathbb{Q}}(\zeta^i)$. En déduire que si $\alpha = a_o + \ldots + a_{p-2}\zeta^{p-2}$ (où $a_i \in \mathbb{Q}$) est un élément de K, $Tr_{K/\mathbb{Q}}(\alpha(\zeta^{-k}-\zeta)) = pa_k$ $(k = 0,\ldots,p-2)$. En déduire que si α est entier sur $\mathbb{Z}$, pa_k appartient à $\mathbb{Z}$.

Démontrer que l'élément $\lambda = 1-\zeta$ est un élément premier de $\mathbb{Z}[\zeta]$ et que $p = \varepsilon(1-\zeta)^{p-1}$ où ε est un élément inversible de $\mathbb{Z}[\zeta]$.

On écrit $p\alpha$ sous la forme $c_o + c_1\lambda + \ldots + c_{p-2}\lambda^{p-2}$. On démontre, par récurrence, sur k que c_k est un entier divisible par p: supposant démontré que $c_o, \ldots, c_{k-1}$ sont divisibles par p, on écrit $c_k\lambda^k \equiv 0$ (modulo λ^{k+1}). On en déduit que c_k est divisible par $1-\zeta$ puis par p.

Quelques précisions supplémentaires concernant le théorème de Fermat *et les corps cyclotomiques:*

L'anneau A ci dessus est un anneau de Dedekind. Ses idéaux fractionnaires non nuls forment donc un groupe multiplicatif dont les idéaux principaux non nuls forment un sous-groupe. Le groupe quotient est d'ordre h *fini*. La finitude de cet ordre est en effet vraie pour tout corps de nombres algébriques et a été prouvée par Dirichlet.

Le nombre premier p est dit *régulier* s'il ne divise pas h. On démontre (Kummer) que si p est régulier l'équation

$$x^p + y^p = z^p$$

n'a pas de solution (x,y,z) avec $xyz \neq 0$ dans K^3 et donc, a fortiori dans $\mathbb{Q}^3$.

Kummer a donné un critère de régularité du nombre premier impair p faisant intervenir des nombres de Bernoulli. Le lecteur pourra se référer à [22].

(22) (Lemme de Dedekind)

Soient G un groupe noté multiplicativement, k un corps, $s_1, \ldots, s_n$

(*) Le résultat est encore vrai pour un entier quelconque $p > 2$ mais sa démonstration est plus délicate dans le cas général.(par exemple, Ribenboim. Algebraic Numbers. Pure and Applied Mathematics. 1972, 268-269).

des homomorphismes *distincts* de G dans le groupe multiplicatif k^* de k.

Démontrer que $s_1,\dots,s_n$ sont linéairement idépendants sur k

(Raisonner par l'absurde en supposant, aprés renumérotation éventuelle,

$a_1s_1+\dots+a_rs_r = 0$ avec $a_1,\dots,a_r$ *non nuls* et r *minimal*

Démontrer que, pour $g \in G$ tel que $s_1(g) \neq s_2(g)$,

$a_1s_1(g)s_1+\dots+a_rs_r(g)s_r = 0$

En déduire l'égalité

$a_2(s_1(g)-s_2(g))s_2+\dots+a_r(s_1(g)-s_r(g))s_r = 0.$)

(23) (Discriminant d'une extension séparable de degré fini)

Soient k un corps, K/k une extension séparable de degré fini de k, $\overline{K}$ une clôture algébrique de K.

Si $\{e_1,\dots,e_n\}$ est une base du k-espace vectoriel K, on appelle *discriminant de* $\{e_1,\dots,e_n\}$ l'élément $\det(\mathrm{Tr}_{K/k}(e_ie_j))$ de k. *On le note* $\mathrm{disc}_{K/k}(e_1,\dots,e_n)$

1. Soit $f_1,\dots,f_n$ une autre base, $f_1 = \Sigma a_{ij}e_j (i = 1,\dots,n)$.

Calculer $\mathrm{disc}_{K/k}(f_1,\dots,f_n)$ en fonction de $\mathrm{disc}_{K/k}(e_1,\dots,e_n)$

2. Soient $s_1,\dots,s_n$ les homomorphismes distincts de K dans $\overline{K}$ prolongeant 1_k.

Démontrer $\mathrm{disc}_{K/k}(e_1,\dots,e_n) = \det((s_i(e_j))^2$.

(Utiliser le fait que $\mathrm{Tr}_{K/k}(e_ie_j) = \sum_{k=1}^{n} s_k(e_ie_j) = \sum_{k=1}^{n} s_k(e_i)s_k(e_j)$)

En déduire que $\mathrm{disc}_{K/k}(e_1,\dots,e_n)$ est non nul.

(Utiliser le lemme de Dedekind)

En déduire que la forme bilinéaire $(x,y) \longmapsto \mathrm{Tr}_{K/k}(xy)$ est *non dégénérée*, i.e. que $\mathrm{Tr}_{K/k}(xy) = 0$ pour tout $y \in K$ implique $x = 0$.

Démontrer l'existence d'une base $\{e_1^*,\dots,e_n^*\}$ de K sur k (dite *duale de* $\{e_1,\dots,e_n\}$) telle que $\mathrm{Tr}_{K/k}(e_ie_j^*) = \delta_{ij}$ $(i,j = 1,\dots,n)$

3. Calculer $\mathrm{disc}_{K/k}(1,t,\dots,t^{n-1})$ où t est un élément *primitif* de K/k.

Démontrer que si $f(X) = \mathrm{irr}(X,t,k)$, $\mathrm{disc}_{K/k}(1,t,\dots,t^{n-1}) = (-1)^{n(n-1)/2}\prod_{i\neq j}(t_i-t_j)$ si $f(X) = \prod_{i=1}^{n}(X-t_i)$ (avec $t_1=t$).

En déduire l'égalité $\mathrm{disc}_{K/k}(1,t,\dots,t^{n-1}) = (-1)^{n(n-1)/2}N_{k(t)/k}(f'(t))$ (où f'(X) est le polynôme *dérivé* de f(X)).

Réciproquement, si f(X) est un polynôme (unitaire) *irréductible* de $k[X]$, on définit le *discriminant de* f(X) *sur* k par l'égalité ci dessus où t est une racine de f(X) dans une clôture algébrique de k. *On le note* $\mathrm{disc}_{K/k}(f)$.

4. Calculer $\mathrm{disc}_{K/k}(f)$ dans les cas suivants:

$f(X) = X^2+aX+b$ (On trouve a^2-4b)

$f(X) = X^3+pX+q$ (On trouve $-(4p^3+27q^2)$

$f(X) = (X^p-1)/(X-1)$ (polynôme cyclotomique; p *premier*)

(On trouve $(-1)^{(p-1)/2}p^{p-2}$)

(24) (Application du discriminant au calcul de certains anneaux d'entiers algébriques)

Soient K une extension de degré n du corps $\mathbb{Q}$ des rationnels, A l'anneau des entiers de K.

1. Démontrer l'existence d'un élément $t \in A$ tel que $K = \mathbb{Q}(t)$

2. Le $\mathbb{Z}$-module A est libre et admet une base $\{f_1,\ldots,f_n\}$ ayant n éléments. Pourquoi ?

Que peut-on dire de $\mathrm{disc}_{K/\mathbb{Q}}(f_1,\ldots,f_n)$.

Soit $t^{i-1} = \sum_{j=1}^{n} a_{ij}f_j$ $(i = 1,\ldots,n)$ où $a_{ij} \in \mathbb{Z}$.

Déduire de l'égalité $d = \det(a_{ij})^2\mathrm{disc}_{K/\mathbb{Q}}(f_1,\ldots,f_n)$ que, *si d n'a pas de facteur carré dans* $\mathbb{Z}$, la matrice (a_{ij}) est inversible dans $M_n(\mathbb{Z})$.

Qu'en résulte-t-il pour A ?

Appliquer au cas des corps quadratiques (chap. 4 ex)

3. *On suppose que* A *contient un sous-anneau* A_1 *contenant strictement* $\mathbb{Z}[t]$.

Démontrer que d a un facteur carré dans $\mathbb{Z}$.

Soit $\{e_1,\ldots,e_n\}$ (resp. $\{f_1,\ldots,f_n\}$) une base de A (resp. A_1) sur $\mathbb{Z}$.

Ecrire les égalités liant d, $\mathrm{disc}_{K/\mathbb{Q}}(e_1,\ldots,e_n)$, $\mathrm{disc}_{K/\mathbb{Q}}(f_1,\ldots,f_n)$.

En déduire que, *si* $d = p^2\mathrm{disc}_{K/\mathbb{Q}}(e_1,\ldots,e_n)$ *avec p premier*, on a l'égalité

$$\mathrm{disc}_{K/\mathbb{Q}}(e_1,\ldots,e_n) = \mathrm{disc}_{K/\mathbb{Q}}(f_1,\ldots,f_n)$$

et qu'alors $A = A_1$

4. Appliquer ceci au cas où K est obtenu par adjonction à $\mathbb{Q}$ d'une racine t du polynôme X^3-3X+9 (dont on prouvera l'irréductibilité dans $\mathbb{Q}[X]$).

On trouvera alors que $d = -(3)^3\times7\times11$.

On pose $u = 3/t$. Démontrer que u appartient à A puis que le sous-module du $\mathbb{Z}$-module K engendré par $1,t,u$ est un sous-anneau de A contenant strictement $\mathbb{Z}[t]$. Démontrer que A est égal à ce sous-anneau.

(Le lecteur pourra trouver d'autres exemples intéressants dans (24)ch.13.

(25). Soit k un corps. Une extension finie K/k est dite *cyclique* si $Gal(K/k)$ est un groupe cyclique.

Soient K/k une extension cyclique de degré n de k, s un générateur de $Gal(K/k)$.

1. (Théorème 90 de Hilbert. Forme multiplicative). Soit $x \in K$.

Démontrer les équivalences: (i) $N_{K/k}(x) = 1$

(ii) Il existe $c \in K^*$ tel que $x = \frac{c}{s(c)}$

(Pour démontrer (i) $\Longrightarrow$ (ii), considérer la résolvante de Lagrange-Hilbert de K/k, $t = 1_K + xs + (xs(x))s^2 + \ldots + (xs(x)\ldots s^{n-2}(x))s^{n-1}$.

Utiliser l'indépendance linéaire de $1_K, s, s^2, \ldots, s^{n-1}$ sur K (ex.22) pour justifier l'existence de $z \in K$ tel que $t(z) = c$ soit $\neq 0$. Utiliser alors l'égalité $N_{K/k}(x) = xs(x)\ldots s^{n-1}(x) = 1$ pour démontrer l'égalité $xs(c) = c$.)

2. On suppose n non divisible par la caractéristique de k et l'existence dans k d'une racine primitive n-ième de l'unité z.

Démontrer l'existence de $c \in K$ tel que $K = k(c)$ et c soit racine d'un polynôme $X^n - a$, où $a \in k$.

(Remarquer $N_{K/z}(z^{-1}) = 1$. Utiliser 1. pour justifier l'existence de $c \in K^*$ tel que $s(c) = zc$.)

3. Déduire de ce qui précède que, si k est un corps de caractéristique 0, et si f(X) est un polynôme non constant de $k[X]$ de groupe de Galois résoluble, alors f(X) est résoluble par radicaux sur k.

(Démontrer l'exsitence d'une tour $k = k_0 \subset k_1 \ldots \subset k_r$ d'extensions telles que k_r contienne le corps de décomposition de f(X) sur k, l'extension k_{i+1}/k_i soit cyclique ($i = 0, \ldots, r-1$) et k_i contienne une racine primitive de l'unité d'ordre celui de $Gal(k_{i+1}/k_i)$.)

4. (Théorème 90 de Hilbert. Forme additive). Soit $x \in K$.

Démontrer les équivalences: (i) $Tr_{K/k}(x) = 0$

(ii) Il existe $c \in K$ tel que $x = c - s(c)$

(26) (Théorème d'Artin-Schreier). On suppose k de caractéristique $p > 0$ et l'extension cyclique K/k de degré p. Démontrer l'existence de $c \in K$ tel que $K = k(c)$ et c soit racine d'un polynôme $X^p - X - a$, où $a \in k$.

Démontrer, réciproquement, que, si $a \in k$, le polynôme $X^p - X - a$ a toutes ses racines dans k ou est irréductible et que, dans ce dernier cas, l'extension k(c)/k où c est racine de ce polynôme est cyclique d'ordre p sur k.

(27) Soient Ω une extension d'un corps k, K/k une sous-extension galoisienne, L/k une sous-extension.

1. Démontrer que $K(L)$ est extension galoisienne de L et que K est extension galoisienne de $K \cap L$. Comparer $Gal(K(L)/L)$ et $Gal(K/(K \cap L))$. Comparer $[K(L):K]$ et $[L:k]$.

2. Soient K_1/k et K_2/k deux sous-extensions galoisiennes de Ω/k.

Démontrer que l'application naturelle de $Gal(K_1(K_2),k)$ dans $Gal(K_1,k) \times Gal(K_2,k)$ est injective, et que c'est un isomorphisme si $K_1 \cap K_2 = k$.

(28) (Théorie de Galois infinie)

1. Soient I un ensemble préordonné filtrant, $(G_i, f_{ij})_{i,j \in I}$ un système projectif de la catégorie des groupes (non nécessairement commutatifs), G le sous-groupe de $\prod_{i \in I} G_i$ $\{(g_i)_{i \in I} / j \leqslant i \Longrightarrow x_i = f_{ij}(x_j)\}$, f_i la restriction à G de la projection pr_i.

Démontrer que $(G, f_i)_{i \in I}$ est limite projective du système dans la catégorie des groupes.

2. Soient k un corps, K/k une extension algébrique galoisienne (de degré quelconque) de k, F l'ensemble des sous-extensions finies galoisiennes de k

Démontrer que F, ordonné par inclusion, est filtrant.

Si L, $L' \in F$ et $L' \subset L$, on note $\rho_{L'L}$ l'homomorphisme de restriction de $Gal(L/k)$ dans $Gal(L'/k)$.

On obtient ainsi un système projectif $(Gal(L/k), \rho_{L'L})_{L,L' \in F}$ de groupes.

On note ρ_L l'homomorphisme de restriction $Gal(K/k) \longrightarrow Gal(L/k)$.

Démontrer que $(Gal(K/k), \rho_L)_{L \in F}$ est limite projective, dans la catégorie des groupes, du système projectif $(Gal(L/k), \rho_{L'L})_{L,L' \in F}$.

3. On munit $Gal(K/k)$ de la topologie, invariante par translation, dans laquelle un système fondamental de voisinage de 1_K est formé des groupes $Gal(L/k)$ où $L \in F$.

Démontrer que la topologie ainsi définie sur $Gal(K/k)$ est la topologie limite projective, i.e. la topologie induite par la topologie produit sur $\prod_{L \in F} Gal(L/k)$.

Démontrer que $Gal(K/k)$ est compact, totalement discontinu, i.e. tel que la composante connexe de tout point soit réduite à ce point.

4. Démontrer que, si H est un sous-groupe de $Gal(K/k)$, H est dense dans $Gal(Inv(H)/k)$.

En déduire les équivalences:

(i) $H = Gal(Inv(H)/k)$

(ii) H est un sous-groupe fermé de $Gal(K/k)$

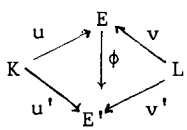
(29) Soient k un corps, Ω une extension de k, K et L deux sous-extensions de Ω.

Le corps $K(L) = L(K)$ est la plus petite sous-extension de Ω contenant K et L.

Il est le corps des fractions de l'anneau $K[L]$.

Le problème plus général suivant est naturel: soient K et L deux extensions de k (non plongées dans une extension commune). Existe-t-il une extension E de k et des k-homomorphismes injectifs $u:K \longrightarrow E$ et $v:L \longrightarrow E$? Existe-t-il plusieurs tels triplets (E,u,v) et combien si on impose de plus à E des conditions naturelles de minimalité ?

Deux triplets (E,u,v) *et* (E',u',v') *sont dits isomorphes* s'il existe un k-isomorphisme $\phi:E \longrightarrow$ tel que le diagramme



soit commutatif.

Le triplet (E,u,v) est appelé *extension composée de* K/k *et* L/k si E est engendré par $u(K) \cup v(L)$.

1. Soit (E,u,v) une extension composée de K et L.

Soient w l'homomorphisme (noté u.v dans la suite) de $K \underset{k}{\otimes} L$ dans E tel que $w(x \otimes y) = u(x)v(y)$, p l'idéal premier ker(w), E' le corps des fractions de l'anneau intègre $(K \underset{k}{\otimes} L)/p$, u' (resp. v') le composé de l'homomorphisme $x \longmapsto x \otimes 1$ (resp. $y \longmapsto 1 \otimes y$) de K (resp. L) dans $K \underset{k}{\otimes} L$, de la surjection canonique $K \underset{k}{\otimes} L \longrightarrow (K \underset{k}{\otimes} L)/p$ et de l'injection canonique de $(K \underset{k}{\otimes} L)/p$ dans E'.

Démontrer que (E',u',v') est isomorphe à (E,u,v).

2. Soit, réciproquement, p un idéal premier de $K \underset{k}{\otimes} L$. Démontrer que (E',u',v') où E',u',v' sont définis comme ci dessus est une extension composée de K et L.

Démontrer que deux idéaux premiers distincts de $K \underset{k}{\otimes} L$ conduisent à des extensions composées non isomorphes.

Par conséquent, *les classes d'isomorphismes d'extensions composées de* K/k *et* L/k *sont en bijection avec* $\mathrm{Spec}(K \otimes_k L)$.

3. Soient Ω/k une extension *algébriquement close* de k, K/k une sous-extension de Ω/k, L/k une extension de k.

Un suppose $d°tr(\Omega/k) \geqslant d°tr(L/k)$. Démontrer que toute extension composée de K/k et L/k est isomorphe à une extension (E,u,v) où E est un sous-corps de Ω contenant K, u l'injection canonique de K dans E.

Cas particulier où L/k est aussi une sous-extension de Ω/k ?

4. On revient au cas général et on suppose K/k séparable de degré fini et L/k de degré fini. Démontrer que l'anneau $K \otimes_k L$ est artinien *réduit* et donc est isomorphe à un produit de corps $\prod_{i=1}^{m} E_i$.

Quelles sont alors les extensions composées de K/k et L/k ?

(L'hypothèse que K/k est de degré fini est inutile. On pourra se reporter pour le cas général au chapitre 9: dérivations et differentielles).

(30) *Soient* k *un corps,* Ω/k *une extension de* k, K/k *et* L/k *deux sous-extensions.*

1. Démontrer l'équivalence des assertions:

(i) tout système (fini) d'éléments de K linéairement indépendants sur k est linéairement indépendant sur L.

(ii) tout système (fini) d'éléments de L linéairement indépendants sur k est linéairement indépendant sur K.

(iii) l'homomorphisme naturel $x \otimes y \longmapsto xy$ de $K \otimes_k L$ sur le sous-k espace vectoriel de Ω engendré par les produits xy ($x \in K, y \in L$) est un isomorphisme.

Si ces assertions sont vérifiées on dit que K et L sont *linéairement disjoints sur* k.

2. *Soit* M/k *une sous-extension de* L/k. On note MK le sous corps de Ω engendré par K et M. Démontrer l'équivalence des assertions:

(i) K et L sont linéairement disjoints sur k

(ii) K et M sont linéairement disjoints sur k et, d'autre part, L et KM sont linéairement disjoints sur M.

(31) Les notations sont celles de l'exercice précédent.

1. Démontrer les équivalences:

(i) tout système (fini) d'éléments de K algébriquement indépendants sur k est algébriquement indépendant sur L.

(ii) tout système (fini) d'éléments de L algébriquement indépendants sur k est algébriquement indépendant sur K.

Si ces assertions sont vérifiées, on dit que K et L sont *algébriquement indépendants* sur k.

2. Démontrer que la disjonction linéaire de K/k et L/k implique l'indépendance algébrique.

CHAPITRE 6

Éléments de géométrie algébrique

L'étude des courbes algébriques planes complexes, définies dans le chapitre 2, est une partie de la branche des mathématiques appelée *géométrie algébrique*.

Cette géométrie, en raison même des problèmes successifs qu'elle s'est posée, a subi de nombreuses modifications de formes.

Il ne pouvait être question ici de faire un exposé exhaustif de cette évolution. Le lecteur pourra, par exemple, se reporter à (28).

Nous sommes partis ici du point de vue classique des (k,Ω)-ensembles algébriques, où Ω est un corps algébriquement clos et k un sous-corps tel que le degré de transcendance de Ω/k soit suffisamment grand. Un tel (k,Ω)-ensemble algébrique est l'ensemble des zéros dans Ω^n d'une famille de polynômes à n indéterminées à coefficients dans k.

Une interprétation convenable de la notion de point permet d'identifier un tel ensemble au spectre d'une k-algèbre de type fini, son algèbre affine et, d'ailleurs, ce faisant d'éliminer Ω.

Ce spectre est muni de manière naturelle d'une topologie, la topologie spectrale ou de Zariski, et d'un faisceau de k-algèbres dont la fibre en chaque point est l'anneau local des germes de fonctions "rationnelles" au voisinage du point et l'anneau des sections globales s'identifie à l'algèbre affine.

Plus généralement, on peut associer à tout anneau A un espace topologique, son spectre, et munir ce spectre d'un faisceau d'anneaux dont l'anneau A est l'anneau des sections globales. On obtient ainsi ce qu'on appelle un *schéma affine*.

Le plan de ce chapitre est le suivant:

Dans I, on développe le point de vue des (k,Ω)-ensembles algébriques.

Dans II, on définit la notion de schéma affine.

Dans III, on étudie le spectre maximal d'un anneau et les propriétés éventuelles de densité de ce spectre maximal dans le spectre.

Dans IV, on donne quelques éléments de géométrie algébrique projective

I. Eléments de géométrie algébrique affine

1. Introduction

Définitions

Soient Ω *un corps,* $X_1,\ldots,X_n$ *des indéterminées,* $f_i(X_1,\ldots,X_n) \in \Omega[X_1,\ldots,X_n]$ $(i \in I)$ *une famille de polynômes.*

1. Un point $(x_1,\ldots,x_n)$ *de* Ω^n *est dit un zéro de la famille* $(f_i)_{i\in I}$ *si* $\forall\, i \in I,\ f_i(x_1,\ldots,x_n) = 0$.

2. Le sous-ensemble H *de* Ω^n *des zéros de* $(f_i)_{i\in I}$ *est appelé le sous-ensemble algébrique fermé, ou plus simplement le sous-ensemble algébrique, de* Ω^n *d'équations* $f_i = 0$ $(i \in I)$.

3. Un sous-ensemble H *de* Ω^n *est dit algébrique (fermé*(*)*) s'il existe une famille* $(f_i)_{i\in I}$ *d'éléments de* $\Omega[X_1,\ldots,X_n]$ *tel que* H *soit le sous-ensemble algébrique de* Ω^n *d'équations* $f_i = 0$ $(i \in I)$.

Il existe un sous-corps k de Ω éventuellement distinct de Ω tels que H soit l'ensemble des zéros d'une famille de polynômes à coefficients dans k (et non plus dans Ω).

Il résulte notamment du théorème de Hilbert que H admet un système *fini* d'équations.

Les coefficients des polynômes correspondants engendrent une extension *de type fini* du corps premier de Ω.

Des raisons techniques: validité du théorème des zéros de Hilbert, *existence de points génériques, conduisent à considérer un couple* (k,Ω) *d'un corps* Ω *et d'un sous-corps* k *de* Ω *tel que* Ω *soit algébriquement clos et de degré de transcendance infini sur* k.

Les équations seront définies par des polynômes à coefficients dans k mais on considérera des points à coordonnées dans Ω.

Définition

Soit k *un corps. Un domaine universel pour* k *est une extension* Ω/k *de degré de transcendance infini sur* k *tel que* Ω *soit algébriquement clos.*

(*)

La notion d'ensemble algébrique *fermé* devient rapidement insuffisante.

On doit considérer aussi comme ensembles algébriques des ouverts, pour une topologie convenable, de Ω^n ou d'un ensemble fermé.

Dans la suite, ensemble algébrique signifie ensemble algébrique fermé.

2. Ensembles algébriques affines

Dans la suite, Ω est un corps, k un sous-corps de Ω, le corps de base.

Des hypothèses seront faites ultérieurement sur le couple (Ω,k) mais on n'exclut pas provisoirement le cas $k = \Omega$, par exemple, $k = \Omega = \mathbb{R}$ ou $\mathbb{C}$.

Conformément à un usage commode, il nous arrivera de noter $k[X]$ *l'anneau* $k[X_1,\ldots,X_n]$ *des polynômes à coefficients dans* k *en les* n *indéterminées* $X_1,\ldots,X_n$ *et* (x) *l'élément* $(x_1,\ldots,x_n)$ *de* Ω^n.

On notera alors, si $f(X) \in k[X]$, $f(x)$ *l'élément* $f(x_1,\ldots,x_n)$ *de* Ω.

Définition

Un ensemble H est dit un (k,Ω)*-ensemble algébrique s'il existe un entier* $n \geqslant 1$ *et une partie* F *de l'anneau* $k[X_1,\ldots,X_n]$ *dont H soit l'ensemble des zéros dans* Ω^n.

On dit aussi que *H est un* k*-ensemble algébrique de* Ω^n ou, plus simplement, s'il n'y a pas d'ambiguité sur le couple (k,Ω), *un ensemble algébrique.*

Exemple

Soit $f(X_1,X_2) \in \mathbb{C}[X_1,X_2]$. L'ensemble des couples $(x_1,x_2) \in \mathbb{C}$ tels que $f(x_1,x_2) = 0$ est *l'ensemble vide* (qui est donc algébrique) si f est constant non nul, une *courbe algébrique plane complexe* si f n'est pas constant (par exemple, le cercle de centre (0,0) et de rayon 1 si $f(X_1,X_2) = X_1^2+X_2^2-1$), le plan complexe $\mathbb{C}^2$, qui est donc un ensemble algébrique, si $f = 0$.

Notations

1. Si F est une partie de $k[X_1,\ldots,X_n]$, *on note* $V_\Omega(F)$ *le sous-ensemble de* Ω^n, *ensemble algébrique des zéros de F*

2. Soit H un sous-ensemble, non nécessairement algébrique, de Ω^n. *On note*

$I_k(H)$ *l'idéal* $\{f \in k[X_1,\ldots,X_n] / (x_1,\ldots,x_n) \in H \Longrightarrow f(x_1,..,x_n) = 0\}$ *des polynômes s'annulant en tout point de H.*

Exemple

Soit *H* une partie *partout dense* du cercle d'équation $X_1^2 + X_2^2 - 1 = 0$, dans $\mathbb{C}^2$. On démontre aisément que $I_k(H)$ est l'idéal engendré par $X_1^2+X_2^2-1$.

Les applications $F \longmapsto V_\Omega(F)$ *et* $H \longmapsto I_k(H)$ *sont liées par des propriétés simples explicitées ci dessous.*

Proposition I.1

Soient F, F_1, F_2, $F_i (i \in I)$ (resp. H, H_1, H_2, $H_i (i \in I)$) *des parties de* $k[X_1,\ldots,X_n]$ (resp. Ω^n).

1. $F_1 \subset F_2 \Longrightarrow V_\Omega(F_2) \subset V_\Omega(F_1)$
2. $H_1 \subset H_2 \Longrightarrow I_k(H_2) \subset I_k(H_1)$
3. $V_\Omega(\bigcup_{i\in I} F_i) = \bigcap_{i\in I} V_\Omega(F_i)$
4. $I_k(\bigcup_{i\in I} H_i) = \bigcap_{i\in I} I_k(H_i)$
5. $I_k(V_\Omega(F)) \supset F$
6. $V_\Omega(I_k(H)) \supset H$
7. $V_\Omega(I_k(V_\Omega(F))) = V_\Omega(F)$
8. $I_k(V_\Omega(I_k(H))) = I_k(H)$

Démonstration

1,2,5,6 sont évidents.

La démonstration de 3 est donnée par les équivalences:

$(x) \in V_\Omega(\bigcup_{i\in I} F_i) \Longleftrightarrow \forall i \in I, \forall f \in F_i,\ f(x) = 0 \Longleftrightarrow \forall i \in I,\ (x) \in V_\Omega(F_i) \Longleftrightarrow (x) \in \bigcap_{i\in I} V_\Omega(F_i)$

Celle de 4 est analogue.

Démonstration de 7

De $I_k(V_\Omega(F)) \supset F$ et de 1. on déduit

$V_\Omega(I_k(V_\Omega(F))) \subset V_\Omega(F)$

Appliquant 6. à $H = V_\Omega(F)$, on obtient

$V_\Omega(I_k(V_\Omega(F))) \supset V_\Omega(F)$

La démonstration de 8. est analogue

Définitions

1. *Soit* H *un ensemble algébrique* .

L'idéal $I_k(H)$ *de* $k[X]$ *est appelé l'idéal de définition de l'ensemble algébrique* H.

2. *Un idéal* I *de* $k[X]$ *est dit idéal de définition d'un ensemble algébrique s'il est de la forme* $I_k(H)$ *où* H *est un sous-ensemble* (algébrique) *de* Ω^n.

Corollaire

L'application $a \longmapsto V_\Omega(a)$ *est une bijection décroissante de l'ensemble des idéaux de* $k[X]$ *qui sont idéaux de définition d'ensembles algébriques sur l'ensemble des sous-ensembles algébriques de* Ω^n.

La bijection réciproque est l'application $H \longmapsto I_k'(H)$.

Démonstration

C'est une conséquence immédiate de la définition et de 7. et 8.

On rappelle que la *racine $r(a)$ d'un idéal a* est l'intersection des idéaux premiers contenant a. Si $a = A$, $r(a)$ est l'intersection de la famille vide d'idéaux premiers de A. Conformément à l'usage, on définit cette intersection comme égale à A.

1. Un idéal de définition a est égal à sa racine.

Soit $f(X) \in k[X]$ tel que, pour un entier $r \geqslant 1$, f^r appartienne à a.

Alors, pour tout $x \in V_\Omega(a)$, $f^r(x) = f(x)^r = 0$, et donc $f(x) = 0$.

Par conséquent, $f \in I_k(V_\Omega(a)) = a$.

Il existe donc des idéaux de $k[X]$ qui ne sont pas des idéaux de définition.

2. *Si on ne fait pas d'hypothèse sur Ω* (en fait, si on ne suppose pas Ω algébriquement clos), *il peut exister des idéaux de $k[X]$ égaux à leurs racines mais qui ne soient pas idéaux de définition.*

Exemples

1. $n = 1$, $\Omega = k = \mathbb{R}$. L'idéal principal (X^2+1) de $\mathbb{R}[X]$ est égal à sa racine. Il n'est pas idéal de définition car $V(X^2+1)$ est vide et donc, $I(V(X^2+1)) = \mathbb{R}[X]$.

2. $n = 1$, $k = \Omega = \mathbb{Q}$. L'idéal principal (X^2-2) de $\mathbb{Q}[X]$ est égal à sa racine mais n'est pas idéal de définition.

3. Si, dans les exemples ci dessus, on suppose $\Omega = \mathbb{C}$, les idéaux considérés deviennent des idéaux de définition car $V(X^2+1) = \{+i,-i\}$ et $V(X^2-2) = \{\sqrt{2}, -\sqrt{2}\}$ et $I(V(X^2+1)) = (X^2+1)$, $I(V(X^2-2)) = (X^2-2)$.

3. Caractérisation des idéaux de définition. Théorème des zéros de Hilbert

Le théorème des zéros admet plusieurs énoncés et de nombreuses démonstrations différentes.

L'examen du cas d'un anneau de polynômes à *une* indéterminée montre, conformément aux exemples donnés plus haut, que l'hypothèse que le corps Ω est algébriquement clos, est indispensable à sa validité.

Théorème I.2 (Théorème des zéros de Hilbert)

Soient Ω un corps algébriquement clos, k un sous-corps de Ω, $k[X]$ l'anneau des polynômes à n indéterminées $X_1,\ldots,X_n$ à coefficients dans k, a un idéal de $k[X]$.

1. Les assertions suivantes sont équivalentes:

(i) a est un idéal de définition d'un (k,Ω)-ensemble algébrique.

(ii) $a = r(a)$, racine de a

2. $I_k(V_\Omega(a)) = r(a)$

3. *Si* $a \neq k[X]$, *l'ensemble* $V_\Omega(a)$ *est non vide*

4. *Soit* m *un idéal maximal de* $k[X]$, $V_\Omega(m)$ *est non vide*

Démonstration du théorème

Démonstration de 4 : le corps quotient $k[X_1,\ldots,X_n]/m$ est une k-algèbre de type fini. Il est donc algébrique sur k (chap. 5. prop. I.2). Il résulte du théorème II.5 du chapitre 5, qu'il existe un homomorphisme (injectif) de ce corps quotient dans Ω, *supposé algébriquement clos.*

On peut, grâce à cet homomorphisme, identifier la classe x_i de X_i modulo m à un élément de Ω et donc le point $(x_1,\ldots,x_n)$ à un point de Ω^n.

Ce point est un zéro de m et donc $V_\Omega(m)$ est non vide.

Démonstration de 3 : dire que l'idéal a est distinct de $k[X]$ c'est dire qu'il existe un idéal maximal m de $k[X]$ contenant a. Comme $V_\Omega(a)$ contient $V_\Omega(m)$, il est non vide en vertu de 4.

Démonstration de 2: *on déduit 2. de 3. grace à une astuce due* à Rabinowitsch.

Soit $f \in I_k(V(a))$. On peut le supposer non nul.

Soient X_{n+1} une autre indéterminée, b l'idéal de $k[X_1,\ldots,X_n,X_{n+1}]$ engendré par a et le polynôme $1-X_{n+1}f(X_1,\ldots,X_n)$.

L'ensemble $V_\Omega(b)$ est vide: dire que $(x_1,\ldots,x_n,x_{n+1})$ appartient à $V_\Omega(b)$ c'est, en effet, dire, d'une part que $(x_1,\ldots,x_n)$ appartient à $V_\Omega(a)$ ce qui implique $f(x_1,\ldots,x_n) = 0$, et, d'autre part, que $1-x_{n+1}f(x_1,\ldots,x_n) = 0$, ce qui est impossible puisque $1-x_{n+1}f(x_1,\ldots,x_n) = 1$.

Il résulte de 3., appliqué à b, que l'on doit avoir $b = k[X_1,\ldots,X_n,X_{n+1}]$.

On a donc une égalité

$$1 = \sum_{i=1}^{r} g_i(X_1,\ldots,X_n,X_{n+1})f_i(X_1,\ldots,X_n)+p(X_1,\ldots,X_n)(1-X_{n+1}f(X_1,\ldots,X_n$$

où $f_i \in a$, $g_i \in k[X_1,\ldots,X_n,X_{n+1}]$ $(i=1,\ldots,r)$, $p \in k[X_1,\ldots,X_n,X_{n+1}]$.

On donne à X_{n+1} la valeur $1/f(X_1,\ldots,X_n)$. Le second membre devient une fraction rationnelle en $X_1,\ldots,X_n$ dont le numérateur est un élément de a (présence des f_i) et de dénominateur une puissance f^s de f.

Par multiplication par ce dénominateur, on voit que f^s appartient à a, i.e. que f appartient à $r(a)$.

Démonstration de 1. : on sait déjà que (i) implique (ii). Soit, réciproquement, a un idéal égal à sa racine. D'après 2. $a = I_k(V_\Omega(a))$ et donc a est idéal de définition.

Le corollaire suivant illustre très concrètement le théorème des zéros.

Corollaire

Les hypothèses sont celles du théorème I.2. *Soit* Ω' *la fermeture algébrique de* k *dans* Ω. (C'est un corps algébriquement clos).

Soient V_1 *et* V_2 *deux* (k,Ω)*-ensembles algébriques de* Ω^n.

Si les traces de V_1 *et* V_2 *sur le sous-ensemble* Ω'^n *de* Ω^n *sont égales,* $V_1 = V_2$.

Autrement dit, un (k,Ω)*-ensemble algébrique de* Ω^n *est parfaitement déterminé par ses points à coordonnées algébriques sur* k.

Corollaire

Soit a_i l'idéal $I_k(V_i)$ (i=1,2). On remarque que $V_i \cap \Omega'^n$ est l'ensemble

$$\{(x_1,\ldots,x_n) \in \Omega'^n / f \in a_i \Longrightarrow f(x_1,\ldots,x_n) = 0\}$$

i.e. $V_{\Omega'}(a_i)$. Donc, $V_{\Omega'}(a_1) = V_{\Omega'}(a_2)$

Comme Ω' est algébriquement clos, $a_1 = I_k(V_{\Omega'}(a_1)) = I_k(V_{\Omega'}(a_2)) = a_2$. Par conséquent $V_1 = V_\Omega(a_1) = V_\Omega(a_2) = V_2$.

On peut énoncer ce corollaire en disant que les points à coordonnés algébriques sur le corps de base k déterminent parfaitement le k-ensemble algébrique. Dans nombre de questions, on peut se limiter à ces seuls points et donc, en particulier si le corps k est algébriquement clos, aux points à cooordonnées dans k, points qui sont dits *rationnels*.

Remarques

1. Il existe de nombreuses démonstrations du théorème des zéros de Hilbert et, notamment, de l'assertion 4. du théorème I.2.

Une d'elles, valable dans le cas où le corps k *n'est pas dénombrable*, a été donnée dans un cas particulier (chapitre 2. lemme du §3).

La démonstration en est la même dans le cas général.

Une autre démonstration utilise le lemme de normalisation, démontré dans le chapitre 7 mais dont la preuve est assez élémentaire pour

être faite avec les seules connaissances du chapitre 4.

2. Le théorème des zéros de Hilbert est à rapprocher du théorème suivant:

Soient X *un espace topologique compact,* $C(X)$ *l'anneau des applications continues de* X *dans* $\mathbb{R}$.

L'application: $x \in X \longmapsto \{f \in C(X)/f(x) = 0\}$ *est une bijection de* X *sur l'ensemble des idéaux maximaux de l'anneau* $C(X)$. (ex.4)

Le lecteur peut se référer pour des compléments à (Gillman-Jerrison *Rings of continuous functions*. Van Nostrand)

3. Le corollaire du théorème I.2 suggère une propriété de *densité des points à coordonnées algébriques* sur le corps de base k d'un (k,Ω)-ensemble algébrique.

Une autre démonstration du théorème des zéros est fondée sur cette idée. Elle utilise le fait qu'une algèbre affine est un anneau de Jacobson i.e. un anneau dans lequel tout idéal *premier* est intersection des idéaux *maximaux* qui le contiennent. Cette question est reprise dans III.

4. Topologie de Zariski

Un ensemble algébrique de $\mathbb{R}^n$ ou $\mathbb{C}^n$ hérite d'une structure topologique, induite par celle de l'espace dans lequel il est plongé. Des propriétés importantes d'un tel ensemble sont, en fait, topologiques: *connexité, existence de points isolés, nature topologique des singularités.*

D'autre part, la géométrie élémentaire qui est, en fait, pour une part l'étude de courbes algébriques simples utilise systèmatiquement la notion de *lieu d'un point*. Ce point est appelé suivant les auteurs: point courant, point général ou point générique.

Il est intuitif que le lieu d'un point est l'adhérence de ce point pour une topologie convenable.

Cette topologie doit possèder un certain nombre de propriétés simples.

Elle doit rendre continues les fonctions polynomiales définies par les polynômes à coefficients dans le corps de base. Les points à coordonnées dans ce corps de base doivent être fermés.

On choisit la topologie la moins fine satisfaisant à ces exigences. C'est la topologie de Zariski ou topologie spectrale.

Si le corps de base est $\mathbb{R}$ ou $\mathbb{C}$, la topologie de Zariski est moins fine que la topologie usuelle qui doit rendre continues beaucoup plus de fonctions.

Proposition I.3 (définition de la topologie de Zariski)

1. *Il existe une topologie sur* Ω^n *dont les fermés sont les* k*-ensembles algébriques.*

2. *Les points à coordonnées dans* k *sont fermés.*

Démonstration

1. D'abord $V_\Omega(1) \neq 0$ et $V_\Omega(0) = \Omega^n$.

Si, ensuite, $(H_i)_{i\in I}$ est une famille de k-ensembles algébriques de Ω^n, $\bigcap_{i\in I} H_i = V_\Omega(\bigcup_{i\in I} I_k(H_i))$ est un k-ensemble algébrique de Ω^n.

Enfin, une réunion finie de k-ensembles algébriques de Ω^n est un k-ensemble algébrique de Ω^n en vertu du lemme suivant.

Lemme

Soient $H_1,\ldots,H_r$ *des* k*-ensembles algébriques de* Ω^n.

Alors $\bigcup_{i=1}^r H_i = V_\Omega(\prod_{i=1}^r I_k(H_i))$.

Démonstration

Des inclusions $\prod_{i=1}^r I_k(H_i) \subset \bigcap_{i=1}^r I_k(H_i) \subset I_k(H_j)$ (pour $j = 1,\ldots,r$), on déduit les inclusions

$V_\Omega(\prod_{i=1}^r I_k(H_i)) \supset V_\Omega(I_k(H_j)) = H_j$ et donc $V_\Omega(\prod_{i=1}^r I_k(H_i)) \supset \bigcup_{i=1}^r H_i$.

Si, d'autre part, $(x) = (x_1,\ldots,x_n)$ n'appartient pas à $\bigcup_{i=1}^r H_i$, il existe, pour tout $i \in I$, $f_i \in I_k(H_i)$ tel que $f_i(x) \neq 0$.

Alors, $f = f_1,\ldots,f_r$ appartient à $\prod_{i=1}^r I_k(H_i)$ et $f(x) \neq 0$ n'appartient pas à $V_\Omega(\prod_{i=1}^r I_k(H_i))$

2. Soit $(a_1,\ldots,a_n) \in k^n$. Alors $\{(a_1,\ldots,a_n)\} = V_\Omega(X_1-a_1,\ldots,X_n-a_n)$ est fermé.

Définition

La topologie définie sur Ω^n *dans la proposition* I.3 *s'appelle la* k*-topologie de* Zariski *de* Ω^n.

La topologie induite sur un fermé de Ω^n, *i.e. un* k*-ensemble algébrique, s'appelle la* k*-topologie de* Zariski *de ce fermé.* Les fermés en sont les k-sous-ensembles algébriques.

Remarques

1. Le corps de base joue un rôle essentiel dans la définition de la topologie de Zariski: par exemple, les fermés de Ω dans la Ω-topologie de

Zariski sont Ω et les sous-ensembles *finis* de Ω. Mais si $d^\circ tr(\Omega/k) \geqslant 1$, il existe des fermés de Ω dans la k-topologie de Zariski qui ne sont ni Ω ni finis.

2. De l'égalité $V(F) = \bigcap_{f \in F} V(\{f\})$, on déduit que tout fermé de Ω^n est une intersection de fermés de la forme $V(\{f\})$. On notera $V(f)$ au lieu de $V(\{f\})$ dans la suite. L'ensemble algébrique $V(f)$ est appelé, *si f n'est pas une constante* (auquel cas il est Ω^n où $\emptyset$), une *hypersurface*.

Les complémentaires $D(f)$ des ensembles $V(f)$ sont quelquefois appelés *ouverts spéciaux*. Ils forment une *base des ouverts de la k-topologie de* Zariski *de* Ω^n, i.e. tout ouvert de Ω^n est une réunion d'ouverts spéciaux.

5. Ensembles algébriques irréductibles

Définition

Un k-ensemble algébrique H de Ω^n est dit irréductible s'il est non vide et s'il n'est pas réunion de sous k-ensembles algébriques H_1 et H_2 distincts de H.

On dit alors que c'est une k-variété algébrique.

Proposition I.4 (caractérisation des ensembles algébriques irréductibles)

Soit H un k-ensemble algébrique.

Les assertions suivantes sont équivalentes:

(i) H est irréductible

(ii) $I(H)$ est un idéal premier.

(iii) Si a est un idéal tel que $H = V(a)$, la racine $r(a)$ de a est un idéal premier.

Démonstration

L'équivalence de (iii)et (ii) est une conséquence immédiate du théorème des zéros.

(non(ii)) $\Longrightarrow$ (non(i))

Soient f et g tels que $f \notin I(H)$, $g \notin I(H)$ *et* $fg \in I(H)$, a (resp. b) l'idéal $I(H) + (f)$ (resp. $I(H) + (g)$).

Alors $ab \subset I(H)$ et donc $V(ab) = V(a) \cup V(b) \supset V(I(H)) = H$ et $H = V(a) \cup V(b)$.

Comme a (resp. b) et donc, a fortiori, $r(a)$ (resp. $r(b)$) contient *strictement* $I(H)$, $V(a)$ (resp. $V(b)$) est strictment contenu dans H qui est réductible.

(non(i)) $\Longrightarrow$ (non(ii))

Soient H_1 et H_2 deux sous-ensembles algébriques *stricts* de H. Alors $I(H_i)$ et $I(H_2)$ contiennent *strictement* $I(H)$. Si $H = H_1 \cup H_2$, $I(H_1)I(H_2) \subset I(H)$. Donc $I(H)$ n'est pas premier.

Définition

Une réunion $H_1 \cup \ldots \cup H_n$ *de* k*-ensembles algébriques est dite réduite si, pour tout* $i \in \{1,\ldots,n\}$ H *n'est pas contenu dans* $\bigcup_{j\neq i} H_j$.

Ceci revient à dire que $I(H_i)$ ne contient pas $\prod_{j\neq i} I(H_j)$ (qui est contenu dans $I(\bigcup_{j\neq i} H_j)$). Si H_i est irréductible, i.e. si $I(H_i)$ est premier, ceci signifie qu'il n'existe pas $j \neq i$ tel que $I(H_i)$ contienne $I(H_j)$, i.e. tel que H_i soit contenu dans H_j.

Corollaire

Soit $a = q_1 \cap \ldots \cap q_r$ *une décomposition primaire réduite de l'idéal* a *distinct de* $k[X_1,\ldots,X_n]$ *où* q_i *est* p_i*-primaire,* $q_1,\ldots,q_s$ *sont des composantes isolées et* q_i *est une composante immergée pour tout* $i > s$.

Alors, $V(a) = V(q_1) \cup \ldots \cup V(q_s)$ *est une représentation de l'ensemble algébrique* $V(a)$ *comme réunion réduite d'ensembles algébriques irréductibles.*

C'est l'unique représentation de $V(a)$ *comme réunion réduite d'ensembles algébriques irréductibles.*

Démonstration

Comme si $i > s$, $r(q_i) = p_i$ contient $r(q_j) = p_j$ pour un $j \in \{1,\ldots,s\}$, $V(q_i) = V(p_i)$ est contenu dans $V(q_1) \cup \ldots \cup V(q_s)$, d'où l'égalité $V(a) = V(q_1) \cup \ldots \cup V(q_s)$.

Si $V(a) = H_1 \cup \ldots \cup H_t$ est une représentation de $V(a)$ comme réunion réduite d'ensembles algébriques irréductibles, $r(a) = I(V(a)) = I(H_1) \cap \ldots \cap I(H_t)$ est une décomposition primaire réduite de $r(a)$ où $I(H_j)$ est premier. Donc $t=s$, et après renumérotation éventuelle, $I(H_j) = p_j$.

Exemple

Soit a l'idéal (X^2,XY) de $k[X,Y]$. Une décomposition primaire réduite de a est $(X) \cap (Y+cX,X^2)$ (pour un élément quelconque c de k); alors $V(a)$ est l'axe OY, $V(X)$ est l'axe OY, $V((Y+cX,X^2))$ est l'origine (0,0) qui appartient à cet axe.

Les résultats énoncés ci dessus sont, en fait, de nature topologique et peuvent être obtenus dans un contexte plus général.

Définitions

1. *Un espace topologique* X *est dit irréductible s'il est non vide et s'il satisfait aux conditions équivalentes suivantes:*

(*i*) *la réunion de deux fermés distincts de* X *est distincte de* X

(*ii*) *l'intersection de deux ouverts non vides de* X *est non vide.*

2. *On appelle composante irréductible d'un espace topologique un sous-espace irréductible maximal* (dans l'ensemble, ordonné par inclusion, des sous-espaces irréductibles)

3. *Un espace topologique est dit noethérien si toute suite décroissante de fermés de* X *est stationnaire.*

Remarques

1. *Un espace irréductible est connexe:* il ne peut être réunion de deux ouverts non vides disjoints.

2. *Un ouvert non vide* Y *d'un espace irréductible* X *est partout dense:* tout voisinage ouvert de $x \in X$ rencontre Y et donc x est adhérent à Y.

3. *Un sous-espace* Y *d'un espace topologique* X *est irréductible si et seulement si son adhérence* $\overline{Y}$ *est irréductible:*

Un fermé Z de Y est, en effet, de la forme $\overline{Z} \cap Y$ où $\overline{Z}$ est l'adhérence de Z dans X, qui est contenue dans $\overline{Y}$. Il est donc égal à Y si et seulement si $\overline{Z} = \overline{Y}$.

Comme l'adhérence de la réunion de deux sous-ensembles est la réunion des adhérences de ceux ci, on voit qu'une égalité $Y = Z \cup T$ où Z et T sont des fermés de Y distincts de Y équivaut à l'égalité $\overline{Y} = \overline{Z} \cup \overline{T}$ où $\overline{Z}$ et $\overline{T}$ sont des fermés de $\overline{Y}$ distincts de $\overline{Y}$.

4. *Un ensemble algébrique est noethérien* (dans la topologie de Zariski). C'est la traduction géométrique du fait que l'anneau des polynômes à n indéterminées à coefficients dans un corps est noethérien.

Proposition I.5

Soit X *un espace topologique.*

1. *Une composante irréductible de* X *est fermée*

2. *Tout sous-espace irréductible est contenu dans une composante irréductible*

3. *Si* X *est noethérien, il n'admet qu'un nombre fini de composantes irréductibles.*

4. *L'espace* X *est réunion de ses composantes irréductibles.*

5. Une composante connexe de X est réunion de composantes irréductibles.

Démonstration

1. Un sous-espace Y est irréductible si et seulement si son adhérence l'est.

2. L'ensemble des parties irréductibles de X contenant le sous-espace irréductible Y est non vide. Ordonné par inclusion, il est *inductif*: soit, en effet, $(Y_i)_{i\in I}$ une famille totalement ordonnée d'éléments de cet ensemble. L'ensemble $Z = \bigcup_{i\in I} Y_i$ est irréductible: soient U et V deux ouverts de X rencontrant Z; il existe $i \in I$ tel que U et V rencontrent Y_i; comme Y_i est irréductible, $U \cap V$ rencontre Y_i et donc, a fortiori, Z. Donc, Z est borne supérieure de la famille $(Y_i)_{i\in I}$ dans l'ensemble considéré. *Il suffit alors d'appliquer le théorème de* Zorn.

3. L'existence d'une suite infinie de composantes irréductibles $(Y_n)_{n\in N}$ de X implique l'existence de la suite infinie strictement décroissante $(Z_n)_{n\in N}$ de fermés de X où $Z_n = \bigcap_{m\leq n} Y_m$ et donc le fait que X n'est pas noethérien.

4. Il suffit de remarquer que tout point de X est un sous-espace irréductible et d'appliquer 2.

5. Tout sous-espace irréductible est connexe et donc contenu dans une composante connexe.

6. Algèbre affine d'un ensemble algébrique. Point générique d'une variété algébrique

La courbe algébrique plane *H* d'équation $X^2-Y^3 = 0$ admet la *représentation paramétrique* $X = T^3$, $Y = T^2$ obtenue en coupant par la droite d'équation $X = TY$.

On peut considérer T comme un élément du domaine universel Ω et (T^3,T^2) comme un point de *H*.

Dans l'exemple du chapitre 4.III d'anneau non intégralement clos, on a remarqué que l'idéal premier (X^2-Y^3) de $\mathbb{C}[X,Y]$ est le noyau de l'homomorphisme ϕ de $\mathbb{C}$-algèbres: $g(X,Y) \longmapsto g(T^3,T^2)$ de $\mathbb{C}[X,Y]$ dans $\mathbb{C}[T]$.

L'adhérence dans la $\mathbb{C}$-topologie de Zariski du point (T^3,T^2) est $\bigcap_g V(g)$, où g parcourt l'ensemble des polynômes de $\mathbb{C}[X,Y]$ s'annulant en (T^3,T^2), i.e. l'ensemble des éléments de $\ker(\phi) = (X^2-Y^3)$. Cette adhérence est donc *H*.

On dit que (T^3,T^2) est un *point générique* de H et que H et le *lieu* de (T^3,T^2) sur $\mathbb{C}$.

On remarque que ϕ définit un isomorphisme $\overline{\phi}$ de $\mathbb{C}$-algèbres de $\mathbb{C}[X,Y]/I(H)$ sur $C[T^3,T^2]$ qui applique la classe de X (resp. Y) sur T^3 (resp. T^2). Si donc x (resp. y) est la classe de X (resp. Y) modulo $I(H)$, (x,y) est point générique de H.

C'est à ce type de questions qu'est consacré ce paragraphe.

On commence par donner des définitions qui gardent un sens dans n'importe quel espace topologique.

Définitions

Soit X *un espace topologique.*

1. On dit que $x \in X$ *est un point générique de* X *si* X *est l'adhérence* $\{\overline{x}\}$ *de* $\{x\}$

2. Un point $y \in X$ *est appelé une spécialisation d'un point* $x \in X$ *si* y *appartient à l'adhérence de* $\{x\}$. *On dit alors que* x *est une générisation de* y.

Dire que x est un point générique de X c'est dire que X est l'ensemble des spécialisations de x.

3. Deux points x *et* y *de* X *sont dits spécialisations génériques l'un de l'autre si* x *est spécialisation de* y *et* y *est spécialisation de* x.

Ceci veut dire que $\{\overline{x}\} = \{\overline{y}\}$.

On remarque que *si l'espace topologique* X *admet un point générique il est irréductible*: si, en effet, X est réductible, $X = X_1 \cup X_2$ où X_1 et X_2 sont des fermés *distincts* de X. L'adhérence d'un point de X est contenue dans X_1 ou X_2 et est donc distincte de X.

Un espace topologique peut, d'autre part, *avoir plusieurs point génériques.*

Soit, par exemple, un élément U de Ω algébriquement indépendant de T sur $\mathbb{C}$. Le point (U^3,U^2) est aussi point générique de $V(X^2-Y^3)$.

Définition

Soit H *un* k*-ensemble algébrique de* Ω^n.

On appelle k*-algèbre affine*, ou, simplement, algèbre affine, *de* H *l'algèbre quotient* $k[X_1,\ldots,X_n]/I(H)$. *On la note* $k[H]$.

C'est une k-algèbre de type fini réduite.

Réciproquement, soit R une k-algèbre de type fini réduite: elle est isomorphe à une k-algèbre de la forme $k[X_1,\ldots,X_n]/a$ où a est un idéal égal à sa racine. Elle est donc la k-algèbre affine de l'ensemble algébrique $V(a)$.

Une conséquence immédiate de la proposition I.4 est le résultat suivant.

Soit H un k-ensemble algébrique.

Les assertions suivantes sont équivalentes:

(i) H est irréductible

(ii) $k[H]$ est intègre

Interprétation fonctionnelle

Le corps algébriquement clos Ω est infini.

On peut donc identifier un élément f de $k[X_1,\ldots,X_n]$ à la fonction polynomiale:

$$(x_1,\ldots,x_n) \longmapsto f(x_1,\ldots,x_n)$$

de Ω^n dans Ω qu'il définit.

Dire que f appartient à $I(H)$ c'est dire que la fonction, induite sur H par la fonction polynomiale définie par f, est nulle.

L'algèbre affine $k[H]$ de H s'interprète donc comme l'algèbre des fonctions sur H, à valeurs dans Ω, induites par les fonctions polynomiales de Ω^n dans Ω définies par les éléments de $k[X_1,\ldots,X_n]$.

Théorème I.6 (ensembles algébriques irréductibles et points génériques)

Soient k un corps, Ω un domaine universel pour k, H un k-ensemble algébrique de Ω^n.

Les assertions suivantes sont équivalentes:

(i) H est irréductible

(ii) H a un point générique

Démonstration

(ii) $\Longrightarrow$ (i). Déjà vu.

(i) $\Longrightarrow$ (ii). Comme H est irréductible, l'idéal $I(H)$ est premier. L'algèbre affine $k[H]$ de H est intègre.

Si x_i est la classe de X_i modulo $I(H)$, $k[H] = k[x_1,\ldots,x_n]$ et le corps $k(H)$ des fractions de $k[H]$ est $k(x_1,\ldots,x_n)$.

Quitte à renuméroter $X_1,\ldots,X_n$, on peut supposer que $\{x_1,\ldots,x_r\}$ est une base de transcendance de $k(H)/k$.

Comme $d°tr(\Omega/k) \geqslant r$, il existe des éléments $y_1,\ldots,y_r$ de Ω algébriquement indépendants sur k et un homomorphisme θ de k-algèbres de $k(x_1,\ldots,x_r)$ dans Ω tel que $\theta(x_i) = y_i$.

Comme $k(H)$ est algébrique sur $k(x_1,\ldots,x_r)$ et Ω est algébriquement clos, θ se prolonge en un homomorphisme, encore noté θ, de $k(H)$ dans Ω.

Soit $y_i = \theta(x_i)$ pour $i = 1,\ldots,n$. Le point $(y_1,\ldots,y_n)$ de Ω^n est un point générique de H sur k. On a, en effet, pour $g(X_1,\ldots,X_n) \in k[X_1,\ldots,X_n]$ les équivalences:

(i) $g(y_1,\ldots,y_n) = 0$

(ii) $g(x_1,\ldots,x_n) = 0$

(iii) $g \in I(H)$

L'adhérence de $\{(y_1,\ldots,y_n)\}$ est donc $\bigcap_{g \in I(H)} V(g) = V(I(H)) = H$.

Dimension d'un k-ensemble algébrique

On appelle dimension du k-ensemble algébrique H la dimension de Krull de son algèbre affine $k[H]$.

Un idéal premier p de $k[H]$ correspond à un idéal premier P de $k[X]$ contenant $I(H)$ et donc à un k-ensemble algébrique irréductible V contenu dans H. La dimension de H est donc égale à la borne supérieure des longueurs de chaînes décroissantes d'ensembles algébriques irréductibles contenus dans H.

On verra, au chapitre 7, que la dimension de H est finie et que si H est irréductible elle est égale au degré de transcendance de l'extension $k(H)/k$. L'existence d'un point générique de H implique donc que le degré de transcendance de Ω/k est supérieure ou égal à la dimension de H.

7. Points géométriques. Spectre premier d'une algèbre affine

Point géométrique

On définit dans Ω^n une relation d'équivalence R par $(x)R(y)$ si et seulement si l'adhérence $\overline{\{(x)\}}$ de $\{(x)\}$ est égale à l'adhérence $\overline{\{(y)\}}$ de $\{(y)\}$.

Une classe d'équivalence modulo R est appelée un point géométrique sur k à valeur dans Ω.

Un point géométrique sur k à valeur dans Ω est donc l'ensemble des spécialisations génériques sur k d'un point de Ω^n.

Exemples

1. $n = 1$. Soit $f(X)$ un polynôme *irréductible* de $k[X]$.

L'adhérence d'une racine x de $f(X)$ dans Ω est l'ensemble des racines de $f(X)$ dans Ω.

Par exemple, $\{+i,-i\}$, où $i^2 = -1$, est un point géométrique sur $\mathbb{R}$ à valeurs dans Ω.

2. La classe modulo R d'un point à coordonnées rationnelles $(a_1,\ldots,a_n)$ de k^n est l'ensemble réduit à ce point.

On peut donc identifier un point à coordonnées rationnelles au point géométrique correspondant.

3. Soient $\{x_1,\ldots,x_n\}$ et $\{y_1,\ldots,y_n\}$ deux sous-ensembles de Ω algébriquement indépendants sur k. Les points $(x_1,\ldots,x_n)$ et $(y_1,\ldots,y_n)$ sont spécialisations génériques l'un de l'autre sur k. Ils définissent le même point géométrique.

Voici quelques propriétés liées à cette notion de point géométrique.

1. Un k-ensemble algébrique H de Ω^n étant fermé est saturé pour la relation R, i.e. est réunion de points géométriques sur k à valeurs dans Ω.

On note $H_{géom}$ l'ensemble quotient H/R, i.e. l'ensemble des points géométriques définis par les points de H.

2. La topologie quotient de la topologie de Zariski de H est appelée la *k-topologie de* Zariski *de* $H_{géom}$. C'est la topologie la plus fine rendant continue la surjection canonique de H sur $H_{géom}$. Les fermés en sont les ensembles de la forme $H'_{géom}$, où H' est un sous-ensemble algébrique de H.

3. *Soient $\bar{x}$ et $\bar{y}$ des points géométriques sur k à valeurs dans Ω*

La condition:

$(x_1,\ldots,x_n)$ *est spécialisation* (resp. *générisation*) *de* $(y_1,\ldots,y_n)$ *sur* k

est indépendante du choix des représentants respectifs $(x_1,\ldots,x_n)$ et $(y_1,\ldots,y_n)$ de $\bar{x}$ et $\bar{y}$.

Elle se traduit par le fait que $\bar{x}$ appartient à l'adhérence de $\{\bar{y}\}$ dans la topologie de Zariski de $(\Omega)^n_{géom}$ (resp. que $\bar{y}$ appartient à l'adhérence de $\bar{x}$) i.e. que $\bar{x}$ est spécialisation (resp. générisation) de $\bar{y}$.

On remarquera que contrairement à ce qui se passait pour les points au sens usuel, dire *que $\bar{x}$ est spécialisation générique de $\bar{y}$ revient à dire que* $\bar{x} = \bar{y}$.

4. Soit H un k-ensemble algébrique.

Les assertions suivantes sont équivalentes:

(i) H est irréductible

(ii) $H_{\text{géom}}$ est irréductible (dans la topologie de Zariski)

(iii) $H_{\text{géom}}$ a un point générique

Si elles sont satisfaites, $H_{\text{géom}}$ a un seul point générique.

La vérification est immédiate.

5. On peut développer un point de vue fonctionnel. On se limite ici à un cas simple.

Soient $\overline{x}$ un point géométrique sur k à valuers dans Ω, $(x_1,\ldots,x_n)$ et $(y_1,\ldots,y_n)$ deux représentants de $\overline{x}$ dans Ω^n, $f(X_1,\ldots,X_n) \in k[X_1,\ldots,X_n]$.

Les points $f(x_1,\ldots,x_n)$ et $f(y_1,\ldots,y_n)$ sont spécialisations génériques l'un de l'autre sur k.

Soit, en effet, $g(T) \in k[T]$, où T est une indéterminée. On a les équivalences:

$g(f(x_1,\ldots,x_n)) = 0$

$g \circ f \in I((x_1,\ldots,x_n))$

$g \circ f \in I((y_1,\ldots,y_n))$

$g(f(y_1,\ldots,y_n)) = 0$

On définit la valeur $f(\overline{x})$ de f en $\overline{x}$ comme le point géométrique de Ω, classe de $f(x_1,\ldots,x_n)$ modulo R.

L'application: $\overline{x} \longrightarrow f(\overline{x})$ de $(\Omega^n)_{\text{géom}}$ dans $\Omega_{\text{géom}}$ est appelé *fonction polynomiale définie par le polynôme* f.

La restriction de cette fonction à k^n, considéré comme sous-ensemble de $(\Omega^n)_{\text{géom}}$, est la fonction polynomiale usuelle de k^n dans k.

Spectre premier d'une algèbre affine

Il est commode d'introduire la définition suivante:

Soit $\overline{x} \in (\Omega^n)_{\text{géom}}$. On appelle lieu de $\overline{x}$ sur k l'adhérence $\{\overline{x}\}$ de $\{\overline{x}\}$.

Le point $\overline{x}$ est donc point générique de son lieu.

Si $(x_1,\ldots,x_n) \in \Omega^n$ est un représentant de $\overline{x}$, le lieu de $\overline{x}$ est l'ensemble des point géométriques sur k, à valeurs dans Ω, de l'adhérence de $\{(x_1,\ldots,x_n)\}$ dans k-topologie de Zariski, adhérence appelée lieu de $(x_1,\ldots,x_n)$ en géométrie élémentaire.

Théorème I.7 (les trois interprétations d'un ensemble algébrique)

Soient k *un corps,* Ω *un domaine universel pour* k, H *un* k*-ensemble algébrique de* Ω^n, $A = k[H]$ *la* k*-algèbre affine de* H.

1. L'application qui fait correspondre à un point géométrique de H, *sur* k *à valeur dans* Ω, *son lieu sur* k *est une bijection de* $H_{\text{géom}}$ *sur l'ensemble des sous-ensembles algébriques irréductibles de* H.

La bijection réciproque fait correspondre à un sous-ensemble algébrique irréductible H' *de* H *le point générique de* $H'_{\text{géom}}$.

2. L'application qui à un point géométrique $\overline{x}$ *de* $H_{\text{géom}}$ *fait correspondre l'idéal premier* $p_{\overline{x}} = \{\text{classe modulo } I(H) \text{ de } f/f(\overline{x}) = 0\}$ *est un homéomorphisme de* $H_{\text{géom}}$ *sur l'espace* Spec(A) *muni de la topologie spectrale.*

Elle fait correspondre aux points fermés de $H_{\text{géom}}$ *les idéaux maximaux de* Spec(A).

La bijection réciproque fait correspondre à l'idéal premier p *de* A *le point générique de* $V(q)_{\text{géom}}$, *où* q *est l'idéal premier de* $k[X_1,\ldots,X_n]$ *tel que* $p = q/I(H)$.

Démonstration

On laisse au lecteur la vérification des assertions du théorème autres que celles explicitées ci dessous.

L'application: $\theta : \overline{x} \longmapsto p_{\overline{x}}$ est un homéomorphisme; il suffit, évidemment de démontrer qu'elle applique l'ensemble des fermés de $H_{\text{géom}}$ sur l'ensemble des fermés de Spec(A).

Ceci résulte de ce que, pour tout $f \in k[X_1,\ldots,X_n]$, l'image par θ du fermé $V(f)_{\text{géom}}$ est le fermé $V(\overline{f}) = \{p \text{ Spec(A)}/\overline{f} \in p\}$ de Spec(A), où $\overline{f}$ est la classe de f modulo $I(H)$.

Il est clair que l'adhérence de $\{p\}$, où $p \in$ Spec(A), est $V(p)$. (On pourra se reporter à II.Lemme 1). Les points fermés de Spec(A) sont donc les idéaux maximaux.

Dire que $p_{\overline{x}}$ est maximal, c'est dire que $k[x_1,\ldots,x_n]$, où $(x_1,\ldots,x_n)$ est un représentant de $\overline{x}$, est un coprs car cet anneau est isomorphe à $k[H]/p_{\overline{x}}$. Compte tenu du théorème des zéros (forme faible), ceci revient à dire que $x_1,\ldots,x_n$ sont algébriques sur k.

8. Morphismes d'ensembles algébriques

Il est bien naturel de définir un morphisme de k-ensembles algébriques de Ω^n dans Ω^m comme une application polynomiale ϕ:

$$(x_1,\ldots,x_n) \longmapsto (P_1(x_1,\ldots,x_n),\ldots,P_m(x_1,\ldots,x_n))$$

où $P_i(X_1,\ldots,X_n) \in k[X_1,\ldots,X_n]$.

On a vu, d'autre part, que si $(x_1,\ldots,x_n) \in \Omega^n$ est spécialisation de $(x'_1,\ldots,x'_n)$ sur k, $(P_1(x_1,\ldots,x_n),\ldots,P_m(x_1,\ldots,x_n))$ est spécialisation de $(P_1(x'_1,\ldots,x'_n),\ldots,P_m(x'_1,\ldots,x'_n))$. L'application ci dessus définit donc une application encore notée ϕ de $\Omega^n_{géom}$ dans $\Omega^m_{géom}$. On appellera *morphisme de* $\Omega^n_{géom}$ *dans* $\Omega^m_{géom}$ une application de cette forme.

Un tel morphisme donne un *homomorphisme de k-algèbres de* $k[\Omega^m] = k[Y_1,\ldots,Y_m]$ *dans* $k[\Omega^n] = k[X_1,\ldots,X_n]$: l'homomorphisme de substitution f défini par

$$f(Q(Y_1,\ldots,Y_m)) = Q(P_1(X_1,\ldots,X_n),\ldots,P_m(X_1,\ldots,X_n))$$

Réciproquement, un homomorphisme f de k-algèbres de $k[\Omega^m]$ dans $k[\Omega^n]$ est déterminé par les polynômes $f(Y_i) = P_i(X_1,\ldots,X_n) \in k[X_1,\ldots,X_n]$ $(i = 1,\ldots,m)$ et est l'homomorphisme de substitution correspondant.

Interprétation en termes de spectres

Soit ϕ *un morphisme de* $\Omega^n_{géom}$ *dans* $\Omega^m_{géom}$.

Le point $\xi \in \Omega^n_{géom}$ de représentant $(x_1,\ldots,x_n)$ correspond à l'idéal premier p_ξ noyau de l'homomorphisme de k-algèbres: $u(X_1,\ldots,X_n) \longmapsto u(x_1,\ldots,x_n)$ de $k[\Omega^n]$ dans Ω. Le point $\phi(\xi)$ de $\Omega^m_{géom}$ a pour représentant $(P_1(x_1,\ldots,x_n),\ldots,P_m(x_1,\ldots,x_n))$. Il correspond au noyau de l'homomorphisme de k-algèbres:

$$v(Y_1,\ldots,Y_m) \longmapsto v(P_1(x_1,\ldots,x_n),\ldots,P_m(x_1,\ldots,x_n)) \text{ de } k[\Omega^m] \text{ dans } \Omega.$$

Ce noyau est $f^{-1}(p_\xi)$ où f est l'homomorphisme de substitution de $k[\Omega^m]$ dans $k[\Omega^n]$.

Ainsi, *le morphisme* ϕ *s'identifie à l'application* Spec(f).

Définition

Soient H *et* H' *des* k*-ensembles algébriques de* Ω^n *et* Ω^m *respectivement.*

On appelle morphisme de H *dans* H' *un morphisme* ϕ *de* Ω^n *dans* Ω^m *tel que* $\phi(H) \subset H'$.

Un tel morphisme définit par passage au quotient une application encore notée ϕ de $H_{géom}$ dans $H'_{géom}$. *On appelle morphisme de* $H_{géom}$ *dans* $H'_{géom}$ *une application de cette forme.*

Compte tenu du fait que $I(H)$ et $I(H')$ sont les intersections des idéaux premiers qui les contiennent, on remarque les *équivalences pour*

un morphisme ϕ *de* k*-ensembles algébriques de* Ω^n *dans* Ω^m *correspondant à un homomorphisme* f *de* k*-algèbres de* $k[\Omega^m]$ *dans* $k[\Omega^n]$:

(i) $\phi(H) \subset H'$

(ii) $p \in \mathrm{Spec}(k[\Omega^n])$ et $p \supset I(H) \Longrightarrow f^{-1}(p) \supset I(H')$

(iii) $f^{-1}(I(H)) \supset I(H')$

(iv) $f(I(H')) \subset I(H)$

(v) f *définit par passage au quotient un homomorphisme* $\overline{f}$ *de* k*-algèbres:*

$$k[H'] = k[\Omega^m]/I(H') \longrightarrow k[H] = k[\Omega^n]/I(H)$$

On remarquera alors que $\overline{f}$ est l'homomorphisme de substitution:

$$\lambda \longrightarrow \lambda \circ \overline{f}$$

avec l'interprétation fonctionnelle de $k[H]$ et $k[H']$.

De plus, ϕ s'identifie à l'application: $p \longmapsto \overline{f}^{-1}(p)$ de $\mathrm{Spec}(k[H])$ dans $\mathrm{Spec}(k[H'])$, i.e. à $\mathrm{Spec}(\overline{f})$.

Le composé de deux morphismes est un morphisme. L'application identique d'un k-ensemble algébrique est un morphisme. On a donc défini la *catégorie des* k*-ensembles algébriques*. On a, en particulier, la notion d'isomorphisme: un isomorphisme de k-ensembles algébriques correspond à un isomorphisme des k-algèbres affines.

Produit d'ensembles algébriques

On peut démontrer l'existence du produit de deux objets dans la catégorie des (k,Ω)-ensembles algébriques.

D'un point de vue ensembliste, la situation est simple: l'ensemble sous-jacent au produit catégorique est l'ensemble produit.

Le point de vue fonctionnel est plus compliqué et c'est là une des premières difficultés de la théorie.

Voici quelques indications sur cette question.

1. *Soient* H_1 *et* H_2 *deux* k*-ensembles algébriques respectifs de* Ω^{n_1} *et* Ω^{n_2}.

L'ensemble produit $H_1 \times H_2$ est le k-ensemble algébrique $V((I(H_1), I(H_2))$ de $\Omega^{n_1+n_2}$, où $(I(H_1), I(H_2))$ désigne l'idéal de $k[X_1,\ldots,X_{n_1},Y_1,\ldots Y_{n_2}]$ engendré par les idéaux $I(H_1)$ de $k[X_1,\ldots,X_{n_1}]$ et $I(H_2)$ de $k[Y_1,\ldots,Y_{n_2}]$.

On pourrait s'attendre à ce que la somme $k[H_1] \otimes_k k[H_2]$ des k-algè-

bres affines $k[H_1]$ et $k[H_2]$ dans la catégorie des k-algèbres soit la k-algèbre affine de l'ensemble $H_1 \times H_2$.

Il en est bien ainsi si cette k-algèbre est réduite, i.e., comme elle est isomoprhe à $k[X_1,\ldots,X_{n_1}, Y_1,\ldots,Y_{n_2}]/(I(H_1),I(H_2))$, si l'idéal $(I(H_1),I(H_2))$ est égal à sa racine.

Il n'en est pas toujours ainsi comme le prouve l'exemple suivant:

Soient k *un corps non parfait,* p > 0 *sa caractéristique,* a *un élément de* k *sans racine* p-ième *dans* k.

La k-algèbre $k[X,Y]/(X^p-a,Y^p-a)$ n'est pas réduite car, si x et y désignent les classes respectives de X et Y, $x^p = a = y^p$ et donc, $(x-y)^p = 0$ alors que x-y est non nul.

Cette algèbre est la somme dans la catégorie des k-algèbres de deux copies de la k-algèbre affine du point $a^{p^{-1}}$ de Ω. Elle n'est pas l'algèbre affine du point

$(a^{p^{-1}},a^{p^{-1}})$ de Ω^2.

2. Le type de difficulté rencontré ci dessus, ainsi que d'autres de même nature, peut être levé de deux manières différentes.

Dans le point de vue d'A. Weil (34), on restreint les objets en ne considérant que des Ω-ensembles algébriques irréductibles (variétés absolument irréductibles). Il faut alors vérifier que chaque contruction conduit à une telle variété et cette vérification se traduit en une vérification sur le corps des fractions des algèbres affines.

Dans le point de vue de A. Grothendieck, on considère au contraire des objets plus généraux que les ensembles algébriques, les schémas affines dont la définition est donnée plus loin.

9. Fonctions rationnelles sur une variété. Anneau local d'un point

Soit H *une* k-*variété*, i.e. un k-ensemble algébrique irréductible.

Le corps $k(H)$ *des fractions de l'algèbre affine* $k[H]$, *corps des fonctions rationnelles sur* H, *a une interprétation fonctionnelle:*

Soit $\psi = \overline{f}/\overline{g}$, *où* $\overline{f}$, $\overline{g}$ ε $k[H]$ *un élément de* $k(H)$.

Si $\overline{x}$ *est un point géométrique* appartenant à l'ouvert $D(\overline{g})$ de H, i.e. si un représentant $(x_1,\ldots,x_n)$ de $\overline{x}$ appartient à $D(\overline{g})$, on définit la valeur de ψ en $\overline{x}$ comme le point géométrique de Ω de représentant

$f(x_1,\ldots,x_n)/g(x_1,\ldots,x_n)$

(où f et g sont des représentant de $\bar{f}$ et $\bar{g}$ dans $k[X_1,\ldots X_n]$). *On la note* $\psi(\bar{x})$.

Cette définition a un sens car si $\psi = \bar{f}_1/\bar{g}_1$ et $\bar{x}$ appartient à $D(\bar{g}_1)$, avec des notation naturelles f_1g-fg_1 appartient à $I(H)$ et

$$f_1(x_1,\ldots,x_n)g(x_1,\ldots,x_n) = f(x_1,\ldots,x_n)g(x_1,\ldots,x_n).$$

Si ψ appartient à $k[H]$, $\psi(\bar{x})$ s'interprète comme dans le paragraphe 7 comme la valeur en $\bar{x}$ de la *fonction polynomiale* ψ.

On dit que ψ *s'annule en* $\bar{x}$ *et on écrit* $\psi(\bar{x}) = 0$ si $\psi(\bar{x})$ est le point géométrique de représentant le point fermé 0 de Ω (avec lequel on peut l'identifier).

Soient maintenant $\bar{x}$ *un point géométrique de* H, ψ *un élément de* $k(H)$.

On dit que ψ est *définie en* $\bar{x}$ si ψ admet une représentation $\bar{f}/\bar{g}$ où $\bar{f}, \bar{g} \in k[H]$ et $\bar{x}$ appartient à $D(\bar{g})$ (i.e. $\bar{g}(\bar{x}) \neq 0$).

Proposition I.8 (anneau local d'un point géométrique)

Le sous-ensemble de $k(H)$ *des fonctions définies en un point géométrique* $\bar{x}$ *de* H *est un sous-anneau de* $k(H)$.

Ce sous-anneau est local d'idéal maximal les fonctions rationnelles s'annulant en $\bar{x}$.

Si $\bar{x}$ *est le point générique de* H, *ce sous-anneau est* $k(H)$.

Démonstration

Elle est facile et laissée en exercice.

Notion de modèle affine d'une extension de type fini d'un corps

Soient H *et* H' *deux* k*-ensembles algébriques irréductibles.*

On dit que H *et* H' *sont birationnellement équivalents sur* k *si les* k*-algèbres* $k(H)$ *et* $k(H')$ *sont isomorphes.*

La relation sur la classe des k-ensembles algébriques: *être birationnellement équivalents* est une relation d'équivalence.

L'étude des propriétés invariantes par cette relation est la *géométrie birationnelle.*

Soit K *une extension de type fini de* k. On peut la supposer contenue dans Ω.

Un k-ensemble algébrique H est appelé un *modèle affine* de K si $k(H)$ est isomorphe en tant que k-algèbre à K.

Deux modèles affines de K *sont birationnellement équivalents.*

D'autre part, K *admet un modèle affine*: en effet, $K = k(x_1,\ldots,x_n)$. Le lieu sur k du point de représentant $(x_1,\ldots,x_n)$ est un modèle affine de K.

Notion de courbe algébrique

Un k-ensemble algébrique irréductible H est appelé une *courbe algébrique* (resp. *une surface algébrique*) s'il est de dimension 1 (resp. 2), i.e. si $d°tr(k(H)/k) = 1$ (resp.2)

On remarquera qu'une courbe algébrique plane irréductible au sens du chapitre 2 est une courbe algébrique en ce sens. Soit, en effet, $f(X,Y) \in \mathbb{C}[X,Y]$ le polynôme irréductible définissant l'équation de la courbe. S'il est indépendant de Y, et donc de la forme X-a où $a \in C$, son algèbre affine est $\mathbb{C}[X,Y]/(X-a) = \mathbb{C}[Y]$ et donc son corps des fonctions est C(Y). S'il dépend de Y, son algèbre affine est $\mathbb{C}[X,y]$ où y est algébrique sur $\mathbb{C}[X]$; son corps de fonctions est alors $\mathbb{C}(X)[y]$ qui est algébrique sur $\mathbb{C}(X)$.

II. Spectre d'un anneau

Même pour les seuls problèmes de la géométrie algébrique classique, la considération de spectres *d'algèbres de type fini et réduites sur un corps* n'est pas toujours suffisante.

Voici quelques remarques sur ce sujet.

On a déjà vu que, si H_1 et H_2 sont des k-ensembles algébriques irréductibles, la k-algèbre de type fini $k[H_1] \otimes_k k[H_2]$, n'est pas toujours réduite et n'est donc pas l'algèbre affine de l'ensemble produit $H_1 \times H_2$. On démontre que l'algèbre affine de ce produit est l'algèbre réduite de $k[H_1] \otimes_k k[H_2]$. La difficulté provient donc de l'existence éventuelle d'éléments nilpotents non nuls dans $k[H] \otimes_k k[H_2]$.

La considération d'éléments nilpotents non nuls est aussi importante, dans des questions différentielles. En voici un exemple simple.

Soit H un k-*ensemble algébrique.* Un homomorphisme surjectif ϕ de l'algèbre affine $k[H] = k[x_1,\ldots,x_n]$ sur k définit le point fermé $(\phi(x_1),\ldots,\phi(x_n))$ de H.

On peut remplacer le corps k *par la* k-*algèbre* $k[X]/(X^2)$ *des nombres duaux.*

Soit ε la classe de X modulo (X^2) en sorte que $k[X]/(X^2) = k[\varepsilon]$.

Un homomorphisme ϕ de k-algèbres de $k[H]$ dans $k[\varepsilon]$, i.e ce qu'on

doit appeler raisonnablement "un point de H à valeurs dans $k[\varepsilon]$", s'interprète comme un *élément infinitésimal du premier ordre* comme suit:

Si $f \in k[H]$, on pose $\phi(f) = \phi_1(f) + \varepsilon D(f)$.

L'application ϕ_1 est un homomoprhisme de k-algèbres de $k[H]$ dans k qui définit un point (y) de H tel que $\phi_1(f) = f(y)$. L'application D de $k[H]$ dans k est telle que, pour tout couple (f,g) d'éléments de $k[H]$, $D(fg) = f(y)D(g) + g(y)D(f)$.

C'est ce qu'on appelle une k-*dérivation* de $k[H]$ dans k et une telle dérivation s'interprète comme un vecteur tangent en (y) à H. (chapitre 9)

La donnée de ϕ est donc celle d'un point de H et d'un vecteur tangent à H en ce point. (*)

Des considérations arithmétiques naturelles conduisent, enfin, à faire de la géométrie algébrique non seulement sur un corps mais aussi sur l'anneau $\mathbb{Z}$ *des entiers, sur anneau d'entiers algébrique ou plus généralement sur certains anneaux de Dedekind* (M. Nagata) et donc à considérer des algèbres de type fini sur de tels anneaux.

En fait, on a maintenant pris l'habitude d'associer à chaque anneau un espace topologique, son *spectre*, qui est l'ensemble des idéaux premiers muni d'une topologie naturelle. On a vu, dans I, que, dans le cas d'algèbres de type fini réduites sur un corps, ce spectre s'interprète en termes géométriques.

La donnée du seul espace topologique ne permet évidemment pas de récupérer l'anneau et, par exemple, de tenir compte des phénomènes différentiels: un anneau et son anneau réduit ont des spectres homéomorphes.

On introduit donc la notion de *schéma affine* en munissant le spectre d'un anneau d'un faisceau d'anneaux dont l'anneau de départ s'identifie à l'anneau des sections globales, i. e. des fonctions définies sur le spectre tout entier.

1. Spectre d'un anneau

Soit A *un anneau. On note* Spec(A) *l'ensemble des idéaux premiers de* A *et on l'appelle le spectre de* A.

(*) Le lecteur désirant d'autres motivations de nature analogue pourra lire avec profit l'introduction de *Lecture on curves on an algebraic surface* de D. Mumford. Annals of Mathematics Studies. Princeton 1966 et, bien sur, ultérieurement l'ouvrage tout entier.

1. *Les sous-ensembles de la forme* $V(a) = \{p \in \mathrm{Spec}(A)/a \subset p\}$ où a parcourt l'ensemble des parties de a (ou, ce qui est équivalent, des idéaux de A égaux à leurs racines), *sont les fermés d'une topologie dite topologie spectrale ou topologie de* Zariski.

L'application $p \longrightarrow p/a$ *est un homéomorphisme de* $V(a)$ *sur* $\mathrm{Spec}(A/a)$ (a idéal de A). En particulier, prenant pour a le nilradical de A, on voit que Spec(A) est homéomorphe à $\mathrm{Spec}(A_{red})$.

2. Les complémentaires $D(a)$ des ensembles $V(a)$ sont les ouverts de la topologie.

Les ouverts de la forme $D(f) = D(\{f\})$, *dits ouverts spéciaux, forment une base des ouverts de la topologie spectrale* quand f parcourt A, car $D(a) = \bigcup_{f \in a} D(f)$.

De l'égalité $D(fg) = D(f) \cap D(g)$ $(f,g \in A)$, on déduit que les ouverts spéciaux (resp. les ouverts spéciaux contenus dans un ouvert Spec(A)) forment un ensemble ordonné filtrant pour la relation d'ordre opposée à l'inclusion.

3. Lemme 1.

Soit $p \in \mathrm{Spec}(A)$.

L'adhérence de $\{p\}$ *est* $V(p)$.

Démonstration

Dire que $q \in \mathrm{Spec}(A)$ appartient à l'adhérence de $\{p\}$ c'est dire que l'on a l'implication: $[f \in A \text{ et } p \in D(f) \Longrightarrow q \in D(f)]$, soit $[f \in q \Longrightarrow f \in p]$ et donc que $q \in V(p)$.

Il en résulte que *les points fermés de* Spec(A) *sont les idéaux maximaux de* A.

4. *Soit* $\phi : A \longrightarrow B$ *un homomorphisme d'anneaux.*

L'application $\mathrm{Spec}(\phi) : \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ *définie par* $\mathrm{Spec}(\phi)(q) = \phi^{-1}(q)$ *est continue* car $\mathrm{Spec}(\phi)^{-1}(D(f)) = D(\phi(f))$.

Les applications $A \longmapsto \mathrm{Spec}(A)$, $\phi \longmapsto \mathrm{Spec}(\phi)$ *définissent un foncteur contravariant, noté Spec, de la catégorie Ann des anneaux commutatifs dans la catégorie Top des espaces topologiques.*

5. Lemme 2.

Soit $f \in A$.

L'application $\mathrm{Spec}(i_A^f)$ *est un homéomorphisme de* $\mathrm{Spec}(A_f)$ *sur* $D(f)$.

Démonstration

On sait (chap. 1. prop.III.3 cor. 1) que $\mathrm{Spec}(i_A^f)$ est une *bijection* de $\mathrm{Spec}(A_f)$ sur $D(f)$.

Pour démontrer que un *homéomorphisme*, il suffit, puisqu'elle est continue de démontrer que c'est une application *ouverte*, i.e. d'inverse continue.

Un ouvert spécial de $\mathrm{Spec}(A_f)$ est de la forme $D(g/f^r) = D(g/1)$. L'image de cet ouvert est l'ouvert $D(g) \cap D(f)$.

Exemples de spectre

1. Le spectre d'un *corps* est réduit à l'idéal (0), i.e. à un seul point *fermé*.

2. Le spectre d'un anneau *artinien local* est réduit à l'idéal maximal, i.e. à un seul point *fermé*.

Le spectre d'un anneau *artinien* est un ensemble fini *de points fermés*.

3. Le spectre d'un anneau principal est formé *d'un point non fermé*, l'idéal (0), qui en est le point générique, et *de points fermés*, les idéaux maximaux.

2. Propriétés topologiques caractéristiques d'un spectre d'anneau

Définitions

Soit X *un espace topologique.*

1. On dit que X *est* T_0 (resp. *séparé au sens de* Haussdorff) *si, pour tout couple* {x,y} *de points distincts de* X, *il existe un voisinage de l'un des points ne contenant pas l'autre* (resp. *un voisinage de* x *et un voisinage de* y *disjoints*).

2. Un point x *de* X *est dit générique si* X *est l'adhérence* $\{\overline{x}\}$ *de* {x}.

3. L'espace X *est dit quasi-compact* (resp. *compact*) *si de tout recouvrement ouvert on peut extraire un recouvrement fini* (resp. *s'il est quasi-compact et séparé au sens de* Haussdorf).

Les propriétés énoncées dans le théorème ci dessous sont caractéristiques des espaces topologiques homéomorphes au spectre d'un anneau.

Théorème II.1

Soit X *un espace topologique.*

On considère les assertions

(i) X *est homéomoprhe au spectre d'un anneau*

(ii) X *satisfait aux conditions suivantes:*

(S1) X *est* T_0

(S2) Tout fermé irréductible de X *a un point générique*

(S3) Toute intersection finie d'ouverts quasi-compacts de X *est un ouvert quasi-compact*

(S4) X *est quasi-compact et a une base d'ouverts quasi-compacts*

Alors, (i) $\Longrightarrow$ *(ii)*

Avant de donner la démonstration de ce théorème, il faut signaler que l'implication (ii) $\Longrightarrow$ (i) est vraie. La démonstration due à Höchster est donnée en appendice.

Démonstration

(i) $\Longrightarrow$ (S1).

On peut, évidemment, se limiter au cas où X = Spec(A). Soient p et q deux idéaux premiers *distincts* de A. Si tout voisinage ouvert de p contient q, q appartient à l'adhérence de p, donc est contenu dans p (lemme 1). Il existe donc $f \in p$ n'appartenant pas à q et $D(f)$ est un voisinage ouvert de q ne contenant pas f.

(i) $\Longrightarrow$ (S2)

Un fermé de Spec(A) *est de la forme* $V(a)$ *où* a *est un idéal égal à sa racine.*

Il est *irréductible* si et seulement si l'idéal a (égal à sa racine) est *premier.*

La démonstration de ce fait est analogue à celle de la proposition I.5 si l'on remarque que, *pour deux idéaux* b *et* c *de* A, *l'inclusion* (resp. *l'inclusion stricte*) $V(b) \subset V(c)$ *équivaut à l'inclusion* (resp. *l'inclusion stricte*) $r(c) \subset r(b)$, puisqu'elle signifie que tout idéal premier contenant b contient c.

La condition (S2) résulte alors de ce que si p est un idéal premier, p est point générique de $V(p)$.

(i) $\Longrightarrow$ (S3) et (S4)

Un ouvert quasi-compact est une réunion *finie* d'ouverts spéciaux. Comme une intersection *finie* d'ouverts spéciaux est un ouvert spécial (puisque $\bigcap_{i=1}^{n} D(f_i) = D(\prod_{i=1}^{n} f_i)$, *il suffit de démontrer* qu'un ouvert spécial est quasi-compact et, compte tenu du lemme 2, *que* Spec(A) *est quasi-compact.*

La démonstration de cette quasi-compacité résulte de l'existence de l'analogue des partitions de l'unité, si utiles en géométrie différentielle.

On doit démontrer qu'une égalité $\mathrm{Spec}(A) = \bigcup_{i\in I} D(f_i)$ *implique l'existence d'un sous-ensemble FINI* J *de* I *tel que* $\mathrm{Spec}(A) = \bigcup_{i\in J} D(f_i)$ $(f_i) \in A$)

Or, $\bigcup_{i\in I} D(f_i) = D((f_i)_{i\in I})$. L'égalité $\mathrm{Spec}(A) = \bigcup_{i\in I} D(f_i)$ équivaut donc à la condition : $1 \in r((f_i)_{i\in I})$ soit $1 \in (f_i)_{i\in I}$.

Elle équivaut donc à l'existence d'un sous-ensemble *fini* J de I et d'éléments a_i de A($i \in J$) tels que $1 = \sum_{i\in J} a_i f_i$. Il en résulte que $\mathrm{Spec}(A) = \bigcup_{i\in J} D(f_j)$.

Remarque

Le théorème II.1 montre que le foncteur *Spec n'est pas essentiellement surjectif.*

Il existe, en effet, des espaces topologiques ne satisfaisant pas aux conditions (S1) ou (S2) ou (S3) ou (S4).

Le foncteur *Spec n'est donc pas une équivalence de Ann° dans Top.*

On peut remarquer que le foncteur *Spec n'est pas non plus pleinement fidèle: soient* k *un corps,* k' *un sous-corps de* k, i *l'injection canonique de* k' *dans* k.

L'application Spec(i) est un homéomorphisme de Spec(k) sur Spec(k') ces deux espaces étant réduits à un point fermé. Si $k' \neq k$, i n'est pas un isomorphisme.

Proposition II.2 (critère d'irréductibilité du spectre d'un anneau)

Soit A *un anneau.*

Les assertions suivantes sont équivalentes:

(i) Spec(A) *est irréductible*

(ii) le nilradical de A *est un idéal premier*

Démonstration

Il suffit de remarquer que $\mathrm{Spec}(A) = V((0)) = V(r(0))$ et donc que l'irréductibilité de Spec(A) équivaut au fait que le nilradical $r(0)$ de A est premier.

Proposition II.3 (un critère de densité)

Soient $f : A \longrightarrow B$ *un homomorphisme d'anneaux,* $\phi = \mathrm{Spec}(f)$, $X = \mathrm{Spec}(A)$, $Y = \mathrm{Spec}(B)$.

Les assertions suivantes sont équivalentes:

(i) $\phi(Y)$ *est dense dans* X. On dit alors que le morphisme ϕ est *dominant*

(ii) ker(f) *est contenu dans le nilradical de* A

Démonstration

L'adhérence $\overline{\phi(Y)}$ de $\phi(Y)$ est $V(a)$ où $a = \bigcap_{q\in Y} f^{-1}(q) = f^{-1}(\bigcap_{q\in Y} q) = f^{-1}(n(B))$, où $n(B)$ est le nilradical de B. On remarque que $\ker(f) \subset a$ et que a contient le nilradical $n(A)$ de A.

(i) $\Longrightarrow$ (ii)

Dire que $\phi(Y)$ est dense dans X c'est dire que $V(a) = X$ et donc, puisque a contient $n(A)$, que $a = n(A)$. Il en résulte $\ker(f) \subset n(A)$.

(ii) $\Longrightarrow$ (i)

Si $\ker(f) \subset n(A)$, $a = f^{-1}(n(B)) = n(A)$ et donc $\overline{\phi(Y)} = V(a) = X$.

Corollaire

Si, de plus, A *est réduit,* $\phi(Y)$ *est dense dans* X *si et seulement si l'homomorphisme* f *est injectif.*

Exemple

Soient $A = k[X]$, $B = k[X,Y]/(XY-1)$, f *l'homomorphisme, évidemment injectif, composé de l'injection de* $k[X]$ *dans* $k[X,Y]$ *et de la surjection canonique de* $k[X,Y]$ *sur* B.

Alors Spec(A) est l'axe des X, Spec(B) est l'hyperbole d'équation $XY-1 = 0$, ϕ est la projection de l'hyperbole sur l'axe des X.

L'image de l'hyperbole par ϕ est l'axe des X privé de l'origine. Elle est bien dense.

3. Spectre d'un produit fini d'anneaux. Connexité

Soient H_1 et H_2 deux k-ensembles algébriques de Ω^n. S'il existe $f \in k[X_1,\ldots,X_n]$ prenant la valeur 0 sur H_1 et la valeur 1 sur H_2, les ensembles H_1 et H_2 sont disjoints. La réciproque est vraie: en effet, soit $p_i = I(H_i)$; la disjonction de H_1 et H_2 signifie qu'il n'existe pas d'idéal maximal de $k[X_1,\ldots,X_n]$ contenant p_1 et p_2; donc $p_1+p_2 = k[X_1,\ldots,X_n]$ et $1 = f+g$ où $f \in p_1$ et $g \in p_2$ et f prend la valeur 0 sur H_1 et la valeur 1 sur H_2.

Soient $\overline{f}$ et $\overline{g}$ les images de f et g dans l'algèbre affine $k[H]$ de $H = H_1 \cup H_2$, $k[H] = k[X_1,\ldots,X_n]/(p_1 \cap p_2)$. Alors $\overline{fg} = 0$ car $fg \in p_1p_2$ et comme $1 = \overline{f} + \overline{g}$, $\overline{f} = \overline{f}^2$, $\overline{g} = \overline{g}^2$. Ainsi, $\overline{f}$ est un idempotent de $k[H]$ et $\overline{g}$ un idempotent orthogonal à $\overline{f}$.

Les résultats de ce paragraphe constituent une généralisation de ces remarques

Proposition II.4 (Spectre d'un produit fini)

Soient $A_1,\ldots,A_n$ *des anneaux,* A *l'anneau produit* $\prod_{i=1}^{n} A_i$, p_i *la projection de* A *sur* A_i, α_i *l'application* $\mathrm{Spec}(p_i)$ *de* $\mathrm{Spec}(A_i)$ *dans* Spec(A) (i = 1,...,n). *Alors,* $(\mathrm{Spec}(A),\alpha_i)_{i=1,\ldots,n}$ *est somme des espaces* $\mathrm{Spec}(A_i)$ (i = 1,...,n) *dans la catégorie Top des espaces topologiques.*

Démonstration

Soit $p \in \mathrm{Spec}(A)$. Il existe un élément i et un seul de {1,...,n} et un idéal premier p_i et un seul de A_i tel que $p = \prod_{j=1}^{n} B_j$, où $B_j = A_j$ si $j \neq i$ et $B_i = p_i$.

Donc, $(\mathrm{Spec}(A),\mathrm{Spec}(p_i))_{i=1,\ldots,n}$ est somme de la famille $(\mathrm{Spec}(A_i))_{i=1,\ldots,n}$ dans la catégorie *Ens* des ensembles.

Si $f = (f_i)_{i=1,\ldots,n}$ où $f_i \in A_i$, $D(f) = \bigcup_{i=1}^{n} \mathrm{Spec}(p_i)(D(f_i))$. On en déduit qu'un sous-ensemble U de Spec(A) est ouvert si et seulement si $U \cap \mathrm{Spec}(p_i)(\mathrm{Spec}(A_i))$ est ouvert dans $\mathrm{Spec}(A_i)$ (i = 1,...,n), et, donc, que la topologie sur Spec(A) est la topologie la plus fine rendant continues les applications $\mathrm{Spec}(p_i)$.

On laisse au lecteur le soin d'achever la démonstration.

Proposition II.5

Soient A *un anneau,* X *son spectre. L'application* $e \longmapsto D(e)$ *est une bijection de l'ensemble* Idemp(A) *des idempotents de* A *sur l'ensemble des parties de* X *qui sont ouvertes et fermées.*

Démonstration

Si e est un idempotent, il en est de même de f = 1 - e et ef = 0.

L'ensmeble ouvert $D(e)$ *est fermé* comme complémentaire de l'ensemble ouvert $D(f)$: en effet,

$D(e) \cup D(f) = D((e,f)) = D(1) = \mathrm{Spec}(A)$

$D(e) \cap D(f) = D(ef) = D(0) = \emptyset$

L'application $\phi : e \longrightarrow D(e)$ *est surjective:* soit U un ouvert et fermé de X et soit V son complémentaire. Alors $U = V(a)$ et $V = V(b)$ où a et b sont des idéaux.

De $\emptyset = U \cap V = V(a+b)$, on déduit l'égalité $a+b = A$.

Soient α et β des éléments de a et b tels que $\alpha+\beta = 1$. Alors, $V(\alpha\beta) \supset V(ab) = V(a) \cup V(b) = X$. Donc, $\alpha\beta$ est nilpotent.

Soit n un entier naturel tel que $\alpha^n\beta^n = 0$ et soient c et d des éléments de A tels que $c\alpha^n + d\beta^n = 1$. Alors, les éléments $f = c\alpha^n$ et $e = d\beta^n$ sont des idempotents orthogonaux de somme 1. On en déduit que $V(e)$ et $V(f)$ forment une partition ouverte de X. Comme $U \subset V(f)$ et $V \subset V(e)$, il en résulte que $U = V(f)$ et $V = V(e)$ et donc que $U = D(e)$.

L'application ϕ est injective: L'égalité $D(e) = D(e')$ équivaut à l'égalité $r(e) = r(e')$ et si e et e' sont des idempotents à des égalités

$$e = ae' \qquad e' = be$$

où a, b $\in$ A. On en déduit

$$ee' = ae'^2 = ae' = e \quad \text{et} \quad ee' = be^2 = be = e'$$

soit e = e'.

Corollaire 1

Soit A *un anneau. Les assertions suivantes sont équivalentes:*

(i) A *n'a pas d'autre idempotent que* 0 *et* 1.

(ii) Spec(A) *est connexe.*

On dit alors que A est connexe. Exemples: un anneau local est connexe. Un anneau intègre est connexe.

Corollaire 2

Soient A *un anneau,* n *un entier* > 1.

L'application $(e_i)_{i=1,\ldots,n} \longmapsto (D(e_i))_{i=1,\ldots,n}$ *est une bijection de l'ensemble* E *des familles de* n *idempotents orthogonaux de somme* 1 *sur l'ensemble des partitions de* Spec(A) *en* n *ouverts.*

Démonstration

Soit $(e_i)_{i=1,\ldots,n}$ une famille de n idempotents orthogonaux de somme 1. Comme $e_ie_j = 0$ si $i \neq j$, $D(e_i) \cap D(e_j) = D(e_ie_j) = D(0) = \emptyset$. D'autre part, $\bigcup_{i=1}^{n} D(e_i) = D((e_1,\ldots,e_n)) = D(1) = \mathrm{Spec}(A)$. Donc, $(D(e_i))_{i=1,\ldots,}$ est une partition ouverte de Spec(A).

Soit, réciproquement, $(U_i)_{i=1,\ldots,n}$ une partition ouverte de Spec(A) Il résulte de la proposition II.4 que $U_i = D(e_i)$ où e_i est un idempotent déterminé de manière unique. Si $i \neq j$, $U_i \cap U_j = \emptyset = D(e_i\, e_j)$ et donc $e_i\, e_j = 0$. D'autre part, $D((e_1,\ldots,e_n)) = U_1 \cup \ldots \cup U_n = \mathrm{Spec}(A)$. Il existe, par conséquent, des éléments $a_1,\ldots,a_n$ de A tels que $1 = a_1e_1 + \ldots + a_ne_n$. Multipliant cette égalité par e_i, on voit que $e_i = a_ie_i$ et donc que $1 = e_1 + \ldots + e_n$.

Corollaire 3

Soient A *un anneau,* a *un idéal de* A *formé d'éléments nilpotents,* π *la surjection canonique de* A *sur* A/a, I *un ensemble fini.*

L'application $(e_i)_{i\in I} \longmapsto (\pi(e_i))_{i\in I}$ *est une bijection de l'ensemble des familles indexées par* I *d'idempotents orthogonaux de somme* 1 *de* A *sur l'ensemble des familles indexées par* I *d'idempotents orthogonaux de somme* 1 *de* A/a.

Démonstration

Il suffit de remarquer que Spec(π) est un homéomorphisme de Spec(A/a) sur Spec(A) et d'appliquer le corollaire 2.

4. Notion de schéma affine

Disons qu'un espace topologique est *spectral* s'il est homéomorphe au spectre d'un anneau. On sait caractériser *intrinséquement* un tel espace (49).

Le foncteur *Spec* de la catégorie *Ann* des anneaux commutatifs dans la sous-catégorie pleine de *Top* dont les objets sont les espaces spectraux est, par définition même de ceux ci, *essentiellement surjectif.*

Il n'est pas *pleinement fidèle.* Afin de remédier à cet inconvénient et d'obtenir une équivalence de la catégorie Ann°, opposée à *Ann*, et d'une catégorie d'objets géométriques, on munit le spectre d'un anneau d'un faisceau d'anneaux, obtenant un espace annelé particulier appelé un *schéma affine.*

On se contente ici de donner les éléments de cette théorie des schémas affines.

Voici quelques remarques préliminaires.

Soient A *un anneau,* X = Spec(A), f $\in$ A .

Si x $\in$ X, on note k(x) le corps des fractions de l'anneau intègre A/x (corps résiduel de x).

Identifions tous les corps résiduels k(x), où x parcourt X, à des sous-corps d'un corps Ω (Dans le cas où A est l'algèbre affine de l'ensemble algébrique H de Ω'^{n}, où Ω' est un domaine universel sur le corps de base, on pourra prendre $\Omega = \Omega'$). L'élément f définit, alors, une application : $x \longmapsto f(x)$, classe modulo x de f, de X dans Ω.

Ainsi à l'anneau A *est associé un espace topologique, son spectre, et un anneau de fonctions sur ce spectre.*

Il va d'autre part, être nécessaire comme dans d'autres géométries de recoller des ouverts d'espaces spectraux. Il faut donc attacher plus généralement à *tout ouvert de* Spec(A) un anneau de fonctions de manière à obtenir un espace annelé, i.e. un espace muni d'un faisceau d'anneaux.

Expliquons le processus dans un cas simple. La situation dans le cas le plus général sera analogue. Soit H *un* k*-ensemble algébrique irréductible.*

On a vu qu'un élément f/g du corps k(H), où f, g $\in k[H]$, définit une fonction sur l'ouvert $D(g)$, fonction qui au point $\bar{x}$ de représentant $(x_1,\ldots,x_n)$ de H fait correspondre l'élément $(f/g)(\bar{x})$, valeur de f/g au point $\bar{x}$.

La fonction correspondante est définie sur un ouvert $D(h)$, où $h \in k[H]$, si et seulement si, pour une représentation convenable de f $D(h) \subset D(g)$. Ainsi les fonctions définies sur $D(h)$ proviennent des éléments de l'anneau A_h.

On va donc attacher à l'ouvert $D(h)$ l'anneau de fractions A_h.

Un ouvert U de H est la réunion d'ouverts de la forme $D(h)$. Une fonction définie sur U est la donnée, pour tout ouvert $D(h)$ contenu dans U, d'une fonction définie sur $D(h)$ (sa restriction) avec la condition évidente que, pour deux ouverts $D(h)$ et $D(h')$ contenus dans U, les fonctions considérées sur $D(h)$ et $D(h')$ aient même restriction sur l'intersection $D(h) \cap D(h')$.

On en déduit aisément que la donnée d'une fonction sur U est celle d'un élément de la limite projective du système projectif des anneaux de fonctions définies sur les ouverts $D(h)$ contenus dans U, avec pour morphismes de transition les restrictions, l'ensemble des ouverts $D(h)$ étant munis de la relation d'inclusion.

Définition d'un préfaisceau d'anneaux sur le spectre

Soient A *un anneau,* X = Spec(A).

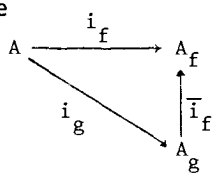
On va définir sur X *un préfaisceau* $\tilde{A}$ *d'anneaux:* on doit donc associer à tout ouvert U de X un anneau $\tilde{A}(U)$ et, à tout couple (U,V) d'ouverts tel que $U \subset V$ un homomorphisme (dit de restriction) ρ_{UV} de $\tilde{A}(V)$ dans $\tilde{A}(U)$, ces homomorphismes satisfaisant aux conditions usuelles de transitivité.

1. Cas des ouverts spéciaux

Soient $f, g \in A$. L'inclusion $D(f) \subset D(g)$ implique l'existence de $n \in \mathbb{N}^*$ et $h \in A$ tels que $f^n = gh$.

Soient i_f *et* i_g *les homomorphismes canoniques respectifs de* A *dans* A_f *et* A_g.

L'élément $i_f(g)$ est inversible dans A_f. Il existe donc un homomorphisme $\overline{i}_f$ d'anneaux et un seul de A_g dans A_f rendant commutatif le diagramme



Il est facile de vérifier que $\overline{i}_f(\phi/g^m) = (\phi h^m)/f^{nm}$ (avec des abus d'écriture évidents).

Si $D(f) = D(g)$, $\overline{i}_f$ *est un isomorphisme d'anneaux.* On identifie dans la suite A_f et A_g au moyen de cet isomorphisme.

On pose $\tilde{A}(D(f)) = A_f$ *et si* $D(f) \subset D(g)$ *on définit l'homomorphisme de restriction* $\rho_{D(f)D(g)}$ *comme étant* $\overline{i}_f$.

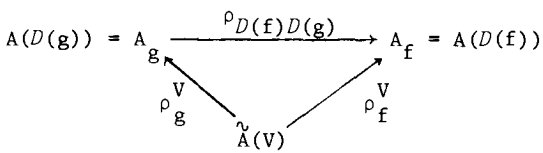
2. Cas général

Soit U *un ouvert de* X.

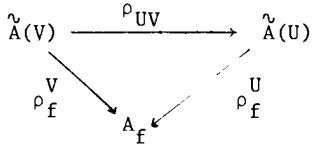
L'ensemble $(A_f, \rho_{D(f)D(g)})_{D(f),D(g) \subset U}$ est un système projectif d'anneaux.

On définit l'anneau $\tilde{A}(U)$ *comme la limite projective de ce système.* Pour tout $f \in A$ tel que $D(f) \subset U$ on a un homomorphisme ρ_f^U d'anneaux de $\tilde{A}(U)$ dans A_f.

Soit V *un ouvert contenant* U. Pour tout couple $f, g \in A$ tel que $D(f) \subset D(g) \subset U$, on a un diagramme commutatif



Il en résulte l'existence d'un homomorphisme d'anneaux et d'un seul, noté ρ_{UV}, de $\tilde{A}(V)$ dans $\tilde{A}(U)$ tel que, pour tout $D(f) \subset U$, le diagramme



soit commutatif.

On remarque que, si $U = D(f)$, $\rho_{UV} = \rho_f^V$ et que, si $U = D(f)$ et $V = D(g)$, $\rho_{UV} = \rho_{D(f)D(g)}$.

Proposition II.6

Le préfaisceau $\tilde{A}$ *est un faisceau. Autrement dit, soient* U *un ouvert de* $X = \mathrm{Spec}(A)$, $(U_i)_{i\in I}$ *un recouvrement ouvert de* U, *pour tout* $i \in I$ $\theta_i \in \tilde{A}(U_i)$ *tel que, quels que soient* $i, j \in I$, $\rho_{(U_i \cap U_j)U_i}(\theta_i) = \rho_{(U_i \cap U_j)U_j}(\theta_j)$.

Il existe alors un élément θ *et un seul de* $\tilde{A}(U)$ *tel que, pour tout* $i \in I$, $\theta_i = \rho_{U_i U}(\theta)$.

Démonstration

1. *Cas où* $U = D(f)$

Puisque U est homéomorphe à $\mathrm{Spec}(A_f)$, quitte à remplacer A par A_f, on peut supposer $U = \mathrm{Spec}(A)$.

Comme les ouverts spéciaux forment une base des ouverts de X, on peut supposer

$$U_i = D(f_i).$$

Enfin, comme X est quasi-compact, on peut supposer I *fini*.

On peut alors écrire l'élément θ_i de A_{f_i} sous la forme λ_i/f_i^n avec le *même exposant* n pour tous les $i \in I$.

La condition $\rho_{(U_i \cap U_j)U_j}(\theta_j) = \rho_{(U_i \cap U_j)U_i}(\theta_i)$ se traduit par l'égalité

$$(\lambda_i f_j^n)/(f_i f_j)^n = (\lambda_j f_i^n)/(f_i f_j)^n$$

dans l'anneau $A_{f_i f_j}$ et donc par l'existence de $r_{ij} \in N$ tel que

$$(f_i f_j)^{r_{ij}}(\lambda_i f_j^n - \lambda_j f_i^n) = 0$$

Soient $r = \sup(r_{ij})$, $s = n + r$ en sorte que

$$\lambda_i f_i^r f_j^s = \lambda_j f_j^r f_i^s$$

On pose $\lambda f_i^r = \mu_i$, d'où $\theta_i = \mu_i/f_i^s$. On a l'égalité $\mu_i f_j^s = \mu_j f_i^s$.

La condition $X = \bigcup_{i\in I} D(f_i) = \bigcup_{i\in I} D(f_i^s) = D((f_i^s)_{i\in I})$ se traduit par une égalité

$$1 = \sum_{i\in I} a_i f_i^s$$

L'élément $\theta = \sum_{i\in I} a_i \mu_i$ satisfait aux conditions de l'énoncé.

En effet, $f_j^s\theta = \sum_{i\in I} a_i\mu_i f_j^s = \sum_{i\in I} a_i\mu_j f_i^s = \mu_j(\sum_{i\in I} a_i f_i^s) = \mu_j$. Donc

$\rho_{U_j X}(\theta) = \mu_j/f_j^s = \theta_j$.

On a donc démontré *l'existence* de θ. On démontre maintenant *l'unicité*.

Soient θ et θ' deux éléments de A tels que, pour tout $i \in I$

$\rho_{U_i X}(\theta) = \rho_{U_i X}(\theta')$.

Il existe donc $s \in N$ tel que $f_i^s(\theta-\theta')$. Puisque $\sum_{i\in I} a_i f_i^s = 1$, $\theta = \theta'$.

2. Cas général

On peut toujours supposer que $U_i = D(f_i)$ $(i\in I)$(mais U n'est pas forcément quasi-compact).

Les conditions sur les restrictions aux intersections $D(f_i)\cap D(f_j)$ s'interprètent par le fait que θ_i est la projection sur $\tilde{A}(D(f_i))$ d'un élément θ de la limite projective du système projectif $(\tilde{A}(D(g)), \rho_{D(g)D(h)})_{D(g),D(h)\subset U}$. Cet élément appartient donc, par définition, à $\tilde{A}(U)$ et satisfait aux conditions.

L'unicité se prouve comme dans le cas 1.

Proposition II.7

Soit $x \in X$ *correspondant à l'idéal premier* p *de* A.

La fibre $\tilde{A}_x$ *en* x *du faisceau* $\tilde{A}$ *est l'anneau local* A_p.

Démonstration

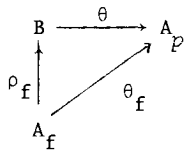
On doit démontrer que A_p est la limite inductive du système inductif *filtrant* $(A_f, \rho_{D(f)D(g)})_{D(f),D(g)\ni x}$, où l'ensemble des ouverts $D(f)$ contenant l'élément x est *ordonné par la relation opposée à la relation d'inclusion*. L'ensemble de ces ouverts, en effet, est *cofinal* dans l'ensemble des voisinages ouverts de x.

La condition $x \in D(f)$ équivaut à la condition $f \notin p$. L'élément $i_p(f)$, où i_p est l'homomorphisme canonique de A dans A_p, est donc inversible. Il existe donc un homomorphisme $\theta_f : A_f \longrightarrow A_p$ tel que

$\theta_\rho(\phi/f_n^h) = \phi/f_n^n$ (la première fraction étant dans A_f, la seconde dans A_p).

Si $D(f) \subset D(g)$, $\theta_g = \theta_f \circ \rho_{fg}$ où on a posé $\rho_{fg} = \rho_{D(f)D(g)}$.

Il existe donc un homomorphisme θ et un seul de $B = \varinjlim (A_f, \rho_{fg})$ dans A_p tel que pour tout $f \notin p$ de diagramme



soit commutatif.

Cet homomorphisme est *bijectif*.

Il est *surjectif* car $A_p = \bigcup_{f \notin p} \theta_f(A_f)$.

Il est *injectif*: soit $b \in B$ tel que $\theta(b) = 0$. Il est de la forme $\rho_f(a/f^n)$ où l'élément a/f^n de A_p est nul. Il existe donc $g \notin p$ tel que $ga = 0$. Alors $b = \rho_{fg}((g^n a)/(fg)^n) = 0$

Définitions

1. *Un espace annelé est un couple* $(X, \mathcal{A})$ *d'un espace topologique* X *et d'un faisceau* $\mathcal{A}$ *d'anneaux sur* X.

2. *L'espace annelé* $(X, \mathcal{A})$ *est dit annelé en anneaux locaux si, pour tout* $x \in X$, *la fibre* $\mathcal{A}_x = \varinjlim_{U \ni x} (\mathcal{A}(U), \ldots)$ (où U parcourt l'ensemble des voisinages ouverts de x) *est un anneau local.*

Un exemple de tel espace est fourni par $(\mathrm{Spec}(A), \tilde{A})$ où A est un anneau.

3. *Un morphisme de l'espace annelé* $(X, \mathcal{A})$ *dans l'espace annelé* $(X', \mathcal{A}')$ *est la donnée d'une application continue* $f : X \longrightarrow X'$ *et, pour tout ouvert* U' *de* X', *d'un homomorphisme d'anneaux* $\theta_{U'}$ *de* $\mathcal{A}'(U')$ *dans* $\mathcal{A}(f^{-1}(U'))$ *tel que pour tout couple* (U',V') *d'ouverts de* X' *avec* $U' \supset V'$ *le diagramme*

$$\begin{array}{ccc} \mathcal{A}'(V') & \xrightarrow{\theta_{V'}} & \mathcal{A}(f^{-1}(V')) \\ \downarrow{\scriptstyle \rho_{U'V'}} & & \downarrow{\scriptstyle \rho_{f^{-1}(U')f^{-1}(V')}} \\ \mathcal{A}'(U') & \xrightarrow{\theta_{U'}} & \mathcal{A}(f^{-1}(U')) \end{array}$$

soit commutatif.

Pour tout $x \in X$, un tel morphisme définit un homomorphisme θ_x de la fibre $\mathcal{A}'_{f(x)}$ dans la fibre $\mathcal{A}_x$.

4. *Si les espaces annelés* $(X, \mathcal{A})$ *et* $(X', \mathcal{A}')$ *sont annelés en anneaux lo-*

caux on dit que le morphisme (f,θ) *est un morphisme d'espaces annelés en anneaux locaux, si pour tout* $x \in X$, *l'homomorphisme* θ_x *est local.*

Le composé de deux morphismes d'espaces annelés en anneaux locaux est un morphisme d'espace annelé en anneaux locaux.

On définit donc une catégorie, *la catégorie des espaces annelés en anneaux locaux.*

Un schéma affine est un espace annelé en anneaux locaux isomorphe (au sens de la catégorie des espaces annelés en anneaux locaux) *à un espace annelé de la forme* $(\mathrm{Spec}(A),\tilde{A})$.

Un fait essentiel est le suivant non démontré ici.

Soient A *et* B *des anneaux.*

Un morphisme d'espaces annelés en anneaux locaux de l'espace $(\mathrm{Spec}(B),\tilde{B})$ *dans l'espace* $(\mathrm{Spec}(A),\tilde{A})$ *est de la forme* $(\mathrm{Spec}(\rho),\tilde{\rho})$ *où* ρ *est un homomorphisme d'anneaux de* A *dans* B *et* $\tilde{\rho}_{D(f)} : \tilde{A}(D(f)) = A_f \longrightarrow \tilde{B}(D(\rho(f))) = B_{\rho(f)}$ *et l'homorphisme déduit de* ρ.

Et la conséquence de ce résultat qui est que la *catégorie des schémas affines est équivalentes à la catégorie* Ann^o.

III. Spectre maximal. Anneaux de Jacobson

Définition

On appelle spectre maximal de l'anneau A *le sous-espace topologique de* Spec(A) *dont les éléments sont des idéaux maximaux de* A, *i.e. les points fermés de* Spec(A).

On le note Max(A).

Exemple

Soient k *un corps,* Ω *un domaine universel pour* k, H *un* k*-ensemble algébrique de* Ω^n, $A = k[H]$ *son algèbre affine.*

En vertu du théorème des zéros de Hilbert, Max(A) est l'ensemble des points géométriques sur k à valeurs dans Ω dont un représentant dans Ω^n a ses coordonnées algébriques sur k.

L'ensemble de ces points détermine H de manière unique et, plus précisément $I(H)$ est l'idéal des polynômes qui s'annulent en ces points.

Ceci suggère une propriété de densité de Max(A) *dans* Spec(A).

Soient $p \in \mathrm{Spec}(A)$, q *l'idéal premier de* $k[X_1,\ldots,X_n]$ *tel que* $p = q/I(H)$ *et* $f \in A$.

L'idéal p correspond à la sous-variété $V(p)$ de H de point générique

$(\overline{X}_1,\ldots,\overline{X}_n)$ où $\overline{X}_i$ est la classe de X_i modulo q.

Dire que f n'appartient pas à p c'est dire que f ne s'annule pas en ce point générique.

Le théorème des zéros de Hilbert appliqué à $V(p)$ indique alors l'existence d'un idéal maximal m de A, contenant p, correspondant à un point fermé spécialisation du point $(\overline{X}_1,\ldots,\overline{X}_n)$ tel que f ne s'annule pas en ce point, c'est à dire tel que f n'appartienne pas à p.

On voit donc que *l'idéal premier p est l'intersection des idéaux maximaux qui le contiennent.*

Cette propriété n'est pas vraie dans un anneau quelconque, par exemple dans un anneau local ayant d'autres idéaux premiers que l'idéal maximal.

C'est à elle que l'on s'intéresse dans ce paragraphe.

Définition

Soient X *un espace topologique,* Y *un sous-ensemble de* X.

On dit que Y *est localement fermé dans* X *si* $Y = U \cap V$ *où* U (resp. V) *est un ouvert* (resp. *fermé*) *de* X.

Il revient au même de dire que $Y = U \cap \overline{Y}$ où $\overline{Y}$ est l'adhérence de Y dans X: en effet, $\overline{Y} \subset V$ et donc $Y \subset U \cap \overline{Y} \subset U \cap V = Y$.

Si X = Spec(A), un sous-ensemble localement fermé est de la forme $V(a) \cap (\bigcup_{i\in I} D(f_i))$ où a est un idéal de A que l'on peut choisir égal à sa racine, i.e. de la forme $\bigcap_{j\in J} p_j$, où $p_j \in \mathrm{Spec}(A)$.

Un sous-ensemble localement fermé de Spec(A) *est donc une réunion de sous-ensembles localement fermés de la forme* $V(p) \cap D(f)$ *où p est un idéal premier de* A *et* $f \in A$.

Proposition III.1

Soit A *un anneau.*

Les assertions suivantes sont équivalentes:

(i) tout sous-ensemble localement fermé non vide de Spec(A) *rencontre* Max(A).

(ii) tout idéal premier de A *est intersection des idéaux maximaux qui le contiennent.*

(iii) Dans tout quotient de A, *le nilradical est égal au radical.*

Démonstration

(i) $\Longrightarrow$ (ii): Soit $p \in \mathrm{Spec}(A)$. Si $f \in A-p$, $V(p) \cap D(f)$ est un sous-es-

pace localement fermé non vide car il contient p. Il existe donc $m \in \mathrm{Max}(A)$ appartenant à $V(p) \cap D(f)$, i.e. contenant p et ne contenant pas f.

(ii) $\Longrightarrow$ (i): il suffit de démontrer que, si $V(p) \cap D(f)$ est non vide, il rencontre $\mathrm{Max}(A)$. Ceci résulte de l'existence de $m \in \mathrm{Max}(A)$ contenant p et ne contenant pas f; s'il n'existait pas un tel m, l'intersection des idéaux maximaux contenant p contiendrait f et serait distincte de p.

(iii) $\Longrightarrow$ (ii): il suffit d'appliquer (iii) au quotient A/p où $p \in \mathrm{Spec}(A)$.

(ii) $\Longrightarrow$ (iii): le nilradical (resp. le radical) est l'intersection des idéaux premiers (resp. maximaux)

Définition

Un anneau A *satisfaisant aux conditions équivalentes de la proposition* III.1 *est dit anneau* Jacobson.(*)

Proposition III.2 (exemples d'anneaux de Jacobson)

1. *Un quotient d'un anneau de* Jacobson *est un anneau de* Jacobson.

2. *Un anneau de fractions d'un anneau de* Jacobson *est un anneau de* Jacobson.

3. *Un corps est un anneau de* Jacobson

4. *Un anneau principal ayant une infinité de classes d'éléments irréductibles* (pour la relation d'association) *est un anneau de* Jacobson.

Par exemple, $\mathbb{Z}$ *ou l'anneau* $k[X]$ *des polynômes à une indéterminée à coefficients dans un corps* k *est un anneau de* Jacobson.

5. *Soient* A *un anneau,* f *un homomorphisme entier de* A *dans un anneau* B.

Si A *est un anneau de* Jacobson, *il en est de même de* B.

6. *Un anneau local est de* Jacobson *si son spectre est réduit à son idéal maximal.*

Démonstration

Les assertions 1., 2., 3., 6., sont évidentes.

(*) Certains auteurs disent anneau de Hilbert, d'autres anneau de Hilbert-Jacobson. On verra plus loin le lien de cette notion avec le théorème des zeros.

4. Si A est principal, son seul idéal premier non maximal est (0). Soit f non nul ε A.

Un élément irréductible ne divisant pas f engendre un idéal maximal ne contenant pas f.

5. Soient $q \varepsilon \mathrm{Spec}(B)$, $p = f^{-1}(q)$. Passant au quotient par q, on se ramène au cas où A et B sont intègres et où f est injectif et à démontrer alors que l'idéal (0) de B est intersection des idéaux maximaux de B.

Soit r le radical de B. On sait (chapitre 4. corollaire du théorème I.12) que $r \cap A$ est le radical de A. Puisque A est de Jacobson intègre, $r \cap A = 0$.

Il en résulte que $r = 0$; il suffit, en effet, de considérer pour $x \varepsilon r$ une équation de dépendance intégrale de degré minimal sur A et d'utiliser l'intégrité de B.

Remarques

1. Un sous-ensemble *ouvert* de Spec(A) étant localement fermé, on voit que, *si* A *est de* Jacobson, tout ouvert non vide de Spec(A) rencontre Max(A) et donc que Max(A) *est dense dans* Spec(A).

2. Il est possible d'obtenir une autre caractérisation intéressante des anneaux de Jacobson en ne considérant dans la caractérisation (i) de la proposition III.1 que les sous-ensembles localement fermés de Spec(A) qui sont réduits à un point.

Si $p \varepsilon \mathrm{Spec}(A)$, l'adhérence de $\{p\}$ est $V(p)$. Si $\{p\}$ est localement fermé, on doit avoir $\{p\} = V(p) \cap (\bigcup_{i \varepsilon I} D(f_i))$, i.e. $\{p\} = V(p) \cap D(f)$ pour un élément f de A.

Si A est de Jacobson, ce sous-espace doit rencontrer Max(A), i.e. p doit être maximal.

Proposition III.3

Soit A *un anneau.*

Les assertions suivantes sont équivalentes:

(i) A *est de* Jacobson (i.e. tout idéal premier est intersection des idéaux maximaux qui le contiennent).

(ii) tout idéal premier non maximal de A *est intersection des idéaux premiers qui le contiennent strictement.*

(iii) Toute A*-algèbre de type fini qui est un corps est une* A*-algèbre finie.*

Démonstration

(ii) $\Longrightarrow$ (i)

L'assertion (ii) signifie que, pour tout idéal premier p non maximal de A et tout $g \in A-p$, il existe un idéal premier q contenant p strictement et ne contenant pas g.

Soit m un idéal maximal dans l'ensemble des idéaux (non nécessairement premiers) contenant p et ne rencontrant pas $\{g^n\}_{n\in\mathbb{N}}$. C'est un idéal premier. Il est maximal car sinon il existerait un idéal premier q le contenant strictement et ne contenant pas g. Ceci prouve l'assertion (i) qui signifie que, pour tout idéal premier p et tout $g \in A-p$, il existe un idéal maximal contenant p et ne contenant pas g.

(i) $\Longrightarrow$ (ii): évident.

(ii) $\Longrightarrow$ (iii): Soit $f:A \longrightarrow B$ une A-algèbre de type fini où B est un *corps*.

Quitte à remplacer A par $A/\ker(f)$, *on peut supposer que* A *est un sous-anneau de* B.

Soit K le corps des fractions de A. Alors B contient K et est, a fortiori, une K-algèbre de type fini. Il résulte du théorème des zéros de Hilbert que B est une K-algèbre finie. Il existe donc g non nul dans A tel que B soit une A_g-algèbre finie: prendre pour g un dénominateur commun des coefficients d'équations de dépendance intégrale d'un système fini de générateurs de B. Donc, A_g est un corps et puisque A est de Jacobson, il en est de même de A: en effet, s'il n'en était pas ainsi, l'idéal (0) serait premier non maximal et il existerait un idéal premier non nul q ne contenant pas g; l'idéal qA_g de A_g serait premier non nul. Donc, $A = A_g$ et B est une A-algèbre finie.

(iii) $\Longrightarrow$ (ii): Soient p un idéal premier non maximal de A, $g \in A-p$, $\bar{g}$ la classe (non nulle) de g dans $B = A/p$. Comme B n'est pas un corps, il existe $\bar{a}$ non nul $\in B$ n'appartenant pas à $S_{\bar{g}} = \{\bar{g}^n\}_{n\in\mathbb{N}}$. Un idéal maximal dans l'ensemble des idéaux de B contenant $\bar{a}$ et ne rencontrant pas $S_{\bar{g}}$ est premier. Il est de la forme q/p où q est premier, contient strictement p et ne contient pas g.

Corollaire (théorème des zéros de Hilbert)

Une algèbre de type fini sur un anneau de Jacobson *est un anneau de* Jacobson.

Démonstration

Soient A un anneau de Jacobson, B une A-algèbre de type fini.

Une B-algèbre de type fini C est une A-algèbre de type fini. Si C est un corps, c'est une A-algèbre finie et donc, a fortiori, une B-algèbre finie. Il suffit alors d'appliquer (iii) de la proposition III.3.

IV. Eléments de géométrie algébrique projective

Une droite non parallèle aux axes rencontre l'hyperbole H d'équation $XY - 1 = 0$ en deux points tandis qu'une droite parallèle aux axes ou bien la rencontre en un point ou bien ne la rencontre pas. Plus généralement, en géométrie algébrique *affine*, il n'existe pas de formule simple donnant le nombre de points d'intersection de deux courbes algébriques planes sans composante irréductible commune.

La géométrie algébrique affine est donc inadaptée à l'étude des problèmes de dénombrement dont l'ensemble contitue ce que l'on appelle la *géométrie énumérative*.

Pour remédier aux inconvénients rencontrés ci dessus, on adjoint aux ensembles algébriques affines, des points à l'infini, obtenant des ensembles *algébriques projectifs*.

Si l'on veut suivre un chemin analogue à celui fait dans la partie I, il faut travailler avec un couple (k,Ω) d'un corps k et d'un domaine universel Ω pour k. On est ainsi conduit à la notion de spectre *homogène* d'un anneau *gradué* qui remplace celle de spectre premier du cas affine.

Pour simplifier, on va se placer dans le cas où $\Omega = k$. Le lecteur adaptera sans difficulté au cas général.

1. Espaces projectifs. Ensembles algébriques projectifs

Soient k *un corps,* n *un entier* > 1. *On suppose* k *infini.* (*)

On désigne par O l'origine $(0,\ldots,0)$ de k^{n+1}.

Définition

Un sous-ensemble C *de* k^{n+1} *est appelé un cône de sommet* O *s'il est invariant globalement par les homothéties de centre* O ou encore si, avec un point distinct de O, il contient toute la droite passant par ce point et O.

(*) Cette hypothèse est inutile si on admet des points à coordonnées dans un domaine universel pour k.

Lemme

Les assertions suivantes sont équivalentes pour un ensemble algébrique C *de* k^{n+1}.

(*i*) C *est un cône de sommet* O

(*ii*) *l'idéal* $I(C)$ *de* $k[X_0,\ldots,X_n]$ *est homogène*

Démonstration

(ii) $\Longrightarrow$ (i): évident

(i) $\Longrightarrow$ (ii): c'est clair si $C = \{0\}$ auquel cas $I(C) = (X_0,\ldots,X_n)$. *On suppose donc* $C \neq 0$.

Soit $(x_0,\ldots,x_n)$ un point de C distinct de O. Soit $f \in I(C)$, $f = \Sigma_i f_i$ où f_i est homogène de degré i. Pour tout $a \in k$, $f(ax_0,\ldots,ax_n) = 0$, d'où $\Sigma_i a^i f_i(x_0,\ldots,x_n) = 0$ et, comme k est *infini*, pour tout i, $f_i(x_0,\ldots,x_n) = 0$. Donc $f_i \in I(C)$ et $I(C)$ est homogène.

Remarque

Si C est un cône algébrique de sommet O, l'algèbre affine $k[C]$ de C est un anneau *gradué*.

Notation

Si E *est un sous-ensemble de* k^{n+1}, *on note* E^* *l'ensemble* $E - \{0\}$; *on l'appelle l'ensemble épointé défini par* E.

Définition de l'espace projectif $P_n(k)$

1. *L'espace projectif* $P_n(k)$ *est l'ensemble quotient* $(k^{n+1})^*/R$ *où* R *est la relation d'équivalence définie sur* $(k^{n+1})^*$ *par*

$(x_0,\ldots,x_n)\ R\ (y_0,\ldots,y_n)$

si et seulement si il existe $a \in k^*$ tel que, pour tout $i \in \{1,\ldots,n\}$, $y_i = ax_i$.

Un point de $P_n(k)$ est donc une droite épointée issue de O.

2. *Soit* $\xi \in P_n(k)$. *Si* $(x_0,\ldots,x_n)$ *est un représentant de* ξ *dans* $(k^{n+1})^*$, *on dit que* $x_0,\ldots,x_n$ *est un système de coordonnées homogènes (ou projectives) de* ξ.

On désigne dans la suite par p la surjection canonique de $(k^{n+1})^*$ sur $P_n(k)$.

3. *Un sous-ensemble* H *de* $P_n(k)$ *est dit algébrique (fermé) s'il est égal à* $p(C^*)$ *où* C *est un cône algébrique de* k^{n+1}, *appelé cône représentatif de* H. *On dit que* $k[C]$ *est l'anneau des coordonnées homogènes de* H.

Proposition IV.1 (topologie de Zariski)

1. *Les ensembles algébriques de* $P_n(k)$ *sont les fermés d'une topologie sur* $P_n(k)$, *appelée topologie de Zariski de* $P_n(k)$.

2. *La topologie de* Zariski *de* $P_n(k)$ *est la topologie quotient de la topologie induite sur* $(k^{n+1})^*$ *par la topologie de* Zariski *de* k^{n+1}.

3. *Un ensemble algébrique de* $P_n(k)$ *est irréductible* (au sens de la topologie de Zariski) *si et seulement si son cône représentatif est irréductible.*

Démonstration

Elle est laissée au soin du lecteur.

Idéal d'un ensemble algébrique de $P_n(k)$

Soient H *un ensemble algébrique de* $P_n(k)$, C *son cône représentatif.*

L'idéal homogène $I(C)$ *est appelé l'idéal de* H *et noté* $I(H)$.

On remarque les équivalences:

(i) $f \in I(H)$

(ii) $\forall\ \xi \in H$, il existe un système $x_o,\ldots,x_n$ de coordonnées homogènes de ξ tel que $f(x_o,\ldots,x_n) = 0$

Proposition IV.2 (théorème des zéros projectifs)

On suppose le corps k *algébriquement clos.*

L'application $H \longmapsto I(H)$ *est une bijection décroissante de l'ensemble des ensembles algébriques de* $P_n(k)$ *sur l'ensemble des idéaux homogènes de* $k[X_o,\ldots,X_n]$ *qui sont égaux à leurs racines, exception faite de* $(X_o,\ldots,X_n)$.

Elle induit une bijection de l'ensemble des ensembles algébriques irréductibles *sur l'ensemble des idéaux* premiers *homogènes de* $k[X_o,..,X_n]$ *distincts de* $(X_o,\ldots,X_n)$.

Démonstration

Elle est une conséquence immédiate du lemme et du théorème des zéros.

On remarque que l'idéal $(X_o,\ldots,X_n)$ définit le cône de k^{n+1} réduit à O et donc l'ensemble vide de $P_n(k)$. Il faut l'éliminer.

Exemples

1. Un sous-espace vectoriel V de k^{n+1} est un cône algébrique de k^{n+1}.

Un ensemble algébrique de $P_n(k)$ dont le cône représentatif est un sous-espace vectoriel de k^{n+1} est appelé une *variété linéaire projective de* $P_n(k)$.

Si E est une variété linéaire projective de $P_n(k)$ de cône représentatif C, on définit la dimension de E, notée dim(E), comme étant $[C:k]-1$

Ainsi, $P_n(k)$ *est une variété linéaire projective de dimension* n.

On appelle *hyperplan projectif de* $P_n(k)$ une variété linéaire projective de dimension n-1.

2. Un sous-ensemble algébrique H de $P_n(k)$ est dit *hypersurface algébrique* si son cône représentatif est une hypersurface de k^{n+1}, i.e. est $V(f)$ où f est un polynôme *homogène* non constant de $k[X_o,\ldots,X_n]$. On dit alors que $f = 0$ est l'équation de l'hypersurface H: un point ξ de $P_n(k)$ appartient à H si et seulement si, pour *un* système $x_o,\ldots,x_n$ de coordonnées homogènes de ξ, $f(x_o,\ldots,x_n) = 0$ et il en est alors ainsi pour *tout* système de coordonnées homogènes.

En particulier, si $n = 2$, une hypersurface algébrique du *plan projectif* $P_2(k)$ est appelé *une courbe algébrique projective plane.*

Une telle courbe est donc donnée par un polynôme homogène non constant $f(X_o,X_1,X_2) \in k[X_o,X_1,X_2]$. Elle est l'ensemble des points ξ de $P_2(k)$ admettant un système x_o,x_1,x_2 de coordonnées homogènes tel que $f(x_o,x_1,x_2) = 0$.

2. Structure de variété topologique de l'espace projectif. Complétion projective d'un ensemble algébrique affine.

Si l'on munit $P_n(\mathbb{C})$ de la topologie quotient de la topologie induite sur $(\mathbb{C}^{n+1})^*$ par la topologie naturelle de $\mathbb{C}^{n+1}$ (topologie plus fine que la $\mathbb{C}$-topologie de Zariski) on sait que $P_n(\mathbb{C})$ acquiert une structure de *variété analytique compacte.*

Un processus analogue est possible dans le cas général par utilisation de la topologie de Zariski et l'on obtient ce que l'on doit considérer comme un cas particulier d'une notion raisonnable de variété algébrique.

On ne définira pas ici cette notion en toute généralité. On se contentera de démontrer que $P_n(k)$ est muni d'une structure de variété "topologique modelée sur des ouverts de k^n".

Soit H_i *l'hyperplan de* $P_n(k)$ *d'équation* $X_i = 0$ $(i = 0,\ldots,n)$

C'est un fermé. Son complémentaire U_i est donc un *ouvert.*

Il est clair que $P_n(k) = \bigcup_{i=0}^{n} U_i$: soit, en effet $\xi \in P_n(k)$; si

$(x_0,\dots,x_n)$ est un système de coordonnées homogènes de ξ, il existe i tel que $x_i \neq 0$ et $\xi \in U_i$.

L'application ρ_i de k^n dans U_i qui associe à $(a_1,\dots,a_n)$ le point ξ de coordonnées homogènes $x_0,\dots,x_n$, avec $x_j = a_{j-1}$ si $j < i$, $x_i = 1$, $x_j = a_j$ si $j \geqslant i$, est une *bijection* de bijection réciproque associant à un point ξ de coordonnées homogènes $(a_1,\dots,\underbrace{1}_{i},\dots,a_n)$ le point $(a_1,\dots,a_n)$

C'est un homéomorphisme de k^n *muni de sa topologie de* Zariski *sur* U_i:

Il suffit, en effet, de remarquer que c'est une *application ouverte* et même que, pour tout $f \in k[X_1,\dots,X_n]$, $\rho_i(D(f))$ est un ouvert de $P_n(k)$.

On va le démontrer pour $i = 0$. Soit $\overline{f}(X_0,\dots,X_n)$ le polynôme *homogène* $X_0^r f(X_1/X_0,\dots,X_n/X_0)$, où r est le degré (total) de f.

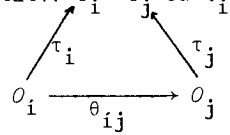
Dire que $(a_1,\dots,a_n) \in D(f)$ c'est dire que $\overline{f}(1,a_1,\dots,a_n) \neq 0$. Il en résulte que $\rho_0(D(f)) = p(D(X_0\overline{f})$ est bien un ouvert de $P_n(k)$.

En résumé, $P_n(k)$ *admet un recouvrement par des ouverts* $U_0,\dots,U_n$ *homéomorphes à des espaces* k^n.

C'est donc l'analogue d'une variété topologique. On peut dire que c'est une variété topologique modelée par des ouverts de k^n.

Soient $i,j \in \{0,\dots,n\}$ *avec* $i < j$, O_i (resp. O_j) l'ouvert $\{(a_1,\dots,a_n)/a_j \neq 0$ (resp. $a_i \neq 0)\}$ *de* k^n.

On a un diagramme commutatif $U_i \cap U_j$ où τ_i (resp. τ_j) est la restric-



tion de ρ_i (resp. ρ_j) et $\theta_{ij}(a_1,\dots,a_n) = (\underbrace{a_1/a_j,\dots,1/a_j,\dots,a_i/a_j}_{i+1},\dots,a_n/a_j)$

L'application θ_{ij} a pour inverse θ_{ji}. C'est un *isomorphisme de* O_i *sur* O_j *en un sens naturel.*

De la même manière, soit H un ensemble algébrique de $P_n(k)$, on vérifie que, pour tout $i \in \{0,\dots,n\}$, $H \cap U_i$ est un ensemble algébrique de U_i.

Complétion projective d'un ensemble algébrique affine

L'application i qui associe au point $(x_1,\dots,x_n)$ de k^n le point de

$P_n(k)$ de coordonnées homogènes $1,x_1,\ldots,x_n$ est *injective. On identifie dans la suite* k^n *à un sous-ensemble de* $P_n(k)$ *au moyen de* i. Le complémentaire de k^n est l'hyperplan H_o d'équation $X_o = 0$, *dit à l'infini.*

Proposition IV.3

Soit H *un ensemble algébrique de* k^n.

L'adhérence $\overline{H}$ *de* H *dans* $P_n(k)$ (muni de sa topologie de Zariski) *est l'ensemble algébrique de* $P_n(k)$ *de cône représentatif* $V(\overline{I})$ *où* $\overline{I}$ *est l'idéal engendré par les polynômes homogènes de la forme*

$$X_o^{d^\circ f} f(X_1/X_o,\ldots,X_n/X_o)$$

où f *parcourt* $I(H)$.

Démonstration

L'adhérence $\overline{H}$ de H est l'intersection des hypersurfaces algébriques de $P_n(k)$ contenant H. Les assertions suivantes sont équivalentes pour un polynôme *homogène* $\overline{f}(X_o,\ldots,X_n) \in k[X_o,\ldots,X_n]$:

(i) l'hypersurface d'équation $\overline{f} = 0$ contient H

(ii) $(x_1,\ldots,x_n) \in H \Rightarrow \overline{f}(1,x_1,\ldots,x_n) = 0$

(iii) $\overline{f}(1,X_1,\ldots,X_n) \in I(H)$

(iv) il existe $f(X_1,\ldots,X_n) \in I(H)$ tel que $\overline{f}(1,X_1,\ldots,X_n) = f(X_1,\ldots,X_n)$

(v) il existe $f(X_1,\ldots,X_n) \in I(H)$ tel que

$$\overline{f}(X_o,\ldots,X_n) = X_o^{d^\circ f} f(X_1/X_o,\ldots,X_n/X_o)$$

On en déduit que $\overline{H}$ est l'ensemble algébrique de cône représentatif $V((\overline{f}/\overline{f} = X_o^{d^\circ f} f(X_i/X_o)$ avec $f \in I(H))$.

Définition

L'adhérence $\overline{H}$ *de* H *dans* $P_n(k)$ *est appelée la complétion projective de* H

On remarque que $\overline{H} \cap k^n = H$ et que le complémentaire de H dans $\overline{H}$ est $\overline{H} \cap H_o$.

On remarque aussi que l'idéal $\overline{I}$ est égal à sa racine et que si H est irréductible $\overline{I}$ est premier et donc $\overline{H}$ est irréductible. Cette dernière assertion résulte également du fait évident que i identifie k^n muni de sa topologie à un sous-espace de $P_n(k)$.

Exemple

La complétion projective de la courbe algébrique plane d'équation

$X_1X_2 - 1 = 0$ est la courbe algébrique projective plane d'équation $X_o^2((X_1/X_o)(X_2/X_o)-1) = 0$ soit $X_1X_2-X_o^2 = 0$.

Elle est obtenue par adjonction à l'hyperbole d'équation $X_1X_2-1 = 0$ les deux points à l'infini de coordonnées homogènes respectives: 0,1,0 et 0,0,1.

Exercices du chapitre 6

La lettre k *désigne un corps, la lettre* Ω *un domaine universel pour* k.

(1). Soient X_1,X_2,T des indéterminées, ϕ l'homomorphisme de k-algèbres de $k[X_1,X_2]$ dans $k[T]$ tel que $\phi(X_1) = T(1+T^2)$ et $\phi(X_2) = 1+T^2$.

1. Démontrer que ker (ϕ) est égal à $(X_1^2+X_2^2-X_2^3)$. En déduire l'irréductibilité du polynôme $X_1^2+X_2^2-X_2^3$ dans $k[X_1,X_2]$.

2. On note C_k l'ensemble $\{(x_1,x_2) \in k^2 / x_1^2+x_2^2-x_2^3 = 0\}$ i.e. l'ensemble des points rationnels sur k de la courbe d'équation $X_1^2+X_2^2+X_2^3 = 0$.

Démontrer l'irréductibilité de C_k pour la k-topologie de Zariski.

Démontrer que $C_{\mathbb{C}}$ est irréductible pour la topologie usuelle de $\mathbb{C}^2$.

Démontrer que $C_{\mathbb{R}}$ a un point isolé et donc n'est pas connexe. Est-elle irréductible pour la topologie usuelle de $\mathbb{R}^2$?

3. L'algèbre affine de $C = C_\Omega$ est $k[T(1+T^2),1+T^2]$. Quelle est sa clôture intégrale ?

(2). On suppose k de caractéristique 0.

Démontrer qu'une courbe algébrique irréductible définie sur k est birationnellement équivalente à une courbe algébrique *plane*.

(Utiliser le théorème de l'élément primitif).

(3). Soient H un k-ensemble algébrique, $g \in k[H] = k[x_1,\ldots,x_n]$. Démontrer que l'ouvert spécial $D(g)$ de H est un k-ensemble algébrique d'algèbre affine $k[H]_g = k[x_1,\ldots,x_n,1/g]$.

(4). Soient V et W deux k-ensembles algébriques. On suppose que V est irréductible et qu'il existe un morphisme ϕ dominant, i.e. d'image dense de V dans W.

Est ce que W est irréductible ?

Expliciter un morphisme surjectif et donc dominant de Ω sur la courbe algébrique $V(Y^2-XZ,YZ-X^3,Z^2-X^2Y)$ (exemple 2 du chapitre 3.II.§5)

En déduire l'irréductibilité de cette courbe.

(5). Démontrer l'irréductibilité dans $k[X,Y]$ du polynôme $XY-(X+Y)(X^2+Y^2)$.

Ce polynôme reste-t-il irréductible dans l'anneau $k[[X,Y]]$ des séries formelles ?

(6). Expliciter un point générique de $V(X^2-Y^3, Y^2-Z^3)$. En déduire l'irréductibilité de cet ensemble algébrique.

(7). Soient H_1 et H_2 des k-ensembles algébriques respectifs de Ω^{n_1} et Ω^{n_2}.

Démontrer que la k-algèbre affine de l'ensemble algébrique produit $H_1 \times H_2$ est $(k[H_1] \otimes_k k[H_2])_{red}$.

(Utiliser le fait que $k[H_1] \otimes_k k[H_2]$ est isomorphe à $k[X_1,\ldots,X_{n_1},Y_1,\ldots,Y_{n_2}]/J$ où J est l'idéal engendré par $I(H_1)$ et $I(H_2)$.)

(8). Soient X un espace topologique, $C(X)$ l'anneau des fonctions définies et continues sur X à valeurs dans $\mathbb{R}$.

Si $x \in X$, soit m_x l'idéal maximal de $C(X)$ noyau de l'homomorphisme surjectif: $f \longmapsto f(x)$ de $C(X)$ sur $\mathbb{R}$.

On suppose X *compact. On se propose de démontrer que l'application* $x \longmapsto m_x$ *est un homéomorphisme de* X *sur* $\mathrm{Max}(C(X))$, muni de la topologie induite par la topologie spectrale de $\mathrm{Spec}(C(X))$.

1. Soit m un idéal maximal de $C(X)$.

Démontrer que $V(m) = \{x \in X / f(x) = 0 \ \forall f \in m\}$ est non vide. En déduire que si $x \in V(m)$, $m = m_x$.

(Raisonner par l'absurde, supposant $V(m)$ vide. Utilisant la compacité de X, démontrer l'existence d'une famille finie $\{U_1,\ldots,U_n\}$ d'ouverts de X et d'une famille finie $\{f_1,\ldots,f_n\}$ d'éléments de m telles que f_i ne s'annule pas sur U_i $(i = 1,\ldots,n)$. Considérant $f = f_1^2 + \ldots + f_n^2$, démontrer que m contient un élément inversible de $C(X)$).

2. On rappelle que, pour tout couple (x,y) de points *distincts* de X, il existe $f \in C(X)$ tel que $f(x) = 0$ et $f(y) = 1$.

En déduire que l'application: $x \longmapsto m_x$ est *injective* et donc bijective.

3. Démontrer que cette application est un homéomorphisme.

(9). Le calcul qui suit est tiré de l'article de A. Micali. *Sur les algèbres universelles. Ann. Inst. Fourier. 14,2, 1964.*

Soient n un entier $\geqslant 2$, $X_1,\ldots,X_n,Y_1,\ldots,Y_n,T,U$ des indéterminées, R l'anneau $k[X_1,\ldots,X_n,Y_1,\ldots,Y_n]$, a l'idéal *homogène* $(X_iY_j-X_jY_i)_{i,j=1,\ldots,n}$

A l'anneau quotient $k[X_1,\ldots,X_n,Y_1,\ldots,Y_n]/a$, θ l'homomorphisme de k-algèbres de R dans $k[X_1,\ldots,X_n,T,U]$ tel que $\theta(X_i) = TX_i$ et $\theta(Y_i) = UX_i$ $(i = 1,\ldots,n)$.

Démontrer que a est égal à $\ker(\theta)$.

(Remarquer qu'il suffit de démontrer que si $f = \sum_{r,s} f_{r,s}$ où $f_{r,s}$ est *homogène* de degré r en $X_1,\ldots,X_n$ et s en $Y_1,\ldots,Y_n$ appartient à $\ker(\theta)$, alors $f_{r,s}$ appartient à a.

Démontrer cette assertion par récurrence sur le degré total r+s.

A cet effet, remarquer que si $r \geqslant 1$, et $s \geqslant 1$, et si $f_{r,s} \in \ker(\theta)$, $f_{r,s}$ est combinaison linéaire à coefficients dans k de polynôme de la forme

$$(1)\quad X_1^{p_1}\ldots X_n^{p_n} Y_1^{q_1}\ldots Y_n^{q_n} - X_1^{i_1}\ldots X_n^{i_n} Y_1^{j_1}\ldots Y_n^{j_n} = g(X_1,\ldots,X_n,Y_1,\ldots,Y_n)$$

où $i_k \neq p_k$, $j_k \neq q_k$ $(k = 1,\ldots,n)$, $p_1+\ldots+p_n = i_1+\ldots+i_n = r$, $q_1+\ldots+q_n = j_1+\ldots+j_n = s$.

Démontrer ensuite que si $g(X_1,\ldots,X_n,X_1,\ldots,X_n) = 0$, g appartient à a.

Examiner le cas où g est multiple d'une des indéterminées. Dans le cas contraire soit M(resp. M') $= \{i' \in \{1,\ldots,n\}/p_{i'} > 0$ (resp. $q_{i'}>0)\}$ Démontrer que l'on peut supposer $M = \{1,\ldots,m\}$ et $M' = \{m+1,\ldots,m'\}$ et que l'on peut écrire g sous la forme $(X_1Y_{m'} - X_{m'}Y_1)g_1 + Y_1X_{m'}\, g_2$ et utiliser l'hypothèse de récurrence pour prouver que g_2 appartient à a.)

Démontrer un résultat analogue en remplaçant les algèbres de polynômes par des algèbres de séries formelles.

(10). Soient V et W deux k-ensembles algébriques irréductibles, $A = k[V]$, $B = k[W]$ leurs algèbres affines, $f:A \longrightarrow B$ un homomorphisme de k-algèbres (correspondant à un morphisme de k-ensembles algébriques de W dans V), W' un sous-ensemble algébrique de W, q l'idéal de W' dans B en sorte que $k[W'] = B/q$.

On suppose que l'homorphisme composé: $A \xrightarrow{f} B \longrightarrow B/q$ est plat.

1. Démontrer que, si a est un élément non nul de A, $q = B \cap qB_{f(a)}$.
(Remarquer que f(a) est régulier dans B/q).

2. Soient W'_1 et W'_2 deux sous-ensembles algébriques de W satisfaisant à la condition ci dessus. On suppose de plus qu'il existe a non nul tel que $W'_1 \cap D(f(a)) = W'_2 \cap D(f(a))$.

Démontrer l'égalité $W'_1 = W'_2$

(Un morphisme $\phi : W \longrightarrow V$ de k-ensembles algébriques est dit plat si l'homomorphisme f de k-algèbres de $k[V]$ dans $k[W]$ est plat. Cette notion de morphismes plats est très utilisée en géométrie algébrique où elle fournit des conditions de continuité. Le lecteur pourra remarquer qu'un homomorphisme $f : A \longrightarrow B$ est plat, si, pour tout $q \in \mathrm{Spec}(B)$, le morphisme f_q de $A_{f^{-1}(q)}$ dans B_q, déduit de f, est plat.)

(11). Soient V et W des k-ensembles algébriques irréductibles, ϕ un morphisme de W dans V.

1. On suppose ϕ *dominant*, i.e. d'image dense.

Démontrer que l'homomorphisme $f : \lambda \longrightarrow \lambda \circ \phi$ de $k[V]$ dans $k[W]$ est injectif. Il se prolonge donc en un homomorphisme de k-algèbres, encore noté f, de $k(V)$ dans $k(W)$.

2. Démontrer les équivalences:

(i) il existe un homomorphisme f de k-algèbres de $k(V)$ dans $k(W)$

(ii) il existe $g \in k[W]$ et un morphisme dominant ϕ de l'ouvert spécial (affine) $W_g = D(g)$ de W dans V tel que f se déduise de ϕ comme dans 1.

Un tel morphisme ϕ est appelé un morphisme *rationnel* de W dans V. (Attention! Un tel morphisme n'est pas forcément défini sur tout W.)

3. Un morphisme ϕ de W dans V est dit *birationnel* s'il est rationnel et si l'homomorphisme f de $k(V)$ dans $k(W_g) = k(W)$ qu'il définit est un isomorphisme de k-algèbres. Un *isomorphisme* de V sur W est un tel morphisme.

Démontrer les équivalences pour le morphisme rationnel ϕ:

(i) ϕ est birationnel

(ii) il existe un ouvert spécial W_g de W et un ouvert spécial V_h de V tel que ϕ induise un isomorphisme de W_g sur V_h.

Démontrer l'existence d'un inverse (en un sens que l'on précisera) d'un morphisme birationnel.

Les ensembles algébriques irréductibles V et W sont dits *birationnellement* équivalents s'il existe un morphisme birationnel ϕ de V dans W, i.e. s'il existe un isomorphisme de k-algèbres de $k(V)$ sur $k(W)$.

4. Soit V un ensemble algébrique irréductible de dimension r. (Ceci peut s'interpréter en disant que $d^\circ tr(k(V)/k) = r$.)

On dit que V est *unirationnel* s'il existe un morphisme rationnel ϕ

de l'espace affine Ω^r de dimension r dans V ou, ce qui est équivalent, si $k(V)$s'identifie à une sous-algèbre de l'algèbre $k(T_1,\ldots,T_r)$ des fractions rationnelles à r indéterminées $T_1,\ldots,T_r$ à coefficients dans k.

On dit que V est *rationnel* si V est birationnellement équivalent à Ω i.e. si $k(V)$ s'identifie à $k(T_1,\ldots,T_r)$.

On s'intéresse ci dessous au cas $r = 1$, i.e. au cas où V est une courbe.

On désignera par $(x_1,\ldots,x_n)$ un point générique de V sur k en sorte que $k(V) = k(x_1,\ldots,x_n)$.

Démontrer que V est unirationnelle (on dit aussi unicursale) si et seulement si il existe des polynômes $f_1(T),\ldots,f_n(T),g(T) \in k[T]$ tels que les fractions $f_i(T)/g(T)$ ne soient pas toutes des constantes et que tout point de V, sauf éventuellement un nombre fini, soit de la forme $(f_1(t)/g(t),\ldots,f_n(t)/g(t))$.

Démontrer que V est rationnel si, de plus, tout point de V, sauf éventuellement un nombre fini, est obtenu pour une valeur et une seule du paramètre t.

Interpréter le théorème de Lurôth (passage d'une représentation paramétrique éventuellement impropre (exemple: $x_1 = T^4$, $x_2 = T^6$ qui donne $k(V) = k(T^2)$) à une représentation paramètrique propre (exemple ci dessus: $x_1 = U^2$, $x_2 = U^3$)).

(12). Soient A un anneau, $X = \mathrm{Spec}(A)$, x et y deux points distincts de X.

1. Démontrer que l'une des deux conditions suivantes est satisfaite:

- il existe un voisinage ouvert U (resp. V) de x (resp. y) tels que $U \cap V = \emptyset$.
- x et y ont une générisation commune

2. Démontrer que le spectre minimal (ensemble des idéaux premiers minimaux) de A muni de la topologie induite de celle de Spec(A) est séparé (au sens de Haussdorff. On dit encore T_2).

3. Démontrer que Max(A) vérifie la condition suivante

- (T_1) soient x et y des points distincts de Max(A). Il existe un voisinage ouvert U (resp. V) de x (resp. y) ne contenant pas y (resp. x)

(13). Donner des exemples d'espaces topologiques irréductibles non vides

- admettant plusieurs points génériques
- n'admettant pas de point générique. (On pourra utiliser un k-en-

semble algébrique H et se limiter au seuls points de H à coordonnées dans k).

(14). Un espace topologique est dit *sobre* si tout fermé irréductible non vide de cet espace admet un point générique et un seul..

Démontrer que le foncteur inclusion dans *Top* de la sous-catégorie pleine dont les objets sont les espaces topologiques sobres admet un adjoint à gauche.

(Associer à un espace topologique X l'espace topologique ^{s}X dont les éléments sont les parties fermées irréductibles de X et les ouverts les ensembles de la forme $\overset{\circ}{V}$ = { parties fermées irréductibles de X rencontrant V}, où V parcourt l'ensemble des ouverts de X).

(Ref. A. Grothendieck. J.A. Dieudonné. *Eléments de géométrie algébrique. Springer Verlag, 1971. 2.9. p. 67-70)*

(15). Soit $f:A \longrightarrow B$ une A-algèbre de type fini. On suppose que A est un anneau de Jacobson.

Que peut-on dire de l'image réciproque par f d'un idéal maximal de B ?

(16). Soient X un espace topologique, Y un sous-espace de X.

Démontrer que les assertions suivantes sont équivalentes

(i) tout sous-ensemble localement fermé non vide de X rencontre Y

(ii) pour tout fermé F de X, $(\overline{F \cap Y}) = F$

(iii) l'application: $U \longmapsto U \cap Y$ de l'ensemble des ouverts de X sur l'ensemble des ouverts de Y est une bijection.

Si elles sont satisfaites, on dit que Y est *très dense* dans X.

Démontrer que les assertions suivantes sont équivalentes pour un anneau A:

(i) A est de Jacobson

(ii) Max(A) est très dense dans Spec(A).

(17). Soient f un polynôme homogène $\varepsilon\ k[X_o,\ldots,X_n]$, $f = f_1.\ldots.f_r$ une décomposition de f en facteurs irréductibles.

Démontrer que $f_1,\ldots,f_r$ sont homogènes.

(Utiliser l'ordre et le degré)

(18).Soit f un polynôme homogène non constant $\varepsilon\ k[X_o,\ldots,X_n]$.

Démontrer les équivalences:

(i) le polynôme f est irréductible

(ii) la courbe algébrique plane projective d'équation $f = 0$ est irréductible

(19). Soient $C_1,\dots,C_n$ des courbes algébriques planes, $\overline{C}_1,\dots,\overline{C}_n$ leurs complétions projectives respectives.

Quelle est la complétion projective de la courbe $C_1 \cup \dots \cup C_n$?

(20). Soient k un corps, X une indéterminée, $f(X) = a_0X^n+\dots+a_n$, $g(X) = b_0X^m+\dots+b_m \in k[X]$.

1. Démontrer que les assertions suivantes sont équivalentes:

(i) $f(X)$ et $g(X)$ ont un diviseur non constant dans $k[X]$ ou $a_0=b_0=0$.

(ii) il existe $\phi(X)$ de degré $\leqslant m-1$ et $\psi(X)$ de degré $\leqslant n-1$ et non nuls de $k[X]$ tels que $\phi(X)f(X) = \psi(X)g(X)$

(iii) le déterminant de la matrice à $n+m$ lignes et colonnes

$$\begin{vmatrix} a_0 & a_1 & \dots & a_n & & \\ & a_0 & a_1 & \dots & a_n & \\ & & \ddots & & & \ddots \\ b_0 & b_1 & \dots & b_m & & \\ & b_0 & b_1 & \dots & b_m & \\ & & \ddots & & & \ddots \end{vmatrix}$$

(dont les m premières lignes s'obtennent par décalage à partir de la ligne $a_0 \quad a_1 \dots a_n$, les n dernières à partir de la ligne $b_0 \quad b_1 \dots b_m$, les éléments non écrits étant nuls) est nul.

Ce déterminant est appelé le *résultant de* f *et* g *et noté* $R(f,g)$

2. Considérant $a_0,\dots,a_n,b_0,\dots,b_m$ comme des inconnues, résoudre le système d'équations linéaires $X^if(X) = a_0X^{n+i}+\dots+a_nX^i$, $X^jg(X) = b_0X^{m+j}+\dots+b_mX^j$ $(i = 1,\dots,m-1;\ j = 1,\dots,n-1)$ et en déduire une identité.

$$R(f,g) = Af + Bg$$

où A et B sont des polynômes en X, a_i, b_j à coefficients dans k.

3. Démontrer que $R(f,g)$ est homogène de degré n (resp. m) en $a_0,\dots,a_n$ (resp. $b_0,\dots,b_m$). A un monôme $ca_{i_1}\dots a_{i_r}b_{j_1}\dots b_{j_s}$ où $c \in k$ on attache son *poids* $i_1+\dots+i_r+j_1+\dots+j_s$.

Démontrer que tous les monômes de $R(f,g)$ ont même poids nm.

4. Soient $f(X_0,X_1,X_2) = \sum_{i=0}^{n} a_i(X_0,X_1)X_2^i$ où $a_i(X_0,X_1) \in k[X_0,X_1]$ un polynôme homogène de degré n, $g(X_0,X_1,X_2) = \sum_{j=0}^{m} b_j(X_0,X_1)X_2^j$ où $b_j(X_0,X_1) \in k[X_0,X_1]$ un polynôme homogène de degré m. Donc, a_i (resp. b_j) est homogène de degré $n-i$ (resp. $m-j$).

Démontrer que le résultant $R(f,g)$ de f et g considérés comme polynômes en X_2 à coefficients dans $k(X_o,X_1)$ est un polynôme homogène de degré $mn \in k[X_o,X_1]$, ou que les courbes projectives planes d'équations $f = 0$ et $g = 0$ ont une infinité de points communs. (On suppose que le corps k est le corps $\mathbb{C}$ des complexes).

CHAPITRE 7

Homomorphismes d'anneaux et morphismes d'ensembles algébriqu

On étudie dans ce chapitre quelques propriétés des homomorphismes d'anneaux, notamment des homomorphismes *entiers* qui s'introduisent naturellement en géométrie algébrique, et des morphismes correspondants pour les spectres associés.

Cette étude est menée tantôt dans le cas plus général tantôt dans le cas particulier des algèbres de type fini sur un corps, cas qui correspond géométriquement à celui des ensembles algébriques.

Soient f : A $\longrightarrow$ B *un homomorphisme d'anneaux,* ϕ = Spec(f) : Spec(B) $\longrightarrow$ Spec(A). La fibre de ϕ en $p \in$ Spec(A), i.e. $\phi^{-1}(p)$, est appelée la *fibre de* f *en* p.

Un problème naturel est celui de l'étude de cette fibre et, en particulier, *de l'obtention de critères permettant d'affirmer que cette fibre est non vide.*

Une réponse a déjà été donnée *dans le cas où* f *est entier* injectif par le premier théorème de Cohen-Seidenberg : en tout $p \in$ Spec(A), la fibre de f est alors non vide.

Dans le même ordre d'idées, le *lemme de normalisation* d'E. Noether affirme que, pour tout (k,Ω)-ensemble algébrique H, il existe un entier naturel r égal, en fait à la *dimension de* H, et un morphisme *surjectif* d'ensembles algébriques de H sur Ω.

Un autre problème traité ici est celui de l'étude de l'image d'un fermé de Spec(B) *par* ϕ.

Des exemples géométriques simples montrent que ce n'est pas en général un fermé.

Toutefois, si A et B sont des k-algèbres de type fini et si f est un homomorphisme de k-algèbres, cas où Spec(A) et Spec(B) sont des ensembles algébriques et ϕ un morphisme d'ensembles algébriques, un théorème de C. Chevalley affirme que l'image par ϕ d'un fermé est un ensemble *constructible*, i.e. réunion finie d'ensembles qui sont l'intersection d'un ouvert et d'un fermé.

Voici le plan de ce chapitre.

Dans I, on donne un critère pour que la fibre d'un homomorphisme en un idéal premier soit non vide et on démontre les théorèmes de Cohen-Seidenberg pour un homomorphisme entier.

Dans II, on donne une démonstration algébrique du lemme de normalisation d' E. Noether et son interprétation géométrique.

Enfin, dans III, on étudie l'image d'un fermé par un morphisme, donnant d'abord un critère de densité puis le théorème de C. Chevalley sur les ensembles constructible.

I. Fibres d'un homomorphisme d'anneaux . Cas d'un homomorphisme entier

1. Fibres d'un homomorphisme

Définition

Soient $f : A \longrightarrow B$ *un homomorphisme d'anneaux,* p *un idéal premier de* A.

Un idéal premier q *de* B *est dit au dessus de* p *si* $f^{-1}(q) = p$.

En particulier, si A est un sous-anneau de B et f l'injection canonique, dire que q est au dessus de p c'est dire que $q \cap A = p$.

Soient $X = \mathrm{Spec}(A)$, $Y = \mathrm{Spec}(B)$, $\phi = \mathrm{Spec}(f) : Y \longrightarrow X$.

L'ensemble des idéaux premiers de B *au dessus de* $p \in X$ *est la fibre* $\phi^{-1}(p)$.

On l'appelle la fibre de f *en* p.

Exemples

1. Soient S *une partie multiplicative de* A, $B = S^{-1}A$, $f = i_A^S$, p *un idéal premier de* A.

Si $p \cap S = \emptyset$ (resp. $\neq \emptyset$) la fibre de f en p est réduite à l'élément $s^{-1}p$ *(resp. est vide).*

2. Soient a *un idéal de* A, $B = A/a$, f *la surjection canonique,* p *un idéal premier de* A *contenant* a. La fibre de f en p est $\{p/a\}$.

3. Soient k *un corps,* V *et* W *des* k*-ensembles algébriques,* $A = k[V]$, $B = k[W]$. Un homomorphisme de k-algèbres $f : A \longrightarrow B$ correspond à un morphisme $\phi = \mathrm{Spec}(f)$ de W dans V.

La fibre de ϕ en un idéal premier p, correspondant à un point géométrique $(x_1,\ldots,x_n)$ de V, s'identifie à l'ensemble des points géométriques $(y_1,\ldots,y_m)$ de W tels que $\phi(y_1,\ldots,y_m) = (x_1,\ldots,x_n)$.

L'exemple 1 montre que la fibre de f en p peut être vide. Voici un critère simple permettant d'affirmer que cette fibre ne l'est pas.

Proposition 1.1

Les assertions suivantes sont équivalentes :

(i) la fibre de f *en* p *est non vide*

(ii) $f^{-1}(pB) = p$

(iii) $B_p \neq pB_p$

Démonstration

(i) $\Longrightarrow$ (ii). Soit q un élément de la fibre f en p. De l'inclusion $pB \subset q$, on déduit les inclusions $p \subset f^{-1}(pB) \subset f^{-1}(q) = p$ et donc l'égalité $f^{-1}(pB) = p$.

(ii) $\Longrightarrow$ (iii). L'égalité $f^{-1}(pB) = p$ implique l'égalité $pB \cap f(A-p) = \emptyset$.

Il suffit alors de remarquer que, si $T = f(A-p)$, B_p est $T^{-1}B$ et que, comme $pB \cap T = \emptyset$, $T^{-1}(pB) = pB_p$ est distinct de $T^{-1}B = B_p$.

(iii) $\Longrightarrow$ (i).

Il est utile pour la suite de démontrer le lemme plus précis suivant.

Lemme

On suppose vérifiée l'assertion (iii), i.e. $B_p \neq pB_p$.

L'application : $m \longmapsto (i_B^p)^{-1}(m)$ *est une bijection de l'ensemble des idéaux premiers de* B_p *contenant* pB_p *sur l'ensemble des idéaux premiers de* B *au dessus de* p.

Démonstration du lemme

Compte tenu des résultats du chapitre 1, il suffit de démontrer que si m est un idéal premier de B_p contenant pB_p, $q = (i_B^p)^{-1}(m)$ est au dessus de p.

On a un diagramme commutatif

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle i_A^p}\downarrow & & \downarrow{\scriptstyle i_B^p} \\ A_p & \xrightarrow[g]{} & B_p \end{array}$$

où g est défini de manière naturelle.

Alors $f^{-1}(q) = (i_A^p)^{-1}(g^{-1}(m))$ est égal à p car $g^{-1}(m)$ est un idéal premier de A_p contenant pA_p et donc égal à pA_p.

L'assertion (i) se déduit de (iii) en prenant pour m un idéal premier contenant pB_p (par exemple un idéal maximal) et $q = (i_B^p)^{-1}(m)$.

Corollaire

On suppose f *fidèlement plat.*

L'application Spec(f) : Spec(B) $\longrightarrow$ Spec(A) *est surjective.*

Démonstration

L'assertion (ii) est, en effet, vérifiée (confer., par exemple, (FFAC).chap.5.prop.III.7).

Proposition I.2 (*interprétation de la fibre en terme de spectre*)

Soit $f : A \longrightarrow B$ *un homomorphisme d'anneaux.*

L'application $q \longmapsto qB_p/pB_p$ *est une bijection croissante de la fibre de* f *en* p *sur* $\mathrm{Spec}(B \underset{A}{\otimes} k(p))$ (où $k(p) = A_p/pA_p$ est le corps résiduel de A en p en sorte que $B \underset{A}{\otimes} k(p) = B_p/pB_p$).

Démonstration

On va expliciter la bijection réciproque β.

Du diagramme commutatif $\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow & & \downarrow \\ k(p) & \longrightarrow & B \underset{A}{\otimes} k(p) \end{array}$ où les flèches sont naturelles, on déduit le diagramme commutatif

$$\begin{array}{ccc} \mathrm{Spec}(A) & \xleftarrow{\phi} & \mathrm{Spec}(B) \\ \alpha\uparrow & & \uparrow\beta \\ \mathrm{Spec}(k(p)) & \xleftarrow[\psi]{} & \mathrm{Spec}(B \underset{A}{\otimes} k(p)) \end{array}$$

où $\phi = \mathrm{Spec}(f)$, α applique l'unique point (fermé) de $\mathrm{Spec}(k(p))$ sur p, ψ applique tout point de $\mathrm{Spec}(B \underset{A}{\otimes} k(p))$ sur l'unique point de $\mathrm{Spec}(k(p))$.

L'application β fait correspondre à un idéal premier m/pB_p l'idéal $(i_B^p)^{-1}(m)$ de la fibre de f en p. Elle est *injective* en vertu du lemme de la proposition I.1.

L'assertion est claire, compte tenu de la proposition I.1, si $B \underset{A}{\otimes} k(p) = (0)$ car alors la fibre de f en p est vide et il en est de même de $\mathrm{Spec}(B \underset{A}{\otimes} k(p))$.

Si $B \underset{A}{\otimes} k(p) \neq (0)$, l'application ψ est *surjective*. On a alors :

$$\mathrm{Spec}(B \underset{A}{\otimes} k(p)) = \psi^{-1}(\alpha^{-1}(p)) = \beta^{-1}(\phi^{-1}(p)) = \beta^{-1} \text{ (fibre de f en } p)$$

L'injectivité de β permet de conclure.

2. Interprétation topologique de la notion d'homomorphisme entier

Soit $f : A \longrightarrow B$ *un homomorphisme entier injectif.*

Il résulte du premier théorème de Cohen-Seidenberg (chap.4.Théorème I.12.1) que l'application $\mathrm{Spec}(f) : \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ est *surjective*.

Soit, plus généralement, $f : A \longrightarrow B$ *un homomorphisme entier.*

Si b est un idéal de B, l'homomorphisme injectif f_b de $A/f^{-1}(b)$ dans B/b, défini à partir de f par passage au quotient, est entier injectif. Donc, $\mathrm{Spec}(f_b)$ est surjective.

Identifiant alors $\mathrm{Spec}(B/b)$ à $V(b)$ et $\mathrm{Spec}(A/f^{-1}(b))$ à $V(f^{-1}(b))$, on voit que $\mathrm{Spec}(f_b)$ s'identifie à la restriction de Spec(f) à $V(b)$ et que $\mathrm{Spec}(f)(V(b))$ s'identifie au fermé $V(f^{-1}(b))$.

L'application Spec(f) *est donc fermée*, i.e. applique tout fermé de Spec(B) sur un fermé de Spec(A).

Définition

Un homomorphisme $f : A \longrightarrow B$ *est dit universellement fermé si, pour tout* A*-algèbre* C, *l'application* $\mathrm{Spec}(f \otimes C) : \mathrm{Spec}(B \underset{A}{\otimes} C) \longrightarrow \mathrm{Spec}(A \underset{A}{\otimes} C) = \mathrm{Spec}(C)$ *est fermée.*

Proposition I.3 [27]

Soit : $f : A \longrightarrow B$ *un homomorphisme d'anneaux.*

Les assertions suivantes sont équivalentes :

(i) f *est entier*

(ii) f *est universellement fermé*

(iii) si X *est une indéterminée, l'application* $\mathrm{Spec}(f[X]) : \mathrm{Spec}(B[X]) \longrightarrow \mathrm{Spec}(A[X])$ *est fermée* (où $B[X]$ étant identifié à $B \underset{A}{\otimes} A[X]$, $A[X]$ à $A \underset{A}{\otimes} A[X]$, $f[X]$ est $f \otimes A[X]$).

Démonstration

(i) $\Longrightarrow$ (ii). C'est la proposition I.5 du chapitre 4.

(ii) $\Longrightarrow$ (iii). Evident.

(iii) $\Longrightarrow$ (i). Soit $b \in B$. On a un diagramme commutatif :

$$\begin{array}{ccc} A[X] & \xrightarrow{f[X]} & B[X] \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ A' & \xrightarrow[f']{} & B_b = B[X]/(bX-1) \end{array}$$

où A' est le sous-anneau de B_b engendré par f(A) et $1/b$, α et β les homomorphismes de A et B-algèbres respectivement appliquant X sur $1/b$ et f' l'homomorphisme injectif de A' dans B_b.

On en déduit un diagramme commutatif en passant aux spectres. Comme α et β sont surjectives, $\mathrm{Spec}(\alpha)$ et $\mathrm{Spec}(\beta)$ sont injectives. Il en résulte que $\mathrm{Spec}(f')$ est fermée comme $\mathrm{Spec}(f[X])$. Mais, puisque f' est injective, l'ensemble $\mathrm{Spec}(f')$ $(\mathrm{Spec}(B_b))$ est dense dans $\mathrm{Spec}(A')$ et donc

puisqu'il est fermé est égal à Spec(A'). Donc, Spec(f') est *surjective*.

L'ensemble des idéaux premiers de A' contenant 1/b est donc vide car c'est l'image de l'ensemble des idéaux premiers de B_b contenant 1/b. Par conséquent, 1/b est inversible dans A'. On a donc une égalité $b = f(a_{n-1})(1/b)^{n-1}+\ldots+f(a_o)$, où $a_i \in A$. On en déduit une équation de dépendance intégrale de b sur f(A).

Exemple : Un cas particulier d'homomorphisme entier

On rencontre quelquefois la situation suivante :

Soient B *un anneau intègre de caractéristique* p>0, A *un sous-anneau de* B *tel que pour tout* $b \in B$, *il existe* $n(b) \in \mathbb{N}^*$ *tel que* b^{n} *appartienne à* A.

Soit $p \in \mathrm{Spec}(A)$. *L'ensemble* $q = \{b \in B \mid \exists\ n \in \mathbb{N}^*$ tel que x^{p^n} appartienne à $p\}$ *est l'unique idéal premier de* B *au dessus de* p.

L'application $q \longmapsto q \cap A$ *est fermée et bijective. C'est donc un homéomorphisme.*

La démonstration en est laissée à titre d'exercice.

3. Action d'un groupe d'automorphismes sur une fibre. Deuxième théorème de Cohen-Seidenberg

Proposition I.4

Soient B *un anneau,* G *un groupe fini d'automorphisme de* B, $A = B^G$ *le sous-anneau* $\{x \in B \mid \forall\ s \in G,\ s(x) = x\}$.

1. L'anneau B *est entier sur* A.

2. Le groupe G *opère transitivement sur l'ensemble des idéaux premiers de* B *au dessus d'un idéal premier* p *de* A.

Démonstration

1. Si $x \in B$, le polynôme unitaire $\prod_{s \in G}(X-s(x))$ appartient à $A[X]$.

En effet, si $t \in G$, le polynôme $({}^{t}f(X)) = \prod_{s \in G}(X-t(s(X))$, obtenu en appliquant t aux coefficients de f(X), est égal à f(X). Les coefficients de f(X) sont donc invariants par G et appartiennent à A. L'élément x racine de f(X) est donc entier sur A. Par conséquent, B est entier sur A.

2. Soient q et q' deux idéaux premiers de B au dessus de l'idéal premier p de A.

Si $x \in q'$, l'élément $\prod_{s \in G} s(x)$ appartient à $q' \cap A = p$ et donc à q. Il existe donc un élément t de G tel que t(x) appartienne à q. Si $s = t^{-1}$, x appartient à $s(q)$. Ainsi, on a l'inclusion $q' \subset \bigcup_{s \in S} s(q)$. Il existe donc

s de G tel que q' soit contenu dans $s(q)$. Mais il est clair que $s(q)$ est un idéal premier de B au dessus de p. Comme il n'y a pas de relation d'inclusion stricte entre idéaux premiers de B au dessus de p, q' est égal à $s(q)$.

Proposition I.5

Soient A un anneau intégralement clos, K son corps des fractions, L une extension galoisienne de K, B la fermeture intégrale de A dans L.

Le groupe de Galois de L/K opère transitivement sur l'ensemble des idéaux premiers de B au dessus d'un idéal premier p de A.

Démonstration

1. On suppose L/K finie

Soit G le groupe de Galois de L/K. Il est fini. Un élément s de G induit un A-automorphisme de B : en effet, si $x \in B$ et si $f(X)$ est un polynôme unitaire à coefficients dans A tel que $f(x) = 0$, on a $f(s(x)) = 0$ et donc $s(x)$ appartient à B. La restriction de s à B est donc un homomorphisme de B dans B qui admet pour inverse la restriction de s^{-1} à B. C'est donc un A-automorphisme de B. On remarque d'ailleurs qu'un A-automorphisme de B se prolonge de manière unique en un K-automorphisme de L, en sorte que l'on peut identifier le groupe de Galois de L/K au groupe des A-automorphismes de B.

Il résulte de la théorie de Galois que K est le corps L^G des invariants de G.

On en déduit que A est l'anneau B^G des invariants de G. Il suffit alors d'appliquer la proposition I.4.

2. Cas général

Soient q et q' deux idéaux premiers de B au dessus de l'idéal premier p de A.

Soit Φ l'ensemble des couples (M,t) où M est une sous extension galoisienne de L/K et t un K-automorphisme de M tel que, C désignant la fermeture intégrale de A dans M, $t(q' \cap C) = q \cap C$. Cet ensemble non vide est inductif si on l'ordonne par inclusion des corps et prolongement des K-automorphismes. Soit (L',t') un élément maximal de Φ. On va prouver L'=L. Sinon, soit L" une extension galoisienne de degré fini sur L' contenue dans L et contenant L' strictement.

Il existe un automorphisme t" de L" prolongeant t'. Alors, si D dé-

signe la fermeture intégrale de A dans L", les idéaux premiers $t''(q' \cap D)$ et $q \cap D$ sont au dessus du même idéal premier $q \cap C$ de C. Il résulte de 1. qu'il existe un L'-automorphisme u de L" tel que $u(t''(q' \cap D)) = q \cap D$. Alors, (L",ut") appartient à Φ et est strictement supérieur à (L',t'). C'est impossible. Donc, L' = L et le résultat est prouvé.

Théorème I.6 (*deuxième théorème de Cohen-Seidenberg, appelé en anglais going down*)

Soient A *un anneau intégralement clos,* B *un anneau contenant* A *comme sous-anneau et entier sur* A.

On suppose que tout élément non nul de A *est régulier dans* B.

Soient p, $p' \in \mathrm{Spec}(A)$ *tels que* $p' \subset p$, $q \in \mathrm{Spec}(B)$ *au dessus de* p.

Il existe alors $q' \in \mathrm{Spec}(B)$ *au dessus de* p' *tel que* $q' \subset q$.

Démonstration

Le produit $S=(A-(0))(B-q)$ des deux parties multiplicatives $A-(0)$ et $B-q$ est une partie multiplicative de B.

Il existe un idéal premier r de B disjoint de S. Cet idéal est contenu dans q et tel que $r \cap A = (0)$. On peut donc identifier A à un sous-anneau de l'anneau intègre $B' = B/r$ et B' est alors entier sur A.

Si $\overline{q}'$ est un idéal premier de B' au dessus de p' et contenu dans $\overline{q} = q/r$, l'image réciproque de $\overline{q}'$ dans la surjection canonique de B sur B' est un idéal premier q' satisfaisant aux conditions de l'énoncé.

On peut donc supposer l'anneau B *intègre.*

Soit, alors, L une extension galoisienne du corps K des fractions de A, contenant B. Quitte à remplacer B par la fermeture intégrale de A dans L, on peut supposer que B est égal à cette fermeture intégrale. Soit alors q_1' un idéal premier de B au dessus de p'. On choisit arbitrairement un idéal premier q_1 de B au dessus de p et contenant q_1'. Ceci est possible en vertu du premier théorème de Cohen-Seidenberg.

En vertu de la proposition I.5, il existe un élément s de $Gal(L/K)$ tel que $s(q) = q_1$. L'idéal premier $q' = s^{-1}(q_1')$ est au dessus de p' et est contenu dans q. Il satisfait donc aux conditions de l'énoncé.

II. Algèbres de type fini sur un corps. Lemme de normalisation

Le *lemme de normalisation* d' E. Noether a un énoncé algébrique simple et une interprétation géométrique importante : *soit H un* k-*ensemble algébrique de dimension* r.

Il existe un morphisme *surjectif* (d'ensembles algébriques) de H sur un ensemble k^r.

Voici la démonstration de ce fait dans un cas particulier élémentaire.

Soit *H* l'hyperbole d'équation XY-1 = 0, considérée, pour fixer les idées, comme sous-ensemble de $\mathbb{C}^2$.

La projection $(x,y) \longmapsto x$ de $\mathbb{C}^2$ sur $\mathbb{C}$ définit un morphisme de *H* dans $\mathbb{C}$. Ce morphisme n'est pas surjectif car 0 n'est l'image d'aucun point de H. (En géométrie projective, il est l'image du point à l'infini de l'axe OY).

Soit θ l'automorphisme de $\mathbb{C}$-algèbres de $\mathbb{C}[X,Y]$ tel que :

$$\theta(X) = \frac{X+Y}{\sqrt{2}} \qquad \theta(Y) = \frac{X-Y}{\sqrt{2}}$$

Cet automorphisme correspond géométriquement à une rotation des axes de coordonnées. Il définit un isomorphisme d'ensembles algébriques de $\mathbb{C}^2$ sur $\mathbb{C}^2$. L'équation de l'hyperbole *H'* transformée de *H* est $X^2-Y^2-2 = 0$.

La projection $(x,y) \longmapsto x$ est, cette fois ci, un morphisme *surjectif* de *H'* sur $\mathbb{C}$.

1. Automorphisme d'une algèbre de polynômes à coefficients dans un corps

Un problème de géométrie affine se traduit, *après choix d'un système de coordonnées*, par un problème portant sur une algèbre de polynômes.

A un changement de coordonnées, correspond, de la manière bien connue, un automorphisme d'ensembles algébriques de l'espace affine ambiant. Cet automorphisme correspond à un automorphisme de l'algèbre de polynômes.

C'est à l'étude de certains automorphismes d'une algèbre de polynômes qu'est consacré ce qui suit.

Proposition II.1 (*existence de suffisamment d'automorphismes d'une algèbre de polynômes*)

Soient k *un corps*, $X_1,\ldots,X_n$ *des indéterminées*, $P(X_1,\ldots,X_n)$ *un polynôme non constant de* $k[X_1,\ldots,X_n]$.

Il existe un automorphisme ϕ *de* k*-algèbres de* $k[X_1,\ldots,X_n]$ *tel que le terme de plus haut degré en* X_1 *de* $\phi(P)$ *soit de la forme* cX_1^r, *avec* $c \in k^*$ *et* r *entier* $\geqslant 1$.

Démonstration

1er cas : *le corps* k *est infini* (par exemple, algébriquement clos).

On peut alors choisir l'automorphisme ϕ *linéaire*, i.e. tel que $\phi(X_i)$ soit une forme linéaire en $X_1,\ldots,X_n$ $(i = 1, \ldots, n)$.

Soit, en effet, P_r la forme non nulle de plus haut degré de P, en sorte que $P = P_r + Q$ avec $d^\circ(Q) < r$. On peut écrire $P_r(X_1,\ldots,X_n) = X_1^r P_r(1, Y_2,\ldots,Y_r)$ où $Y_1 = X_i/X_1$ $(i = 2, \ldots, n)$. Le polynôme $P_r(1,Y_2,\ldots,Y_r)$ étant non nul et le corps k étant infini, par hypothèse, il existe $a_2,\ldots,a_n \in k$ tels que $P_r(1,a_2,a_n) \neq 0$.

On définit alors ϕ par $\phi(X_1) = X_1$, $\phi(X_i) = X_i + a_i X_1$ $(i = 2,\ldots,n)$. Le coefficient du terme de plus haut degré en X_1 de $\phi(P)$ est l'élément non nul $P_r(1,a_2,\ldots,a_n)$ de k.

2ème cas : cas général (il contient évidemment le cas précédent)

On définit l'automorphisme ϕ par les conditions :

$$\phi(X_1) = X_1 \quad \phi(X_i) = X_i + X_1^{m_i} \quad (i = 2,\ldots,n)$$

où m_i est un entier naturel convenable, en un sens précisé ci-dessous.

On remarque que $\phi(X_1^{p_1}\ldots X_n^{p_n})$ est un polynôme dont le terme de plus haut degré en X_1 est $X_1^{p_1+p_2m_2+\ldots+p_nm_n}$.

On veut s'arranger pour que tous les monômes apparaissant avec des coefficients non nuls dans P donnent lieu à des termes de plus haut degré en X_1 de degrés tous différents, ce qui résoudra le problème posé.

Soit d un entier supérieur au plus grand des degrés en $X_1,\ldots,X_n$ de P.

Si on prend $m_i = (d+1)^{i-1}$ $(i = 2,\ldots,n)$, les nombres $p_1+p_2m_2+\ldots+p_nm_n$ relatifs à tous les monômes $X_1^{p_1}\ldots X_n^{p_n}$ apparaissant avec un coefficient non nul, ce qui implique $p_i \leqslant d$, sont tous distincts : en effet, un nombre s'écrit de manière unique dans le système de base (d+1) et donc une égalité

$$p_1 + p_2m_2 + \ldots + p_nm_n = p'_1 + p'_2m_1 + \ldots + p'_nm_n$$

avec $0 \leqslant p_i, p'_i < (d+1)$ implique les égalités $p_i = p'_i$.

2. Lemme de normalisation

Il existe des analogues *formels*, i.e. pour les anneaux quotients d'anneaux de séries formelles, et *analytiques*, i.e. pour les algèbres analytiques, quotients d'algèbres de séries convergentes à coefficients dans $\mathbb{R}$ ou $\mathbb{C}$, du résultat algébrique démontré ci-dessous.

Ces analogues sont alors les conséquences d'un théorème fondamental, *le théorème de préparation* de Weierstrass dont d'autres corollaires sont les théorèmes bien connus de la fonction implicite et de la fonction réciproque.

Il n'existe pas pour les polynômes d'analogue de ce théorème de préparation.

Proposition II.2

Soient k *un corps,* $A = k[x_1,\dots,x_n]$ *une* k*-algèbre de type fini,* $y_1 \in A-k$.

Il existe $y_2,\dots,y_n \in A$ *tels que* A *soit entier sur* $k[y_1,\dots,y_n]$.

Démonstration

Soit $P(X_1,\dots,X_n) \in k[X_1,\dots,X_n]$ tel que $y_1 = P(x_1,\dots,x_n)$. Comme $y_1 \notin k$, il en est de même de P. On choisit les entiers $m_2,\dots,m_n$ comme dans la proposition II.1. On pose $y_i = x_i - x_1^{m_i}$ $(i = 2,\dots,n)$ et $Q(X_1,Y_2,\dots,Y_n) = P(X_1,Y_2 + X_1^{m_2},\dots,Y_n + X_1^{m_n})$. Alors $y_1 = Q(x_1,y_2,\dots,y_n)$ et $Q(X_1,Y_2,\dots,Y_n)$ a un terme de plus haut degré en X_1 de la forme cX_1^r où $c \in k^*$. L'équation $c^{-1}Q(X_1,y_2,\dots,y_n) - c^{-1}y_1 = 0$ est une équation de dépendance intégrale de x_1 sur $k[y_1,\dots,y_n]$. On en déduit le résultat.

Proposition II.3

Soient k *un corps,* $A = k[x_1,\dots,x_n]$ *une* k*-algèbre de type fini,* a *un idéal de* A *distinct de* A.

Il existe $y_1,\dots,y_n \in A$ *et un entier* $r \leqslant n$ *tels que :*

1. y_i *appartienne à* a *si* $i \leqslant n$
2. $a \cap k[y_{r+1},\dots,y_n] = (0)$
3. $k[x_1,\dots,x_n]$ *soit entier sur* $k[y_1,\dots,y_n]$

Démonstration

C'est clair si $a = (0)$: on prend $y_i = x_i$ et $r = 0$. C'est clair si $n = 0$.

Démonstration par récurrence sur n dans le cas $a \neq (0)$.

Soit $y_1 \neq 0$, $y_1 \in a$. D'après la proposition 2, il existe $z_2,\dots,z_n \in A$ tels que A soit entier sur $k[y_1,z_2,\dots,z_n]$.

Par hypothèse de récurrence, il existe $y_2,\dots,y_n \in k[z_2,\dots,z_n]$ et $r \leqslant n$ tels que :

1. $y_2,\dots,y_r$ appartiennent à $a \cap k[z_2,\dots,z_n]$

2. $a \cap k[y_{r+1},\ldots,y_n] = (0)$

3. $k[z_2,\ldots,z_n]$ soit entier sur $k[y_2,\ldots,y_n]$.

Alors, y_1, y_2, ..., y_n et r satisfont aux conditions exigées.

Théorème II.4 (*le lemme de normalisation d'E. Noether*)

Soient k *un corps,* $A = k[x_1,\ldots,x_n]$ *une* k*-algèbre de type fini.*

1. Il existe des éléments $y_1,\ldots,y_s$ *de* A *algébriquement indépendants sur* k *tels que* A *soit entier sur* $k[y_1,\ldots,y_s]$.

2. Soit, de plus, a un idéal de A *distinct de* A. *On peut choisir* $y_1,\ldots,y_s$ *en sorte que l'idéal* $a \cap k[y_1,\ldots,y_s]$ *soit engendré par* $y_1,\ldots,y_r$ *avec* $r \leqslant s$.

Démonstration

1. Soit $A = k[X_1,\ldots,X_n]/b$. On déduit de la proposition II.3 l'existence de $Z_1,\ldots,Z_n \in k[X_1,\ldots,X_n]$ et d'un entier r tels que :

$Z_1,\ldots,Z_r$ appartienne à b

$b \cap k[Z_{r+1},\ldots,Z_n] = (0)$

$k[X_1,\ldots,X_n]$ soit entier sur $k[Z_1,\ldots,Z_n]$

Soit y_i' la classe de Z_{r+i} modulo b $(i = 1,\ldots,s=n-r)$. Alors, A est entier sur $k[y_1',\ldots,y_s']$ et $y_1',\ldots,y_s'$ sont algébriquement indépendants sur k parce que la restriction à $k[Z_{r+1},\ldots,Z_n]$ de la surjection canonique de $k[X_1,\ldots,X_n]$ sur A est un isomorphisme sur $k[y_1',\ldots,y_s']$.

2. On applique la proposition II.3 à la k-algèbre $k[y_1',\ldots,y_s']$ et à l'idéal $a \cap k[y_1',\ldots,y_s']$. Il existe des éléments $y_1,\ldots,y_s$ de $k[y_1',\ldots,y_s']$ et un entier $r \leqslant s$ tels que $y_1,\ldots,y_r$ appartiennent à a, que $a \cap k[y_{r+1},\ldots,y_s] = (0)$ et que $k[y_1',\ldots,y_s']$ soit entier sur $k[y_1,\ldots,y_s]$. On vérifie que les éléments $y_1,\ldots,y_r$ engendrent l'idéal $a \cap k[y_1,\ldots,y_s]$. Comme $k(y_1',\ldots,y_s')$ est extension algébrique de $k(y_1,\ldots,y_s)$, le degré de transcendance sur k de $k(y_1,\ldots,y_s)$ est s et donc $y_1,\ldots,y_s$ sont algébriquement indépendants que k.

Corollaire 1 (*interprétation géométrique du théorème II.4*)

Soient k *un corps,* V *un* (k,Ω)*-ensemble algébrique.*

Il existe un entier naturel s *et un morphisme surjectif d'ensembles algébriques de* V *sur* Ω^s.

Démonstration

Soit $k[V] = A$ la k-algèbre affine de V. Il existe $y_1,\ldots,y_s \in A$

algébriquement indépendants sur k tels que $k[V]$ soit entier sur $k[y_1,\dots,y_s] = k[\Omega^s]$.

L'injection de $k[\Omega^s]$ dans $k[V]$ définit un morphisme de V dans Ω^s qui au point correspondant à l'idéal premier p de $k[V]$ fait correspondre le point de Ω^s correspondant à l'idéal premier $p \cap k[\Omega^s]$. La surjectivité est une conséquence du théorème de Cohen-Seidenberg.

Corollaire 2

Soient k *un corps,* A *une* k*-algèbre de type fini,* $a_0 \subset \dots \subset a_r$ *une chaîne d'idéaux de* A *avec* $a_r \neq A$.

Il existe des éléments $y_1,\dots,y_s$ *de* A *algébriquement indépendants sur* k *et une suite croissante* $n_0,\dots,n_r$ *d'entiers naturels tels que* A *soit entier sur* $k[y_1,\dots,y_s]$ *et* $a_i \cap k[y_1,\dots,y_s] = (y_1,\dots,y_{n_i})$.

Démonstration

Récurrence sur r, le cas $r = 1$ étant le théorème 4.2. On suppose $r > 1$.

Par hypothèse de récurrence, il existe $z_1,\dots,z_s$ de A algébriquement indépendants sur k tels que A soit entier sur $k[z_1,\dots,z_s]$ et une suite strictement croissante $n_0,\dots,n_{r-1}$ d'entiers naturels tels que $a_i \cap k[z_1,\dots,z_s] = (z_1,\dots,z_{n_i})$ pour $i = 1,\dots,r-1$.

L'anneau A/a_{r-1} est entier sur $k[z_1,\dots,z_s]/(a_{r-1} \cap k[z_1,\dots,z_s])$, isomorphe à $k[z_{n_{r-1}+1},\dots,z_s]$. Il existe $y_{n_{r-1}+1},\dots,y_s \in k[z_{n_{r-1}},\dots,z_s]$, algébriquement indépendants sur k, tels que l'anneau $k[z_{n_{r-1}+1},\dots,z_s]$ soit entier sur $k[y_{n_{r-1}+1},\dots,y_s]$ et que $a_r/a_{r-1} = (y_{n_{r-1}+1},\dots,y_{n_r})$. On pose $y_i = z_i$ si $i \leqslant n_r$.

Corollaire 3

Soient k *un corps,* $X_1,\dots,X_n$ *des indéterminées.*

Alors, $\dim(k[X_1,\dots,X_n]) = n$.

Autrement dit, l'espace affine Ω^n *est en tant qu'ensemble algébrique de dimension* n.

Démonstration

De l'existence de la chaîne $(0) \subset (X_1) \subset \dots \subset (X_1,\dots,X_n)$ d'idéaux premiers, on déduit l'inégalité $\dim(k[X_1,\dots,X_n]) \geqslant n$.

Soit ensuite $p_0 \subset p_1 \subset \dots \subset p_r$ une chaîne d'idéaux premiers. On choi-

sit $y_1,\ldots,y_s$ comme dans le corollaire 2. En raison du théorème de Cohen-Seidenberg, les idéaux $p_i \cap k[y_1,\ldots,y_s]$ sont distincts et forment une chaîne $(y_1,\ldots,y_{n_i})$ d'idéaux premiers de $k[y_1,\ldots,y_s]$. Comme $s = n$, on voit que $r \leqslant n$ et donc que $\dim(k[X_1,\ldots,X_n]) \leqslant n$.

Corollaire 4

Soient k *un corps,* A *une* k*-algèbre de type fini intègre,* K *son corps des fractions.*

Alors, $\dim(A) = d°tr(K/k)$.

Démonstration

Soient $y_1,\ldots,y_s \in A$ algébriquement indépendants sur k tels que A soit entier sur $k[y_1,\ldots,y_s]$. Alors $s = \dim(k[y_1,\ldots,y_s]) = \dim A$.

D'autre part, K est algébrique sur $k(y_1,\ldots,y_s)$ et donc $d°tr(K/k) = s$.

Interprétation

Soit H *un* k*-ensemble algébrique irréductible.* Le corps $k(H)$ des fonctions rationnelles sur H est une extension de type fini de k. Le degré de transcendance de l'extension $k(H)/k$ est égal à la dimension de H. Ce degré est le nombre maximal de fonctions rationnelles sur H linéairement indépendantes sur k. Il mesure en quelque sorte le degré de liberté sur H, i.e. le nombre de paramètres que l'on peut spécialiser librement.

3. Normalisation

Théorème II.5

Soient A *une* k*-algèbre de type fini intègre,* K *son corps des fractions,* L/K *une extension algébrique finie de* K, B *la fermeture intégrale de* A *dans* L.

Alors, B *est un* A*-module de type fini et une* k*-algèbre de type fini.*

Démonstration

Il suffit évidemment de démontrer que B est un A-module de type fini.

Compte tenu d'une proposition du chapitre 5, on peut se limiter au cas où la caractéristique p de k est non nulle et où l'extension L/K de K est radicielle.

Compte tenu du lemme de normalisation, on peut supposer que A est un anneau de polynômes $k[X_1,\ldots,X_n]$. Alors, $L = k(X_1,\ldots,X_n,y_1,\ldots,y_r)$ et

il existe une puissance positive q de p telle que y_i^q appartienne à $k(X_1,\ldots,X_n)$ $(i = 1,\ldots,r)$. Les éléments y_i^q sont des fractions rationnelles en $X_1,\ldots,X_n$. Soient $a_1,\ldots,a_r$ les coefficients non nuls de ces fractions. Le corps L est contenu dans le corps $L' = k(a_1^{q^{-1}},\ldots,a_r^{q^{-1}},X_1^{q^{-1}},\ldots,X_n^{q^{-1}})$ et il suffit évidemment de démontrer que la fermeture intégrale B' de A dans L' est un A-module de type fini et donc noethérien.

Il est clair que B' contient l'anneau $k(a_1^{q^{-1}},\ldots,a_r^{q^{-1}})[X_1^{q^{-1}},\ldots,X_n^{q^{-1}}]$, anneau qui est intégralement clos car il est isomorphe à anneau de polynômes sur le corps $k(a_1^{q^{-1}},\ldots,a_r^{q^{-1}})$. On en déduit que A' est égal à $k(a_1^{q^{-1}},\ldots,a_r^{q^{-1}})[X_1^{q^{-1}},\ldots,X_r^{q^{-1}}]$ i.e. à $k[X_1^{q^{-1}},\ldots,X_r^{q^{-1}}, a_1^{q^{-1}},\ldots,a_r^{q^{-1}}]$ qui est évidemment un $k[X_1,\ldots,X_n]$-module de type fini puisque $X_j^{q^{-1}}$ et $a_i^{q^{-1}}$ sont des entiers sur $k[X_1,\ldots,X_n]$ $(j = 1,\ldots,n ; i = 1,\ldots,r)$.

Interprétation géométrique

Un cas particulier important d'application du théorème II.3 est celui où L = K.

La clôture intégrale de la k-algèbre de type fini intègre A est de la forme $k[X_1,\ldots,X_m]/q$, où q est un idéal premier. Soit H une variété algébrique telle que $A = k[H]$.

La variété algébrique $V(q)$ est appelée *normalisée* de H.

Elle est par définition même birationnellement équivalente à H.

Cas particulier où $d°tr(K/k) = 1$.

Alors H est une *courbe* algébrique irréductible. La normalisation $\overline{H}$ de H, définie à équivalence birationnelle près, est aussi une courbe algébrique irréductible. Le fait que l'algèbre affine $k[\overline{H}]$ soit un anneau intégralement clos sera interprété ultérieurement par le fait que $\overline{H}$ est une courbe algébrique *non singulière*.

On voit ainsi que *toute courbe algébrique irréductible est birationnellement équivalente à une courbe algébrique non singulière*.

Exemple

La courbe algébrique plane d'équation $X^2 - Y^3 = 0$ a pour représentation paramétrique $X = T^3$, $Y = T^2$. Son algèbre affine sur $\mathbb{C}$ est $\mathbb{C}[T^3,T^2] = A$

L'élément T du corps des fractions de cette algèbre est entier sur A Il en résulte que la clôture intégrale de A contient l'anneau $K[T]$. Comme $k[T]$ est intégralement clos, cette clôture intégrale est égale à $k[T]$, qui est l'algèbre affine d'une droite.

III. Ensembles constructibles. Définition et caractérisation

Soient H_1 et H_2 deux k-ensembles algébriques, f un morphisme de H_1 dans H_2.

L'exemple où H_1 est l'hyperbole d'équation $X_1X_2-1 = 0$, H_2 l'axe des X_i et f la projection $(x_1, x_2) \longmapsto x_1$ montre que im(f) n'est pas toujours un fermé de H_2. Il montre également que im(f) n'est pas toujours stable par spécialisation. Un théorème de C. Chevalley affirme que im(f) est une réunion finie de sous-ensembles localement fermés et que, de plus, si im(f) est stable par spécialisation, im(f) est fermée.

1. Définition et caractérisation des ensembles constructibles

Dans tout ce paragraphe, X désigne un espace topologique noethérien.

Pour une définition de la notion d'ensemble constructible dans le cas général, on pourra consulter l'annexe et ses exercices.

Définition

Un sous-ensemble Z de X est dit constructible s'il est une réunion finie de sous-ensembles localement fermés, i.e. intersections d'un ouvert et d'un fermé de X.

Proposition III.1

L'ensemble des parties constructibles de X est le plus petit ensemble de parties de X contenant les ouverts et les fermés et stable par intersection et réunion finie et passage au complémentaire.

Démonstration

Il est clair que, *si Z et Z' sont constructibles, il en est de même de* $Z \cup Z'$.

L'ensemble $Z-Z'$ *est également constructible* : soient, en effet $Z = \cup Z_i$, $Z' = \cup Z'_j$, où Z_i et Z'_j sont localement fermés. Alors, $Z-Z' = Z \cap CZ' = \cup(Z_i \cap (CZ'_j)) = \cup(Z_i - Z'_j)$. Il suffit donc de démontrer que si $Z = U \cap F$ et $Z' = U' \cap F'$, où U et U' sont ouverts, F et F' sont fermés, $Z-Z'$ est constructible. Or,

$$(U \cap F)-(U' \cap F') = (U \cap F) \cap (CU' \cup CF') = (U \cap F \cap CU') \cup (U \cap F \cap CF')$$

est réunion de deux ensembles localement fermés.

On en déduit que CZ *et* CZ' *sont constructibles et donc que* $Z \cap Z' = C(CZ \cup CZ')$ *est constructible.*

Proposition III.2 (*une caractérisation des constructibles*)

Soit Z *un sous-ensemble de* X.

Les assertions suivantes sont équivalentes :

(*i*) Z *est constructible*

(*ii*) *pour toute partie fermée irréductible* F *de* X *telle que* $Z \cap F$ *soit dense dans* F, $Z \cap F$ *contient un ouvert non vide de* F.

Démonstration

(i) $\Longrightarrow$ (ii)

L'ensemble Φ des parties Z de X satisfaisant à (ii) contient les ouverts et les fermés. Il est stable par *réunion finie* : soient Z_1, $Z_2 \in \Phi$, F un fermé irréductible de X tel que $(Z_1 \cup Z_2) \cap F$ soit dense dans F ; alors, par exemple, $Z_1 \cap F$ est dense dans F et contient donc un ouvert non vide de F ; il en est de même, a fortiori, de $(Z_1 \cup Z_2) \cap F$ et $Z_1 \ Z_2$ appartient à Φ. Il est stable par *intersection finie* : soient Z_1, $Z_2 \in \Phi$, F un fermé irréductible de X tel que $(Z_1 \cap Z_2) \cap F$ soit dense dans F ; alors, $Z_1 \cap F$ et $Z_2 \cap F$ sont denses dans F, contiennent respectivement des ouverts non vides U_1 et U_2 de F. Comme F est irréductible, $U_1 \cap U_2$ est un ouvert *non vide* de F, contenu dans $(Z_1 \cap Z_2) \cap F$. Par conséquent, $Z_1 \ Z_2$ appartient à Φ.

L'ensemble Φ contient donc les constructibles.

(ii) $\Longrightarrow$ (i)

On commence par démontrer qu'*un ensemble* Z *satisfaisant à* (ii) *et, de plus, tel que, pour tout fermé* F *de* X *distinct de* X, $F \cap Z$ *soit constructible est constructible.*

Si, en effet, X n'est *pas irréductible*, $X = X_1 \cup X_2$, où X_1 et X_2 sont distincts de X et $Z = (Z \cap X_1) \cup (Z \cap X_2)$ est constructible comme $Z \cap X_1$ et $Z \cap X_2$.

Si X est *irréductible*, ou bien $Z = Z \cap X$ est dense et alors, d'après (ii), il contient un ouvert non vide U et $Z = U \cup (CU \cap Z)$ est constructible comme U et $CU \cap Z$, ou bien Z n'est pas dense et alors CZ contient un ouvert non vide U de X ; alors $Z \cup U$ est constructible d'après ce qui précède ; il en est de même de $CZ \cap CU$, de $CZ = U \cup (CZ \cap CU)$ et donc de Z.

Soit Z un ensemble satisfaisant à (ii). On le suppose *non constructible.*

L'ensemble des fermés F de X distincts de X tels que $F \cap Z$ ne soit

pas constructible est non vide. Comme X est *noethérien*, il admet un élément *minimal* F. L'ensemble $Z_o = F_o \cap Z$ n'est pas constructible dans X et donc dans F_o, qui est fermé. Or, pour tout fermé F de F_o distinct de F_o, $F \cap Z_o = F \cap Z$ est constructible. On obtient une contradiction.

Corollaire

Soient A *un anneau noethérien,* X = Spec(A), Z *un ensemble constructible de* X.

Les assertions suivantes sont équivalentes :

(i) Z *est fermé*

(ii) Z *est stable par spécialisation*

Démonstration

(i) $\Longrightarrow$ (ii)

Un fermé est stable par spécialisation.

(ii) $\Longrightarrow$ (i)

Soit $\overline{Z} = Z_1 \cup \ldots \cup Z_n$ une décomposition de l'adhérence $\overline{Z}$ de Z en fermés irréductibles.

Comme Z est constructible dans X, il l'est dans $\overline{Z}$. Donc, $Z_i \cap Z$ est constructible et dense dans Z_i ; il contient un ouvert U_i de Z_i ; cet ouvert U_i est stable par générisation et contient donc le point générique de Z_i. Par conséquent, Z qui est stable par spécialisation et contient le point générique de Z_i contient Z_i.

Ainsi $Z = \overline{Z}$ et Z est fermé.

2. Le théorème de Chevalley

Théorème III.3

Soient A *un anneau noethérien,* $f : A \longrightarrow B$ *une* A*-algèbre de type fini,* X = Spec(A), Y = Spec(B), ϕ = Spec(f) : Y $\longrightarrow$ X.

Alors im(ϕ) *est un sous-ensemble constructible de* X.

Démonstration

Il suffit, en vertu de la proposition III.2, de démontrer que si $p \in X$ est tel que $\phi(Y) \cap V(p)$ est dense dans $V(p)$, $\phi(Y) \cap V(p)$ contient un ouvert non vide de $V(p)$.

Soient A' = A/p, B' = B/pB, f' l'homomorphisme de A' dans B' déduit de f, ϕ' = Spec(f').

Identifiant $V(p)$ à Spec(A'), on identifie $\phi(Y) \cap V(p)$ à ϕ'(Spec(B')).

Puisque A' est intègre et donc réduit, dire que $\phi'(\mathrm{Spec}(B'))$ est dense dans Spec(A') c'est dire que f' est injectif (chap.6.prop.).

Quitte à remplacer A par A', B par B', f par f', on est conduit à la démonstration de l'assertion suivante.

Soient A *un anneau noethérien intègre,* B *un anneau intègre contenant* A *et* A*-algèbre de type fini,* ϕ *l'application de* Y = Spec(B) *dans* X = Spec(A) *déduite de l'injection de* A *dans* B. *Alors* ϕ(Y) *contient un ouvert non vide.*

Soit $B = A[x_1,\ldots,x_n]$.

L'assertion est claire si $x_1,\ldots,x_n$ sont algébriquement indépendants sur A car alors ϕ est surjective et X est non vide.

On suppose donc $x_1,\ldots,x_r$ algébriquement indépendants sur A et $x_{r+1},\ldots,x_n$ algébriques sur $A[x_1,\ldots,x_r]$. On pose $C = A[x_1,\ldots,x_r]$.

Soit $g_{j,n}(x_1,\ldots,x_r)x_j^{n_j}+\ldots = 0$ une équation de dépendance algébrique de x_j $(j = r+1,\ldots,n)$ sur C, avec $g_{j,n(j)}$ non nul.

Soit a un coefficient non nul du polynôme non nul $\prod_{j=r+1}^{n} g_{j,n(j)}(x_1,\ldots,x_r)$.

On va démontrer l'inclusion $D(a) \subset \phi(Y)$.

Soit $p \in D(a)$. L'idéal $q = pC$ de C est premier et $\prod_{j=r+1}^{n} g_{j,n(j)}$ n'appartient pas à q. Donc, B_q est entier sur C_q ; il existe un idéal premier r de B_q au dessus de qC_q. Alors, $r \cap A = (r \cap C) \cap A = pC \cap A = p$ et comme $p = (r \cap B) \cap A$, p appartient à ϕ(Y).

Corollaire

Les notations et hypothèses sont celles du théorème III.3.

Si Y' *est une partie constructible de* Y, ϕ(Y') *est une partie constructible de* X.

Démonstration

Soient $Y' = \bigcup_{i=1}^{n} D(f_i) \cap V(p_i)$, où $f_i \in B$, $p_i \in \mathrm{Spec}(B)$, $\overline{f}_i$ la classe de f_i modulo p_i, B_i la A -algèbre $(B/p_i)_{\overline{f}_i}$. Alors, $D(f_i) \cap V(p_i)$ est homéomorphe à $\mathrm{Spec}(B_i)$ et Y' à $\mathrm{Spec}(\prod_{i=1}^{n} B_i)$. On vérifie que $\phi(Y') = \mathrm{Spec}(s)(Y')$ où s est l'homomorphisme naturel de A dans $\prod_{i=1}^{n} B_i$. Il suffit d'appliquer le théorème III.3.

Exercices du chapitre 7

(1). Soient k un corps, $X_1,\dots,X_n,Y_1,\dots,Y_m$ des indéterminées, $f_i(X_1,\dots,X_n) \in k[X_1,\dots,X_n]$ $(i = 1,\dots,m)$, f l'homomorphisme de substitution : $g(Y_1,\dots,Y_m) \longmapsto g(f_1(X_1,\dots,X_n),\dots,f_m(X_1,\dots,X_n))$ de $k[Y_1,\dots,Y_m]$ dans $k[X_1,\dots,X_n]$.

Quelle st la fibre de f en (0,...,0) ?

(2). Soient k un corps, $T_1,\dots,T_r,X_1,\dots,X_n$ des indéterminées, $f(X_1,\dots,X_n) = \Sigma a_{i_1\dots i_n}(T_1,\dots,T_r)X_1^{i_1}\dots X_n^{i_n}$ où $a_{i_1\dots i_n}(T_1,\dots,T_r)$ appartient à $k[T_1,\dots,T_r]$, $t_1,\dots,t_r$ des éléments de k.

Quelle est la fibre en l'idéal premier $(T_1-t_1,\dots,T_r-t_r)$ de l'homomorphisme naturel de $k[T_1,\dots,T_r]$ dans $k[T_1,\dots,T_r][X_1,\dots,X_n]/(f(X_1,\dots,X_n))$?

(3). Soient k un corps, X_1,X_2,X_3,Y_1,Y_2 des indéterminées, f l'homomorphisme de k-algèbres de $k[X_1,X_2,X_3]/(X_1X_3-X_2^2)$ dans $k[Y_1,Y_2]$ appliquant la classe de X_1 (resp.X_2 ; resp.X_3) sur Y_1^2 (resp.Y_1Y_2 ; resp.Y_2^2).

Quelle est la fibre de f en l'idéal premier $(X_1-a, X_2-b, X_3-c)/(X_1X_3-X_2^2)$, où (a,b,c) appartient à $k^3 \cap V(X_1X_3-X_2^2)$?

(4). Un homomorphisme $f : A \longrightarrow B$ est dit de *type fini* s'il munit B d'un structure de A-algèbre de type fini.

Soit $f : A \longrightarrow B$ un homomorphisme de type fini.

1. Démontrer les équivalences :

(i) les fibres de f sont des sous-espaces discrets de Spec(B)

(ii) pour tout idéal premier p de A, $B \otimes_A k(p)$ est une algèbre finie sur le corps résiduel $k(p) = A_p/pA_p$ de A en p

2. Démontrer que ces conditions équivalentes impliquent que les fibres de f sont finies et qu'elles sont vérifiées si f est fini.

(On utilisera les équivalences pour un anneau noethérien A : (i) A est artinien ; (ii) Spec(A) est discret et fini ; (iii) Spec(A) est discret).

(5). Soient A et B des anneaux, f un homomorphisme de A dans B. Si $q \in$ Spec(B), on désigne par p l'idéal $f^{-1}(q)$ l'homomorphisme de A_p dans B_q déduit de f.

Démontrer les équivalences :

(i) pour tout $q \in$ Spec(B), f_q est surjectif

(ii) pour tout p de Spec(A), tout q de Spec(B) tel que $f^{-1}(q) = p$,

tout p' de Spec(A) contenu dans p, il existe $q' \in$ Spec(B) contenu dans q tel que $p' = f^{-1}(q')$.

(6). Utiliser le lemme de normalisation pour démontrer la forme faible du théorème des zéros de Hilbert : un corps, algèbre de type fini sur un corps k, est algébrique sur k.

(7). Démontrer, par récurrence sur n, le lemme de normalisation analytique suivant :

Soient k le corps $\mathbb{R}$ ou le corps $\mathbb{C}$, a un idéal de l'anneau $k\{\{X_1,\ldots,X_n\}\}$ des séries convergentes à n indéterminées. Il existe des éléments $y_1,\ldots,y_s$ de $A = k\{\{X_1,\ldots,X_n\}\}/a$ analytiquement indépendants sur k (i.e. tel que l'homomorphisme naturel de $k[[Y_1,\ldots,Y_s]]$, où $Y_1,\ldots,Y_s$ sont des indéterminées, sur $k[[y_1,\ldots,y_s]]$ soit un isomorphisme) tels que A soit un $k\{\{y_1,\ldots,y_s\}\}$-module de type fini.

(8). Soient B un anneau, A un sous-anneau de B tel que B soit entier sur A, a un idéal de A, $\overline{A}$ la fermeture intégrale de A dans B.

Un élément x de B est dit *entier sur* a s'il satisfait à une équation de dépendance intégrale : $x^n + a_1x^{n-1} + \ldots + a_n = 0$, où a_i appartient à a. $(i = 1,\ldots,n)$.

On appelle *fermeture intégrale de* a *dans* B l'ensemble des éléments de B entiers sur a.

1. Démontrer que la fermeture intégrale de a dans B est la racine de l'idéal $a\overline{A}$.

2. On suppose A *intégralement clos*, de corps des fractions K.

Démontrer que, si $x \in B$ est entier sur l'idéal a, $\mathrm{irr}(X,x,K) = X^n + a_1X^{n-1} + \ldots a_n$, où a_i appartient à $r(a)$. $(i = 1,\ldots,n)$.

3. On suppose, de plus, B intègre.

Soient p, $p' \in$ Spec(A) tels que $p' \subset p$, $q \in$ Spec(B) au dessus de p.

Démontrer qu'un élément x de $p'B$ est entier sur p'.

En déduire que irr(X,x,K) est de la forme $X^n + a_1X^{n-1}+\ldots+a_n$, où a_i appartient à p'. $(i = 1,\ldots,n)$.

En déduire que $p'B_q \cap A = p'$ puis qu'il existe $q' \in$ Spec(B) contenu dans q au dessus de p'.

Retrouver ainsi le deuxième théorème de Cohen-Seidenberg.

Les exercices 9,10,11 sont tirés de l'article suivant :

Carlo Traverso. *Seminormality and* Picard *Group. Annali della scuola nor-*

male superiore di Pisa. Classe di Scienze, vol.XXIV, fasc.IV, 1970, 585-595.

(9). Soient B un anneau, A un sous-anneau tel que B soit entier sur A.

On appelle *semi-normalisé de* A *dans* B l'ensemble

$\{b \in B \ / \ \forall p \in \mathrm{Spec}(A),\ i_B^p(b) \in A_p + r(B_p)\}$

où $r(B_p)$ est le radical de B_p.

1. Démontrer que le semi-normalisé de A dans B est le plus grand sous-anneau A' de B possédant les deux propriétés suivantes :

a) pour tout $p \in \mathrm{Spec}(A)$, la fibre de $A \longrightarrow B$ en p est réduite à un point q

b) l'homomorphisme canonique $k(p) \longrightarrow k(q)$ est un isomorphisme

2. On dit que A est *semi-normal dans* B s'il est égal à son semi-normalisé dans B.

Démontrer que, si C est un anneau contenant B tel que C soit entier sur B, si A est semi-normal dans B et B est semi-normal dans C, alors A est semi-normal dans C.

3. Démontrer que, si A est semi-normal dans B, le conducteur $(A:B) = \{x \in B \ / \ xB \subset A\}$ de A dans B est un idéal de B égal à sa racine.

(10). Soient B un anneau, A un sous-anneau *noethérien. On suppose* B *fini sur* A.

Soient $p \in \mathrm{Spec}(A)$, $\{q_1,\ldots,q_n\}$ la fibre en p de l'injection $A \longrightarrow B$, π_i l'homomorphisme canonique $k(p) \longrightarrow k(q_i)$.

On désigne par A' l'ensemble des éléments b B possédant les deux propriétés suivantes :

a) pour tout $i \in \{1,\ldots,n\}$, la classe de b modulo q_i appartient à $\mathrm{im}(\pi_i)$

b) pour tout $i,j \in \{1,\ldots,n\}$, Π_i^{-1} (classe de b modulo q_i) = Π_j^{-1} (classe de b modulo q_j).

1. Démontrer que A' est le plus grand sous-anneau de B contenant A tel que la fibre en p de $A \longrightarrow A'$ soit à un point p' et que l'homomorphisme canonique de $k(p)$ dans $k(p')$ soit un isomorphisme.

En déduire que A' est semi-normal dans B.

On dit que A' est *déduit de* B *par pincement au dessus de* p.

2. Soit $p_1 \in \mathrm{Spec}(A)$ n'appartenant pas à l'adhérence $V(p)$ de p.

Démontre l'existence d'une bijection de la fibre de $A \longrightarrow A'$ en p_1 sur la fibre de $A \longrightarrow B$ en p_1.

3. Démontrer que, si le conducteur $(A:B)$ est intersection d'idéaux premiers de B, pour un idéal premier minimal p de $(A:B)$, considéré comme idéal de A, dont la fibre de $A \longrightarrow B$ est réduite à un point p', l'homomorphisme canonique $k(p) \longrightarrow k(p')$ n'est pas surjectif.

En déduire que le conducteur de A dans le semi-normalisé de A dans B n'est pas intersection d'idéaux premiers de ce semi-normalisé.

(Utiliser l'anneau obtenu par pincement d'un idéal premier minimal de ce conducteur).

(11). Soient B un anneau, A un sous-anneau *noethérien* de B. *On suppose* B *fini sur* A.

1. Démontrer que, si A est semi-normal dans B, il existe une suite

$$B = B_0 \supset B_1 \supset \ldots \supset B_n = A$$

de sous-anneaux de B tel que, pour tout $i = 1,\ldots,n$, B_{i+1} soit déduit de B_i par pincement au dessus d'un idéal premier de A.

(Supposer B_i déjà obtenu, $B_i \neq A$. Considérer un idéal premier $p \in \mathrm{Ass}_A(A:B_i)$. Définir B_{i+1} comme déduit de B_i par pincement au dessus de cet idéal. Remarquer que $(A:B_{i+1}) \supset (A:B_i)$ et que $p \notin \mathrm{Ass}_A(A:B_{i+1})$ et donc que $(A:B_{i+1}) \neq (A:B_i)$.)

2. On suppose A semi-normal dans B. Démontrer que, si S est une partie multiplicative de A, $S^{-1}A$ est semi-normal dans $S^{-1}B$.

Dans l'article mentionné plus haut, C. Traverso démontre le théorème suivant :

Soient A un anneau noethérien réduit dont la fermeture intégrale dans l'anneau total des fractions est un A-module de type fini, $X_1,\ldots,X_n$ des indéterminées, $n>1$.

Les assertions suivantes sont équivalentes :

(i) l'homomorphisme canonique de Pic(A) dans $\mathrm{Pic}(A[X_1,\ldots,X_n])$ est un isomorphisme

(ii) A est semi-normal.

(12). (Théorême de platitude générique)

Soient A un anneau noethérien intègre, $\rho : A \longrightarrow B$ une A-algèbre de type fini, M un A-module de type fini.

Démontrer qu'il existe un élément non nul f de A tel que M_f soit un A_f-module libre.

(Soit $S = A - \{0\}$ en sorte que $S^{-1}A$ est le corps K des fractions de A. Raisonner par récurrence sur $\dim(S^{-1}B)$, en supposant l'assertion vraie si $\dim(S^{-1}N) < n$.

Supposer $\dim(S^{-1}B) = n$.

Utilisant une suite de composition du A-module M comme dans chap.3. proposition II.1 se ramener au cas où M = B et B est intègre.

Considérer des éléments $y_1,\ldots,y_n$ de B, algébriquement indépendants sur K, tels que $S^{-1}B$ soit entier que $K[y_1,\ldots,y_n]$ puis un élément non nul g de A tel que B_g soit entier sur $A_g[y_1,\ldots,y_n]$. Remplacer A par A_b et B par B_g.

Considérer, alors, $b_1,\ldots,b_m \in B$ formant un système maximal d'éléments linéairement indépendants sur $A[y_1,\ldots,y_n]$. En déduire une suite exacte de $A[y_1,\ldots,y_n]$-modules

$$0 \longrightarrow (A[y_1,\ldots,y_n])^m \longrightarrow B \longrightarrow B' \longrightarrow 0$$

où B' est un *module de torsion*, et donc un module sur un quotient strict de $A[y_1,\ldots,y_n]$. Déduire de l'hypothèse de récurrence l'existence de f non nul de A tel que B'_f soit un A_f-module libre et le résultat cherché).

(13). 1. Soient k un corps, B une k-algèbre de type fini, $q \in \mathrm{Spec}(B)$

Démontrer les équivalences :

(i) q est un point isolé dans Spec(B) (i.e., $\{q\}$ est ouvert dans Spec(B))

(ii) il existe $f \in B-q$ tel que $V(f) = \{q\}$

(iii) B_q est une k-algèbre finie

((ii) $\Longrightarrow$ (iii). Remarquer que B_f est local artinien d'idéal maximal qB_f, que B_f/qB_f est une k-algèbre finie (théorème des zéros) puis que B_f est fini sur k.

(iii) $\Longrightarrow$ (ii). Considérer la suite exacte de B-modules

$$0 \longrightarrow N \longrightarrow B \xrightarrow{i_B^q} B_q \longrightarrow Q \longrightarrow 0$$

Démontrer l'existence de $f \in B_q$ tel que $N_f = Q_f = 0$, en remarquant que les supports de N et Q sont des fermés de Spec(B), distincts de Spec(B), puis démontrer l'égalité $\mathrm{Spec}(B_f = \{qB_f\}$.

2. Soient A un anneau, $\rho : A \longrightarrow B$ une A-algèbre de type fini,

$q \in \mathrm{Spec}(B)$, $p = \rho^{-1}(q)$.

Démontrer les équivalences :

(i) q est isolé dans sa fibre

(ii) B_q/qB_q est une $k(p)$-algèbre finie, où $k(p) = A_p/pA_p$.

Si ces conditions équivalentes sont satisfaites, on dit que B est *quasi-finie sur* A en q.

On peut signaler le théorème suivant :

(*Théorème principal de* Zariski). Soient A un anneau, $\rho : A \longrightarrow B$ une A-algèbre de type fini, $\overline{A}$ la fermeture intégrale de $\rho(A)$ dans B, $q \in \mathrm{Spec}(B)$.

Si B est quasi-finie sur A en q, il existe $f \in \overline{A}$, $f \notin q$ tel que $\overline{A}_f = B_f$.

On en trouvera une démonstration , par exemple, dans l'article suivant :

Peskine C. *Le théorème principal de Zariski. Bull.Sc. maths.*, 90, 1966,119-127 ou dans [16] où cette démonstration est reprise.

CHAPITRE 8

Topologie α - adique. Complétion

Soient k *un corps,* $X_1,\ldots,X_n$ *des indéterminées.*

L'anneau $k[[X_1,\ldots,X_n]]$ *des séries formelles* peut être obtenu à partir de l'anneau $k[X_1,\ldots,X_n] = A$ des polynômes par un procédé de complétion pour la métrique d définie comme suit :

Soit a l'idéal $(X_1,\ldots,X_n)$ de A. Si f, g ε A, on pose :

$d(f,g) = e^{-r}$ s'il existe un entier r tel que $f-g \in a^r$ et $f-g \notin a^{r+1}$

(où e est un nombre réel > 1)

= 0 s'il n'existe pas de tel entier r, i.e. si f = g.

La métrique est donc définie par le suite $(a^r)_{r\in\mathbb{N}}$ des puissances de l'idéal a. Les ensembles de la forme $a^r (r\in\mathbb{N})$ forment un système fondamental (dénombrable) de voisinages de 0 dans la topologie associée à la métrique.

On peut obtenir l'anneau $k[[X_1,\ldots,X_n]]$ par le même procédé à partir de l'anneau $k[X_1,\ldots,X_n]_{(X_1,\ldots,X_n)}$ et des puissances de son idéal maximal ou, si k = ℝ ou ℂ, à partir de l'anneau local $k\{\{X_1,\ldots,X_n\}\}$ des séries convergentes, i.e. des séries $\Sigma a_{i_1\ldots i_n} X_1^{i_1}\ldots X_n^{i_n}$ pour lesquelles il existe M ε $\mathbb{R}^+$ (dépendant de la série) tel que, pour tout multi-indice $(i_1,\ldots,i_n)$, l'inégalité de Cauchy $|a_{i_1\ldots i_n}| \leqslant \frac{M}{i_1!\ldots i_n!}$ soit vérifiée.

L'anneau $\hat{\mathbb{Z}}_{(p)}$ *des entiers p-adiques,* important en théorie algébrique des nombres, s'obtient à partir de l'anneau ℤ et des puissances de l'idéal (p) par le même procédé.

Soient, plus généralement, A *un anneau noethérien, a un idéal de* A. On munit A d'une topologie compatible avec la structure d'anneau en prenant pour système fondamental de voisinage de x les ensembles $x + a^n$ $(n\in\mathbb{N})$.

On démontre que si A *est intègre ou si a est contenu dans le radical de* A, cette topologie est *séparée* et on vérifie alors qu'elle est *métrisable*. Le complété $\hat{A}$ de l'espace métrique A ainsi défini, appelé complété *a*-adique de A, est muni d'une structure d'anneau obtenue en prolongeant par continuité les lois de composition de A.

Cet anneau est *noethérien*. De plus, on démontre que $\hat{A}$ est *plat* sur A et même, dans le cas où a est contenu dans le radical de A, *fidèlement plat* sur A.

C'est à l'étude de ce formalisme qu'est consacré ce chapitre.

Voici le plan de ce chapitre.

Le paragraphe I est essentiellement consacré à la démonstration du lemme d'artin-Rees et d'applications de ce lemme tel le théorème d'intersection démontré initialement par Krull en utilisant des décompositions primaires.

Dans II, on étudie le complété d'un anneau et plus généralement d'un module pour une métrique associée à un idéal. L'utilisation de techniques de limites projectives donne à cette question de nature topologique en apparence un aspect purement algébrique.

Dans III, on étudie quelques propriétés importantes du complété (platitude, noethérianité).

Le paragraphe IV traite du théorème de préparation formel sous différentes formes. Ce théorème a pour corollaire le théorème de la fonction implicite ou réciproque.

Le paragraphe V est consacré à un critère de platitude, dû à N. Bourbaki, plus fin que les critère énoncés dans (FFAC) en termes de Tor. Il peut être laissé en première lecture, d'autant plus que, dans certains cas d'utilisation ultérieure, nous ferons une démonstration directe.

I. Filtrations. Lemme d'Artin-Rees

1. Filtrations

Voici quelques définitions classiques d'algèbre topologique générale. Elles ne seront en fait utilisées que dans des cas particuliers.

Groupe topologique

Un groupe topologique est un espace topologique G *muni en outre d'une structure de groupe,* notée ici additivement, *compatible avec la topologie,* i.e. *telle que les applications* : $x \longmapsto -x$ de G *dans* G et $(x,y) \longmapsto x+y$ de $G\times G$, *muni de la topologie produit, dans* G *soient continues.*

On définit la catégorie des groupes topologiques en prenant pour morphismes les applications continues qui sont aussi des homomorphismes de groupes.

Anneau topologique

Un anneau topologique est un groupe topologique A *tel que l'application* $(x,y) \longmapsto xy$ *de* $G\times G$, *muni de la topologie produit, dans* G *soit continue.*

Module topologique

Soit A *un anneau topologique.*

Un A*-module topologique est un* A*-module* M *dont le groupe additif est topologique et tel que l'application* $(a,x) \longmapsto ax$ *de* $A\times M$, *muni de la topologique produit, dans* M *soit continue.*

On définit la catégorie des A-modules topologiques en prenant pour morphismes les applications qui sont à la fois continues et A-linéaires.

Les modules topologiques les plus utiles en algèbre commutative sont obtenus comme suit.

Soient A *un anneau,* a *un idéal,* A *un* A*-module.*

Si X et Y sont des parties de M, on note $X+Y$ l'ensemble $\{x+y/y\in Y,\ x\in X\}$. Si $x\in M$, $x+Y$ est $\{x+y/y\in Y\}$.

On définit sur M *une topologie invariante par translation en prenant comme système fondamental de voisinages de* $x\in M$ *l'ensemble des parties* $x+a^nM$, *où* n *parcourt* N. *On l'appelle la topologie* a*-adique.*

On vérifie que M est alors un module topologique.

Si $M=A$, on vérifie que A est muni d'une structure d'*anneau topologique*. Un A-module M devient alors un A*-module topologique.*

Les topologies a-adiques sont au moins a priori insuffisantes. Soit, en effet, N un sous-module de M. La topologie induite sur N par la topologie a-adique de M n'est pas forcément la topologie a-adique de N. Un système fondamental de voisinages de 0 de N dans cette topologie induite est donné par la *suite décroissante* $a^nM\cap N$ *de sous-modules de* N. Un système fondamental de voisinage d'un point de N s'en déduit par translation.

Définition

Soient A *un anneau,* M *un* A*-module. Une filtration* (décroissante) *de* M *est une suite décroissante* $(M_n)_{n\in N}$ *de sous-modules de* M.

Une telle filtration définit sur M une topologie invariante par translation qui munit M d'une structure de module topologique sur l'anneau A muni de la topologie discrète : un système fondamental de voisinages de $x\in M$ est l'ensemble des parties $x+M_n$ $(n\in N)$.

La filtration $(a^n M)_{n\in N}$, où a est un idéal de A, est appelée la *filtration a-adique* .

Les cas historiquement les plus importants sont ceux où $A = \mathbb{Z}$ et $a = (p)$, où p est un nombre premier, et $A = k[X_1,\ldots,X_n]$ et $a = (X_1,\ldots,X_n)$

Proposition 1.1 (*métrique définie par une filtration séparée*)

Soient A *un anneau, muni de la topologie discrète,* M *un* A*-module,* $(M_n)_{n\in N}$ *une filtration de* M.

1. La suite $(M_n)_{n\in N}$ *est un système fondamental de voisinages de* 0 *d'une topologie sur* M *invariante par translation et munissant* M *d'une structure de* A*-module topologique.*

2. L'adhérence d'une partie X *de* M *dans cette topologie est* $\bigcap_{n\in N} (X+M_n)$.

En particulier, l'espace topologique M *est séparé si et seulement si* $\bigcap_{n\in N} M_n = (0)$.

On dit alors que la filtration $(M_n)_{n\in N}$ *est séparée.*

3. Si la filtration $(M_n)_{n\in N}$ *est séparée, l'application* $d : M\times M \to R$ *définie par :*

$d(x,y) = 0$ *si* $x=y$

$d(x,y) = e^{-n}$, *où* e *est un nombre réel* > 1, *si* $x-y \in M_n$ *et* $x-y \notin M_{n+1}$ *est une distance sur* M.

Cette distance définit la topologie de M *qui est ainsi métrisable.*

Démonstration

On va se contenter de démontrer 2, laissant les autres points au lecteur.

Dire que x appartient à l'adhérence de X c'est dire que, pour tout $n \in N$, $(x+M_n) \cap X$ est non vide et donc que x appartient à $X+M_n$.

Dire que l'espace topologique M est séparé c'est dire, puisque la topologie est invariante par translation, que 0 est fermé.

L'exemple de la filtration a-adique sur l'anneau A et de la filtration induite sur le sous-module N d'un A-module M par la filtration a-adique de M conduit à la définition suivante.

Définition (*filtration compatible avec une filtration d'anneau*)

Une filtration $(a_n)_{n\in N}$ *du* A*-module* A *est dite filtration d'anneau si,*

$\forall\, m,n \in N,\ a_n\, a_m \subset a_{n+m}$

Une filtration $(M_n)_{n\in N}$ *d'un* A*-module* M *est alors dite compatible avec la filtration d'anneau* $(a_n)_{n\in N}$ *de* A *si,* $\forall m,n \in N$, $a_n M_n \subset M_{n+m}$.

Exemples : les filtrations a-adiques définis ci-dessus.

Proposition I.2

Une filtration d'anneau $(a_n)_{n\in N}$ *de* A *munit* A *d'une structure d'anneau topologique.*

Si alors $(M_n)_{n\in N}$ *est une filtration de* M *compatible avec la filtration d'anneau* $(a_n)_{n\in N}$ *de* A, $(M_n)_{n\in N}$ *munit* M *d'une structure de module topologique sur l'anneau topologique* A.

Démonstration

Elle résulte facilement des définitions.

Dans la plupart des problèmes portant sur des modules filtrés, on s'intéresse plus aux topologies définies par les filtrations qu'aux filtrations elles mêmes. La bonne notion de morphisme est donc celle d'application continue. La notion d'application compatible définie ci-dessous est souvent plus agréable. La proposition I.3. permet souvent de travailler avec les applications compatibles.

Définition

1. Soient A *un anneau,* M *un* A*-module,* $(M_n)_{n\in N}$ *et* $(M'_n)_{n\in N}$ *des filtrations de* M.

On dit que $(M'_n)_{n\in N}$ *est cofinale à* $(M_n)_{n\in N}$ *s'il existe une application croissante* $\theta : N \longrightarrow N$ *telle que* $\theta(n)$ *tende vers l'infini avec* n *et, que, pour tout* $n \in N$, $M'_n = M_{\theta(n)}$.

Il est clair que $(M'_n)_{n\in N}$ *et* $(M_n)_{n\in N}$ *définissent sur* M *la même topologie.*

2. Soient M *et* M' *des* A*-modules munis de filtrations* $(M_n)_{n\in N}$ *et* $(M'_n)_{n\in N}$, f *une application* A*-linéaire de* M *dans* M'.

On dit que f *est compatible* (avec les filtrations) *si, pour tout* $n \in N$, $f(M_n) \subset M'_n$.

Proposition I.3

Les notations sont celles de la définition 2, ci-dessus.

1. Si f *est compatible, elle est continue.*

2. Si f *est continue* non nécessairement compatible, *il existe sur* M *une filtration* $(N_n)_{n\in N}$ *cofinale à la filtration* $(M_n)_{n\in N}$ *telle que* f

soit compatible pour les filtrations $(N_n)_{n\in N}$ *et* $(M'_n)_{n\in N}$.

Démonstration

1. Résulte de ce que, pour tout $n\in N$, $f^{-1}(M'_n)$ contient M_n.

2. La continuité de f se traduit par l'existence, pour tout $n\in N$, d'un entier $\theta(n)$ tel que $f(M_{\theta(n)})$ soit contenu dans M'_n. On peut choisir θ *strictement* croissante de N dans N et poser $N_n = M_{\theta(n)}$.

2. Le lemme d'Artin-Rees

Le résultat qui suit, démontré indépendamment par E. Artin et D. Rees, donne une forme *quantitative* au résultat *qualitatif* suivant :

Soient A *un anneau noethérien, a un idéal de* A, M *un* A*-module de type fini,* N *un sous-module de* M. *La topologie sur* N *induite par la topologie a-adique de* M *est la topologie a-adique de* N.

Théorème 1.4 (lemme d'Artin-Rees)

Soient A *un anneau NOETHERIEN, a un idéal de* A, M *un* A*-module de TYPE FINI,* N *un sous-module.*

Il existe $r \in N$ *tel que, pour tout* $n \in N$ *supérieur à* r,

$$a^n M \cap N = a^{n-r}(a^r M \cap N)$$

Démonstration

On pose $N_n = a^n M \cap N$. Il est clair que $aN_n \subset N_{n+1}$.

Le lemme d'Artin-Rees implique les égalités $N_{n+1} = aN_n$ si $n \geqslant r$.

Ceci conduit à donner la définition suivante.

Définition

Soient A *un anneau, a un idéal de* A, M *un* A*-module,* $(M_n)_{n\in N}$ *une filtration de* M.

On dit que la filtration $(M_n)_{n\in N}$ *est a-admissible* (resp. *a-bonne*) *si, pour tout* $n\in N$, $aM_n \subset M_{n+1}$ (resp. $aM_n \subset M_{n+1}$ *et* $aM_n = M_{n+1}$ *pour* n *suffisamment grand*).

On peut traduire comme suit le fait que la filtration $(M_n)_{n\in N}$ est a-admissible :

Un élément du produit tensoriel $A[X] \underset{A}{\otimes} M$ s'écrit, *de manière unique,* $\Sigma_{n\in N} X^n \otimes m_n$ où $m_n \in M$ car $\{X^n\}_{n\in N}$ est une base du A-module $A[X]$. *On écrit, pour simplifier,* $\Sigma_{n\in N} m_n X^n$ *l'élément* $\Sigma_{n\in N} X^n \otimes m_n$ *et on note* $M[X]$ *le* $A[X]$*-module* $A[X] \underset{A}{\otimes} M$.

Soient A' *le sous-anneau de* $A[X]$ *égal à* $\Sigma_{n\in N} a^n X^n$ *(anneau de* Rees *du couple* (A,a)*),* M' *le sous-groupe additif* $\Sigma_{n\in N} X^n \otimes M_n$ *de* $M[X]$ *; un élément de* M' *s'écrit donc, de manière unique,* $\Sigma_{n\in N} m_n X^n$ *où* $m_x \in M_x$.

Lemme 1

Les assertions suivantes sont équivalentes :

(i) la filtration $(M_n)_{n\in N}$ *est a-admissible*

(ii) l'application $(\Sigma a_n X^n, \Sigma m_s X^s) \longmapsto \Sigma(a_n m_s)X^{n+s}$ *de* A'xM' *dans* $M[X]$ *applique* A'xM' *dans* M' *et munit donc* M' *d'une structure de* A'*-module*

Démonstration du lemme 1

Elle est évidente.

Il est également possible, sous hypothèse noethérienne, de traduire le fait que le filtration $(M_n)_{n\in N}$ est a-bonne.

Lemme 2

Soient A *un anneau noethérien,* a *un idéal de* A, M *un* A*-module de type fini,* $(M_n)_{n\in N}$ *une filtration* a*-admissible de* M.

Les assertions suivantes sont équivalentes :

(i) la filtration $(M_n)_{n\in N}$ *est* a*-bonne*

(ii) le A'*-module* M' (défini ci-dessus) *est de type fini*

Démonstration du lemme 2

(i) $\Longrightarrow$ (ii).

De l'égalité $M_n = a^{n-r}M_r$ pour $n \geqslant r$, on déduit $M_n X^n = (a^{n-r}X^{n-r})(M_r X^r)$

Il en résulte que le A'-module M' est engendré par l'ensemble $M_o + \ldots + M_r X^r$.

Si $(x_{i,j})_j$ est un système *fini* (puisque M est noethérien) de générateurs du A-module M_i, $(x_{i,j}X^i)_{i,j}$ $(i = 0,\ldots,r)$ est un système *fini* de générateurs de A'-module M'.

(ii) $\Longrightarrow$ (i).

Soit $(x_1,\ldots,x_u)$ un système fini de générateurs du A'-module M'.

Quitte à remplacer chaque x_i par l'ensemble fini de ses composantes homogènes non nulles, *on peut supposer* x_i *homogène,* i.e. de la forme $y_{d_i} X^{d_i}$. Soit $r = \mathrm{Sup}(d_i)$.

Soient $n \in N$ et $z_n \in M_n$. L'élément $z_n X^n$ de M' s'écrit $\Sigma_{i=1}^u b_i x_i$.

On suppose $n > r$. On va démontrer l'égalité $M_n = aM_{n-1}$.

Ecrivant chacun des éléments b_i $(i = 1,\dots,u)$ comme somme de ses composantes homogènes, on voit que l'on peut supposer b_i homogène de degré $n-d_i$, soit :

$$b_i = a_{n-d_i} X^{n-d_i} \quad \text{avec} \quad a_{n-d_i} \quad \text{dans} \quad a^{n-d_i}.$$

Soit $(\alpha_1,\dots,\alpha_r)$ un système *fini* de générateurs de l'idéal a. Alors, $a_{n-d_i} = \Sigma_{j=1}^{r} \alpha_j v_{ji}$ où v_{ji} appartient à a^{n-d_i-1}.

Alors, $z_n = \Sigma_{j=1}^{r} \alpha_j (\Sigma_{i=1}^{u} v_{ji} y_{d_i})$. Comme l'élément $v_{ji} y_{d_i}$ appartient à $a^{n-d_i-1} M_{d_i}$, il appartient à M_{n-1}, et z_n appartient à aM_{n-1}.

Par conséquent, pour $n > r$, $M_n = aM_{n-1}$ et la filtration $(M_n)_{n\in N}$ est a-bonne.

Fin de la démonstration du lemme d'Artin-Rees

L'anneau de Rees A' *est noethérien.* Il est, en effet, égal à $A[a_1X,\dots,a_rX]$, où $\{a_1,\dots,a_r\}$ désigne un système fini de générateurs de l'idéal a et est donc une algèbre *de type fini* sur l'anneau *noethérien* A.

La filtration $(a^nM)_{n\in N}$ est a-bonne. Le A'-module $M' = \Sigma_{n\in N}(a^nM)X^n$ est donc de type fini, ou, ce qui est équivalent, noethérien. Le sous-module $N' = \Sigma_{n\in N}(a^nM\cap N)X^n$ est de type fini et, par conséquent, la filtration $(a^nM\cap N)_{n\in N}$ de N est a-bonne.

Il existe donc $r \in N$ tel que, si $n \geqslant r$, $(a^nM\cap N) = a^{n-r}(a^rM\cap N)$: en effet, pour $n > r$, $a^nM\cap N = a(a^{n-1}M\cap N)$.

3. Applications du lemme d'Artin-Rees

Proposition 1.5

Soient A *un anneau noethérien,* a *un idéal de* A, M *un* A*-module de type fini,* N *un sous-module.*

La topologie induite sur N *par la topologie* a*-adique de* M *coïncide avec la topologie* a*-adique de* N.

Démonstration

L'inclusion évidente $a^nN \subset a^nM\cap N$ montre que la topologie a-adique de N est *plus fine* que la topologie induite par la topologie a-adique de M.

Il existe, d'autre part, $r \in N$ tel que, si $n \geqslant r$, $a^nM\cap N = a^{n-r}(a^rM\cap N) \subset a^{n-r}N$ et donc la topologie induite est plus fine que la topologie a-adique de N.

Proposition 1.6

Soient A *un anneau noethérien,* a *un idéal de* A, M *un* A*-module de type fini,* $N = \bigcap_{n\in\mathbb{N}} a^n M$ *l'adhérence de* (0) *dans* M *muni de la topologie* a*-adique.*

Alors $aN = N$ *et il existe* $x \in a$ *tel que* $(1-x)N = 0$.

Démonstration

Il est clair que $N = a^n M \cap N$. Il existe donc $r \in \mathbb{N}$ tel que, pour $n \geqslant r$, $N = a^{n-r}(a^r M \cap N)$.

On en déduit les inclusions $N \subset aN \subset N$ et l'égalité $N = aN$.

On utilise alors la *méthode du déterminant de* Krull : soit $(e_1,\ldots,e_s)$ un système fini de générateurs de N. On a des égalités :

$$e_i = \Sigma_{j=1}^{s} a_{ij}e_j \quad (i = 1,\ldots,s) \quad (a_{ij} \in a)$$

soit

$$\Sigma_{j=1}^{s} (\delta_{ij}-a_{ij})e_j = 0$$

d'où $\det(\delta_{ij}-a_{ij})e_k = 0$ $(k = 1,\ldots,s)$ et $\det(\delta_{ij}-a_{ij})N = 0$.

Il suffit alors de remarquer que $\det(\delta_{ij}-a_{ij})$ est de la forme $1-x$ où x appartient à a comme a_{ij}.

Corollaire 1

Soient A *un anneau noethérien,* a *un idéal contenu dans le radical de* A, M *un* A*-module de type fini.*

Tout sous-module de M *est fermé dans la topologie* a*-adique.*

En particulier, (0) *est fermé et donc la topologie* a*-adique de* M *est séparée.*

Démonstration

La topologie a-adique d'un module quotient M/M' est la topologie quotient de la topologie a-adique de M.

Pour démontrer que le sous-module M' de M est fermé, il suffit donc de démontrer que le sous-module (0) du module M/M' est fermé (dans la topologie a-adique).

Il suffit donc de démontrer la deuxième assertion, i.e. que le sous-module (0) de M est fermé. Or, l'adhérence N de (0) vérifie $(1-x)N = 0$ avec $x \in a$ et donc $1-x$ inversible. Il en résulte $N = 0$.

(On peut aussi utiliser $aN = N$ et le lemme de Nakayama, en fait redémontré dans la proposition).

Corollaire 2 (théorème d'intersection de Krull)

Soient A *un anneau noethérien,* a *un idéal de* A *contenu dans le radical.*

Alors $\bigcap_{n=0}^{\infty} a^n = (0)$.

Un cas particulier important est celui où A est un anneau local noethérien et a son idéal maximal.

Corollaire 3

Soient A *un anneau noethérien intègre,* a *un idéal de* A *distinct de* A.

Alors $\bigcap_{n=0}^{\infty} a^n = (0)$.

Démonstration

Il existe $x \in a$ et donc $\neq 1$ tel que $(1-x)(\bigcap_{n=0}^{\infty} a^n) = (0)$.

Le résultat provient de l'intégrité de A.

Proposition I.7

Soient A *un anneau noethérien,* a *un idéal de* A.

Les assertions suivantes sont équivalentes :

(i) a *est contenu dans le radical de* A

(ii) tout sous-module d'un A*-module de type fini est fermé pour la topologie* a*-adique*

(iii) tout idéal maximal de A *est fermé pour la topologie* a*-adique*

Démonstration

(i) $\Longrightarrow$ (ii) : c'est le corollaire 1 de la proposition I.6.

(ii) $\Longrightarrow$ (iii) : un idéal (maximal) est un sous-module du A-module de type fini A.

(iii) $\Longrightarrow$ (i) : on prouve (non i) $\Longrightarrow$ (non iii).

(non i) implique qu'il existe un idéal maximal m ne contenant pas a.

Pour tout $n \in N$, $m+a^n = A$ car m et a^n sont étrangers comme m et a.

Donc, l'adhérence de m dans A qui est $\bigcap_{n=0}^{\infty} (m+a^n)$ est égale à A et distincte de m.

Définition

Un anneau topologique noethérien A *est dit anneau de* Zariski *si sa topologie est une topologie* a*-adique pour un idéal* a *contenu dans le radical de* A.

Exemples

Un anneau local noethérien muni de sa filtration m-adique, où m est

son idéal maximal, est de Zariski.

Plus généralement, un anneau semi-local noethérien muni de la filtration m-adique, où m est le produit de ses idéaux maximaux, est de Zariski.

II. Complétion

Soient A un anneau noethérien, a un idéal de A. On suppose, pour simplifier, la filtration a-adique séparée. On a vu, dans le paragraphe précédent, des cas importants où ceci était réalisé, par exemple $A = \mathbb{Z}$, $a = (p)$ où p est un nombre premier, ou $A = k[X_1,\ldots,X_n]$, $a = (X_1,\ldots,X_n)$.

L'anneau A est alors un espace métrique. Son complété $\hat{A}$ est, en fait, muni d'une structure d'anneau en sorte que A s'identifie à un sous-anneau de $\hat{A}$.

Dans le premier exemple, $\hat{A}$ est l'anneau des entiers p-adiques. Dans le second, c'est l'anneau $k[[X_1,\ldots,X_n]]$ des séries formelles.

L'anneau $\hat{A}$ est souvent plus agréable que l'anneau A. Un procédé naturel consiste donc à travailler dans $\hat{A}$ puis à essayer de redescendre à A.

Voici un exemple géométrique simple suggérant l'intérêt d'une telle démarche.

Deux courbes algébriques planes Γ et Γ' de $\mathbb{C}^2$ passant par l'origine (0,0) sont dites *algébriquement équivalentes à l'origine* si les anneaux locaux de Γ et Γ' en ce point sont des $\mathbb{C}$-algèbres isomorphes.

Les courbes Γ *d'équation* $f(X,Y) = XY - (X+Y)(X^2+Y^2)$ *et* Γ' *d'équation* $XY = 0$ *ne sont pas algébriquement équivalentes à l'origine* : en effet, l'anneau local de l'origine sur Γ est intègre comme l'algèbre affine de Γ car $f(X,Y)$ est irréductible ; par contre, l'anneau local de l'origine sur Γ' n'est pas intègre.

On peut maintenant considérer Γ et Γ' non plus comme des courbes algébriques mais comme des *courbes analytiques* : ceci revient à considérer f et g comme des séries convergentes et à considérer sur Γ et Γ' non seulement les fonctions rationnelles mais aussi les fonctions analytiques.

Les anneaux de germes de fonctions analytiques à l'origine sur Γ et Γ' sont respectivement $A_{an} = \mathbb{C}\{\{X,Y\}\}/(f(X,Y))$ et $A'_{an} = \mathbb{C}\{\{X,Y\}\}/(g(X,Y)$, où $\mathbb{C}\{\{X,Y\}\}$ désigne l'anneau des séries convergentes, qui s'identifie, par le développement de Taylor, à l'anneau des germes de fonctions ana-

lytiques à l'origine de $\mathbb{C}^2$. Les anneaux A_{an} et A'_{an} sont $\mathbb{C}$-isomorphes, i.e., avec une définition naturelle, *les courbes* Γ *et* Γ' *sont analytiquement équivalentes à l'origine* : on vérifie, en effet, par calcul, que $f(X,Y) = (X+a(X,Y))(Y+b(X,Y))$ où $a(X,Y)$ et $b(X,Y)$ sont des séries formelles d'ordre 2 puis que ces séries sont convergentes.

L'application $\phi : (X,Y) \longmapsto (X+a(X,Y), Y+b(X,Y))$ est un automorphisme de la $\mathbb{C}$-algèbre $\mathbb{C}\{\{X,Y\}\}$ tel que $\phi(f(X,Y)) = g(X,Y)$. Elle définit, par passage au quotient, un isomorphisme de $\mathbb{C}$-algèbres de A_{an} sur A'_{an}.

La situation est donc plus simple analytiquement qu'algébriquement.

Un problème analogue se pose pour les courbes Γ et Γ' de mêmes équations mais considérées cette fois-ci comme courbes sur un *corps quelconque* k. La notion de série convergente n'a alors plus de sens en général. On doit la remplacer par celle de série formelle.

Les anneaux formels de l'origine sur Γ et Γ' sont, par définition, $k[[X,Y]]/(f(X,Y))$ et $k[[X,Y]]/(g(X,Y))$. Ils sont les complétés respectifs des anneaux locaux des courbes *algébriques* Γ et Γ'. La validité d'un théorème de la fonction réciproque formel (plus simple à démontrer que le théorème analytique) implique que ces anneaux formels sont des k-algèbres isomorphes. On dit que Γ et Γ' sont *formellement équivalentes à l'origine.*

1. Séparé complété d'un module filtré

On va rappeler, à propos des modules filtrés, des définitions classiques sur les espaces métriques. Le lecteur habitué à ces définitions pourra passer rapidement sur ce paragraphe. Le cas le plus important est celui des filtrations a-adiques traité dans le paragraphe suivant.

Définition

Soient A *un anneau,* M *un* A*-module filtré par une filtration* $(M_n)_{n\in N}$, $(x_n)_{n\in N}$ *une suite d'éléments de* M, x *un élément de* M.

1. On dit que $(x_n)_{n\in N}$ *converge vers* x, qui est alors appelé *une limite de la suite, si,* $\forall n \in N$, *il existe* $r(n) \in N$ *tel que* $m \in N$ *et* $m \geqslant r(n)$ *implique* $x - x_m \in M_n$.

2. On dit que $(x_n)_{n\in N}$ *est une suite de Cauchy si* $\forall n \in N$, *il existe* $s(n) \in N$ *tel que* $m,m' \geqslant s(n) \Longrightarrow x_m - x_{m'} \in M_n$.

Une suite convergente est une suite de Cauchy.

3. Si la réciproque est vraie, on dit que le A-module filtré M est complet

Si la suite $(x_n)_{n\in N}$ converge vers x, les assertions suivantes sont équivalentes pour un élément $y \in M$:

(i) y est limite de $(x_n)_{n\in N}$

(ii) y-x appartient à $\bigcap_{n\in N} M_n$

En particulier, *si le A-module filtré M est séparé, une suite* $(x_n)_{n\in N}$ *d'éléments de M ne peut converger que vers une seule limite.*

Si le A-module filtré M est séparé et complet, on dit qu'il est *séparé complet.*

Notations

L'ensemble $C(M)$ des suites de Cauchy de M est un sous-module du A-module produit M^N.

L'ensemble $N(M)$ des suites qui convergent vers un élément de $\bigcap_{n\in N} M_n$ est un sous-module de $C(M)$.

On note $\hat{M}$ le A-module quotient $C(M)/N(M)$ et α_M l'application A-linéaire qui à $x\in M$ associe la classe modulo $N(M)$ de la suite de Cauchy $(x_n)_{n\in N}$ avec $x_n = x$ pour tout $n \in N$.

Si M est séparé, $N(M)$ est l'ensemble des suites qui convergent vers 0. Il en résulte que α_M *est injective.*

Si M est complet, α_M est surjective : soient, en effet, $\hat{x} \in \hat{M}$, $(x_n)_{n\in N}$ une suite de Cauchy représentant $\hat{x}$, y une limite de $(x_n)_{n\in N}$ dans M. Alors, $\hat{x} = \alpha_M(y)$.

Ainsi, *si le A-module filtré M est séparé complet,* α_M *est un isomorphisme.*

On démontrera plus loin que la réciproque est vraie.

Foncteur complétion

Proposition II.1

Soient M et M' des modules filtrés, f une application A-linéaire de M dans M'.

1. Les assertions suivantes sont équivalentes :

(i) f est continue en 0

(ii) f est continue

(iii) f est uniformément continue, i.e. $\forall n\in N$, *il existe* $t(n) \in N$ tel que $x,x' \in M_{t(n)}$ *implique* $f(x) - f(x') \in M'_n$.

2. Si elles sont vérifiées, $f(C(M))$ *est contenu dans* $C(M')$, *si*

$(x_n)_{n\in N}$ *converge vers* x, $(f(x_n))_{n\in N}$ *converge* $f(x)$ *et* $f(N(M))$ *est contenu dans* $N(M')$.

Démonstration

1. Est classique et résulte immédiatement des définitions.

2. Soit $n\in N$. Il existe $r(n) \in N$ tel que $x-y \in M_{r(n)} \Longrightarrow f(x)-f(y) \in M'_n$ (continuité uniforme). Si $(x_n)_{n\in N}$ est une suite de Cauchy de M, il existe $s(n) \in N$ tel que $m,m' \geqslant s(n) \Longrightarrow x_m - x_{m'} \in M_{r(n)}$. Si donc $m,m' \geqslant s(n)$, $f(x_m) - f(x_{m'}) \in M'_n$. La suite $(f(x_n))_{n\in N}$ est une suite de Cauchy. Ainsi $f(C(M)) \subset C(M')$.

Si la suite de Cauchy $(x_n)_{n\in N}$ converge vers $x\in M$, il existe $s(n) \in N$ tel que $m \geqslant s(n) \Longrightarrow x_m - x \in M_{r(n)}$ (avec les notations ci-dessus) et donc $f(x_m) - f(x) \in M'_n$. La suite de Cauchy $(f(x_n))_{n\in N}$ converge donc vers $f(x)$.

Comme, avec les notation ci-dessus, $f^{-1}(M'_n) \supset M_{r(n)}$, $\bigcap_{n\in N} f^{-1}(M'_n) = f^{-1}(\bigcap_{n\in N} M'_n)$ contient $\bigcap_{n\in N} M_{r(n)}$ et donc, a fortiori, $\bigcap_{n\in N} M_n$. Par conséquent, $\bigcap_{n\in N} M'_n$ contient $f(\bigcap_{n\in N} M_n)$. Il en résulte que $f(N(M))$ est contenu dans $N(M')$.

Corollaire

Avec les notations de la proposition II.1, l'application continue f *définit par passage au quotient, une application* A*-linéaire* f *de* $\hat{M} = C(M)/N(M)$ *dans* $\hat{M}' = C(M')/N(M')$.

Les applications : $M \longmapsto \hat{M}$, $f \longmapsto \hat{f}$ *définissent un foncteur additif covariant de la catégorie des* A*-modules filtrés et applications linéaires continues dans* Mod(A).

Les applications (α_M) *définissent un morphisme fonctoriel du foncteur identique de la catégorie des modules filtrés dans ce foncteur* $\hat{}$.

Démonstration

Les vérifications sont immédiates. Si f est une application linéaire continue du A-module filtré M dans le A-module filtré M', le diagramme

$$\begin{array}{ccc} M & \xrightarrow{f} & M' \\ {\scriptstyle \alpha_M}\downarrow & & \downarrow{\scriptstyle \alpha_{M'}} \\ \hat{M} & \xrightarrow[\hat{f}]{} & \hat{M}' \end{array}$$

est commutatif : à la classe de la suite de Cauchy dont les termes sont tous égaux à $x \in M$, $\hat{f}$ fait correspondre la classe de la suite de Cauchy dont tous les termes sont égaux à $f(x)$.

Proposition II.2

Soit $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ *une suite exacte de* Mod(A), *où* M *est filtré par une filtration* $(M_n)_{n\in N}$, M' *est muni de la filtration induite* $(f^{-1}(M_n))_{n\in N}$ *et* M'' *de la filtration quotient* $(g(M_n))_{n\in N}$.

La suite $0 \longrightarrow \hat{M}' \xrightarrow{\hat{f}} \hat{M} \xrightarrow{\hat{g}} \hat{M}'' \longrightarrow 0$ *est exacte.*

Démonstration

L'injectivité de $\hat{f}$ résulte de l'égalité $C(M') \cap N(M) = N(M')$: une suite d'éléments de M' tend vers 0 dans M' si et seulement si elle tend vers 0 dans M.

Comme le foncteur $\hat{}$ est additif, $\hat{g} \circ \hat{f} = 0$ et donc $\mathrm{im}(\hat{f}) \subset \ker(\hat{g})$.

Soit $\hat{x} \in \ker(\hat{g})$. Si $(x_n)_{n\in N}$ est une suite de Cauchy représentant $\hat{x}$, il existe une fonction *croissante* $\theta : N \longrightarrow N$ telle que, pour tout $n \in N$ $g(x_n) \in M''_{\theta(n)}$ et donc, $y_n \in M_{\theta(n)}$ tel que $g(x_n - y_n) = 0$. Enfin, il existe $x'_n \in M'$ telle que $x_n = f(x'_n) + y_n$.

La suite (x'_n) appartient à $C(M')$. La suite (y_n) appartient à $N(M)$. Par conséquent, $\hat{x} = \hat{f}(\hat{x}')$ où $\hat{x}'$ désigne la classe de (x'_n) et $\hat{x} \in \mathrm{im}(\hat{f})$.

Soient $\hat{x}'' \in \hat{M}''$ et $(x''_n)_{n\in N}$ un représentant dans $C(M'')$. Si $x_n \in M$ est tel que $x''_n = g(x_n)$, $(x_n)_{n\in N}$ appartient à $C(M)$: si $n \in N$, soit $m \in N$ tel que $q,q' \geqslant m \Longrightarrow x''_q - x''_{q'} \in M''_n$.

Alors, $q,q' \geqslant m$ implique $x_q - x_{q'} \in M_n$. Si $\hat{x}$ est la classe de $(x_n)_{n\in N}$, $\hat{x}'' = \hat{g}(\hat{x})$. Donc $\hat{g}$ est surjective.

Proposition II.3

Les notations sont celles de la proposition II.2.

1. Si le sous-module M' *est fermé, le module filtré* M'' *est séparé.*

2. Si le module M *est complet, il en est de même du module* M''.

Démonstration

1. Est clair.

2. Soit $(x''_n)_{n\in N}$ une suite de Cauchy de M'' et soit $x_n \in M_n$ tel que $x''_n = g(x_n)$.

La suite $(x''_{n+1} - x''_n)_{n\in N}$ converge vers 0. Il existe donc une application *croissante* $\theta : N \longrightarrow N$ telle que, pour tout $n \in N$, $x''_{n+1} - x''_n$ appartienne à $M''_{\theta(n)}$. Donc, $x_{n+1} - x_n = a_n - b'_n$ où $a_n \in M_{\theta(n)}$ et $b'_n \in M'$. Soit y_n l'élément $x_n + \sum_{i=0}^{n-1} b'_i$. Alors, $g(y_n) = x''_n$ et la suite $(y_n)_{n\in N}$ est de Cauchy. Soit y une limite de la suite $(y_n)_{n\in N}$ dans M qui est complet. Comme g est continue, g(y) est une limite de $(x''_n)_{n\in N}$ dans M''.

Une filtration naturelle sur $\hat{M}$

Soit M *un* A*-module muni d'une filtration* $(M_n)_{n\in N}$.

Il résulte de la proposition II.2 que, pour tout $n\in N$, la complété $\hat{M}_n$ du A-module M_n muni de la filtration induite $(M_m)_{m\in N}$ s'identifie à un sous-module de $\hat{M}$.

On munit dans la suite le A*-module* $\hat{M}$ *de la filtration* $(\hat{M}_n)_{n\in N}$.

Proposition II.4

Soient M *un* A*-module d'une filtration* $(M_n)_{n\in N}$, $\hat{M}$ *complété.*

1. Le A*-module filtré* $\hat{M}$ *est séparé complet.*

2. $\alpha_M(M)$ *est dense dans* $\hat{M}$.

3. Soit $f : M \longrightarrow M'$ *une application continue de modules filtrés. L'application* $\hat{f}: \hat{M} \longrightarrow \hat{M}'$ *est continue.*

Démonstration

1. La filtration $(\hat{M}_n)$ est séparée : un représentant $(x_n)_{n\in N}$ dans $C(M)$ d'un élément $\hat{x} \in \bigcap_{n\in N} \hat{M}_n$ est un élément de $N(M)$ puisque, pour tout $n\in N$, x_n appartient à $\bigcap_{m\in N} M_m$. Donc, $\hat{x}= 0$.

Le A-module filtré M est complet : Soit $(\hat{x}_n)_{n\in N}$ une suite de Cauchy de $\hat{M}$. Pour tout $n\in N$, il existe $u_n \in M$ tel que $\hat{x}_n - \alpha_M(u_n)$ appartienne à $\hat{M}_n$: si $(x_{n,m})_{m\in N}$ est représentant de $\hat{x}_n$ dans $C(M)$, on choisit $r(n) \geqslant n$ tel que $m \geqslant r(n)$ implique $x_{n,m}-x_{n,r(n)} \in M_n$ et on prend $u_n = x_{n,r(n)}$. La suite $(u_n)_{n\in N}$ est une suite de Cauchy de M : l'entier n étant donné, on choisit $s(n) \in N$ tel que $s(n) \geqslant r(n)$ et $q,q' \geqslant s(n) \Longrightarrow \hat{x}_q - \hat{x}_{q'} \in \hat{M}_n$. Alors, $\hat{x}_q - \alpha_M(u_q) \in \hat{M}_q$, $\hat{x}_{q'} - \alpha_M(u_{q'}) \in \hat{M}_q$, et, donc, $\alpha_M(u_q)-\alpha_M(u_{q'}) \in \hat{M}_n$, d'où $u_q-u_{q'} \in M_n$. Soit $\hat{u}$ la classe modulo $N(M)$ de la suite $(u_n)_{n\in N}$. La suite $(\hat{x}_n)_{n\in N}$ converge vers $\hat{u}$: si $q = s(n)$, $x_{q,m}-u_q \in M_q$ pour m grand et $u_m-u_q \in M_n$. Donc, $x_{q,m}-u_m \in M_n$ et $\hat{x}_q-\hat{u} \in \hat{M}_n$. Donc si $q' \geqslant s(u)$, $\hat{x}_{q'} - \hat{u} \in \hat{M}_n$.

2. Soient $\xi \in \hat{M}, (x_n)_{n\in N}$ une suite de Cauchy représentant ξ. Il existe $r\in N$ tel que $m,m' \geqslant r$ impliquent $x_m-x_{m'} \in M_n$. Alors, $\xi-\alpha_M(x_r)$ appartient à $\hat{M}_n$.

3. Il suffit de remarquer que, f étant continue, pour tout $n\in N$, il existe $m\in N$ tel que $f^{-1}(M'_n)$ contienne M_n. Alors, $\hat{f}^{-1}(\hat{M}'_n)$ contient $\hat{M}_m$: car, un élément de $\hat{M}_m$ admet comme représentant une suite de Cauchy $(x_p)_{p\in N}$ où, pour tout $p\in N$, $x_p \in M_n$. Pour tout $p\in N$, $x_p \in f^{-1}(M'_n)$;

$f(x_p) \in M'_n$ et $\hat{f}(\hat{x})$, qui est de la classe de $(f(x_p))_{p\in N}$ appartient à $\hat{M}'_n$, ou encore $\hat{x}$ appartient à $\hat{f}^{-1}(\hat{M}'_n)$.

Ainsi, *le foncteur* $\hat{}$ *est un foncteur de la catégorie des modules filtrés et applications linéaires continues dans la sous-catégorie pleine des modules filtrés séparés complets. On apelle* $\hat{}$ *le foncteur complétion et, si* M *est un module filtré,* $\hat{M}$ *le séparé complété de* M.

Proposition II.5

Soit M *un* A*-module filtré par une filtration* $(M_n)_{n\in N}$.

1. $\alpha_M^{-1}(\hat{M}_n) = M_n$.

2. $\hat{M}_n$ *est l'adhérence dans* $\hat{M}$ *de* $\alpha_M(M_n)$.

3. α_M *définit, par passage au quotient, un isomorphisme de* M/M_n *sur* $\hat{M}/\hat{M}_n$.

Démonstration

1. Soit $x\in M$. Dire que x appartient à $\alpha_M^{-1}(\hat{M}_n)$ c'est dire que la classe modulo $\mathcal{N}(N)$ de la suite de Cauchy $(x_p)_{p\in N}$, où pour tout $p\in N$, $x_p = x$, appartient à $\hat{M}_n$; c'est donc dire que x appartient à M_n.

2. Le complémentaire du sous-module ouvert $\hat{M}_n$, qui est réunion de classes modulo $\hat{M}_n$ homéomorphes à $\hat{M}_n$, est ouvert et donc $\hat{M}_n$ est fermé. D'autre part, $\alpha_M(M_n)$ est dense dans $\hat{M}_n$.

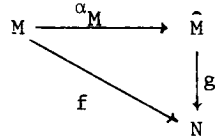
3. Il résulte de 1. que α_M définit, par passage au quotient, une application linéaire *injective*. Elle est *surjective* : soient $\xi \in \hat{M}/\hat{M}_n$, $\hat{x}$ un représentant dans $\hat{M}$, $(x_p)_{p\in N}$ un représentant de $\hat{x}$ dans $\mathcal{C}(M)$. Soit $m\in N$ tel que $p,p' \geqslant m \Longrightarrow x_p - x_{p'} \in M_n$.

Il est clair que, si l'on pose $y_p = x_p$ pour $p \leqslant m$ et $y_p = x_m$ pour $p \geqslant m$, $(y_p)_{p\in N}$ est un élément de $\mathcal{C}(M)$ et que la classe y de $(y_p)_{p\in N}$ est telle que $\hat{y} - \hat{x}$ appartienne à $\hat{M}_n$ et donc que $\hat{y}$ est un représentant de ξ. Or, $\hat{y}$ est visiblement $\alpha_M(x_m)$.

Théorème II.6 (*propriété universelle du séparé complété*)

Soient M *un* A*-module filtré,* N *un* A*-module filtré séparé complet,* f *une application linéaire continue de* M *dans* N.

Il existe une application linéaire continue g *et une seule de* $\hat{M}$ *dans* N *telle que le diagramme*



soit commutatif.

Démonstration

Unicité

Soient $\hat{x} \in \hat{M}$, $(x_n)_{n\in N}$ une suite de Cauchy représentant $\hat{x}$. Alors $\alpha_M(x_n)$ converge vers $\hat{x}$ quand n tend vers l'infini. Comme g est continue, $g(\alpha_M(x_n))$ converge vers $g(\hat{x})$. Donc, $g(\hat{x})$ est *la* limite de la suite de Cauchy $(f(x_n))_{n\in N}$ de N.

Existence

Il suffit de démontrer que l'application $g : \hat{M} \longrightarrow N$ telle que $g(\hat{x})$ = limite de $(f(x_n))_{n\in N}$ où $(x_n)_{n\in N}$ est une suite de Cauchy de M représentant $\hat{x}$ est bien définie (Ceci est laissé au soin du lecteur) et qu'elle est continue.

On peut procéder autrement, remarquant que α_N est un isomorphisme et que l'application $\alpha_N^{-1} \circ \hat{f}$ répond à la question.

Corollaire

Le foncteur $\hat{-}$ *est adjoint à gauche du foncteur inclusion de la sous-catégorie pleine de la catégorie des modules filtrés dont les objets sont les modules filtrés séparés complets.*

Démonstration

Elle est purement formelle et laissée au soin du lecteur. ((FFFAC), chap.1.I.§6).

On a un isomorphisme fonctoriel en le module filtré M et le module filtré séparé complet N : $\Phi_{M,N} : g \longmapsto g\circ\alpha_M$ de $\mathrm{Hom}_{\hat{C}}(\hat{M},N)$ sur $\mathrm{Hom}_C(M,N)$ où C (resp. $\hat{C}$) désigne la catégorie des modules filtrés (resp. filtrés séparés complets).

Remarque

Il est facile de démontrer que le foncteur inclusion de la sous-catégorie pleine C^s *de* C *dont les objets sont les modules séparés admet un adjoint à gauche.*

Si M est un module muni d'une filtration $(M_n)_{n\in N}$, on note M^s le module $M/\bigcap_{n\in N} M_n$ muni de la filtration quotient et p_M la surjection canonique de M sur M^s.

Il est clair que, pour toute application linéaire continue f de M dans un module filtré séparé N, il existe une unique application linéaire continue g de M^s dans N telle que $f = g\circ p_M$.

2. Cas des filtrations a-adiques

Soient A *un anneau, a un idéal de* A.

On munit les A*-modules de la filtration a-adique.*

Soient M *et* M' *des* A*-modules,* f *une application* A*-linéaire de* M *dans* M'.

L'application f est compatible car pour tout $n \in N$, $f(a^n M) \subset a^n M'$. Elle est donc *continue.*

Soient M *un* A*-module,* $\hat{M}$ *son complété,* $\hat{A}$ *le complété du* A*-module* A.

Si $(x_n)_{n\in N} \in C(M)$, $(a_n)_{n\in N} \in C(A)$, $(a_n x_n)_{n\in N}$ appartient à $C(M)$:

En effet, $a_m x_m - a_{m'} x_{m'} = a_m(x_m - x_{m'}) + x_{m'}(a_m - a_{m'})$ appartient à $a^n M$ pour n grand puisque $x_m - x_{m'}$ appartient alors à $a^n M$ et $a_m - a_{m'}$ appartient à a^n.

Si $(x_n)_{n\in N} \in N(M)$ et $(a_n)_{n\in N} \in N(A)$, $(a_n x_n)_{n\in N}$ appartient à $N(M)$.

On définit donc une application $\hat{A}\times\hat{M} \longrightarrow \hat{M}$ qui à $(\hat{a},\hat{x})$ fait correspondre, si $(a_n)_{n\in N}$ (resp. $(x_n)_{n\in N}$) est un représentant de $\hat{a}$ (resp. $\hat{x}$), la classe modulo $N(M)$ de la suite $(a_n x_n)_{n\in N}$, classe notée $\hat{a}\hat{x}$.

On laisse au lecteur le soin de vérifier que $\hat{M}$ *est ainsi muni d'une structure de* $\hat{A}$*-module et qu'en particulier,* $\hat{A}$ *est muni d'une structure d'anneau. L'application* $\alpha_A : A \longrightarrow \hat{A}$ *est un homomorphisme d'anneaux* et munit donc $\hat{A}$ d'une structure de A-algèbre .

Voici quelques propriétés du complété.

Lemme 1

Si le A*-module* M *est de type fini, son séparé complété* $\hat{M}$ *de* M *est un* $\hat{A}$*-module de type fini.*

Démonstration

De la suite exacte $A^n \longrightarrow M \longrightarrow 0$, on déduit la suite exacte de $\hat{A}$-modules $(\widehat{A^n}) \longrightarrow \hat{M} \longrightarrow 0$. Il suffit alors de remarquer que $(\widehat{A^n})$ est isomorphe à $\hat{A}^n$.

Lemme 2

Soit N *un* $\hat{A}$*-module de type fini.*

Alors, le A*-module* $(\alpha_A)_*(N)$ *est complet, pour la filtration a-adique*

Démonstration

Comme N est quotient d'un $\hat{A}$-module $(\hat{A})^n$, $(\alpha_A)_*(N)$ est quotient du A-module $(\alpha_A)_*(\hat{A})^n$.

Compte tenu de la proposition II.3, il suffit de démontrer que

$(\alpha_A)_*(\hat{A})^n$ est complet et donc que $(\alpha_A)_*(\hat{A})$ est complet. C'est la proposition II.4.

Lemme 3

Soient A *un anneau noethérien, a un idéal de* A, M *un* A*-module de type fini.*

1. La filtration a-adique de M' *est cofinale à la filtration induite sur* M' *par la filtration a-adique de* M.

2. Le séparé complété a-adique de M' *coïncide avec le séparé complété de* M' *dans la filtration induite par la filtration a-adique de* M.

Démonstration

1. Le lemme d'Artin-Rees implique l'existence de $r \in N$ tel que, pour tout $n \geqslant r$, $a^n M \cap M' = a^{n-r}(a^r M \cap M')$. On a donc les inclusions $a^n M' \subset a^n M \cap M' \subset a^{n-r} M'$.

2. Il est clair que, les modules $C(M')$ et $N(M')$ correspondants à des filtrations cofinales sont identiques.

Théorème II.7

Soient A *un anneau noethérien, a un idéal de* A, $\hat{A}$ *son séparé complété a-adique.*

Il existe un isomorphisme fonctoriel du foncteur $\hat{A} \underset{A}{\otimes} -$ *de la catégorie des* A*-modules de type fini dans la catégorie des* $\hat{A}$*-modules de type fini, dans le foncteur* $\hat{-}$. *Cet isomorphisme fonctoriel est défini par l'application* $\lambda_M = \hat{A} \underset{A}{\otimes} M \longrightarrow \hat{M}$ *telle que* $\lambda_M(\hat{a} \otimes x) = \hat{a}\alpha_M(x)$.

Démonstration

Soit $\chi_{M,N}$ l'isomorphisme, fonctoriel, en le A-module de type fini M et le $\hat{A}$-module de type fini N, de $\mathrm{Hom}_{\hat{A}}(\hat{A} \underset{A}{\otimes} M, N)$ sur $\mathrm{Hom}_{\hat{A}}(\hat{M}, N)$ composé de l'isomorphisme :

$$\psi_{M,N} : (f : \hat{A} \underset{A}{\otimes} M \longrightarrow N) \longrightarrow (g : M \longrightarrow (\alpha_A)_*(N)) \text{ où } g(x) = f(1 \otimes x)$$

de $\mathrm{Hom}_{\hat{A}}(\hat{A} \underset{A}{\otimes} M, N)$ dans $\mathrm{Hom}_A(M, (\alpha_A)_*(N))$ ((FFAC) chap. 4, Théorème I.5) et de l'isomorphisme fonctoriel $\Phi_{M,N} : g \longrightarrow h : \hat{M} \longrightarrow N$ tel que $g = h \circ \alpha_M$ de $\mathrm{Hom}_A(M, (\alpha_A)_*(N))$ sur $\mathrm{Hom}_{\hat{A}}(\hat{M}, N)$.

En vertu du lemme de Yoneda, l'isomorphisme fonctoriel $\chi_{M,N}$ est $(\mathrm{Hom}_{\hat{A}}(\lambda_M, N))$ où λ_M est l'isomorphisme $\chi_{M,N}(1_{\hat{A} \underset{A}{\otimes} M})$ de $\hat{A} \underset{A}{\otimes} M$ sur $\hat{M}$.

Cet isomorphisme λ_M est tel que $\lambda_M(\hat{a} \otimes x) = \hat{a}\alpha_M(x)$.

Corollaire 1

Le A-module $\hat{A}$ est plat.

Démonstration

Soit $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ une suite exacte de A-modules de type fini.

On a un diagramme commutatif :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \hat{A} \underset{A}{\otimes} M' & \xrightarrow{\hat{A}\otimes f} & \hat{A} \underset{A}{\otimes} M & \xrightarrow{\hat{A}\otimes g} & \hat{A} \underset{A}{\otimes} M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \lambda_{M'}} & & \downarrow{\scriptstyle \lambda_{M}} & & \downarrow{\scriptstyle \lambda_{M''}} & & \\ 0 & \longrightarrow & \hat{M}' & \xrightarrow[\hat{f}]{} & \hat{M} & \xrightarrow[\hat{g}]{} & \hat{M}'' & \longrightarrow & 0 \end{array}$$

dont la ligne inférieure est exacte (proposition II.2). Il en est donc, puisque les flèches verticales sont des isomorphismes, de même de la ligne supérieure.

Le foncteur $\hat{A} \underset{A}{\otimes} -$ est donc exact sur la catégorie des A-*modules de type fini.*

Il en résulte qu'il est exact. En effet, $\mathrm{Tor}_1^A(\hat{A},N) = 0$ pour tout A-module de type fini N (utiliser une suite exacte $0 \longrightarrow R \longrightarrow L \longrightarrow N \longrightarrow 0$ où L est libre de type fini) et donc, puisque Tor commute aux limites inductives filtrantes pour tout A-module N.

Corollaire 2

Soient A un anneau noethérien, a un idéal de A, M un A-module de type fini, $\hat{M}$ son complété a-adique.

Pour tout $n \in N$, $(\widehat{a^n M}) = a^n \hat{M}$.

En particulier, $(\widehat{a^n}) = a^n \hat{A}$.

Démonstration

On remarque que $\lambda_{a^n M}$ est un isomorphisme de $\hat{A} \underset{A}{\otimes} (a^n M)$ sur $(\widehat{a^n M})$. Donc, $(\widehat{a^n M})$ est l'image de l'homorphisme naturel de $\hat{A} \underset{A}{\otimes} (a^n M)$ dans $\hat{M}$. Comme $a^n M$ est l'image de l'homorphisme naturel de $a^n \underset{A}{\otimes} M$, dans M , $(\widehat{a^n M})$ est l'image de l'homomorphisme naturel de $a^n \underset{A}{\otimes} \hat{A} \underset{A}{\otimes} M$ dans $\hat{M}$ et donc de l'homorphisme naturel de $a^n \underset{A}{\otimes} \hat{M}$ dans $\hat{M}$. C'est donc $a^n \hat{M}$.

Ainsi, *la filtration naturelle sur le complété a-adique $\hat{M}$ du A-module de type fini M est la topologie $a\hat{A}$-adique.*

On laisse au lecteur le soin d'énoncer les propriétés formelles résultant de la platitude de $\hat{A}$, analogues à celles des corollaires 2 et 3 de la proposition II.5, du chapitre 1.

La proposition suivante donne une condition nécessaire et suffisante pour que le A-module $\hat{A}$ soit fidèlement plat.

Proposition II.8

Soient A *un anneau noethérien, a un idéal de* A, $\hat{A}$ *le séparé complété de* A *dans la filtration a-adique.*

Les assertions suivantes sont équivalentes :

(i) $\hat{A}$ *est fidèlement plat sur* A

(ii) a est contenu dans le radical de A (i.e. A *muni de la topologie a-adique est un anneau de* Zariski).

Démonstration

(i) $\Longrightarrow$ (ii). On va utiliser le lemme suivant.

Lemme

Soient A *un anneau, a un idéal de* A *(non nécessairement noethérien). Si* A *est séparé et complet dans la topologie a-adique, a est contenu dans le radical* $r(A)$ *de* A.

Démonstration du lemme

Il suffit de démontrer que, pour tout $x \in a$, $1-x$ est inversible. Soit $x_n = 1 + \ldots + x^n$.

La suite $(x_n)_{n\in N}$ est de Cauchy et converge donc vers un élément y de A.

Comme $(1-x)x_n = 1-x^{n+1}$, *la* limite de la suite $((1-x)x_n)_{n\in N}$ est 1. Cet limite est $(1-x)y$. Donc $(1-x)y = 1$ et $1-x$ est inversible.

Comme $\hat{A}$ est fidèlement plat sur A, $r(\hat{A}) \cap A$ est contenu dans $r(A)$: tout idéal maximal de A est, en effet, trace sur A d'un idéal maximal de $\hat{A}$ ((FFAC).chap. 5. proposition III.7). L'anneau $\hat{A}$ est séparé complet dans la filtration $a\hat{A}$-adique.

En vertu du lemme $r(\hat{A})$ contient $a\hat{A}$. Donc, $r(A) \supset r(\hat{A}) \cap A \supset a\hat{A} \cap A = a$ ((FFAC). Idem).

(ii) $\Longrightarrow$ (i).

Si a est contenu dans $r(A)$, tout A-module de type fini M est séparé (corollaire 1 de la proposition I.6). L'application $\alpha_M : M \longrightarrow \hat{M}$ est donc injective. Par conséquent, l'égalité $\hat{A} \underset{A}{\otimes} M = 0$ implique $M = 0$ et $\hat{A}$ est fidèlement plat sur A.

Corollaire

Soient A *un anneau noethérien,* K *son anneau total des fractions, a un idéal de* A *contenu dans le radical de* A, $\hat{A}$ *le complété a-adique de* A.

Alors, K *est contenu dans l'anneau total des fractions de* $\hat{A}$ *et* $K \cap \hat{A} = A$.

Démonstration

Un élément régulier de A est régulier dans $\hat{A}$, par platitude de $\hat{A}$ sur A.

Soient $y/x \in K \cap \hat{A}$, où x,y A et x est régulier dans A. Alors $y \in x\hat{A} \cap A = xA$ et donc, y/x appartient à A.

Séparé complété d'un anneau local

Proposition II.9

Soient A *un anneau local, non nécessairement noethérien,* m *son idéal maximal,* k *son corps résiduel.*

Le séparé complété $\hat{A}$ *de* A *est local d'idéal maximal* $\hat{m}$ *et de corps résiduel* k.

Si, de plus, A *est noethérien,* $\hat{m} = m\hat{A}$.

Démonstration

De l'isomorphisme $A/m \simeq \hat{A}/\hat{m}$ résulte que $\hat{m}$ est un idéal maximal de $\hat{A}$.

Comme $\hat{A}$ est séparé complet dans la topologie $\hat{m}$-adique, il résulte du lemme de la proposition II.8 que $\hat{m}$ est contenu dans le radical de $\hat{A}$. Donc, $\hat{m}$ est l'unique idéal maximal de $\hat{A}$.

Si A est noethérien, l'égalité $\hat{m} = m\hat{A}$ est un cas particulier du corollaire 2 du théorème II.7.

On démontrera plus loin que si l'anneau A est noethérien, il en est de même de $\hat{A}$.

3. Utilisation des limites projectives

On peut interpréter le séparé complété d'un module filtré en termes de limites projectives et déduire certaines propriétés de ce séparé complété de propriétés correspondantes des limites projectives

Cette interprétation est particulièrement commode par utilisation de la propriété d'associativité des limites projectives.

Soient M *un* A*-module,* $(M_n)_{n \in N}$ *une filtration de* M.

On désigne par ϕ_n^M la surjection canonique de M sur M/M_n et si, $m \geqslant n$,

par ϕ^M_{nm} la surjection canonique de M/M_m sur M/M_n.

Le système $(M/M_n, \phi^M_{nm})_{n,m\in N}$ est projectif. *Soit* $\phi^M = \varprojlim(\phi^M_n)$. Donc, ϕ^M est l'application A-linéaire : $x \longmapsto (\phi^M_n(x))_{n\in N}$ de M dans $\varprojlim(M/M_n, \phi^M_{nm})$.

On pose provisoirement $\overline{M} = \varprojlim(M/M_n)$. On note $\overline{M}_n$ le sous-module $\varprojlim(M_m/M_n)$ de $\overline{M}$ des éléments de la forme $(\phi^M_n(x_n))_{n\in N}$ où, pour tout $n\in N$, x_n appartient à M_n.

Le A-module $\overline{M}$ devient un A-module filtré par la filtration $(\overline{M}_m)_{m\in N}$. L'application ϕ^M est *compatible*.

On va démontrer que $(\overline{M}, \phi^M)$ est solution du problème universel du théorème II.6 et donc qu'il existe un isomorphisme λ^M fonctoriel de $\overline{M}$ sur $\hat{M}$ tel que $\alpha^M = \lambda^M \circ \phi^M$.

Lemme 1

Pour tout $n\in N$, ϕ^M *définit, par passage au quotient, un isomorphisme de* M/M_n *sur* $\overline{M}/\overline{M}_n$.

Démonstration

Pour tout $m \geqslant n$, on a une suite exacte :

$$0 \longrightarrow M_n/M_m \longrightarrow M/M_m \longrightarrow M/M_n \longrightarrow 0$$

Passant à la limite projective, on obtient une suite exacte

$0 \longrightarrow \overline{M}_n \longrightarrow \varprojlim(M/M_m) \xrightarrow{\alpha} M/M_n$ (exactitude à gauche du foncteur limite projective).

L'application α est *surjective* : si $\xi \in M/M_n$, $\xi = (\phi^M_m(x))_{n\in N}$ où x est un représentant de ξ dans M et $\xi = \alpha((\phi^M_{nm}(x))$.

On remarque que, par cofinalité, $\overline{M} = \varprojlim_{m\geqslant n}(M/M_m)$. Donc, α définit un isomorphisme $\overline{\alpha}$ de $\overline{M}/\overline{M}_n$ sur M/M_n. Il est clair que son inverse est défini par passage au quotient par ϕ^M.

Lemme 2

1. *Si* M *est séparé,* ϕ^M *est injective.*
2. *Si* M *est complet,* ϕ^M *est surjective.*
3. *Si* M *est séparé complet,* ϕ^M *est un isomorphisme.*

Démonstration

1. On remarque que $\ker(\Phi^M) = \bigcap_{n\in N} M_n$.

2. Dire que $(a_n)_{n\in N} \in \prod_{n\in N} M/M_n$ appartient à $\varprojlim(M/M_n, \phi^M_{nm})$ c'est dire que, si $m \geqslant n$, $\phi^M_{nm}(a_m) = a_n$. Soit alors $x_n \in M_n$ tel que $\phi^M_n(x_n) = a_n$. Si $m > n$, $\phi^M_n(x_m) = \phi^M_{nm}(\phi^M_m(x_m)) = \phi^M_n(x_n)$, i.e. $x_m - x_n \in M_n$. Donc, si $m,m' > n$,

$x_m - x_m$, appartient à M_n et la suite $(x_n)_{n\in N}$ est de Cauchy.

Soit x une limite de la suite (x_n). Il existe $n_o \in N$ tel que, pour $n \geqslant n_o$, $\phi_n^M(x) = \phi_n^M(x_n)$.

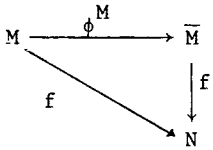
Si $n < n_o$, $\phi_{nn_o}^M(\phi_{n_o}^M(x)) = \phi_{nn_o}^M(\phi_n^M(x_{n_o}))$. Donc, pour tout $n \in N$, $\phi_n^M(x) = \phi_n^M(x_n)$.

Ainsi $(a_n)_{n\in N}$ est $\phi^M(x)$ et ϕ^M est surjective.

Proposition II.10

Soient N *un* A*-module filtré séparé complet,* f *une application* A*-linéaire continue de* M *dans* N.

Il existe alors une application A*-linéaire continue* $\overline{f}$ *et une seule de* $\overline{M}$ *dans* N *telle que le diagramme :*



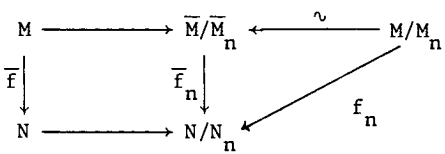
soit commutatif.

Démonstration

Quitte à remplacer la filtration de M par une filtration cofinale et munir alors le A-module $\overline{M}$ de la filtration correspondante, on peut supposer l'application f *compatible*.

L'application $\overline{f}$ cherchée est alors nécessairement compatible.

Pour tout $n\in N$, on doit avoir un diagramme commutatif :



où $\overline{f}_n$ (resp. $\overline{f}$) est déduit de f_n (resp. f) par passage au quotient.

On a donc un diagramme commutatif :

$$\begin{array}{ccc} \overline{M} = \varprojlim(M/M_m) & \longrightarrow & M/M_n \\ \downarrow \overline{f}' & & \downarrow f_n \\ \overline{N} = \varprojlim(N/N_m) & \longrightarrow & N/N_n \end{array} \quad \text{avec } \overline{f}' = \phi^N \circ \overline{f}$$

Il en résulte que l'on doit avoir $\overline{f}' = \varprojlim(f_n)$ et donc $\overline{f} = (\phi^N)^{-1} \circ (\varprojlim(f_n))$.

Ceci démontre l'unicité. L'existence est évidente, compte tenu de ce qui précède.

Corollaire

Soient A *un anneau semi-local,* $m_1,\ldots,m_s$ *ses idéaux maximaux,* r *le radical de* A, i.e. $m_1 \cap \ldots \cap m_s = m_1 \ldots m_s$.

Alors le complété r*-adique* $\hat{A}$ *de* A *est isomorphe à* $\prod_{i=1}^{s} (\hat{A}_{m_i})$ *où* $\hat{A}_{m_i}$ *est le complété de l'anneau local* A_{m_i} *muni de sa filtration* $m_i A_{m_i}$*-adique.*

Démonstration

Comme r^n est l'intersection des idéaux étrangers m_i^n $(i = 1,\ldots,s)$, A/r^n est isomorphe à $\prod_{i=1}^{s} A/m_i^n$. Donc, $\hat{A} = \varprojlim(A/r^n) = \prod_{i=1}^{s} \varprojlim(A/m_i)^n = \prod_{i=1}^{s} \varprojlim(A_{m_i}/m_i^n A_{m_i})$.

Remarque

Dans toute la suite, *le terme complété d'un anneau semi-local est réservé au complété dans la filtration* r*-adique où* r *est son radical. En particulier, le complété d'un anneau local est le complété dans la filtration formée des puissances de son idéal maximal.*

III. Propriétés de transfert

1. Gradué associé à un module filtré

Module gradué

Soient A *un anneau,* P *un* A*-module,* $(P_n)_{n\in N}$ *une suite de sous-modules telle que* P *soit la somme directe interne* $\bigoplus_{n\in N} P_n$ ((FFAC).chap. 3.§5).

On dit que P est *gradué* par la suite $(P_n)_{n\in N}$. Un élément de P_n est dit *homogène de degré* n.

Soit $(P_n)_{n\in N}$ *une suite de* A*-modules.* On identifie, au moyen de l'injection canonique, P_n à un sous-module de $P = \bigoplus_{n\in N} P_n$. Le A-module P est alors *gradué* par la suite $(P_n)_{n\in N}$.

On ne distinguera pas dans la suite ces deux points de vue.

Module gradué associé à un module filtré

Définition

Soit M *un* A*-module muni d'une filtration* $(M_n)_{n\in N}$.

On appelle module gradué associé du module filtré M *le* A*-module*

$$\mathrm{Gr}(M) = \bigoplus_{n\in N} \mathrm{Gr}^n(M)$$

où $\mathrm{Gr}^n(M) = M_n/M_{n+1}$;

Application graduée associée à une application compatible

Soient M *et* N *des* A*-modules munis de filtrations respectives* $(M_n)_{n\in N}$ *et* $(N_n)_{n\in N}$, f *une application* A*-linéaire de* M *dans* N *compatible avec les filtrations, i.e. telle que* $f(M_n) \subset N_n$ $(n \in N)$

On note $\mathrm{Gr}^n(f)$ *l'application linéaire de* $\mathrm{Gr}^n(M)$ *dans* $\mathrm{Gr}^n(N)$ *définie par passage au quotient à partir de la restriction de* f *à* M_n. Si donc l'élément ξ de $\mathrm{Gr}^n(M) = M_n/M_{n+1}$ est la classe de $x_n \in M_n$, $\mathrm{Gr}^n(f)(\xi)$ est la classe de $f(x_n) \in N_n$ modulo N_{n+1}.

L'application A-linéaire $\mathrm{Gr}(f) = \bigoplus_{n\in N} \mathrm{Gr}^n(f)$ de Gr(M) dans Gr(N) est appelée *l'application graduée associée de* f.

Avec des notations évidentes, $\mathrm{Gr}(g\circ f) = \mathrm{Gr}(g)\circ\mathrm{Gr}(f)$ et $\mathrm{Gr}(1_M) = 1_{\mathrm{Gr}(M)}$.

Les applications : $M \longmapsto \mathrm{Gr}(M)$, $f \longmapsto \mathrm{Gr}(f)$ *définissent donc un foncteur covariant de la catégorie des* A*-modules filtrés avec pour morphismes les applications linéaires compatibles dans la catégorie des modules gradués avec pour morphismes les applications linéaires homogènes de degré* 0 (qui appliquent un élément homogène sur un élément de même degré). Ce foncteur est *additif*.

Soit A *un anneau filtré par une suite décroissante* $(a_n)_{n\in N}$ *d'idéaux.*

Le groupe abélien $\mathrm{Gr}(A) = \bigoplus_{n\in N} a_n/a_{n+1}$ est muni d'une structure d'anneau par les applications

$$(\bar{x}_n, \bar{x}_m) \longmapsto \text{classe de } (x_n x_m) \text{ modulo } a_{n+m+1}$$

$$\mathrm{Gr}^n(A) \times \mathrm{Gr}^m(A) \longrightarrow \mathrm{Gr}^{n+m}(A)$$

(où $\bar{x}_n$ et $\bar{x}_m$ désignent les classes modulo a_{n+1} et a_{m+1} de $x_n \in a_n$ et $x_m \in a_m$ respectivement).

Soient A *un anneau filtré par une suite décroissante* $(a_n)_{n\in N}$ *d'idéaux,* M *un* A*-module.*

Une filtration $(M_n)_{n\in N}$ *de* M *est dite compatible avec la filtration de* A *si, pour tout couple* $(m,n) \in N^2$, $a_n M_m$ *est contenu dans* M_{n+m}.

On dit aussi, dans ce cas, que M est un module filtré sur l'anneau filtré A.

S'il en est ainsi, *on munit* Gr(M) *d'une structure de* Gr(A)*-module au moyen des applications*

$(\overline{a}_n, \overline{x}_m) \longmapsto$ classe de $a_n x_n$ modulo M_{n+m+1}

(avec des notations évidentes).

Exemple

Soient k *un anneau,* $(X_i)_{i\in I}$ *une famille (finie) d'indéterminées,* $A = k[[X_i]]_{i\in I}$.

On considère la filtration $(a_n)_{n\in N}$ où a_n est l'idéal $(X_i)^n_{i\in I}$ des séries formelles d'ordre $\geq n$.

On peut identifier, de manière évidente, $Gr^n(A) = a_n/a_{n+1}$ au k-module des polynômes *homogènes de degré* n.

On vérifie aisément que la structure d'anneau sur Gr(A), ainsi identifié à l'anneau $k[X_i]_{i\in I}$ des polynômes, est la structure usuelle.

Proposition III.1

Soient A *un anneau, a un idéal de* A.

Le gradué associé $Gr_a(A)$ *de l'anneau filtré par* $(a^n)_{n\in N}$ *est engendré en tant que* $Gr^0_a(A) = A/a$*-algèbre par* $Gr^1_a(A) = a/a^2$.

Démonstration

Il est clair que $Gr_a(A)$ est une $Gr^0_a(A)$-algèbre d'homomorphisme structural l'injection canonique.

Un élément de $Gr^n_a(A)$ est une somme finie d'éléments de la forme

$$\overline{a_{i_1} \dots a_{i_n}}$$

où $a_{i_j} \in a$ et $\overline{a}$ désigne la classe modulo a^{n+1}.

Un tel élément est le produit $\overline{a}_{i_1} \dots \overline{a}_{i_n}$ des classes modulo a^2 des éléments $a_{i_1}, \dots, a_{i_n}$ comme il résulte de la définition même du produit.

2. Propriétés d'un module filtré et du gradué associé

Soit M *un* A*-module muni d'une filtration* $(M_n)_{n\in N}$.

Il résulte de la proposition II.5.1. que α_{M_n} définit, par passage au quotient, un isomorphisme de M_n/M_{n+1} sur $\hat{M}_n/\hat{M}_{n+1}$.

Il en résulte que $Gr(\alpha_M)$ *est un isomorphisme de* Gr(M) *sur* $Gr(\hat{M})$.

On va voir ci-dessous que certaines propriétés du module filtré M se lisent sur le gradué associé Gr(M).

Par conséquent, il sera possible d'établir, par considération des gradués associés, des propriétés de transfert de M à $\hat{M}$. Le résultat suivant est fondamental à cet égard.

Proposition III.2

Soient M *et* N *deux groupes abéliens munis de filtrations séparées* $(M_n)_{n\in N}$ *et* $(N_n)_{n\in N}$ *respectivement,* f *un homomorphisme de groupes de* M *dans* N *compatible avec les filtrations.*

1. Si Gr(f) *est injectif,* f *est injectif.*

2. On suppose M *complet.*

Si Gr(f) *est surjectif* (resp. *bijectif*), f *est surjectif* (resp. *bijectif*).

Démonstration

1. L'injectivité de Gr(f) équivaut à l'inclusion

$$M_n \cap f^{-1}(N_{n+1}) \subset M_{n+1}$$

pour tout $n \in N$.

On en déduit, pour tout $n \in N$ et tout k tel que $0 \leqslant k \leqslant n$, l'inclusion

$$M_{n-k} \cap f^{-1}(N_{n+1}) \subset M_{n+1}$$

car

$$M_{n-k} \cap f^{-1}(N_{n+1}) \subset M_{n-k} \cap f^{-1}(N_{n+1-k}) \subset M_{n+1-k}$$

et donc

$$M_{n-k} \cap f^{-1}(N_{n+1}) = M_{n+1-k} \cap f^{-1}(N_{n+1}) = \ldots = M_n \cap f^{-1}(N_{n+1}) \subset M_{n+1}.$$

En particulier, pour $k = n$, on obtient :

$$f^{-1}(N_{n+1}) \subset M_{n+1} \text{ et donc } f^{-1}(N_{n+1}) = M_{n+1}.$$

Alors, $\ker(f) = f^{-1}(0) \subset f^{-1}(\bigcap_{n\in N} N_n) = \bigcap_{n\in N} f^{-1}(N_n) = \bigcap_{n\in N} M_n = (0)$ *puisque* M *et* N *sont séparés*. Donc, f est injectif.

2. Compte tenu de 1. il suffit de prouver la surjectivité de f sous hypothèse de surjectivité de Gr(f).

La surjectivité de Gr(f) équivaut à l'égalité $N_n = f(M_n) + N_{n+1}$, pour tout $n \in N$. *On en déduit l'égalité* $N_n = f(M_n)$ et donc la surjectivité de f.

Soit, en effet, $y \in N_n$. On construit une suite de Cauchy $(x_k)_{k\in N}$ de M en posant $x_o = 0$ et en définissant x_{k+1} à partir de x_k comme suit : l'élément $y - f(x_k)$ est par construction un élément de N_{n+k} et s'écrit donc $f(z) + t$ où $z \in M_{n+k}$ et $t \in N_{n+k+1}$. On pose $x_{k+1} = x_k + z$.

Le sous-module M_n de M est fermé et donc complet comme M.

La suite de Cauchy $(x_k)_{k\in\mathbb{N}}$ a donc une limite x dans M_n. Puisque f est continue, f(x) est limite de la suite de Cauchy $(f(x_k))_{k\in\mathbb{N}}$ de N_n. Mais y est aussi limite de cette suite et, comme N est séparé, y = f(x).

Définition

Soit M *un groupe abélien muni d'une filtration séparée* $(M_n)_{n\in\mathbb{N}}$.

Soit x *un élément non nul de* M. *L'entier* n *tel que* $x \in M_n$ *et* $x \notin M_{n+1}$ *est appelé le degré initial de* x.

La classe $\overline{x}$ *de* x *modulo* M_{n+1} *est un élément de* Gr(M) *appelé forme initiale de* x.

Cette dénomination est justifiée par l'exemple $M = k[[X_i]]_{i\in I}$. Un élément non nul x de M s'écrit $f_n(X_i)_{i\in I} + g(X_i)_{i\in I}$ où n est l'ordre de x et g une série d'ordre supérieur à n.

Si l'on identifie Gr(M) à $k[X_i]_{i\in I}$, la forme initiale de x est $f_n(X_i)_{i\in I}$ et le degré initial est n.

Proposition III.3

Soient A *un anneau filtré complet,* M *un* A*-module filtré séparé,* $(x_i)_{i\in I}$ *une famille finie d'éléments de* M *dont les formes initiales engendrent le* Gr(A)*-module* Gr(M).

Les éléments $(x_i)_{i\in I}$ *engendrent alors le* A*-module* M. *De plus,* M *est complet.*

Démonstration

Soient n_i le degré initial de x_i $(i\in I)$, $p = \inf_{i\in I}(n_i)$, $q = \sup_{i\in I}(n_i)$.

On munit le A-module libre $A^{(I)}$ de la filtration décroissante $(L_n)_{n\in\mathbb{N}}$ où

$$L_n = \{(a_i)_{i\in I} \;/\; a_i \in a_{n-n_i}\} \qquad (n \geqslant q)$$

On déduit des inclusions

$$a^{(I)}_{n-q} \subset L_n \subset a^{(I)}_{n-p}$$

que la topologie définie par la filtration $(L_n)_{n\in\mathbb{N}}$ sur $A^{(I)}$ est la topologie produit des topologies définies sur les facteurs A par la filtration $(a_n)_{n\in\mathbb{N}}$.

Il en résulte que $A^{(I)} = L$ est complet.

L'homomorphisme $f : (a_i)_{i\in I} \longmapsto \sum_{i\in I} a_i x_i$ de L dans M est compatible avec les filtrations.

Pour prouver qu'il est surjectif, il suffit en vertu de la

proposition III.2.2. de prouver que Gr(f) est surjectif, i.e. que si $x \in M_n$, il existe $a_i \in a_{n-n_i}$ (i ∈ I) tel que :

(1) $x = \sum_{i\in I} a_i x_i$ modulo M_{n+1}.

Soient $\overline{x}_i$ (i∈I) et $\overline{x}$ les formes initiales de x_i et x. Il existe, par hypothèse, des éléments $\alpha_i \in Gr(A)$ tels que $\overline{x} = \sum_{i\in I} \alpha_i \overline{x}_i$. On peut d'ailleurs choisir α_i homogène de degré $n-n_i$. La condition (1) est satisfaite en prenant pour a_i un représentant de α_i dans a_{n-n_i}.

Corollaire 1

Soient A *un anneau filtré complet,* M *un* A*-module filtré séparé.*

Si le Gr(A)*-module* Gr(M) *est de type fini* (resp. *noethérien*), *le* A*-module* M *est de type fini* (resp. *noethérien*).

Démonstration

Si le Gr(A)-module Gr(M) est de type fini, il admet un système *fini* de générateurs *homogènes*. Il résulte de la proposition III.3 que des représentants dans M de ces générateurs engendrent le A-module M.

Si le Gr(A)-module Gr(M) est noethérien, un sous-module N de M est séparé pour la topologie induite et Gr(N) qui est un sous-module du Gr(A)-module noethérien Gr(M) est de type fini. Il résulte de la première partie de la démonstration que N est un A-module de type fini. Donc, M est noethérien.

Corollaire 2

Soient A *un anneau noethérien, a un idéal de* A.

Le complété séparé de A *dans la topologie a-adique est un anneau noethérien, et, donc, un anneau de* Zariski.

Démonstration

Il suffit de remarquer que $Gr_{a\hat{A}}(\hat{A}) = Gr_a(A)$ et d'appliquer le corollaire 1.

Corollaire 3

Soient A *un anneau, a un idéal de* A.

On suppose l'anneau quotient A/m *noethérien, le* A/m*-module* m/m^2 *de type fini et* A *séparé et complet dans la topologie a-adique.*

Alors l'anneau A *est noethérien.*

Démonstration

La A/*m*-algèbre $Gr_m(A)$ est de type fini puisqu'elle est engendrée par

m/m^2 et donc par un système fini de générateurs de m/m^2 sur A/m.

L'anneau $Gr_m(A)$ est donc noethérien. Il suffit alors d'appliquer le corollaire 1.

Proposition III.4

Soient A *un anneau noethérien, a un idéal de* A, $\hat{A}$ *le séparé complété a-adique de* A.

1. L'application : $m \longmapsto m\hat{A}$ est une bijection de l'ensemble des idéaux maximaux de A *contenant a sur l'ensemble des idéaux maximaux de* $\hat{A}$.

La bijection réciproque est l'application α_A^{-1}, où α_A est l'application naturelle de A *dans* $\hat{A}$ *définie en* II.1.

2. Soit m un idéal maximal de A *contenant a. Le complété $m\hat{A}$-adique de* $\hat{A}$ *est isomorphe au complété m-adique de* A.

Démonstration

On remarque que l'application : $m \longmapsto m/\bigcap_{n\in N} a^n$ est une bijection de $Max(A) \cap V(a)$ sur $Max(A/\bigcap_{n\in N} a^n)$.

On remarque ensuite que le complété séparé a-adique de A est le complété de $A/(\bigcap_{n\in N} a^n)$ dans la topologie $a/(\bigcap_{n\in N} a^n)$: c'est évident avec l'interprétation en terme de limites projectives.

On peut donc supposer A *séparé dans la topologie a-adique et démontrer alors que l'application $m \longmapsto m\hat{A}$ est une bijection de* $Max(A)$ *sur* $Max(\hat{A})$.

Soit $m \in Max(A)$. Comme m contient a, il est ouvert dans la topologie a-adique. Son complémentaire qui est réunion d'ensembles homéomorphes à a (les classes modulo a distinctes de a) est aussi ouvert. Donc, m est fermé.

La topologie a-adique sur le A-module quotient est donc discrète. Il en résulte que le complété de A/m est isomorphe à A/m. Ce complété est $\hat{A}/m\hat{A}$. Donc, $m\hat{A}$ est un idéal maximal de $\hat{A}$.

Soit $\hat{m} \in Max(\hat{A})$. Le A-module $\hat{m}$ est complet.

Soit n un idéal maximal contenant $\alpha_A^{-1}(\hat{m}) = m$. Son complété $n\hat{A}$ est contenu dans $\hat{m}$. Donc, $n\hat{A}$, qui est maximal, est égal à $\hat{m}$. Par fidèle platitude de $\hat{A}$, $n = \alpha_A^{-1}(\hat{m}) = m$ et m est maximal.

2. Résulte de ce que, pour tout $n \in N$, $\hat{A}/m^n\hat{A}$ est isomorphe à A/m^n et donc de ce que le complété $m\hat{A}$-adique de $\hat{A}$, qui est $\varprojlim(\hat{A}/m^n\hat{A})$, est isomorphe à $\varprojlim(A/m^n)$ qui est le complété m-adique de A.

3. Quelques autres propriétés de transfert

Un anneau local noethérien A est dit *analytiquement non ramifié*

(resp. *analytiquement normal*) si son complété $\hat{A}$ est réduit (resp. intégralement clos).

Proposition III.5

Un anneau local noethérien analytiquement réduit (resp. *normal*) A *est réduit* (resp. *intégralement clos*).

Démonstration

L'anneau A est un sous-anneau de $\hat{A}$. Il est donc réduit (resp. intègre) si $\hat{A}$ l'est.

Si $\hat{A}$ est intégralement clos, soient K et $\hat{K}$ les corps des fractions respectifs de A et $\hat{A}$. Un élément de K entier sur A l'est a fortiori sur $\hat{A}$. Il appartient donc à $\hat{A} \cap K$. Or, $\hat{A} \cap K = A$: en effet, soit $a/b \in \hat{A}$ où $a,b \in A$ $(b \neq 0)$; alors $a \in b\hat{A} \cap A$ i.e. $a \in bA$ et donc $a/b \in A$.

La réciproque de la proposition III.4 est fausse. M. Nagata ([13], exemple 6. p. 208) a construit des exemples d'anneaux locaux noethériens intégralement clos analytiquement ramifiés.

Il sera prouvé au chapitre 15 que la réciproque est vraie pour certaines classes d'anneaux locaux et, en particulier, pour les anneaux locaux de la géométrie classique (théorème de Chevalley et Zariski).

En particulier, *un anneau local d'une algèbre de type fini sur un corps ou sur l'anneau* $\mathbb{Z}$ *des entiers est analytiquement non ramifié* (resp. *normal*) *si et seulement si il est réduit* (resp. *intégralement clos*).

IV. Quasi-finitude et finitude

Définition

Soient A *un anneau local, non nécessairement noethérien, d'idéal maximal* m, *de corps résiduel* k, M *un* A*-module.*

On dit que M *est quasi-fini sur* A *si le* k*-espace vectoriel* M/mM *est de dimension finie.*

Un A-module de type fini est quasi-fini. La réciproque n'est pas toujours vraie :

Soient k *un corps,* X *une indéterminée,* $A = k[[X]]$, K *le corps des fractions de* A.

Le A-module K n'est pas de type fini. Pourtant $K = mK$ et $K/mK = (0)$.

Voici une réciproque partielle importante.

Proposition IV.1

Soient A *un anneau noethérien,* m *un idéal de* A, M *un* A*-module.*

On suppose A *séparé complet et* M *séparé dans la topologie* m*-adique.*

Les assertions suivantes sont équivalentes :

(i) M/mM *est un* A/m*-module de type fini.*

(ii) M *est un* A*-module de type fini.*

Démonstration

(ii) $\Longrightarrow$ (i) clair.

(i) $\Longrightarrow$ (ii). Soient $e_1,\dots,e_n$ des éléments de M dont les classes modulo mM engendrent le A/m-module M/mM. Soit $x \in M$. On va construire une suite $(x_{r,i})_{r\geqslant 1}$ d'éléments de A telle que $x_{r+1,i} - x_{r,i} \in m^r$ et que $x - \Sigma_{i=1}^n x_{r,i}e_i \in m^r M$.

On suppose obtenus les éléments $x_{r,i}$ $(i = 1,\dots,n)$. On écrit :

$$x = \Sigma_{i=1}^n x_{r,i}e_i + \Sigma_j \mu_j y_j \quad \text{où} \quad \mu_j \in m^r \quad \text{et} \quad y_j \in M$$

puis

$$y_j = \Sigma_{i=1}^n u_{j,i} e_i + z \quad \text{où} \quad z \in mM$$

On pose alors :

$$x_{r+1,i} = x_{r,i} + \Sigma_j \mu_j u_{j,i}$$

Comme A est séparé complet, la suite de Cauchy $(x_{r,i})_{r\geqslant 1}$ converge vers $x_i' \in A$.

Soit $x' = \Sigma_{i=1}^n x_i' e_i$. Alors, $x-x' \in \bigcap_r m^r M = (0)$ et donc $x = x'$.

Corollaire

Soient A *un anneau local noethérien complet d'idéal maximal* m, M *un* A*-module.*

On suppose M *séparé dans la topologie* m*-adique. Alors* M *est quasi-fini sur* A *si et seulement si il est de type fini sur* A.

La proposition IV.1 contient comme cas particulier le théorème de préparation formel, explicité plus loin.

Définition

Soient A *un anneau local, non nécessairement noethérien,* B *un anneau* f *un homomorphisme d'anneaux de* A *dans* B.

On dit que f *est quasi-fini si le* A*-module* B *défini par* f *est quasi-fini.*

Proposition IV.2

Soient A *et* B *des anneaux locaux, non nécessairement noethériens, d'idéaux maximaux* m *et* n, *de corps résiduels* k *et* k(B), f *un homomorphisme local de* A *dans* B.

La condition

(i) f *est quasi-fini*

implique la condition

(ii) 1. Il existe un entier $r \geqslant 1$ *tel que* $n^r \subset m$B *(autrement dit* mB *est un idéal de définition de la topologie de* B*).*

2. L'extension résiduelle k(B)/k *est finie.*

Si, de plus, l'idéal maximal n *est de type fini, la condition (ii) implique la condition (i).*

Démonstration

(i) $\Longrightarrow$ (ii).

Dire que f est quasi-fini c'est dire que la k-algèbre B/mB est de rang fini.

Il en résulte que la k-algèbre B/n qui en est un quotient est de rang fini, d'où (ii) 2.

L'anneau B est alors artinien et son radical n/mB est nilpotent, d'où la condition (ii)1.

(ii) $\Longrightarrow$ (i) *si* n *est de type fini.*

On considère la suite décroissante

$$B \supset mB+n \supset mB + n^2 \supset \ldots \supset mB + n^r = mB$$

Les quotients successifs $(mB + n^i)/(mB + n^{i+1}) = \overline{n}^i/\overline{n}^{i+i}$, où $\overline{n}$ est l'idéal maximal n/mB de l'anneau local B/mB, sont des k(B)-espaces vectoriels de dimension finie et donc des k-espaces vectoriels de dimension finie. Il en résulte que B/mB est un k-espace vectoriel de dimension finie.

On utilisera souvent dans la suite le corollaire suivant.

Corollaire

Soient A *un anneau locacl noethérien complet d'idéal maximal* m, B *un anneau local noethérien d'idéal maximal* n, *dominant* A.

On suppose que A *et* B *ont même corps résiduel et que* $n = m$B. *Alors,* A = B,

Démonstration

Le A-module B est quasi-fini et donc de type fini (prop. IV.1 et IV.2)

Il résulte alors du lemme de Nakayama que A = B.

Interprétation géométrique

Les notations sont celles de la proposition IV.2.

On a vu dans le chapitre 7 que l'application $q \longmapsto q/m$B est un *homéomorphisme* de la fibre de Spec(f) en m sur Spec(B/mB).

Dire que n est *isolé* dans cette fibre c'est dire que n/mB est isolé dans Spec(B/mB), i.e. que n/mB est le seul idéal premier de B/mB : il doit, en effet, exister $\overline{f} \in$ B/mB n'appartenant pas à n/mB mais appartenant à tout autre idéal premier de B/mB.

Si on suppose de plus B noethérien, l'anneau B/mB est *artinien* local d'idéal maximal n/mB. Il existe donc $r \in N^*$ tel que $n^r \subset m$B.

Si on suppose de plus que l'extension résiduelle k(B)/k *est finie*, dire que n est isolé dans sa fibre c'est dire que l'homomorphisme f est quasi-fini.

Cette hypothèse de finitude sur l'extension k(B)/k est souvent satisfaite. Elle l'est notamment, en raison du théorème des zéros de Hilbert, si B est une A-algèbre de type fini.

Définition

Soient A *un anneau local d'idéal maximal* m, X *une indéterminée,* f(X) *un élément de* $A[[X]]$, $f(x) = \Sigma_{i \in N} a_i X^i$.

On dit que f(X) *est régulier d'ordre* n *si* $a_i \in m$ (i = 0,...,n-1) *et* $a_n \notin m$.

Théorème IV.3 (*théorème de préparation formel*)

Soient A *un anneau local noethérien complet d'idéal maximal* m, X *une indéterminée,* f(X) *un élément de* $A[[X]]$ *régulier d'ordre* n.

Pour tout élément $g(X) \in A[[X]]$, *il existe* $q(X) \in A[[X]]$ *et* r(X) *de degré* $\leqslant$ n-1 *dans* $A[X]$ *tels que*

$g(X) = q(X)f(X) + r(X)$

Les éléments q(X) *et* r(X) *sont déterminés de manière unique par les conditions ci-dessus.*

Démonstration

Soient B l'anneau quotient $A[[X]]/(f(X))$, $\overline{f}(X)$ l'image de f(X) dans l'anneau $k[[X]]$.

Alors, B/mB = $k[[X]]/(\overline{f}(X))$. La série $\overline{f}(X)$ est un polynôme de degré n.

Il est clair que B/mB est un k-espace vectoriel de base $\{1, X, \ldots, X^{n-1}\}$.

Le A-module B est quasi-fini. Il est évidemment séparé. Il est donc de type fini et les éléments $1, X, \ldots, X^{n-1}$ forment un système de générateurs du A-module B.

On en déduit l'existence de $q(X)$ et $r(X)$.

On peut traduire ce résultat en disant que

$$A[[X]] = f(X)A[[X]] + M$$

où M est le sous-module libre de $A[[X]]$ de base $1, X, \ldots, X^{n-1}$.

L'unicité de $q(X)$ *et* $r(X)$ *va résulter des assertions suivantes :*

1) $f(X)A[[X]] \cap M = (0)$, *qui donne l'unicité de* $r(X)$

2) $f(X)$ *n'est pas un diviseur de zéro dans* $A[[X]]$, *qui donne alors l'unicité de* $q(X)$.

Démonstration de 1)

On démontre qu'une égalité

$(\Sigma_{i \in N} b_i X^i) f(X) = c_0 + c_1 X + \ldots + c_{n-1} X^{n-1}$, où b_j, c_i appartiennent à A implique $b_j = 0$ pour tout j.

Comme $\bigcap_{n>0} m^n = (0)$, il suffit de démontrer que b_j appartient à m^n pour tout n.

Ceci se démontre par double récurrence : le cas n=0 est évident.

On suppose que $b_j \in m^{n-1}$ pour tout j et $b_j \in m^n$ pour tout $j < k$. On démontre qu'alors b_k appartient aussi à m^n.

Soit $f(X) = \Sigma_{i \in N} a_i X^i$. Le coefficient

$$(b_0 a_{n+k} + \ldots + b_{k-1} a_{n+1}) + b_k a_n + (b_{k+1} a_{n-1} + \ldots + b_{k+n} a_0)$$

de X^{n+k} dans le produit $(\Sigma_{i \in N} b_i X^i) f(X)$ est nul.

Les termes de la première parenthèse appartiennent à m^n par hypothèse Ceux de la seconde appartiennent à $m^{n-1} m = m^n$ car $b_{k+1}, \ldots, b_{k+n}$ appartiennent à m^n et $a_{n-1}, \ldots, a_0$ appartiennent à m.

Par conséquent, $b_k a_n$ appartient à m^n et comme a_n n'appartient pas à m, b_k appartient à m^n.

L'assertion 2) est un cas particulier de ce qui précède.

V. Le critère local de platitude

On va démontrer ici un critère souvent utilisé dans la suite.

Voici d'abord quelques remarques. *Soient* A *un anneau,* a *un idéal de* A, M *un* A*-module.*

1. Si le A-module M est plat, il en est de même, pour tout entier n,

du A/a^n-module M/a^nM. La réciproque est-elle vraie ?

2. On suppose A *local* d'idéal maximal a. Si le A-module M est *de type fini*, et si A est *noethérien*, on a les équivalences :

(i) M est un A-module libre

(ii) $\mathrm{Tor}_1^A(M,A/a) = 0$

On a, en effet, une suite exacte : $0 \longrightarrow R \longrightarrow L=A^n \xrightarrow{u} M \longrightarrow 0$ avec $R \subset aL$, obtenue à partir d'un système $\{e_1,\ldots,e_n\}$ *minimal* de générateurs de M en définissant u par $u((a_i)) = \Sigma_{i=1}^n a_i e_i$.

On en déduit la suite exacte des Tor, où $k = A/a$,

$$0 = \mathrm{Tor}_1^A(L,K) \longrightarrow \mathrm{Tor}_1^A(M,k) \longrightarrow R/aR=R \underset{A}{\otimes} k \longrightarrow L/aL \xrightarrow{\bar{u}} M/aM \longrightarrow 0$$

Or, l'application $\bar{u}$ est un isomorphisme car son noyau est $(R+aL)/aL$ et donc, $R/aR = \mathrm{Tor}_1^A(M,k)$. Le lemme de Nakayama permet alors de conclure en raison de la finitude de R.

On a souvent besoin d'un résultat plus général, à savoir :

Théorème V.1

Soient A *et* B *des anneaux locaux noethériens,* f *un homomorphisme local de* A *dans* B, k *le corps résiduel de* A, M *un* B*-module de type fini.*

Les assertions suivantes sont équivalentes :

(i) M *est un* A*-module plat*

(ii) $\mathrm{Tor}_1^A(M,k) = 0$

Si B=A, $f=1_A$, on retrouve le résultat précédent.

La réciproque de 1. et le théorème V.1 sont des cas particuliers d'un même théorème appelé critère local de platitude. Avant de démontrer ce théorème, il faut donner une définition.

Définition

Soient A *un anneau, a un idéal de* A, M *un* A*-module.*

On dit que M *est idéalement séparé pour a si, pour tout idéal b de* A, *le* A*-module* $b \underset{A}{\otimes} M$ *est séparé pour la topologie* a-adique.

Sous les hypothèses du théorème V.1, on remarque que M est idéalemen séparé pour m.

En effet, pour tout idéal b de A, le B-module $b \underset{A}{\otimes} M$ est de type fini comme M et b. Il est donc séparé dans la topologie mB-adique et donc dans la topologie m-adique.

Soient A *un anneau, a un idéal de* A, M *un* A*-module.*

L'application $(\bar{a},\bar{x}) \longmapsto$ classe de ax modulo $a^{n+1}M$ où $\bar{a}$ (resp. $\bar{x}$) es

la classe de l'élément a de a^n modulo a^{n+1} (resp. x de M modulo aM) est A/a-bilinéaire.

Elle définit donc une application A/a*-linéaire* c_n *de* $a^n/a^{n+1} \underset{A/a}{\otimes} M/aM$ *dans* $a^nM/a^{n+1}M$.

Théorème V.2 (critère local de platitude)

Soient A *un anneau,* a *un idéal de* A, M *un* A*-module.*

On suppose vérifiée l'une des conditions suivantes :

1. a *est nilpotent*

2. A *est noethérien et* M *est idéalement séparé pour* a

Les assertions suivantes sont équivalentes :

(i) M *est plat sur* A

(ii) $\mathrm{Tor}_1^A(M,N) = 0$ *pour tous les* A/a*-modules* N

(iii) M/aM *est plat sur* A/a *et l'homomorphisme canonique* $a \underset{A}{\otimes} M \longrightarrow aM$ *est un isomorphisme*

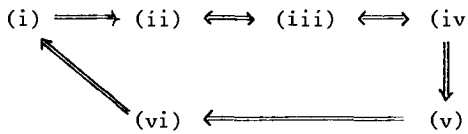
(iv) M/aM *est plat sur* A/a *et* $\mathrm{Tor}_1^A(M,A/a) = 0$

(v) M/aM *est plat sur* A/a *et, pour tout* $n \in N$, c_n *est un isomorphisme*

(vi) Pour tout $n \in N$, M/a^{n+1} *est plat sur* A/a^{n+1}

Démonstration

Elle se fait suivant le schéma d'implications :



la seule implication faisant intervenir l'une des conditions 1. et 2. étant d'ailleurs l'implication (vi) $\Longrightarrow$ (i) qui sera la seule utilisée dans un certain nombre de démonstrations dans la suite.

(vi) $\Longrightarrow$ (i). Elle est claire sous l'hypothèse 1. On suppose donc l'hypothèse 2.

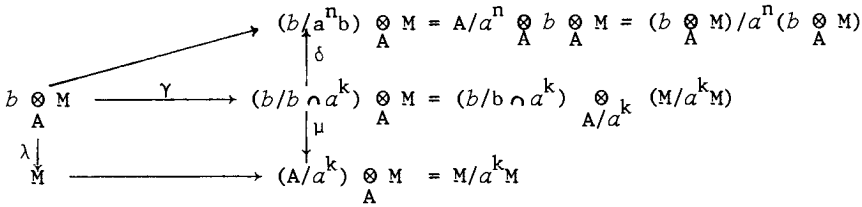
On va démontrer que, pour tout idéal b de A, l'application canonique $\lambda : b \underset{A}{\otimes} M \longrightarrow M$ est injective, ce qui est suffisant en vertu de (FFAC). Théorème V.2. (vi).

Puisque $b \underset{A}{\otimes} M$ est idéalement séparé, il suffit de démontrer que $\ker(\lambda)$ est contenu, pour tout $n \in N$, dans $a^n(b \underset{A}{\otimes} M)$.

Soit k un entier naturel tel que $b \cap a^k$ soit contenu dans $a^n b$.

On considère la diagramme commutatif suivant dont on vérifiera que

les flèches sont naturelles :



où μ est l'application naturelle, injective parce que, par hypothèse, $M/a^k M$ est un A/a^k-module plat et δ est surjective.

Si $\xi \in \ker(\lambda)$, $(\delta \circ \gamma)(\xi) = 0$ et donc ξ appartient à $a^n(b \underset{A}{\otimes} M)$ comme désiré.

(i) $\Longrightarrow$ (ii). Evident car $\mathrm{Tor}_1^A(M,N) = 0$ pour tout A-module N.

(ii) $\Longrightarrow$ (iii). De la suite exacte $0 \longrightarrow a \longrightarrow A \longrightarrow A/a \longrightarrow 0$, on déduit la suite exacte $0 = \mathrm{Tor}_1^A(M,A/a) \longrightarrow a \underset{A}{\otimes} M \longrightarrow M$ et donc l'homomorphisme $a \underset{A}{\otimes} M \longrightarrow M$ est injectif.

Soit $0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$ une suite exacte de A/a-modules.

La suite $0 = \mathrm{Tor}_1^A(M,N'') \longrightarrow M \underset{A}{\otimes} N' \longrightarrow M \underset{A}{\otimes} N$ est exacte. Mais $M \underset{A}{\otimes} N' = (M/aM) \underset{A/a}{\otimes} N'$ et $M \underset{A}{\otimes} N = (M/aM) \underset{A/a}{\otimes} N$, d'où la platitude du A/a-module M/aM.

(iii) $\Longleftrightarrow$ (iv). Clair.

(ii) $\Longrightarrow$ (v). La démonstration du fait que c_n est un isomorphisme se fait par considération du diagramme commutatif à lignes exactes :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & a^{n+1} \underset{A}{\otimes} M & \longrightarrow & a^n \underset{A}{\otimes} M & \longrightarrow & (a^n/a^{n+1}) \underset{A}{\otimes} M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha_{n+1}} & & \downarrow{\scriptstyle \alpha_n} & & \downarrow{\scriptstyle c_n} & & \\
0 & \longrightarrow & a^{n+1}M & \longrightarrow & a^n M & \longrightarrow & a^n M/a^{n+1}M & \longrightarrow & 0
\end{array}$$

déduit de la suite exacte $0 \longrightarrow a^{n+1} \longrightarrow a^n \longrightarrow a^n/a^{n+1} \longrightarrow 0$, où α_n est l'application canonique surjective. On sait que α_1 est injective (condition (iii)). On en déduit de proche en proche que $\alpha_2, \ldots, \alpha_n, \ldots$ sont injectives. Par conséquent, α_n est un isomorphisme et il en est de même de c_n

(v) $\Longrightarrow$ (vi). Par hypothèse, l'assertion (vi) est vraie pour $n = 0$. On suppose donc $n > 0$.

On a un diagramme commutatif à lignes exactes :

$$\begin{array}{ccccccc}
(a^{i+1}/a^{n+1}) \underset{A}{\otimes} M & \longrightarrow & (a^i/a^{n+1}) \underset{A}{\otimes} M & \longrightarrow & (a^i/a^{i+1}) \underset{A}{\otimes} M & \longrightarrow & 0 \\
\downarrow{\scriptstyle \beta_{i+1}} & & \downarrow{\scriptstyle \beta_i} & & \downarrow{\scriptstyle c_i} & & \\
0 \longrightarrow a^{i+1}M/a^{n+1}M & \longrightarrow & a^iM/a^{n+1}M & \longrightarrow & a^iM/a^{i+1}M & \longrightarrow & 0
\end{array}$$

où les applications naturelles β_{i+1}, β_i sont surjectives et où, par hypothèse, c_i est un isomorphisme. Il en résulte, par le lemme des quatre, que β_i est injective et est donc un isomorphisme. Or, β_1 est l'application naturelle de $(a/a^{n+1}) \underset{A/a^{n+1}}{\otimes} M/a^{n+1}M$ dans $(a/a^{n+1})(M/a^{n+1}M)$. Le A/a^{n+1}-module $M/a^{n+1}M$ satisfait à la condition (iii) avec l'idéal *nilpotent* a/a^{n+1}.

Il suffit donc de démontrer l'implication (ii) $\Longrightarrow$ (i) *sous l'hypothèse 1.*

Il suffit, à cet effet, de démonter que, pour tout A-module N, $\mathrm{Tor}_1^A(M,N) = 0$.

De la suite exacte $0 \longrightarrow a^{n+1}N \longrightarrow a^nN \longrightarrow a^nN/a^{n+1}N \longrightarrow 0$, on déduit la suite exacte :

$\mathrm{Tor}_1^A(M,a^{n+1}N) \longrightarrow \mathrm{Tor}_1^A(M,a^nN) \longrightarrow \mathrm{Tor}_1^A(M,a^nN/a^{n+1}N) = 0$, puisque $a^nN/a^{n+1}N$ est annulé par a. Partant de l'entier naturel m tel que $a^m = 0$, on voit que $\mathrm{Tor}_1^A(M,a^{m-1}N) = 0$, $\mathrm{Tor}_1^A(M,a^{m-2}N) = 0$ et, finalement, $\mathrm{Tor}_1^A(M,N) = 0$.

Exercice du chapitre 8

(1). Soient k un corps, $X_1,\ldots,X_n$ des indéterminées.

Quel est le complété d'un anneau quotient de l'anneau $k[[X_1,\ldots,X_n]]$?

(2). Soient A un anneau, M un A-module, $(M_n)_{n\in N}$ et $(M'_n)_{n\in N}$ deux filtrations séparées sur M. On note dans la suite M_1 (resp. M_2) le A-module filtré par $(M_n)_{n\in N}$ (resp. $(M'_n)_{n\in N}$).

1. On suppose de plus que, pour tout $n\in N$, M_n est contenu dans M'_n

Que peut-on dire de l'application 1_M de M_1 dans M_2 ? d'une suite de Cauchy de M_1 considérée comme suite de M_2 ?

2. *On suppose de plus que, pour tout* $n\in N$, M_n *est fermé dans* M_2.

Démontrer que, si x est une limite dans M_2 d'une suite $(x_n)_{n\in N}$ de Cauchy de M_1, x est aussi limite de $(x_n)_{n\in N}$ dans M_1.

En déduire que, si M_2 est complet, il en est de même de M_1.

3. Soient A un anneau *noethérien*, a et b deux idéaux de A *contenus dans le radical de* A *et tels que* $b \subset a$.

On suppose A *complet dans la topologie* a-adique. Quel est le complété de A dans la topologie b-adique ?

(3). Soient A un anneau local noethérien, $\hat{A}$ son complété.

1. Soit $\mathcal{J}$ l'ensemble des idéaux a de A tels que l'anneau quotient A/a soit complet.

Démontrer : a) si $a \in \mathcal{J}$ et b est un idéal de A contenant a, $b \in \mathcal{J}$.

b) si a et a' appartiennent à $\mathcal{J}$, aa' appartient à $\mathcal{J}$.

2. En déduire que les assertions suivantes sont équivalentes :

(i) A est complet

(ii) pour tout idéal premier minimal p de A, l'anneau A/p est complet.

3. Soit, si $a,a' \in \mathcal{J}$ et $a \subset a'$, $f_{aa'}$ la surjection canonique : $A/a \longrightarrow A/a'$.

Démontrer que $\varprojlim(A/a, f_{aa'})_{a,a' \in \mathcal{J}}$ est isomorphe à $\hat{A}$.

(Remarquer $\varprojlim_{a \in \mathcal{J}}(A/a) = \varprojlim_{a \in \mathcal{J}}(\varprojlim_{n \in \mathbb{N}} (\hat{A}/a^n\hat{A}) = \varprojlim_{a \in \mathcal{J}}(\hat{A}_{a\hat{A}})$, où $\hat{A}_{a\hat{A}}$ est le complété $a\hat{A}$-adique de $\hat{A}$).

(4). Soient A un anneau, a un idéal de A, $a_1,\ldots,a_r \in a$, $X_1,\ldots,X_r$ des indéterminées, $\hat{A}$ le séparé complété de A dans la topologie a-adique. Si $b \in A$, on note $\overline{b}$ l'image de b dans $\hat{A}$.

1. Soit $f(X_1,\ldots,X_r) = \sum \lambda_{i_1\ldots i_r} X_1^{i_1}\ldots X_r^{i_r} \in A[[X_1,\ldots,X_r]]$.

Pour $n \in \mathbb{N}$, on pose $x_n = \sum_{\substack{(i_1,\ldots,i_r) \\ i_1+\ldots+i_r \leq n}} \overline{\lambda}_{i_1\ldots i_n} \overline{a}_1^{i_1}\ldots\overline{a}_r^{i_r}$.

Démontrer que la suite $(x_n)_{n\in\mathbb{N}}$ est une suite de Cauchy de $\hat{A}$. On note, dans la suite, $f(a_1,\ldots,a_r)$ la limite de cette suite (i.e. la somme $\sum \lambda_{i_1\ldots i_r} \overline{a}_1^{i_1}\ldots\overline{a}_r^{i_r}$ de la série de terme général $(\overline{\lambda}_{i_1\ldots i_r} \overline{a}_1^{i_1}\ldots\overline{a}_r^{i_r})$).

Démontrer que l'application $\theta : f(X_1,\ldots,X_r) \longmapsto f(a_1,\ldots,a_r)$ de $A[[X_1,\ldots,X_r]]$ dans $\hat{A}$ est un homomorphisme d'anneaux et que, si $\{a_1,\ldots,a_r\}$ est un système de générateurs de l'idéal (alors de type fini) a, cet homomorphisme est surjectif.

2. *On suppose* a *de type fini,* $\{a_1,\ldots,a_r\}$ *système de générateurs de* A *et* A *séparé dans la topologie* a*-adique.*

Démontrer que $\ker(\theta)$ est l'adhérence de l'idéal $(X_1-a_1,\ldots,X_r-a_r)$

dans la topologie de $A[[X_1,\ldots,X_r]]$ définie par l'idéal $aA[[X_1,\ldots,X_r]] + \Sigma_{i=1}^{r}(X_i-a_i)A[[X_1,\ldots,X_r]]$ de $A[[X_1,\ldots,X_r]]$.

3. *On suppose* A *noethérien et* a *contenu dans le radical de* A.

Démontrer que l'idéal $aA[[X_1,\ldots,X_r]]$ est alors contenu dans le radical de $A[[X_1,\ldots,X_r]]$.

En déduire que le complété de A dans la topologie a-adique est isomorphe à l'anneau quotient $A[[X_1,\ldots,X_r]]/(X_1-a_1,\ldots,X_r-a_r)$.

(5). Soient A un anneau noethérien, a un idéal contenu dans le radical de A, M un A-module de type fini, $\hat{M}$ le complété de M dans la topologie a-adique.

Démontrer que si l'élément a de A n'est pas diviseur de zéro dans M il n'at pas diviseur de zéro dans $\hat{M}$.

(6). Soient A un anneau, m un idéal de A, $\hat{A}$ le séparé complété de A dans la topologie m-adique.

1. Démontrer l'isomorphisme $\widehat{A^n} \simeq \hat{A}^n$.

En déduire que, si M est un A-module *de type fini*, un élément du séparé complété $\hat{M}$ de M dans la topologie m-adique s'écrit $\Sigma\lambda_i\alpha_M(x_i)$ où $\lambda_i \in \hat{A}$, $x_i \in M$.

2. En déduire que si m est *de type fini*, $\hat{m} = m\hat{A}$.

(7). Soient A un anneau, m un idéal *de type fini* de A. On suppose A *séparé complet* dans la topologie m-adique et A/m *noethérien*.

Démontrer que A est noethérien.

En déduire que le séparé complété de l'anneau $\mathcal{E}_n$ des germes à l'origine des fonctions de classe C^∞ au voisinage de 0 dans $\mathbb{R}^n$ est noethérien.

(On peut démontrer que ce séparé complété est isomorphe à l'anneau $\mathbb{R}[[X_1,\ldots,X_n]]$ des séries formelles à n indéterminées $X_1,\ldots,X_n$).

(8). Soient A un anneau, C une catégorie de A-modules filtrés avec pour morphismes les applications A-linéaires continues, C^s la sous-catégorie pleine de C dont les objets sont les modules filtrés *séparés*.

Démontrer que le foncteur d'inclusion de C^s dans C admet un adjoint à gauche $(-)^s$. Etudier le cas où A est noethérien et C est la catégorie des A-modules a-adiques où a est un idéal de A. Soit alors $S = 1 + a$.

Démontrer que le foncteur $(-)^s$ est isomorphe au foncteur $S^{-1}(-)$.

Que peut-on dire de l'idéal $S^{-1}a$ de l'anneau $S^{-1}A$?

(9). Soient A un anneau intègre, X une indéterminée, $R = A[[X]]$, S une partie multiplicative de A.

Démontrer que l'on a une inclusion $S^{-1}R \subset (S^{-1}A)[[X]]$ et que cette inclusion est en général stricte. (Prendre $A = \mathbf{Z}$, $S = \{2^n\}_{n\in N}$ et considérer $\Sigma_{n\in N} X^i/2^i$).

Démontrer que, si T est la partie multiplicative $\{f(X) \in R / f(0) \in S\}$ de R, $T^{-1}R$ est le séparé de $S^{-1}R$, pour la topologie (X)-adique.

Démontrer que $(S^{-1}A)[[X]]$ est le complété séparé de $S^{-1}R$ dans la topologie (X)-adique.

(10). Utiliser la proposition II.9 et les propriétés d'exactitude des limites projectives ((FFAC). Chap.3. Prop. V.4) pour donner une autre démonstration de la proposition II.2.

(11).(Théorème de Chevalley)

Soient A un anneau *semi-local noethérien complet*, m son radical, $(a_n)_{n\in N}$ une suite décroissante d'idéaux de A telle que $\bigcap_{n\in N} a_n = (0)$.

Démontrer qu'il existe une application : $n \longmapsto s(n)$ de N dans N telle que $s(n)$ tende vers ∞ avec n et que, pour tout $n\in N$, $a_n \subset m^{s(n)}$.

(Autrement dit, *la topologie naturelle de A est la moins fine des topologies linéaires séparées de A*).

(Raisonner par l'absurde, supposant l'existence de $s \in N$ tel que, pour tout $n \in N$, $a_n \not\subset m^s$. Utiliser le fait que, dans l'anneau artinien A/m^s, $\bigcap_{n\in N} (a_n+m^s)/m^s \neq (0)$, pour démontrer l'existence de x_s appartenant à a_n+m^s, pour tout $n\in N$, mais n'appartenant pas à m^s. Définir alors une suite de Cauchy $(x_t)_{t\geq s}$ de A telle que $x_t = x_s \pmod{m^s}$ et $x_t \in a_n+m^t$, pour tout $n\in N$. Démontrer que la limite x de cette suite est 0 mais n'appartient pas à m^s).

(12). Soient A un anneau, a un idéal de A. On suppose A séparé complet dans la topologie a-adique. Soit $(x_n)_{n\in N}$ une suite d'éléments de A. On pose $S_n = \Sigma_{i=0}^{n} x_i$.

On dit que la *série* de terme général x_n est *convergente* si la suite $(S_n)_{n\in N}$ l'est.

La limite de la suite $(S_n)_{n\in N}$ est appelée la *somme de la série* et notée $\Sigma_0^\infty x_i$.

Démontrer les équivalences :

(i) la série de terme général x_n est convergente

(ii) x_n tend vers 0 quand n tend vers l'infini.

(13). Soit p un nombre premier. On considère le complété $\widehat{(\mathbf{Z}_{(p)})}$ de l'anneau local $\mathbf{Z}_{(p)}$ ou ce qui revient au même de l'anneau $\mathbf{Z}$ dans la topologie p-adique.

1. Quelles sont les sommes des séries suivantes :

terme général p^n ?

terme général $(p-1)p^n$?

série $x_o = 3$, $x_{2n} = 6.7^{2n}$, $x_{2n+1} = 2.7^{2n+1}$ (avec $p = 7$) ?

2. Démontrer qu'un élément de $\mathbb{Z}$ s'écrit *de manière unique* $\Sigma_{n=0}^{\infty} a_n p^n$ où $a_n \in \{0,\ldots,p-1\}$.

Que peut-on dire de cette représentation pour un élément de N?

3. Démontrer que tout élément de $(\widehat{\mathbb{Z}_{(p)}})$ s'écrit de manière unique $\Sigma_{n=0}^{\infty} a_n p^n$ où $a_n \in \{0,\ldots,p-1\}$. Comment s'écrit un élément *inversible* de $(\widehat{\mathbb{Z}_{(p)}})$?

4. Démontrer que l'anneau $(\widehat{\mathbb{Z}_{(p)}})$ est intègre. Son corps des fractions est noté $\mathbb{Q}_p$ et appelé le *corps des nombres p-adiques*. L'anneau $(\widehat{\mathbb{Z}_{(p)}})$ est appelé *l'anneau des entiers p-adiques*.

Démontrer qu'un élément de $\mathbb{Q}_p$ s'écrit de manière unique $\Sigma_{n\geq m} a_n p^n$ où $a_n \in \{0,\ldots,p-1\}$ et m est un entier positif, nul ou négatif . (La représentation ci-dessus est appelée la *représentation p-adique* de l'élément considéré de $\mathbb{Q}_p$).

Quels sont les éléments de $\mathbb{Q}_p$ qui admettent une représentation p-adique *périodique* , i.e. telle qu'il existe $r \in N$ et $s \in \mathbb{Z}$ tels que $a_{s+qr} = a_s$, $a_{s+1+qr} = a_{s+1},\ldots,a_{s+r-1+qr} = a_{s+r-1}$ pour tout $q \in N$?

(14). Soient A un anneau semi-local, r son radical.

Démontrer les équivalences :

(i) A est noethérien

(ii) les deux conditions suivantes sont satisfaites :

1. tout idéal de A est fermé pour la topologie r-adique
2. tout idéal maximal de A est de type fini

(15). Soient A un anneau local, non nécessairement noethérien, *séparé complet*, m son idéal maximal, k son corps résiduel, X une indéterminée.

Si $f(X) \in A[X]$, on note $\overline{f}(X)$ son image dans $k[X]$ (obtenue en remplaçant les coefficients de $f(X)$ par leurs classes modulo m).

Démontrer que, si $f(X)$, $g_o(X)$, $h_o(X)$ appartiennent à $A[X]$, $g_o(X)$ étant unitaire, sont tels que $\overline{f}(X) = \overline{g}_o(X)\overline{h}_o(X)$ et $(\overline{g}_o(X),\overline{h}_o(X)) = 1$, il existe $g(X)$, $h(X) \in A[X]$ tels que $g(X)$ soit unitaire, $\overline{g}(X) = \overline{g}_o(X)$, $\overline{h}(X) = \overline{h}_o(X)$ et $f(X) = g(X)h(X)$.

(Démontrer, de proche en proche, l'existence de représentants $g_n(X)$

unitaires de $\overline{g}_o(X)$ et $h_n(X)$ de $h_o(X)$ tels que $f(X) - g_n(X)h_n(X)$ appartienne à $m^{n+1}A[X]$).

(16). Soient A un anneau, $(a_n)_{n\in N}$ une filtration de A, $X_1,\ldots,X_r$ des indéterminées.

Une série formelle $\Sigma c_{i_1\ldots i_r} X_1^{i_1}\ldots X_r^{i_r} \in A[[X_1,\ldots,X_r]]$ est dite *restreinte* si $c_{i_1\ldots i_r}$ tend vers 0 quand $\inf(i_1,\ldots,i_r)$ tend vers l'infini.

Démontrer que les séries formelles restreintes forment un sous-anneau de $A[[X_1,\ldots,X_r]]$ noté $A\{X_1,\ldots,X_r\}$.

Démontrer que si A est séparé complet dans la filtration $(a_n)_{n\in N}$ l'anneau $A\{X_1,\ldots,X_r\}$ des séries formelles restreintes est isomorphe à $\varprojlim_{n\in N} ((A/a_n)[X_1,\ldots,X_r]$.

Soit B un anneau séparé complet pour une filtration $(b_n)_{n\in N}$ et soit u une application linéaire continue de A dans B. Démontrer que, pour toute famille $(b_i)_{i=1,\ldots,r}$ d'éléments de B, il existe un homomorphisme continu v et un seul de $A\{X_1,\ldots,X_r\}$, muni de la filtration $(F_n)_{n\in N}$, où F_n est l'idéal des séries dont tous les coefficients appartiennent à a_n, dans B tel que $v(a) = u(a)$ pour tout $a \in A$ et $v(X_i) = b_i$ $(i = 1,\ldots,r)$.

CHAPITRE 9

Dérivations et différentielles

C'est de manière *purement algébrique* qu'apparaissent les notions de dérivations et différentielles à propos des *polynômes* et des *séries formelles* mais on oublie souvent ce point de vue en raison de l'importance de ces notions dans les cours de calcul différentiel à propos des *fonctions différentiables* dont les polynômes à coefficients réels, par exemple, sont des cas particuliers.

Voici quelques rappels qui figurent, en général, *au début d'ouvrages de géométrie différentielle.*

Soient U *un ouvert de* $\mathbb{R}^n$, B *la* $\mathbb{R}$*-algèbre des fonctions de classe* C^∞ *de* U *dans* $\mathbb{R}$.

Un *champ de vecteurs* (de classe C^∞) *sur* U est la donnée d'une application : $X : (x_1,\ldots,x_n) \longmapsto (a_i(x_1,\ldots,x_n))_{i=1,\ldots,n}$ (de classe C^∞) de U dans $\mathbb{R}^n$.

On peut interpréter, en termes de fonctions, un tel champ de vecteur comme suit :

Soit D *l'application de* B *dans* B **telle** que :

$D(f)(x_1,\ldots,x_n) = \Sigma_{i=1}^n a_i(x_1,\ldots,x_n)\partial f/\partial X_i(x_1,\ldots,x_n)$

Elle vérifie les conditions :

(1) $D(f+g) = D(f) + D(g)$

(2) $D(fg) = gD(f) + fD(g)$

(3) $D(\mathbb{R}) = 0$, où $\mathbb{R}$ est identifié à la sous-algèbre de B des fonctions constantes.

Soit, réciproquement, D *une application de* B *dans* B *satisfaisant aux conditions* (1), (2) *et* (3).

On vérifie qu'elle est de la forme :

$f \longrightarrow \Sigma_{i=1}^n a_i(x_1,\ldots,x_n)\ \partial f/\partial X_i(x_1,\ldots,x_n)$ où a_i est de classe C^∞.

Une application de B dans B satisfaisant aux conditions (1), (2) et (3) est appelée une $\mathbb{R}$*-dérivation* de B *dans* B.

L'ensemble $\mathrm{Der}_{\mathbb{R}}(B,B)$ des $\mathbb{R}$-dérivations de B dans B est muni d'une structure naturelle de B-module : en termes de champs de vecteurs, si X est un champ de vecteurs et $f \in B$, fX est le champ de vecteurs : $(x_1,\ldots,x_n) \longmapsto ((fa_i)(x_1,\ldots,x_n))$.

Soit maintenant $f \in B$.

La différentielle df de f est l'application de U dans le dual $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n,\mathbb{R})$ de $\mathbb{R}^n$:

$$(x_1,\ldots,x_n) \longmapsto ((h_1,\ldots,h_n) \longmapsto \Sigma_{i=1}^n h_i \partial f/\partial X_i(x_1,\ldots,x_n))$$

Le sous-module du B-module des applications de U dans $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n,\mathbb{R})$ engendré par les différentielles df des éléments f de B est appelé le *module des différentielles de la* $\mathbb{R}$*-algèbre* B *et noté* $\Omega_{B/\mathbb{R}}$.

Un élément de $\Omega_{B/\mathbb{R}}$ est souvent appelé une *forme différentielle de degré* 1 *sur* U.

Le B-module $\Omega_{B/\mathbb{R}}$ est libre de base, les différentielles dx_i (i=1,...,n) des projections de U sur les facteurs de $\mathbb{R}^n$. C'est une circonstance assez particulière et on verra dans l'étude faite dans ce chapitre que la situation est souvent moins simple.

L'application ϕ de $\Omega_{B/\mathbb{R}} \times \mathrm{Der}_{\mathbb{R}}(B,B)$ dans B définie par :

$$(\phi(gdf,D))(x_1,\ldots,x_n) = g(x_1,\ldots,x_n)\Sigma_{i=1}^n a_i(x_1,\ldots,x_n)\partial f/\partial X_i(x_1,\ldots,x_n)$$

(où D correspond à l'application $(x_1,\ldots,x_n) \longmapsto (a_i(x_1,\ldots,x_n))_{i=1,\ldots,n}$) est B-bilinéaire.

Elle permet d'identifier le B-module $\mathrm{Der}_{\mathbb{R}}(B,B)$ au dual du B-module $\Omega_{B/\mathbb{R}}$.

Ces rappels de calcul différentiel étant faits, voici l'idée de l'étude algébrique effectuée dans ce chapitre.

Soient A *un anneau,* B *une* A*-algèbre.*

On définit les A-dérivations de B dans un B-module M comme les applications de B dans M vérifiant les conditions (1) et (2) et l'analogue de (3).

L'ensemble $\mathrm{Der}_A(B,M)$ de ces dérivations est muni d'une structure de B-module.

On définit, de manière naturelle, un *foncteur*, noté $\mathrm{Der}_A(B,-)$ de Mod(B) dans Mod(B). Ce foncteur est *représentable*. Un représentant est un couple $(\Omega_{B/A},d_{B/A})$ d'un B-module $\Omega_{B/A}$, appelé *module des différentielles de la* A*-algèbre* B, et d'une A-dérivation $d_{B/A}$ de B dans $\Omega_{B/A}$ telle que, toute A-dérivation de B dans un B-module M se factorise de manière unique par $d_{B/A}$ et une application B-linéaire de $\Omega_{B/A}$ dans M. Autrement dit, on a un isomorphisme fonctoriel en M,

$$\mathrm{Der}_A(B,M) \simeq \mathrm{Hom}_B(\Omega_{B/A},M)$$

qui dans le cas M=B redonne le fait que $\mathrm{Der}_A(B,B)$ est isomorphe au dual de $\Omega_{B/A}$.

Dans I, on définit la notion de dérivation et on donne deux constructions du module des différentielles.

Dans II, on étudie parallèlement le comportement des modules de dérivations et de différentielles par les opérations usuelles (localisation et quotient par exemple). On en déduit des procédés de calcul, en particulier, celui du module de différentielles d'une algèbre affine.

Dans III, on applique les notions différentielles introduites au problèmes de séparabilité.

I. Définition des dérivations et différentielles

1. *Définition des dérivations*

Soient A *un anneau,* B *une* A*-algèbre d'homomorphisme structural* ρ, M *un* B*-module.*

Une dérivation de B *dans* M *est une application* $D : B \longrightarrow M$ *satisfaisant aux conditions suivantes*

(1) $\forall x,y \in B,\ D(x+y) = D(x) + D(y)$

(2) $\forall x,y \in B,\ D(xy) = xD(y) + yD(x)$

(3) $D(\rho(A)) = 0$

On dit aussi, plus simplement, que D est une A*-dérivation de* B *dans* M

Exemple

Un anneau B est muni d'une structure de $\mathbb{Z}$-algèbre au moyen de l'homomorphisme $\rho : n \longmapsto n1$. Une dérivation de la $\mathbb{Z}$-algèbre ainsi définie B dans M est appelée une *dérivation de l'anneau* B *dans* M.

On peut remarquer que, pour une telle dérivation, la condition (3) devient inutile car $D(1) = D(1^2)$; donc d'après (2), $D(1^2) = 2D(1)$ et $D(1) = 0$. Il en résulte $D(n1) = 0$ si $n \in \mathbb{N}$, d'après (1). Comme D est un homomorphisme de groupes additifs, $D(\rho(\mathbb{Z})) = 0$.

Avec les notations de la définition , on désigne par $\mathrm{Der}_A(B,M)$ *l'ensemble des* A*-dérivations de* B *dans* M.

On rappelle que $\rho_*(M)$ est le A-module obtenu par restriction des scalaires à partir du B-module M.

Proposition 1.1

Les notations sont celles de la définition.

1. Une A*-dérivation de* B *dans* M *est une application* A*-linéaire de* B *dans* $\rho_*(M)$.

2. Le sous-ensemble $\mathrm{Der}_A(B,M)$ *de* $\mathrm{Hom}_A(B,\rho_*(M))$ *est un sous-module de* $\mathrm{Hom}_A(B,\rho_*(M))$.

Démonstration

1. Soient $D \in \mathrm{Der}_A(B,M)$, $a \in A$, $x \in B$. Alors,

$D(ax) = D(\rho(a)x) = \rho(a)D(x) + xD(\rho(a)) = \rho(a)D(x) = aD(x)$.

2. est clair.

Le foncteur $\mathrm{Der}_A(B,-)$

Proposition 1.2

Soient A *un anneau,* B *une* A*-algèbre,* M *et* M' *des* B*-modules,* f *une application* B*-linéaire de* M *dans* M'.

Si $D \in \mathrm{Der}_A(B,M)$, $f \circ D$ *appartient à* $\mathrm{Der}_A(B,M')$.

Démonstration

Il suffit de vérifier que $f\circ D$ satisfait à la condition (3).

Or, $(f\circ D)(xy) = f(xD(y)+yD(x)) = xf(D(y))+yf(D(x)) = x(f\circ D)(y)+y(f\circ D)(x)$

On note $\mathrm{Der}_A(B,f)$ *l'application* : $D \longmapsto f\circ D$ *de* $\mathrm{Der}_A(B,M)$ *dans* $\mathrm{Der}_A(B,M')$.

Il est clair que les applications : $M \longmapsto \mathrm{Der}_A(B,M)$; $f \longmapsto \mathrm{Der}_A(B,f)$ définissent *un foncteur covariant,* noté $\mathrm{Der}_A(B,-)$, *de la catégorie* Mod(B) *des* B*-modules dans elle-même* (et donc, par oubli de structure, dans *Ens*).

On verra ultérieurement que ce foncteur de Mod(B) dans *Ens* est représentable.

Proposition 1.3 (*comportement de* $\mathrm{Der}_A(B,M)$ *en* B)

Soient A *un anneau,* B *une* A*-algèbre,* σ *un homomorphisme d'anneaux de* B *dans* C, M *un* C*-module.*

1. Si $D \in \mathrm{Der}_A(C,M)$, $D \circ \sigma$ *appartient à* $\mathrm{Der}_A(B,\sigma_*(M))$.

2. Si σ *est surjectif, l'application* $D \longrightarrow D \circ \sigma$ *est une bijection de* $\mathrm{Der}_A(C,M)$ *sur le sous-module de* $\mathrm{Der}_A(B,\sigma_*(M))$ *des dérivations s'annulant sur* $\ker(\sigma)$.

Démonstration

1. $(D\circ\sigma)(xy) = D(\sigma(x)\sigma(y)) = \sigma(x)(D\circ\sigma)(y)+\sigma(y)(D\circ\sigma)(x)=x(D\circ\sigma)(y) + y(D\circ\sigma)(x)$.

2. Il est clair que $D \circ \sigma$ s'annule sur $\mathrm{Ker}(\sigma)$, car D est un homomorphisme de groupes additif.

Soit, réciproquement, $D' \in \mathrm{Der}_A(B,\sigma_*(M))$ s'annulant sur $\ker(\sigma)$. Elle définit, par passage au quotient, une application A-linéaire de $B/\ker(\sigma)=C$ dans M. Cette application est une A-dérivation de C dans M.

On démontrera, ultérieurement (première suite exacte fondamentale. II.4) un résultat plus général.

2. Exemples de dérivations

1. Soit B *la* $\mathbb{R}$*-algèbre des fonction de classe* C^∞ *sur une variété différentiable* X, *par exemple un ouvert de* $\mathbb{R}^n$.

Un élément de $\mathrm{Der}_{\mathbb{R}}(B,B)$ est un *champ de vecteurs sur* X.

2. Soit D *un tel champ de vecteurs.* Soit $x \in X$. L'application $f \longmapsto f(x)$ de B dans $\mathbb{R}$ est un homomorphisme surjectif qui munit $\mathbb{R}$ d'une structure de B-module.

L'application $D_x : B \longmapsto \mathbb{R}$ définie par $D_x(f) = D(f)(x)$ est appelé un *vecteur tangent en* x à X. Elle vérifie la condition :

$$(1)\quad D_x(fg) = f(x)D_x(g) + g(x)D_x(f) \qquad (f,g \in B)$$

Elle se prolonge en une application, encore notée D_x, de l'anneau local A des germes de fonctions C^∞ en x telle que :

$$D_x(\widetilde{f/g}) = (D_x(f)g(x) - D_x(g)f(x))/g(x)^2$$

où $\widetilde{f/g}$ est le germe en x de f/g $(f,g \in B/g(x) \neq 0)$

L'application ainsi prolongée vérifie encore (1). *C'est une dérivation de* A *dans* $\mathbb{R}$.

3. Il est possible de donner une version algébrique de cette situation.

Soient A *un anneau local,* m *son idéal maximal,* k *son corps résiduel.*

On note x l'unique point fermé de Spec(A). Si $f \in A$, on rappelle que *la valeur de* f *en* x *est l'élément classe de* f *modulo* m *du corps* $k(x) = k$.

On suppose que la surjection canonique de A *sur* k *admet une section* qui permet alors d'identifier k à un sous-corps de A. Cette condition est vérifiée dans les cas géométriques classiques.

Soit D *une application de* A *dans* k *telle que :*

$$(2)\quad D(fg) = f(x)D(g) + g(x)D(f) \qquad (f,g \in A)$$

Il est clair que $D(m^2) = 0$ puisque un élément de m^2 est somme finie

d'éléments de la forme fg où f et g appartiennent à m, i.e. sont tels que $f(x) = g(x) = 0$.

L'application D définit donc une application k-linéaire u du K-espace vectoriel m/m^2 dans k par $u(\overline{f}) = D(f)$ où f est un représentant dans m de l'élément $\overline{f}$ de m/m^2.

Réciproquement, *soit u une forme linéaire sur* m/m^2. Il existe une application D de A dans k et une seule satisfaisant à (2) et telle que $u(\overline{f}) = D(f)$: elle est définie par $D(f) = u(\overline{f-f(x)})$ où $f(x)$ est identifié à un élément de A au moyen de la section S.

Ainsi, *l'ensemble des applications* D *de* A *dans* k *vérifiant* (2), i.e. *l'ensemble* $\mathrm{Der}_k(A,k)$ *est un* k*-espace vectoriel isomorphe au dual* $\mathrm{Hom}_k(m/m^2,k) = (m/m^2)^*$ *du* k*-espace vectoriel* m/m^2.

L'interprétation des cas classiques conduit à la définition suivante.

Définition

Soient A *un anneau local,* m *son idéal maximal,* k *son corps résiduel. L'espace vectoriel* $(m/m^2)^*$ *sur le corps* k *est appelé l'espace tangent de* A. *L'espace vectoriel* m/m^2 *est appelé l'espace cotangent de* A.

4. Soient A *un anneau,* B *une* A*-algèbre d'homomorphisme structural* ρ, M *un* B*-module.*

On munit l'ensemble $D_B(M) = B \times M$ d'une structure d'anneau en définissant la somme et le produit par :

$$(x,m) + (x',m') = (x+x',\ m+m')$$

$$(x,m)(x',m') = (xx',\ xm' + x'm)$$

et d'une structure de B-algèbre d'homomorphisme structural l'injection $i : x \longrightarrow (x,0)$ de B dans $D_B(M)$.

Ainsi, $D_B(M)$ est muni d'une structure de A-algèbre d'homomorphisme structural $i \circ \rho$.

L'application $m \longmapsto (0,m)$ est un isomorphisme de B-modules de M sur un idéal de carré nul de $D_B(M)$ *auquel on l'identifie dans la suite.*

Si p est la projection $(x,m) \longmapsto x$ de $D_B(M)$ sur B, on a une suite exacte de B-modules

$$0 \longrightarrow M \xrightarrow{i} D_B(M) \xrightarrow{p} B \longrightarrow 0$$

Proposition 1.4

Soient B *une* A*-algèbre,* M *un* B*-module.*

L'application $D \longmapsto 1_B+D$, *où* $(1_B+D)(x) = (x,D(x))$, *est une bijection*

de l'ensemble $\mathrm{Der}_A(B,M)$ *sur l'ensemble des homomorphismes de* A*-algèbres de* B *dans* $D_B(M)$ *inverses à droite de* p.

Démonstration

Soit D une A-dérivation de B dans M. Posant $1_B+D = u$, on a, pour $x,x' \in B$, $u(xx')=(xx',D(xx'))=(xx',xD(x')+x'D(x))=(x,D(x))(x',D(x'))=u(x)u(x')$.

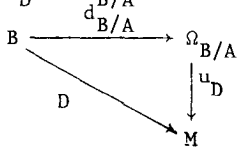
Soient $a \in A$, $x \in B$. Alors, $u(ax)=u(\rho(a)x)=(\rho(a)x,\rho(a)D(x))=au(x)$ et donc u est un homomorphisme de A-algèbres de B dans $D_B(M)$. Il est clair que $p \circ u = 1_B$.

Réciproquement, soit u un homomorphisme de A-algèbres de B dans $D_B(M)$ tel que $p \circ u = 1_B$. Si x est un élément de B, u(x) s'écrit (x,D(x)). La définition du produit dans $D_B(M)$ montre que D est une dérivation de B dans M. C'est une A-dérivation car, si $a \in A$, $u(\rho(a)) = (\rho(a),0)$.

3. Première construction du module des différentielles

Soient A *un anneau,* B *une* A*-algèbre.*

On va démontrer que *le foncteur* $\mathrm{Der}_A(B,-)$ *de* Mod(B) *dans Ens est représentable* et en expliciter un représentant, i.e. *un* B*-module* $\Omega_{B/A}$ *et une* A*-dérivation* $d_{B/A}$ *de* B *dans* $\Omega_{B/A}$ *tels que, pour tout* B*-module* M *et toute* A*-dérivation* D *de* B *dans* M, *il existe une application* B*-linéaire et une seule* u_D *de* $\Omega_{B/A}$ *dans* M *tel que la diagramme*



soit commutatif.

La construction ci-dessous "par générateurs et relations" est bien naturelle.

Soit $B^{(B)}$ *le* B*-module libre engendré par l'ensemble* B, i.e.(FFAC.) le B-module des applications de B dans B à support fini. *Soit* i *l'application de* B *dans* $B^{(B)}$ *qui associe à* x *l'application* e_x *telle que* $e_x(y) = 0$ *si* $y \neq x$ *et* $e_x(x) = 1$.

On désigne par $\Omega_{B/A}$ *le* B*-module quotient de* $B^{(B)}$ *par le sous-module* R *engendré par les éléments d'une des formes :*

$$e_{xx'} - xe_{x'} - x'e_x \qquad (x,x' \in B)$$
$$e_{\rho(a)} \qquad (a \in A)$$

et par $d_{B/A}$ *le composé* $p \circ i$, *où* p *désigne la surjection canonique de* $B^{(B)}$ *sur* $\Omega_{B/A}$.

Proposition 1.5

Le couple $(\Omega_{B/A}, d_{B/A})$ *représente le foncteur* $\mathrm{Der}_A(B,-)$.

Démonstration

Par construction même, $d_{B/A}$ est une A-dérivation.

Soit D une A-dérivation de B dans un B-module M. Elle définit alors une unique application B-linéaire v_D de $B^{(B)}$ dans M telle que $D = v_D \circ i$, i.e $v_D(e_x) = D(x)$ pour $x \in B$.

Comme D est une dérivation, le noyau de v_D contient R et v_D définit par passage au quotient une application B-linéaire $u_D : \Omega_{B/A} \longrightarrow M$. Cette application est telle que $D = v_D \circ i = u_D \circ p \circ i = u_D \circ d_{B/A}$.

Les éléments $d_{B/A}(x)$ où x parcourt B forment un système de générateurs du B-module $\Omega_{B/A}$. On en déduit que, si u est une application B-linéaire de $\Omega_{B/A}$ dans M telle que $D = u \circ d_{B/A}$, on a l'égalité $u = u_D$.

4. Deuxième construction du module des différentielles

On va commencer par rappeler quelques résultats classiques.

Soit f *une fonction définie dans un voisinage ouvert* U *de* $x \in \mathbb{R}^n$ *à valeurs dans* $\mathbb{R}^m$.

On dit que f *est différentiable en* x s'il existe une application linéaire L de $\mathbb{R}^n$ dans $\mathbb{R}^m$ tel que, pour $h \in \mathbb{R}^n$ tel que $x+h \in U$,

$$f(x+h) = f(x) + L(h) + ||h||g(h)$$

où g(h) tend vers 0 avec h.

L'application linéaire L est alors appelée la *différentielle de* f en x et notée df(x).

Si $h = (h_1,\ldots,h_n)$, $L(h) = \Sigma_{i=1}^n A_i h_i$ où A_i est la dérivée partielle $\partial f/\partial X_i(x)$ et on a :

$$f(x_1+h_1,\ldots,x_n+h_n) - f(x_1,\ldots,x_n) = \Sigma_{i=1}^n A_i h_i + ||h||g(h)$$

En particulier, si f est une fonction polynôme, ou plus généralement une fonction admettant un développement limité à l'ordre 2 en x, on voit que df(x)(h) *est la partie homogène du premier ordre de* $f(x_1+h_1,\ldots,x_n+h_n) - f(x_1,\ldots,x_n)$.

On peut donner une interprétation algébrique dans le cas des polynômes

Soient A *un anneau,* $X_1,\ldots,X_n,H_1,\ldots,H_n$ *des indéterminées,* $f(X_1,\ldots,X_n) \in A[X_1,\ldots,X_n]$. On peut écrire :

$f(X_1+H_1,\dots,X_n+H_n) - f(X_1,\dots,X_n)=\Sigma_{i=1}^{n} A_iH_i + g(X_i,\dots,X_n,H_i,\dots,H_n)$ où g appartient à l'idéal α de $A[X_1,\dots,X_n,H_1,\dots,H_n]$ engendré par les éléments H_iH_j $(i,j = 1,\dots,n)$.

On peut *identifier* la différentielle de f en $(x_1,\dots,X_n)$ à la classe modulo l'idéal α de $\Sigma_{i=1}^{n} A_iH_i$ et, en particulier, la différentielle notée dX_i de la fonction polynôme $(X_1,\dots,X_n) \longmapsto X_i$, à la classe de H_i modulo α.

Si on pose $Y_i = X_i + H_i$ $(i = 1,\dots,n)$, les éléments $Y_1,\dots,Y_n$ sont évidemment algébriquement indépendants sur l'anneau $A[X_1,\dots,X_n]$ et peuvent être considérées comme des indéterminées.

On a un isomorphisme de A-algèbres de $B \underset{A}{\otimes} B$ sur $A[X_1,\dots,X_n,Y_1,\dots,Y_n]$

$f(X_1,\dots,X_n) \otimes g(X_1,\dots,X_n) \longmapsto f(X_1,\dots,X_n)g(Y_1,\dots,Y_n)$

On peut écrire, après identification par cet isomorphisme,

$f(Y_1,\dots,Y_n) - f(X_1,\dots,X_n) = 1 \otimes f(X_1,\dots,X_n) - f(X_1,\dots,X_n) \otimes 1$

$= \Sigma_{i=1}^{n} A_i(1 \otimes X_i - X_i \otimes 1) + g$ où g appartient à l'idéal de $B \underset{A}{\otimes} B$ engendré par les éléments $(1 \otimes X_i - X_i \otimes 1)(1 \otimes X_j - X_j \otimes 1)$ $(i,j = 1,\dots,n)$.

En définitive, soit I l'idéal de $B \underset{A}{\otimes} B$ engendré par les éléments $1 \otimes f(X_1,\dots,X_n) - f(X_1,\dots,X_n) \otimes 1$. Il est engendré en tant que B-module, où B opère sur le facteur B de gauche, par les éléments $1 \otimes X_i - X_i \otimes 1$.

On appelle *différentielle de* B *sur* A la classe modulo I^2 d'un élément de I. Plus précisément, la différentielle de l'élément f de B est la classe modulo I^2 de $1 \otimes f - f \otimes 1$.

Soient A *un anneau,* B *une* A*-algèbre.*

L'application A*-bilinéaire* $(x,x') \longmapsto xx'$ *de* $B\times B$ *dans* B *définit une application* A*-linéaire* ε *de* $B \underset{A}{\otimes} B$ *dans* B *telle que* :

(2) $\varepsilon(\Sigma x_i \otimes x_i') = \Sigma x_i x_i'$

Cette application est un homomorphisme de A-algèbres. Il est *surjectif* et, de plus, si i_1 et i_2 sont les homomorphismes de A-algèbres de B dans $B \underset{A}{\otimes} B$ définis par :

(3) $i_1(x) = x \otimes 1 \qquad i_2(x) = 1 \otimes x$

on a :

(4) $\varepsilon \circ i_1 = \varepsilon \circ i_2 = 1_B$

On munit dans la suite $B \underset{A}{\otimes} B$ *de la structure de* B*-algèbre d'homomorphisme structural* i_1.

Il est clair que ε est un homomorphisme de B-algèbres.

Lemme 1

Le noyau I *de* ε *est l'idéal de* $B \underset{A}{\otimes} B$ *engendré par les éléments* $1\otimes x - x\otimes 1$ $(x \in B)$.

Démonstration

Il est clair que $\varepsilon(1\otimes x - x\otimes 1) = 0$. D'autre part, si $\Sigma x_i \otimes x_i'$ appartient à I, on peut écrire, puisque $\Sigma x_i x_i' = 0$

$$\Sigma x_i\otimes x_i' = \Sigma(x_i\otimes x_i') - \Sigma(x_i x_i')\otimes 1 = \Sigma(x_i\otimes 1)(1\otimes x_i' - x_i'\otimes 1)$$

Lemme 2

$$B \underset{A}{\otimes} B = i_1(B) \oplus I.$$

Démonstration

L'égalité $B \underset{A}{\otimes} B = i_1(B) + I$ résulte de l'égalité

$$x\otimes x' = (xx')\otimes 1 + (x\otimes 1)(1\otimes x' - x'\otimes 1) \quad \text{si } x,x' \in B$$

L'égalité $\varepsilon\circ i_1 = 1_B$ montre alors que $I \cap i_1(B) = (0)$.

Il résulte du lemme 2 que $(B \underset{A}{\otimes} B)/I^2 = i_1(B) \oplus I/I^2$.

Soient ψ *l'isomorphisme* $i_1 \oplus 1_{I/I^2}$ *du* B*-module* $D_B(I/I^2)$ $B\oplus I/I^2$ *sur* $(B \underset{A}{\otimes} B)/I^2$, π *la surjection canonique de* $B \underset{A}{\otimes} B$ *sur* $(B \underset{A}{\otimes} B)/I^2$. La suite d'homomorphismes de A-algèbres

$$B \xrightarrow{i_2} B \underset{A}{\otimes} B \xrightarrow{\pi} (B \underset{A}{\otimes} B)/I^2 \xrightarrow{\psi^{-1}} D_B(I/I^2) \xrightarrow{p} B$$

$$x \longrightarrow 1\otimes x \longrightarrow (x\otimes 1, \pi(1\otimes x - x\otimes 1)) \longrightarrow (x, \pi(1\otimes x - x\otimes 1)) \longrightarrow x$$

indique que l'homomorphisme $u = \psi^{-1} \circ \pi \circ i_2$ de A-algèbres de B dans $D_B(I/I^2)$ est inverse à droite de p.

L'application $d_{B/A}$ de B dans I/I^2 définie par $d_{B/A}(x) = \pi(1\otimes x - x\otimes 1)$ est donc une A-dérivation de B dans le B-module I/I^2.

On pose :

$$\boxed{\Omega_{B/A} = I/I^2}$$

Théorème I.6

Les notations sont celles qui précèdent. Le couple $(\Omega_{B/A}, d_{B/A})$ *représente le foncteur* $\mathrm{Der}_A(B,-)$.

Autrement dit, soit D *une* A*-dérivation de* B *dans un* B*-module* M. *Il existe une unique application* B*-linéaire* $u_D : \Omega_{B/A} \longrightarrow M$ *telle que* $D = u_D \circ d_{B/A}$.

Démonstration

Unicité. Le B-module I est engendré (lemme 1) par les éléments

$1\otimes x - x\otimes 1$ où x parcourt B. Par suite, le B-module $\Omega_{B/A} = I/I^2$ est engendré par les éléments $d_{B/A}(x)$.

Une application B-linéaire u de $\Omega_{B/A}$ dans M telle que $D = u\circ d_{B/A}$ est déterminée par les éléments $D(x) = u(d_{B/A}(x))$.

Existence. L'application $(x,x') \longmapsto xD(x')$ de B×B dans M est A-bilinéaire. Elle définit donc une application A-linéaire α de $B \underset{A}{\otimes} B$ dans M telle que

$$\alpha(\Sigma x_i \otimes x_i') = \Sigma x_i D(x_i')$$

L'application A-linéaire $\varepsilon + \alpha : x\otimes x' \longmapsto xx' + xD(x')$ de $B \underset{A}{\otimes} B$ dans $D_B(M)$ est un homomorphisme de B-algèbres comme ε. Elle induit une application B-linéaire ϕ de I dans $D_B(M)$ et, puisque $\varepsilon(I) = 0$, de I dans M. Donc, $\phi(I^2)$ est contenu dans $M^2 = 0$, où M est identifié à un idéal de $D_B(M)$. Par conséquent, ϕ induit une application B-linéaire u_d de $I/I^2 = \Omega_{B/A}$ dans M. Ainsi, $\phi = u_D \circ (\pi/I)$ où π/I désigne la restriction de π à I. Si $x \in B$, $(1\otimes x - x\otimes 1) = (1\otimes x - x\otimes 1) = D(x) - xD(1) = D(x)$ d'où $(u_D\circ d_{B/A})(x) = D(x)$ et $D = u_D\circ d_{B/A}$.

Le B-module $\Omega_{B/A}$ est appelé le module des différentielles de la A-algèbre B. La dérivation $d_{B/A}$ de B dans $\Omega_{B/A}$ est appelée la différentielle extérieure de la A-algèbre B.

II. Propriétés et calcul des modules de dérivations et différentielles

Soient A un anneau, B un A-algèbre.

Nous avons choisi ici de déduire des propriétés des modules $\mathrm{Der}_A(B,M)$ des propriétés du module $\Omega_{B/A}$ par utilisation de l'isomorphisme, fonctoriel en le B-module M, $u \longmapsto u\circ d_{B/A}$ du B-module $\mathrm{Hom}_B(\Omega_{B/A},M)$ sur le B-module $\mathrm{Der}_A(B,M)$ et du lemme de Yoneda.

On peut également, si l'on ne s'intéresse qu'aux propriétés du module des différentielles, obtenir directement les propriétés de celui-ci par utilisation de sa propriété universelle.

1. Changement de base et localisation

Soient A un anneau, B et A' des A-algèbres, B' la A'-algèbre $B \underset{A}{\otimes} A'$, g l'homomorphisme : $x \longmapsto x\otimes 1$ de B dans B' déduit de l'homomorphisme structural de A'.

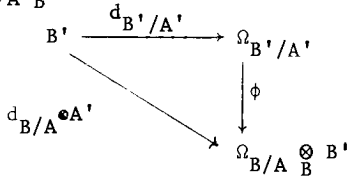
On rappelle que l'application $\lambda : D' \longmapsto D'\circ g$ est un isomorphisme, fonctoriel en le B'-module M', de $\mathrm{Hom}_{A'}(B',M')$ sur $\mathrm{Hom}_A(B,g_*(M'))$ (où $g_*(M')$

est le B-module déduit de M' par restriction des scalaires) et que l'isomorphisme réciproque μ fait correspondre à l'élément D de $\mathrm{Hom}_A(B,g_*(M'))$ l'élément D' de $\mathrm{Hom}_{A'}(B',M')$ défini par $D'(b\otimes a') = (1\otimes a')D(b)$.

Proposition II.1 (*changement de base*)

1. *L'application* : $D' \longmapsto D'\circ g$ *est un isomorphisme, fonctoriel en* M', *de* $\mathrm{Der}_{A'}(B',M')$ *sur* $\mathrm{Der}_A(B,g_*(M'))$.

2. *Il existe un isomorphisme* ϕ *et un seul de* B'*-modules de* $\Omega_{B'/A'}$ *sur* $\Omega_{B/A}\otimes_B B'$ *rendant commutatif le diagramme*



Démonstration

1. Il est facile de vérifier que si $D' \in \mathrm{Der}_{A'}(B',M')$, $D'\circ g$ appartient à $\mathrm{Der}_A(B,g_*(M'))$. Il suffit de vérifier que, avec les notations ci-dessus, si $D \in \mathrm{Der}_A(B,g_*(M))$, $D' = \mu(D)$ appartient à $\mathrm{Der}_{A'}(B',M')$. On se contente ici de vérifier la propriété (2) des dérivations :

$$D'((b\otimes a')(b_1\otimes a_1')) = D'(bb_1)\otimes(a'a_1')) = (1\otimes(a'a_1'))D(bb_1)$$
$$= (1\otimes(a'a_1'))(bD(b_1) + b_1D(b))$$
$$= (1\otimes a'a_1')((b\otimes 1)D(b_1)+b_1\otimes 1)D(b)) = (b\otimes a')(1\otimes a_1')D(b_1)+(b_1\otimes a_1')(1\otimes a')D(b)$$
$$= (b\otimes a')D'(b_1\otimes a_1')+(b_1\otimes a_1')D(b\otimes a')$$

La propriété (2) s'en déduit par linéarité.

2. On a la suite d'isomorphismes, fonctoriels en le B'-module M' :
$\mathrm{Hom}_{B'}(\Omega_{B/A}\otimes_B B',M') \longrightarrow \mathrm{Hom}_B(\Omega_{B/A},g_*(M')) \longrightarrow \mathrm{Der}_A(B,g_*(M')) \longrightarrow \mathrm{Der}_{A'}(B',M')$
$\longrightarrow \mathrm{Hom}_{B'}(\Omega_{B'/A'},M')$, qui, appliquée avec $M' = \Omega_{B/A}\otimes_B B'$, donne pour le morphisme $1_{B/A\otimes B'}$:

$$1_{B/A\otimes B'} \longmapsto (1_{B/A\otimes B'})\circ h \longmapsto (1_{B/A\otimes B'})\circ h\circ d_{B/A} \longmapsto D' \longmapsto \phi$$

où h est le morphisme $x \longmapsto x\otimes 1$ de $\Omega_{B/A}$ dans $\Omega_{B/A}\otimes_B B'$, D' est tel que

$$D'(b\otimes a') = (1\otimes a')((1_{B/A\otimes B'})\circ h\circ d_{B/A})(b) = d_{B/A}(b)\otimes a'$$

et enfin $D' = \phi\circ d_{B'/A'}$, d'où $d_{B/A}(b)\otimes a' = (\phi\circ d_{B'/A'})(b\otimes a') = (d_{B/A}\otimes A')(b\otimes a')$.

Il résulte du lemme d'Yoneda que l'isomorphisme composé de $\mathrm{Hom}_{B'}(\Omega_{B'/A'},M')$ sur $\mathrm{Hom}_{B'}(\Omega_{B/A}\otimes_B B',M')$ est $\mathrm{Hom}(\phi,M')$. Le calcul ci-dessus montre l'égalité $\phi\circ d_{B'/A'} = d_{B/A}\otimes A'$.

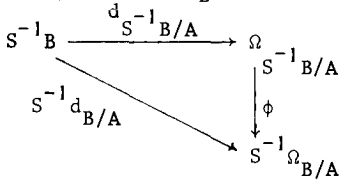
En dépit des apparences, la proposition II.2 n'est pas un corollaire de la proposition II.1 : on considère, en effet, une partie multiplicative de B et non de A.

Proposition II.2 (*localisation*)

Soient S *une partie multiplicative de* B, M *un* $S^{-1}B$*-module.*

1. L'application $D \longmapsto D \circ i_S^B$ *de* $\mathrm{Der}_A(S^{-1}B,M)$ *dans* $\mathrm{Der}_A(B,(i_S^M)^*(M))$ *est un isomorphisme* (de B-modules), *fonctoriel en* M.

2. Il existe un isomorphisme ϕ (et un seul) *de* $S^{-1}B$*-modules de* $\Omega_{S^{-1}B/A}$ *sur* $S^{-1}(\Omega_{B/A}) = \Omega_{B/A} \otimes_B S^{-1}B$ *rendant commutatif le diagramme*



Démonstration

1. En vertu de la proposition I.3, si D appartient à $\mathrm{Der}_A(S^{-1}B,M)$, $D \circ i_S^B$ appartient à $\mathrm{Der}_A(B,(i_S^B)_*(M))$.

Soit $\Delta \in \mathrm{Der}_A(B,(i_S^B)_*(M))$. L'application D de $S^{-1}B$ dans M telle que $D(x/s) = \frac{s\Delta(x)-x\Delta(s)}{s^2}$ est bien définie et appartient à $\mathrm{Der}_A(S^{-1}B,M)$. L'application ainsi définie : $\Delta \longmapsto D$ de $\mathrm{Der}_A(B,(i_S^B)_*(M))$ dans $\mathrm{Der}_A(S^{-1}B,M)$ est l'inverse de l'application : $D \longmapsto D \circ i_S^B$.

2. On utilise la suite d'isomorphismes fonctoriels en M :

$$\mathrm{Hom}_{S^{-1}B}(S^{-1}\Omega_{B/A},M) \longrightarrow \mathrm{Hom}_B(\Omega_{B/A},(i_S^B)_*(M)) \longrightarrow \mathrm{Der}_A(B,(i_S^B)_*(M)) \to \mathrm{Der}_A(S^{-1}B,M)$$

$$\downarrow$$

$$\mathrm{Hom}_{S^{-1}B}(\Omega_{S^{-1}B/A},M)$$

qui fournit un isomorphisme fonctoriel en M de $\mathrm{Hom}_{S^{-1}B}(S^{-1}\Omega_{B/A},M)$ sur $\mathrm{Hom}_{S^{-1}B}(\Omega_{S^{-1}B/A},M)$.

Cet isomorphisme fonctoriel est donné par $\mathrm{Hom}(\phi,M)$ où ϕ est l'isomorphisme de $\Omega_{S^{-1}B/A}$ sur $S^{-1}\Omega_{B/A}$ qui provient (cas $M = S^{-1}\Omega_{B/A}$) de l'élément $1_{S^{-1}\Omega_{B/A}}$.

On laisse au lecteur, à titre d'exercice, le soin de faire les vérifications nécessaires, analogues à celles de la proposition II.1.

Corollaire 1

Soient B *une* A*-algèbre,* L *l'anneau total des fractions de* B, M *un* L*-module.*

L'application $D \longmapsto D \circ i$, *où* i *est l'injection canonique de* B *dans* L, *est un isomorphisme de* $\mathrm{Der}_A(L,M)$ *sur* $\mathrm{Der}_A(B,M)$.

En particulier, $\mathrm{Der}_A(L,L)$ *est isomorphe à* $\mathrm{Der}_A(B,L)$.

Corollaire 2

Soient B *une* A*-algèbre,* S *une partie multiplicative de* A.

On a un isomorphisme de $\Omega_{(S^{-1}B)/(S^{-1}A)}$ *sur* $\Omega_{B/A} \otimes_B S^{-1}B$.

2. Produits et limites inductives filtrantes

Proposition II.3 (*modules de différentielles et de dérivations d'un produit d'algèbres*)

Soient $B_1,\dots,B_r$ *des* A*-algèbres,* B *l'algèbre produit* $\prod_{i=1}^{r} B_i$.

1. Un B*-module* M *est de la forme* $\prod_{i=1}^{r} M_i$, *où* M_i *est un* B_i*-module.*

On a un isomorphisme du B*-module* $\mathrm{Der}_A(B,M)$ *sur* $\prod_{i=1}^{r} \mathrm{Der}_A(B_i,M_i)$, *muni de sa structure de* B*-module.*

2. Il existe un isomorphisme ϕ *et un seul du* B*-module* $\Omega_{B/A}$ *sur* $\prod_{i=1}^{r} \Omega_{B_i/A}$, *muni de structure naturelle de* B*-module rendant commutatif le diagramme*

$$\begin{array}{ccc} A & \xrightarrow{d_{B/A}} & \Omega_{B/A} \\ & \searrow^{\lambda} & \downarrow \phi \\ & & \prod_{i=1}^{r} \Omega_{B_i/A} \end{array}$$

où λ *est l'application :* $a \longmapsto (d_{B_i/A}(a))$.

Démonstration

1. Soit e_i l'idempotent de B associé au facteur B_i. On pose $M_i = e_i M$. C'est un B_i-module et $M = \prod_{i=1}^{r} M_i$. Il est clair que $\mathrm{Hom}_A(B,M) = \prod_{i=1}^{r} \mathrm{Hom}_A(B_i,M_i)$ et que $\mathrm{Der}_A(B,M) = \prod_{i=1}^{r} \mathrm{Der}_A(B_i,M_i)$.

2. Il suffit d'utiliser la suite d'isomorphismes, fonctoriels en le B-module M,

$$\mathrm{Hom}_B(\Omega_{B/A},M) \longrightarrow \mathrm{Der}_A(B,M) \longrightarrow \prod_{i=1}^{r} \mathrm{Der}_A(B_i,M_i) \longrightarrow \prod_{i=1}^{r} \mathrm{Hom}_{B_i}(\Omega_{B_i/A},M_i)$$

$$\downarrow$$

$$\mathrm{Hom}_B(\prod_{i=1}^{r}\Omega_{B_i/A},M)$$

(Pour le dernier isomorphisme, on remarquera que :

$\mathrm{Hom}_{B_i}(\Omega_{B_i/A},M_i) = \mathrm{Hom}_B(\Omega_{B_i/A},M_i)$).

L'isomorphisme composé de $\mathrm{Hom}_B(\Omega_{B/A},M)$ sur $\mathrm{Hom}_B(\prod_{i=1}^{r}\Omega_{B_i/A},M)$ est de la forme $\mathrm{Hom}(\phi^{-1},M)$ où ϕ est l'isomorphisme cherché.

Proposition II.4

Soient $(B_i,f_{ji})_{i,j\in I}$ *un système inductif de* A*-algèbres,* $(B,f_i)_{i\in I}$ *sa limite inductive.*

Il existe un isomorphisme de B*-modules de* $\Omega_{B/A}$ *sur* $\varinjlim(\Omega_{B_i/A} \underset{A}{\otimes} B)$.

Démonstration

Soit ρ l'homomorphisme structural de B.

On rappelle que le système $(\mathrm{Hom}_A(B_i,\rho_*(M)), \mathrm{Hom}_A(f_{ji},\rho_*(M))_{i,j\in I}$ est projectif et que l'on a un isomorphisme fonctoriel en M :

$$\theta_M : \mathrm{Hom}_A(\varinjlim(B_i), \rho_*(M)) \simeq \varprojlim \mathrm{Hom}_A(B_i,\rho_*(M))$$

Il est clair que $\mathrm{Hom}_A(f_{ji},\rho_*(M))(\mathrm{Der}_A(B_j,M)) \subset \mathrm{Der}_A(B_i,M)$ si $i \leqslant j$.

Si g_{ij} est la restriction à $\mathrm{Der}_A(B_j,M)$ de $\mathrm{Hom}_A(f_{ji},\rho_*(M))$, le système $(\mathrm{Der}_A(B_i,M),g_{ij})$ est projectif et θ_M induit un isomorphisme fonctoriel en M

$$\mathrm{Der}_A(\varinjlim(B_i),M) \simeq \varprojlim \mathrm{Der}_A(B_i,M).$$

On en déduit un isomorphisme fonctoriel

$\mathrm{Hom}_B(\Omega_{B/A},M) \simeq \varprojlim \mathrm{Hom}_{B_i}(\Omega_{B_i/A},(f_i)_*(M))$ où f_i est l'homomorphisme de B_i dans B , soit un isomorphisme fonctoriel

$$\mathrm{Hom}_B(\Omega_{B/A},M) \simeq \varprojlim (\mathrm{Hom}_B(\Omega_{B_i/A} \underset{A}{\otimes} B,M)$$

t enfin un isomorphisme fonctoriel

$$\mathrm{Hom}_B(\Omega_{B/A},M) \simeq \mathrm{Hom}_B(\varinjlim (\Omega_{B_i/A} \underset{A}{\otimes} B),M)$$

Cet isomorphisme provient d'un isomorphisme de $\Omega_{B/A}$ sur $\varinjlim(\Omega_{B_i/A} \underset{A}{\otimes} B)$

3. Deux suites exactes

Théorème II.5 *(première suite exacte fondamentale)*

Soit $A \xrightarrow{\rho} B \xrightarrow{\sigma} C$ *une suite d'homomorphismes d'anneaux.*

1. Soient M *un* C*-module,* λ *l'application* $D \longmapsto D_\circ\sigma$ *de* $\mathrm{Der}_A(C,M)$ *dans* $\mathrm{Der}_A(B,M)$. *On munit* $\mathrm{Der}_A(B,M)$ *de sa structure de sous-module du* C*-module* $\mathrm{Hom}_A(B,M)$.

Alors λ *est* C*-linéaire et la suite de* C*-modules*

$$0 \longrightarrow \mathrm{Der}_B(C,M) \longrightarrow \mathrm{Der}_A(C,M) \xrightarrow{\lambda} \mathrm{Der}_A(B,M$$

est exacte.

2. Soient ϕ *l'unique application* C*-linéaire de* $\Omega_{C/A}$ *dans* $\Omega_{C/B}$ *telle que* $d_{C/B} = \phi \circ d_{C/A}$ *et* ψ *l'application* C*-linéaire de* $\Omega_{B/A} \underset{B}{\otimes} C$ *dans* $\Omega_{C/A}$ *déduite de l'application* B*-bilinéaire* $(\omega, c) \longmapsto cv(\omega)$ *de* $\Omega_{B/A} \times C$ *dans* $\Omega_{C/A}$, *où* v *est l'unique application* B*-linéaire de* $\Omega_{B/A}$ *dans* $\Omega_{C/A}$ *telle que* $v \circ d_{B/A} = d_{C/A} \circ \sigma$.

La suite de C*-modules*

$$\Omega_{B/A} \underset{B}{\otimes} C \xrightarrow{\psi} \Omega_{C/A} \xrightarrow{\psi} \Omega_{C/B} \longrightarrow 0$$

est exacte.

Démonstration

1. L'exactitude de $0 \longrightarrow \mathrm{Der}_B(C,M) \longrightarrow \mathrm{Der}_A(C,M)$ est claire : une B-dérivation définit, par restriction des scalaires, une A-dérivation et une seule.

L'exactitude de la suite $\mathrm{Der}_B(C,M) \longrightarrow \mathrm{Der}_A(C,M) \xrightarrow{\lambda} \mathrm{Der}_A(B,M)$ résulte des équivalences : $\lambda(D) = 0 \Longleftrightarrow D \in \mathrm{Der}_B(C,M)$.

2. On déduit de 1. l'exactitude de la suite

$$0 \longrightarrow \mathrm{Hom}_C(\Omega_{C/B}, M) \xrightarrow{\Phi} \mathrm{Hom}_C(\Omega_{C/A}, M) \xrightarrow{\Psi} \mathrm{Hom}_B(\Omega_{B/A}, \sigma_*(M))$$

où $\Phi = \mathrm{Hom}(\phi, M)$ et Ψ rend commutatif le diagramme

$$\begin{array}{ccc} \mathrm{Der}_A(C,M) & \xrightarrow{\lambda} & \mathrm{Der}_A(B,M) \\ \uparrow & & \uparrow \\ \mathrm{Hom}_C(\Omega_{C/A}, M) & \xrightarrow[\psi]{} & \mathrm{Hom}_B(\Omega_{B/A}, \sigma_*(M)) \end{array}$$

L'application

$$u \longmapsto (\Sigma \omega_i \otimes c_i \longmapsto \Sigma c_i \, u(\omega_i))$$

est un isomorphisme de C-modules de $\mathrm{Hom}_B(\Omega_{B/A}, \sigma_*(M))$ sur $\mathrm{Hom}_C(\Omega_{B/A} \underset{B}{\otimes} C, M)$.

On obtient ainsi une suite exacte

$$0 \longrightarrow \mathrm{Hom}_C(\Omega_{C/B}, M) \xrightarrow{\Phi} \mathrm{Hom}_C(\Omega_{C/A}, M) \xrightarrow{\Psi_1} \mathrm{Hom}_C(\Omega_{B/A} \underset{B}{\otimes} C, M)$$

fonctorielle en le C-module M. On vérifie que $\Psi_1 = \mathrm{Hom}(\psi, M)$.

L'exactitude de la suite de 2. en découle.

Complément au théorème

Les notations sont celles du théorème. Les assertions suivantes sont équivalentes :

(i) la suite de C*-modules*

$$0 \longrightarrow \Omega_{B/A} \underset{B}{\otimes} C \xrightarrow{\psi} \Omega_{C/A} \xrightarrow{\phi} \Omega_{C/B} \longrightarrow 0$$

est scindée

(ii) Pour tout C*-module* M*, toute* A*-dérivation de* B *dans* M *se prolonge en une* A*-dérivation de* C *dans* M.

Démonstration

La condition (i) équivaut à l'exactitude pour tout C-module M de :

$$0 \longrightarrow \mathrm{Hom}_C(\Omega_{C/B},M) \xrightarrow{\phi} \mathrm{Hom}_C(\Omega_{C/A},M) \xrightarrow{\psi_1} \mathrm{Hom}_c(\Omega_{B/A} \underset{B}{\otimes} C,M) \longrightarrow 0$$

et donc de la suite :

$$0 \longrightarrow \mathrm{Der}_B(C,M) \longrightarrow \mathrm{Der}_A(C,M) \longrightarrow \mathrm{Der}_A(B,M) \longrightarrow 0$$

Théorème II.6 (deuxième suite exacte fondamentale)

Soient A *un anneau,* B *une* A*-algèbre d'homomorphisme structural* ρ*,* m *un idéal de* B,C = B/m.

L'application $x \longmapsto d_{B/A}(x) \otimes 1$ *de* m *dans* $\Omega_{B/A} \underset{B}{\otimes} C = \Omega_{B/A}/m\,\Omega_{B/A}$ *applique* m^2 *sur* 0 *et définit donc une application* C*-linéaire* δ *de* m/m^2 *dans* $\Omega_{B/A} \underset{B}{\otimes} C$.

La suite de C*-modules*

$$m/m^2 \xrightarrow{\delta} \Omega_{B/A} \underset{B}{\otimes} C \xrightarrow{\psi} \Omega_{C/A} \longrightarrow 0$$

est exacte, où ψ *est l'application définie dans le théorème II.4.*

Démonstration

Soit M un C-module. La suite

$$0 \longrightarrow \mathrm{Hom}_A(B/m,M) \longrightarrow \mathrm{Hom}_A(B,M) \longrightarrow \mathrm{Hom}_A(m,M)$$

est exacte. De plus, p désignant la surjection canonique B $\longrightarrow$ B/m , Hom(p,M)(Der$_A$(B/m,M)) est contenu dans Der$_A$(B,M) et Hom$_A$(m,M) s'injecte dans Hom$_B$(m,M).

On en déduit l'exactitude de la suite

$$0 \longrightarrow \mathrm{Der}_A(C,M) \longrightarrow \mathrm{Der}_A(B,M) \longrightarrow \mathrm{Hom}_B(m,M)$$

puis celle de la suite

$$0 \longrightarrow \mathrm{Hom}_C(\Omega_{C/A},M) \longrightarrow \mathrm{Hom}_B(\Omega_{B/A},M) \longrightarrow \mathrm{Hom}_B(m,M)$$

On remarque enfin que, comme M est annulé par m,

$\mathrm{Hom}_B(m,M) = \mathrm{Hom}_C(m/m^2,M)$ et que $\mathrm{Hom}_B(\Omega_{B/A},M) = \mathrm{Hom}_C(\Omega_{B/A} \otimes_B C,M)$, obtenant une suite exacte, fonctorielle en M,

$$0 \longrightarrow \mathrm{Hom}_C(\Omega_{C/A},M) \xrightarrow{\Psi} \mathrm{Hom}_C(\Omega_{B/A} \otimes_B C,M) \xrightarrow{\Delta} \mathrm{Hom}_C(m/m^2,M)$$

On vérifie que $\Psi = \mathrm{Hom}(\psi,M)$ et $\Delta = \mathrm{Hom}(\delta,M)$.

L'exactitude de la suite du théorème en résulte.

4. Prolongement de dérivations

Soient A *un anneau,* $(X_i)_{i\in I}$ *une famille d'indéterminées.*

On note pour simplifier D_i *la dérivation partielle* $\partial/\partial X_i$. C'est un élément de $\mathrm{Der}_A(A[X_i]_{i\in I}, A[X_i]_{i\in I})$.

Proposition II.7 (*prolongement d'une dérivation à une algèbre de polynômes*

Soient k *un anneau,* A *une* k*-algèbre* $(X_i)_{i\in I}$ *une famille d'indéterminées,* $B = A[X_i]_{i\in I}$, M *un* B*-module,* D_o *une* k*-dérivation de* A, $(m_i)_{i\in I}$ *une famille indexée par* I *d'éléments de* M.

Si $f \in B$, *on note* f^{D_o} *l'élément de* B *obtenu en appliquant la dérivation* D_o *aux coefficients de* f.

Il existe une dérivation D *et une seule de* B *dans* M *de restriction* D_o *à* A *et telle que* $D(X_i) = m_i$ $(i \in I)$.

Elle est donnée par :

$$D(f) = f^{D_o} + \Sigma_{i\in I}\, D_i(f)m_i$$

Démonstration

Il est clair que les applications $f \longmapsto f^{D_o}$ et $f \longmapsto \Sigma_{i\in I}\, D_i(f)m_i$ sont des k-dérivations de B dans M. Il en est donc de même de leur somme.

Soit D une dérivation satisfaisant aux conditions de l'énoncé.

L'application $\Delta = D - \Sigma_{i\in I}\, D_i(\ )m_i$ est une dérivation de B dans M induisant D_o sur A et telle que $\Delta(X_i) = 0$ $(i \in I)$.

Il est clair que $\Delta(a_{i_1\dots i_n} X_1^{i_1} \dots X_n^{i_n}) = D_o(a_{i_1\dots i_n}) X_1^{i_1} \dots X_n^{i_n}$ si $a_{i_1\dots i_n}$ appartient à A.

Le résultat s'en déduit.

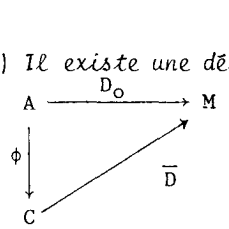
Proposition II.8

Les données sont celles de la proposition II.7.

Soient a *un idéal de* B, C *l'anneau quotient* B/a. *On suppose que* M *est un* C*-module et que sa structure de* B*-module est celle déduite de la surjection canonique* p *de* B *sur* C.

Les assertions suivantes sont équivalentes :

(i) Il existe une dérivation $\overline{D} : C \longrightarrow M$ *rendant commutatif le diagramme*



où ϕ *est le composé de l'injection de* A *dans* B *et de la surjection de* B *sur* C.

(ii) pour tout $f \in a$, $f^{D_o} + \Sigma_{i\in I} D_i(f)m_i = 0$

Si la condition (ii) est satisfaite, la dérivation $\overline{D}$ *de (i) est unique.*

Démonstration

L'unicité de $\overline{D}$ résulte de ce que $\overline{D}\circ p$ est la dérivation D de B dans M définie dans la proposition II.7.

(i) $\Longrightarrow$ (ii). L'application $D = \overline{D} \circ p$ de B dans M satisfait aux conditions de la proposition II.7 et s'annule évidemment sur le noyau a de p. La condition (ii) résulte alors de l'expression donnée précédemment de D.

(ii) implique (i). Soit D l'application de B dans M prolongeant D_o et telle que $D(X_i) = m_i$ $(i\in I)$. La condition (ii) exprime qu'elle s'annule sur a et définit donc par passage au quotient une application $\overline{D}$ de C dans M dont on vérifie que c'est une dérivation.

Les propositions II.7, II.8 et II.2 permettent le calcul des mosules de dérivations pour les algèbres de la géométrie algébrique classique.

On va maintenant traiter le problème des dérivations d'extensions de corps et, plus particulièrement d'extensions monogènes.

Proposition II.9

Soient k *un corps,* K = k(x) *une extension monogène de* k, M *un* K*-espace vectoriel,* D *une dérivation de* k *dans* M.

1. Si x *est transcendant sur* k, *pour tout* $m \in M$, *il existe une dérivation* $\overline{D}$ *et une seule de* K *dans* M *prolongeant* D *et telle que* D(x) = m.

2. Si x *est algébrique sur* k , *soit* f(X) = irr(X,x,k).

Si x *est séparable sur* k, *il existe une seule dérivation* $\overline{D}$ *de* K *dans* M *prolongeant* D. *Elle est telle que* $\overline{D}(x) = -f^D(x)/f'(x)$.

Si x *est inséparable sur* k *et si* $f^D(x) \neq 0$, *il n'existe pas de dérivation de* K *dans* M *prolongeant* D.

Si x *est inséparable sur* k *et si* $f^D(x) = 0$, *pour tout* $m \in M$, *il exis-*

te une dérivation $\overline{D}$ *et une seule de* K *dans* M *prolongeant* D *et telle que* $\overline{D}(x) = m$.

Démonstration

1. Résulte de la proposition II.7.

2. Résulte de ce que $k[X]$ est isomorphe en tant que k-algèbre à $k[X]/(f(X))$ et de la proposition II.8.

5. Applications au calcul de certains modules de différentielles

On commence par le calcul du module des différentielles d'une algèbr de polynômes. C'est un module libre dont une base est formée des différentielles des indéterminées. On en déduit, grace aux résultats déjà obtenus, le module des différentielles d'une algèbre de la géométrie algébrique classique.

Proposition II.10 (*différentielles d'une algèbre de polynômes*)

Soient $k \longrightarrow A$ *un homomorphisme d'anneaux,* $(X_i)_{i\in I}$ *une famille d'indéterminées.*

On note B *l'anneau* $A[X_i]_{i\in I}$ *et* d *la différentielle* $d_{B/A}$.

Alors, $\Omega_{B/k} = (\Omega_{A/k} \underset{A}{\otimes} B) \oplus (\underset{j\in I}{\oplus} Bd(X_j))$

Démonstration

On commence par calculer $\Omega_{B/A}$.

Soit D_i la dérivation partielle $\partial/\partial X_i$. C'est une A-dérivation de B dans B telle que $D_i(X_j) = \delta_{ij}$ (1 si j = i, 0 sinon).

Par propriété universelle de d, il existe une unique application B-linéaire f_i de $\Omega_{B/A}$ dans B telle que $f_i \circ d = D_i$.

Les différentielles $d(X_i)_{i\in I}$ forment un système de générateurs du B-module $\Omega_{B/A}$ car les indéterminées X_i forment un système de générateurs de la A-algèbre B. Elles sont linéairement indépendantes sur B : soit, en effet, $\Sigma_{i\in I} b_i d(X_i) = 0$ avec $b_i \in B$. On obtient $f_j(\Sigma_{i\in I} b_i d(X_i)) = 0 = b_j D_j(X_j) = b_j$.

Donc, $\Omega_{B/A} = \underset{j\in I}{\oplus} Bd(X_j)$.

On va ensuite appliquer le complément du théorème II.4, ce qui est loisible puisque en vertu de la proposition II.6 toute k-dérivation de A se prolonge en une k-dérivation de B.

Corollaire (*module des différentielles d'une algèbre quotient d'une algèbre de polynômes*)

Soient A *un anneau,* $(X_i)_{i\in I}$ *une famille d'indéterminées, a un idéal de* $A[X_i]_{i\in I}$, $B = A[X_i]_{i\in I}/a$.

Le B-module $\Omega_{B/A}$ est le quotient du B-module libre de base $(dX_i)_{i\in I}$ par le sous-module engendré par les éléments $\Sigma_{i\in I}(\overline{\partial f/\partial X_i})dX_i$ où f parcourt a et, si $g \in A[X_i]$, $\overline{g}$ désigne la classe modulo a.

Démonstration

Il suffit d'utiliser la suite exacte

$$a/a^2 \xrightarrow{\delta} \Omega_{R/A}/a\,\Omega_{R/A} \longrightarrow \Omega_{B/A} \longrightarrow 0$$

où $R = A[X_i]_{i\in I}$, le fait que $\Omega_{R/A}$ est le R-module libre de base $(dX_i)_{i\in I}$, le fait que $\mathrm{im}(\delta)$ est l'ensemble des éléments $\overline{d_{R/A}(f)}$ où f parcourt a et enfin l'égalité $d_{R/A}(f) = \Sigma_{i\in I}(\partial f/\partial X_i)dX_i$.

Exemple

Soient k un corps, X_1 et X_2 des indéterminées, B l'algèbre affine $k[X_1,X_2]/(X_1^2-X_2^3)$.

Alors, $\Omega_{B/k}$ est le B-module $(BdX_1 \oplus BdX_2)/(2x_1dX_1-3x_2^2dX_2)$ B où x_i est la classe de X_i modulo $(X_1^2-X_2^3)$ en sorte que $B = k[x_1,x_2]$.

Voici une application différente à la caractérisation différentielle des p-bases.

Proposition II.11

Soient k un corps de caractéristique p>0, k' un sous-corps de k tel que $k^p \subset k' \subset k$, $(x_i)_{i\in I}$ *une famille d'éléments de k.*

1. Les assertions suivantes sont équivalentes :

(i) les éléments $(x_i)_{i\in I}$ sont p-indépendants sur k'

(ii) les éléments $d_{k/k'}(x_i)$ $(i \in I)$ sont linéairement indépendants sur k.

2. Les assertions suivantes sont équivalentes :

(i) les éléments x_i $(i \in I)$ forment une p-base de k sur k'

(ii) les éléments $d_{k/k'}(x_i)$ $(i \in I)$ forment une base de $\Omega_{k/k'}$ sur k

Démonstration

2. est une conséquence facile de 1. On peut, d'autre part, dans 1. remplacer k par $k'(x_i)_{i\in I}$ en sorte que les assertions 1. et 2. deviennent équivalentes.

2. (i) $\Longrightarrow$ (ii)

On note d au lieu de $d_{k/k'}$. On pose $k_i' = k'(x_j)_{j\in I-\{i\}}$.

Alors, $k'(x_i') = k$, $x_i^p \in k_i'$, $x_i \notin k_i'$. Comme $k = k_i'[T]/(T^p-x_i)$, la dérivation usuelle d/dT de $k_i'[T]$, qui est telle que $d/dT(T^p-x_i) = 0$, définit

par passage au quotient une k'-dérivation D_i de k dans k telle que $D_i(x_i) = 1$.

En fait D_i est une k'dérivation de k dans k telle que $D_i(x_j) = \delta_{ij}$.

Il existe une application k-linéaire $f_i : \Omega_{k/k'} \longrightarrow k$ telle que $D_i = f_i \circ d$.

On conclut que les éléments dx_i ($i \in I$) sont linéairement indépendants sur k : une relation $\Sigma_{i\in I} a_i dx_i = 0$ implique $0 = f_j(\Sigma_{i\in I} a_i dx_i) = a_j D_j(x_j) = a_j$.

1. (ii) $\Longrightarrow$ (i)

Il suffit de démontrer que, si $x_1,\ldots,x_n$ sont des éléments de k tels que $d(x_1),\ldots,d(x_n)$ soient linéairement indépendants sur k, il n'existe pas de polynôme non nul $f(X_1,\ldots,X_n) \in k'[X_1,\ldots,X_n]$ de degré $< p$ en chaque X_i tel que $f(x_1,\ldots,x_n) = 0$.

Or, une égalité $f(x_1,\ldots,x_n) = 0$ implique l'égalité

$$\Sigma_{i=1}^{n} \partial f/\partial X_i(x_1,\ldots,x_n)dx_i = 0$$

et donc $\partial f/\partial X_i(x_1,\ldots,x_n) = 0$.

On peut supposer que f a été choisi de degré total minimum. Il en résulte que $\partial f/\partial X_i = 0$ pour $i = 1,\ldots,n$ et donc que $f(X_1,\ldots,X_n) = g(X_1^p,\ldots,X_n^p)$, ce qui contredit le fait que f est de degré $< p$ en chaque X_i.

III. Extensions séparables

La définition d'une extension séparable dans le seul cas algébrique, donnée dans le chapitre 5, est insuffisante pour les applications.

En géométrie algébrique, par exemple, on utilise les corps de fonctions rationnelles de k-ensembles algébriques irréductibles. Ces corps sont des extensions de type fini de k mais ne sont qu'exceptionnellement des extensions algébriques, ou ce qui revient au même finies, de k.

On se propose dans ce paragraphe de donner une définition générale de la notion d'extension séparable.

1. Compléments sur les extensions algébriques séparables

Proposition III.1

Soient k *un corps,* K/k *une extension algébrique de* k.

Les assertions suivantes sont équivalentes :

(i) K *est séparable sur* k

(ii) pour toute extension k'/k *de* k, *l'anneau* $K \underset{k}{\otimes} k'$ *est réduit*

(iii) pour toute extension algébrique k'/k *de* k, *l'anneau* $K \underset{k}{\otimes} k'$ *est réduit*

(iv) pour toute extension algébrique finie k'/k de k, l'anneau $K \underset{k}{\otimes} k'$ *est réduit*

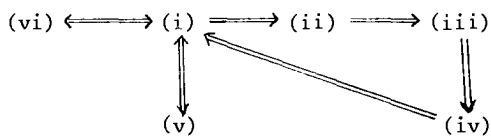
(v) ou bien k est de caractérisation 0 *ou bien k est de caractérisation* $p > 0$ *et l'anneau* $K \underset{k}{\otimes} k^{p^{-1}}$ *est réduit*

(vi) $\Omega_{K/k} = 0$

Démonstration

Il suffit de démontrer les équivalences dans le cas où l'extension K/k est finie : en effet, le produit tensoriel commute aux limites inductives, une limite inductive filtrante d'anneaux réduits est un anneau réduit et une extension algébrique est limite inductive, en fait réunion, filtrante de ses sous-extensions finies.

La démonstration se fait suivant le schéma



Les implications (ii) $\Longrightarrow$ (iii) $\Longrightarrow$ (iv) sont évidentes.

(i) $\Longrightarrow$ (ii) et (i) $\Longrightarrow$ (v).

Par hypothèse, $K = k(x)$ où $f(X) = \mathrm{irr}(X,x,k)$ a ses racines simples dans toute extension algébriquement close de k.

Soit $f(X) = f_1(X)^{a_1} \ldots f_s(X)^{a_s}$ la décomposition de f(X) en facteurs irréductibles distincts $f_1(X),\ldots,f_s(X)$ dans $k'[X]$. Les exposants a_i sont égaux à 1.

Alors $K \underset{k}{\otimes} k' \simeq k[X]/f(X)k[X] \underset{k}{\otimes} k' \simeq k'[X]/f(X)k'[X] \simeq \prod_{i=1}^{s} k'[X]/f_i(X)k'[X]$ est le produit des corps $k'[X]/f_i(X)k'[X]$ (qui sont d'ailleurs des extensions séparables de k').

Donc, $K \underset{k}{\otimes} k'$ est réduit.

Pour démontrer (i) $\Longrightarrow$ (v), on suppose que la caractéristique p de k est non nulle et on applique ce qui précède à $k' = k^{p^{-1}}$.

(i) $\Longrightarrow$ (vi).

On sait que $\Omega_{K/k}$ est limite inductive (et, en fait, réunion car les homomorphismes de transition sont injectifs) des K-espaces vectoriels $\Omega_{K'/k} \underset{K'}{\otimes} K$ où K' parcourt l'ensemble ordonné filtrant des sous-extensions finies de K.

Si K est séparable sur k, une extension finie K' de k contenue dans

K est de la forme k(x) et donc isomorphe à $k[X]/(f(X))$ où f(X) est un polynôme *séparable* de $k[X]$.

Donc, $\Omega_{K/k} = K'dx$ où $f'(x)dx = 0$ et, comme $f'(x) \neq 0$, $\Omega_{K'/k} = 0$.

Par suite, $\Omega_{K/k} = 0$.

(vi) $\Longrightarrow$ (i).

Le raisonnement ci-dessus montre que, pour toute sous-extension (finie) K'/k de K/k, $\Omega_{K'/k} = 0$.

Soit, en particulier, $x \in K$. Posant $K' = k(x) = k[X]/(f(X))$, on doit avoir, comme ci-dessus, $f'(x) \neq 0$. Donc, x est séparable sur k et K l'est aussi.

(non i) $\Longrightarrow$ (non v) et (non iv)

En effet, (non i) implique que la caractéristique p de k est non nulle et qu'il existe $x \in K$ tel que $f(X) = \mathrm{irr}(X,x,k)$ soit de la forme $g(X^p)$ où $g(Y) = \Sigma a_i Y^i \in k[Y]$. Soit k' le corps $k[a_i^{p^{-1}}]$. Dans $k'[X]$, f(X) est de la forme $h(X)^p$ où $h(X) \in k'[X]$.

Alors, $K \underset{k}{\otimes} k'$ qui est isomorphe à $k'[X]/h(X)^p k'[X]$ n'est pas réduit.

Il en est de même, a fortiori, de $K \underset{k}{\otimes} k^{p^{-1}}$.

2. Algèbres séparables sur un corps

Définition

Soit k un corps.

Une k-algèbre B est dite séparable sur k si, pour toute extension algébrique k'/k de k, l'anneau $B \underset{k}{\otimes} k'$ *est réduit.*

Les propriétés suivantes résultent immédiatement de la définition :

1. Si B est séparable sur k, B est réduite.

2. Pour que B soit séparable sur k, il faut et il suffit que, pour toute extension FINIE k'/k de k, $B \underset{k}{\otimes} k'$ *soit réduit.*

3. Pour que la k-algèbre B soit séparable, il faut et il suffit que toute sous-algèbre (resp. *toute sous-algèbre de type fini*) *de B soit séparable.*

La proposition suivante prouve que, pour la séparabilité de B sur k, seules les extensions radicielles k'/k de k comptent.

Proposition III.2

Soient k un corps, B une k-algèbre, k'/k une extension transcendante pure ou une extension algébrique séparable de k.

Si l'anneau B est réduit, il en est de même de l'anneau $B \underset{k}{\otimes} k'$.

Démonstration

Si $k' = k(X_i)_{i\in I}$ est une extension transcendante pure, $B \underset{k}{\otimes} k'$ est un anneau de fractions (par rapport à la partie multiplicative $k[X_i]_{i\in I} - \{0\}$) de l'anneau de polynômes $B[X_i]_{i\in I}$ qui est réduit comme B.

Soit k'/k une extension algébrique séparable de k. On peut supposer que B est de type fini sur k (car B est limite inductive de ses sous-algèbres de type fini).

L'anneau B est alors noethérien. L'anneau total des fractions K de B est réduit et artinien. Il est donc isomorphe à un produit $\prod_{i=1}^{n} k_i$ de corps k_i extensions de k. Comme k'/k est algébrique séparable, $k' \underset{k}{\otimes} k_i$ est réduit (proposition III.1).

Par conséquent, $K \underset{k}{\otimes} k'$ est réduit et il en est de même de $B \underset{k}{\otimes} k'$ qui en est un sous-anneau.

Corollaire

Soit k *un corps parfait* (par exemple un corps premier). *Une* k*-algèbre est séparable si et seulement si elle est réduite.*

La proposition ci-dessous donne une caractérisation des algèbres de type fini séparables.

Proposition III.3

Soient k *un corps,* B *une* k*-algèbre de type fini.*

Les assertions suivantes sont équivalentes :

(i) B *est séparable sur* k, i.e. *pour toute extension algébrique* k'/k *de* k, $B \underset{k}{\otimes} k'$ *est réduit.*

(ii) $\Omega_{B/k} = 0$.

(iii) B *est isomorphe en tant que* k*-algèbre à un produit fini de corps extensions algébriques séparables de* k.

Démonstration

(i) $\Longrightarrow$ (ii).

On va démontrer que, pour tout idéal maximal m de B, $k(m)$ est extension séparable de k. C'est une extension algébrique de k car $k(m)$ est de type fini sur k.

Soit k' une extension algébrique de $k(m)$. L'anneau $B \underset{k}{\otimes} k'$ est réduit. Or, $B \underset{k}{\otimes} k' = B \underset{k}{\otimes} k(m) \underset{k(m)}{\otimes} k' = B/m \underset{k}{\otimes} k(m) \underset{k(m)}{\otimes} k' = k(m) \underset{k}{\otimes} k(m) \underset{k(m)}{\otimes} k' = k(m) \underset{k}{\otimes} k'$. Donc $k(m)$ est séparable sur k et, compte tenu de la proposition

III.1, $\Omega_{k(m)/k} = 0$. Mais, $\Omega_{k(m)/k} = \Omega_{(B_m/k)} \underset{B_m}{\otimes} k(m) = (\Omega_{B/k})_m/m(\Omega_{B/k})_m$.

Comme $\Omega_{B/k}$ est un B-module de type fini, $(\Omega_{B/k})_m$ est un B_m-module de type fini.

Il résulte alors du lemme de Nakayama que $(\Omega_{B/k})_m = 0$ et du lemme de globalisation que $\Omega_{B/k} = 0$.

(ii)$\Longrightarrow$ (iii).

On va démontrer que la condition $\Omega_{B/k} = 0$ implique que B est artinien et réduit. Il résultera alors de la structure des anneaux artiniens que $B = \prod_{i=1}^{r} k_i$ où k_i est un anneau local artinien réduit, i.e. un corps.

Comme $\Omega_{B/k} = \prod_{i=1}^{r} \Omega_{k_i/k}$, $\Omega_{k_i/k} = 0$ et donc k_i/k est une extension séparable de k.

Soit $\bar{k}$ une clôture algébrique de k. On va démontrer que $B \underset{k}{\otimes} \bar{k}$ est un $\bar{k}$-espace vectoriel de dimension finie. Il en résultera que B est un k-espace vectoriel de dimension finie et donc un anneau artinien.

Comme B est sous-anneau de $B \underset{k}{\otimes} \bar{k}$, pour démontrer que B est réduit il suffit de démontrer que $B \underset{k}{\otimes} \bar{k}$ est réduit.

Si l'on remarque enfin que $\Omega_{(B \underset{k}{\otimes} \bar{k})/\bar{k}} = (\Omega_{B/k}) \underset{k}{\otimes} \bar{k} = 0$, on voit que *l'on peut* pour démontrer l'implication *supposer* k *algébriquement clos.*

Soit alors m un idéal maximal de B.

La k-algèbre $B/m = k(m)$ est finie (parce que B est de type fini sur k La suite exacte :

$$0 \longrightarrow m^n/m^{n+1} \longrightarrow B/m^{n+1} \longrightarrow B/m^n \longrightarrow 0 \qquad (n \geqslant 1)$$

de k-espaces vectoriels prouve que B/m^n est aussi une k-algèbre finie : en effet, B étant noethérien, l'idéal m est de type fini et donc m^n/m^{n+1} est d dimension finie sur k ; une démonstration par récurrence donne alors l'assertion.

De $\Omega_{B/k} = 0$, on déduit (théorème II.6) $\Omega_{(B/m^n)/k} = 0$. On en déduit $B/m^n = k$ en vertu du lemme suivant.

Lemme

Soit C *une algèbre finie sur le corps algébriquement clos* k.

Si C *est locale et si* $\Omega_{C/k} = 0$, C = k.

Démonstration du lemme

Soit n l'idéal maximal de C. L'anneau $C \underset{k}{\otimes} C$ est local d'idéal maximal $n(C \underset{k}{\otimes} C)$: en effet, il est fini sur C donc entier sur C ; tout idéal maxi-

mal de $C \underset{k}{\otimes} C$ contient donc $n(C \underset{k}{\otimes} C)$. D'autre part,

$(C \underset{k}{\otimes} C)/n(C \underset{k}{\otimes} C) \simeq (C/n) \underset{k}{\otimes} (C/n) = k \underset{k}{\otimes} k$ puisque C/n est un corps extension algébrique du corps algébriquement clos k. Donc, $(C \underset{k}{\otimes} C)/n(C \underset{k}{\otimes} C) = k$.

La condition $\Omega_{C/k} = 0$ implique que l'homomorphisme canonique $\varepsilon : C \underset{k}{\otimes} C \longrightarrow C$ fait de C un facteur direct de $C \underset{k}{\otimes} C$. Mais, comme $C \underset{k}{\otimes} C$ est connexe, car local, ε est un isomorphisme.

On en déduit l'égalité :

$$[C : k] = [C \underset{k}{\otimes} C : k] = [C : k]^2$$

et donc $[C : k] = 1$, soit $C = k$.

On voir donc que, pour tout $n \geqslant 1$, $B/m^n = k$ et, par suite que $m = m^n$.

L'anneau local B_m est noethérien comme B. Il résulte du théorème d'intersection de Krull que $(0) = \bigcap_{n \in N} m^n B_m = mB_m$. Donc, B_m est un corps.

L'anneau B isomorphe à $\prod_{m \in \mathrm{Max}(B)} B_m$ est donc réduit.

(iii) $\Longrightarrow$ (i).

Evident.

3. Extensions séparablement engendrées. Le critère de Mac-Lane

Définition

Soit K/k *une extension du corps* k.

Une base de transcendance $(x_i)_{i \in I}$ *de* K/k *est dite séparante si* K *est* (algébrique) *séparable sur* $k(x_i)_{i \in I}$.

L'exemple classique suivant montre que la séparabilité de l'extension K/k n'implique pas forcément l'existence d'une base de transcendance séparante :

Soit k *un corps non parfait de caractéristique* p.

L'extension $K = \bigcup_{n \in N} k(X^{p^{-n}})$, où X est une indéterminée, est séparable de degré de transcendance 1 sur k. Elle n'admet pas de base de transcendance séparante.

Il est clair, d'autre part, *que si l'extension* K/k *admet une base de transcendance séparante, elle est séparable* (proposition III.2).

Définition

Si l'extension K/k *de* k *admet une base de transcendance séparante, on dit qu'elle est séparablement engendrée.*

Proposition III.4 (*critère de Mac Lane*)

Soient k *un corps,* K/k *une extension de* k.

Les assertions suivantes sont équivalentes :

(i) K *est séparable sur* k

(ii) la caractéristique de k *est* 0 *ou la caractéristique* p *de* k *est non nulle et, pour toute famille* $(x_i)_{i\in I}$ *linéairement indépendants sur* k, *la famille* $(x_i^p)_{i\in I}$ *est linéairement indépendante sur* k.

Si, de plus, l'extension K/k *est de type fini, elles sont équivalentes à l'assertion.*

(iii) K *est séparablement engendré sur* k

Démonstration

(i) $\Longrightarrow$ (ii). On démontre (non ii) $\Longrightarrow$ (non i)

Soit $\Sigma_{i\in I}\ a_i x_i^p = 0$ une relation où les $a_i \in k$ ne sont pas tous nuls.

Soit $k' = k(a_i^{p^{-1}})$ et soit $y = \Sigma x_i \otimes a_i^{p^{-1}} \in k[x_i] \underset{k}{\otimes} k' \subset K \underset{k}{\otimes} k'$.

Comme les éléments x_i sont linéairement indépendants sur k, l'élément y n'est pas nul. Or, $y^p = \Sigma x_i^p \otimes a_i = (\Sigma a_i x_i^p) \otimes 1 = 0$.

Donc $K \underset{k}{\otimes} k'$ n'est pas réduit et K/k n'est pas séparable.

Pour démontrer les autres équivalences, *on peut* (quitte à considérer les sous-extensions de type fini de K/k) *supposer que* K *est extension de type fini de* k.

On a déjà remarqué que (iii) implique (i).

(ii) $\Longrightarrow$ (iii).

Soient $K = k(x_1,\ldots,x_n)$ où $(x_1,\ldots,x_r)$ est base de transcendance de K/k.

On suppose que $x_{r+1},\ldots,x_q$ sont séparables sur $k(x_1,\ldots,x_r)$ et que x_{q+1} ne l'est pas.

Soit $f(X_1,\ldots,X_r,X_{q+1})$ un polynôme non nul à coefficients dans k *de degré minimal tel que* $f(x_1,\ldots,x_r,x_{q+1}) = 0$.

Il ne peut être de la forme $\Sigma\, c_\alpha\, M_\alpha(X)^p$ où $c_\alpha \in k$ et les monômes $M_\alpha(X)$ sont distincts car, de l'égalité $0 = \Sigma\, c_\alpha\, M_\alpha(x)^p$, on déduirait par hypothèse l'égalité $0 = \Sigma\, c_\alpha\, M_\alpha(x)$ qui contredit la minimalité du degré de f.

On en déduit qu'une des indéterminées $X_1,\ldots,X_r,X_{q+1}$ apparait effectivement dans l'expression de f à une puissance non multiple de p. Ce ne peut être X_{q+1} car alors x_{q+1} serait séparable sur $k(x_1,\ldots,x_r)$. C'est donc par exemple, X_1. Alors, x_1 est séparable sur $k(x_2,\ldots,x_r,x_{q+1})$ et il en est de même, bien sur, de $x_{r+1},\ldots,x_q$.

On remplace la base de transcendance $(x_1,\ldots,x_r)$ par la base $(x_2,\ldots,x_r,x_{q+1})$ et on itère le procédé s'il y a lieu jusqu'à obtenir une base de transcendance séparante de K sur k.

4. Degré de transcendance et dimension de l'espace vectoriel des différentielles d'une extension de corps

Proposition III.5

Soient k *un corps,* K/k *une extension de type fini de* k, L/K *une extension de type fini de* K.

1. $[\Omega_{L/k}:L] \geq [\Omega_{K/k}:K] + d°tr(L/K)$.
2. *Si* L *est séparablement engendrée sur* K, *on a l'égalité*

$$[\Omega_{L/k}:L] = [\Omega_{K/k}:K] + d°tr(L/K)$$

Démonstration

On peut se limiter au cas où L *est une extension monogène* K(x) *de* k.

Quatre cas sont alors possibles.

1er cas : x *est transcendant sur* K

Alors, $\Omega_{K[x]/k} = (\Omega_{K/k} \underset{K}{\otimes} K[x]) \oplus K[x]dx$ et, par localisation,

$\Omega_{L/k} = (\Omega_{K/k} \underset{K}{\otimes} L) \oplus Ldx$

On a alors, $[\Omega_{L/k}:L] = [\Omega_{K/k}:K] + 1 = [\Omega_{K/k}:K] + d°tr(L/K)$

2ème cas : x *est algébrique séparable sur* k

Soit alors f(X) = irr(X,x,K).

On sait que $\Omega_{L/k} = ((\Omega_{K/k} \underset{K}{\otimes} L) \oplus LdX)/(f^{d_{K/k}}(x)L \oplus (f'(x)dX)L)$ et donc puisque f'(x) est inversible, $\Omega_{L/k} = \Omega_{K/k} \underset{K}{\otimes} L$.

Par conséquent, $[\Omega_{L/k}:L] = [\Omega_{K/k}:K] = [\Omega_{K/k}:K] + d°tr(L/K)$

3ème cas : *la caractéristique* p *de* k *est non nulle et* x *est racine d'un polynôme* X^p-a *où* a *n'appartient pas à* $K^{p^{-1}}$ *et* $d_{K/k}(a) = 0$.

Alors, $L = K[x] = K[X]/(x^p-a)$ et $\Omega_{L/k} = (\Omega_{K[x]/k} \underset{K}{\otimes} L) \oplus Ld_{L/K}(x)$.

Par conséquent, $[\Omega_{L/k}:L] = [\Omega_{K/k}:K] + 1$ est strictement plus grand que $[\Omega_{K/k}:K] + d°tr(L/K)$.

4ème cas : les hypothèses sont celles du 3ème cas sauf que $d_{K/k}(a) \neq 0$.

On obtient alors comme dans le 2ème cas, $\Omega_{L/k} = \Omega_{K/k} \underset{K}{\otimes} L$ et donc $[\Omega_{L/k}:L] = [\Omega_{K/k}:K] + d°tr(L/K)$.

On applique au cas où K = k. Le 4ème cas envisagé ci-dessus est alors exclus puisque $d_{K/k} = 0$. On obtient donc le résultat suivant.

Corollaire 1

Soit L/k *une extension de type fini de* k.

1. $[\Omega_{L/k}:L] \geqslant d^\circ tr(L/k)$

2. *L'égalité* $[\Omega_{L/k}:L] = d^\circ tr(L/k)$ *équivaut au fait que* L/k *est séparablement engendrée, i.e. est séparable.*

Corollaire 2

Les hypothèses sont celles du corollaire 1.

Les assertions suivantes sont équivalentes :

(i) L *est ALGEBRIQUE séparable sur* k

(ii) $\Omega_{L/k} = 0$.

Exercices du chapitre 9

(1). Soient k un corps.

Calculer le module des différentielles $\Omega_{A/k}$ dans les cas suivants :

$A = k[X,Y]/(1-Y^2(1-X^2))$

$A = k[X,Y]/(X^2-Y^3)$

Examiner s'il a de la torsion.

(2). Démontrer, en utilisant la propriété universelle des différentielles, la proposition II.1(2), la proposition II.2(2), la proposition II.3(2) et les théorèmes II.5 et II.6.

(3). Calculer $\Omega_{(A \otimes B)/k}$, où $k \longrightarrow A$ et $k \longrightarrow B$ sont deux k-algèbres, en fonction de $\Omega_{A/k}$ et $\Omega_{B/k}$.

(4). Les notations sont celles du théorème II.5. Soit c un idéal de

Exprimer en termes de modules de différentielles le fait que, pour tout C-module M *annulé par* c, toute A-dérivation de B dans M se prolonge e une A-dérivation de C dans M.

(5). La plupart des résultats suivants s'étendent au cas d'algèbres non commutatives. Le lecteur pourra consulter, par exemple, l'ouvrage suivant : Frank DeMeyer - Edward Ingraham. *Separable Algebras over commutative Rings. Lecture Notes in Mathematics.* 181 . *Springer-Verlag* dont nous avons suivi l'exposé.

Il faut signaler qu'ici l'étude du cas non commutatif est essentiell notamment pour l'étude du groupe de Brauer.

Soient A *un anneau,* B *une* A*-algèbre commutative.*

On note ε l'application : $\Sigma x_i \otimes y_i \longmapsto \Sigma x_i y_i$ de $B \underset{A}{\otimes} B$ sur B. Elle munit B d'une structure de $B \underset{A}{\otimes} B$-module.

1. Démontrer l'équivalence des assertions :

(i) B est un $B \underset{A}{\otimes} B$-module projectif

(ii) La suite $0 \longrightarrow I \longrightarrow B \underset{A}{\otimes} B \xrightarrow{\varepsilon} B \longrightarrow 0$ est scindée

(iii) Il existe un élément e de $B \underset{A}{\otimes} B$ tel que $\varepsilon(e) = 1$ et $Ie = 0$.

Démontrer que cet élément e est un idempotent de $B \underset{A}{\otimes} B$.

Si le A-algèbre B satisfait à ces conditions équivalentes, on dit qu'elle est séparable. On verra, plus loin, que, si A est un corps, on retrouve la notion exposée dans III.

2. Si M est un $B \underset{A}{\otimes} B$-module, on note M^B le B-module $\{x \in M / \forall a \in A, (a \otimes 1)x = 1 \otimes a)x\}$.

Définir, de manière naturelle, un foncteur $(-)^B$ de la catégorie des $B \underset{A}{\otimes} B$-modules dans la catégorie des B-modules.

Démontrer que les applications : $f \longmapsto f(1)$ de $\mathrm{Hom}_{B \underset{A}{\otimes} B}(B,M)$ dans M^B définissent un isomorphisme fonctoriel de $\mathrm{Hom}_{B \underset{A}{\otimes} B}(B,-)$ sur $(-)^B$.

Démontrer que $\mathrm{Hom}_{B \underset{A}{\otimes} B}(B,B)$ est isomorphe à B et que $\mathrm{Hom}_{B \underset{A}{\otimes} B}(B, B \underset{A}{\otimes} B)$ est isomorphe à l'annulateur de I.

Démontrer que la A-algèbre B est séparable si et seulement si le foncteur $(-)^B$ est exact à droite.

3. Soient C_1 et C_2 des A-algèbres, B_1 (resp. B_2) une C_1 (resp. C_2)-algèbre séparable.

Démontrer que la $C_1 \underset{A}{\otimes} C_2$-algèbre $B_1 \underset{A}{\otimes} B_2$ est séparable.

En déduire, en particulier, que la notion d'algèbre séparable est stable par changement de base.

4. Soient C_1 et C_2 des A-algèbres, B_1 (resp. B_2) une C_1 (resp. C_2)-algèbre.

On suppose que la $C_1 \underset{A}{\otimes} C_2$-algèbre $B_1 \underset{A}{\otimes} B_2$ est séparable et que le A-module B_2 est fidèle et contient A comme facteur direct.

Démontrer qu'alors B_1 est séparable sur A_1.

En déduire que, si B est une A-algèbre, C une A-algèbre contenant A comme facteur direct (en tant que A-module) et si $B \underset{A}{\otimes} C$ est une C-algèbre séparable, B est une A-algèbre séparable.

5. Soient B une A-algèbre séparable, C une B-algèbre séparable.

Démontrer que C est une A-algèbre séparable (transitivité de la séparabilité).

6. Soit B une A-algèbre séparable.

On suppose que le A-module B est projectif.

Démontrer que le A-module B est de type fini.

(Considérer une famille $(f_i)_{i\in I}$ (resp. $(x_i)_{i\in I}$) d'éléments de $\mathrm{Hom}_A(B,A)$ (resp. B) telle que, tout $x \in B$ s'écrive $\Sigma f_i(x)x_i$. ((FFAC. Chap. 5. Prop. II.1) et un idempotent e de $B \underset{A}{\otimes} B$ comme dans (iii) de 1.

Calculer $x = \varepsilon((1\otimes x)e) = \Sigma_i\ (B\otimes f_i)((1\otimes x)e)x_i = \Sigma_{i,j} f_i(t_j x)z_j x_i$ si $e = \Sigma z_j \otimes t_j$).

7. Soit B une A-algèbre séparable.

Démontrer qu'un B-module qui est projectif en tant que A-module l'est aussi en tant du B-module.

(Partir d'une suite exacte de B-modules : $0 \longrightarrow M' \longrightarrow M \xrightarrow{g} M'' \longrightarrow$ où M'' est projectif en tant que A-module. Considérer une section h A-linéaire de g.

Démontrer que eh, où e est un idempotent de $B \underset{A}{\otimes} B$ comme dans (iii) d 1, est une section B-linéaire de g).

8. Démontrer que, si A est un corps, et si B est une A-algèbre séparable au sens de l'exercice elle l'est au sens de III. du texte.

(Soit K une extension de A. Démontrer que tout $B \underset{A}{\otimes} K$-module est projectif en utilisant 7. Utiliser alors le fait qu'un anneau artinien sur lequel tout module est projectif est réduit).

(6). *(Théorie de* Galois *des anneaux commutatifs)*

Soient B *un anneau,* A *un sous-anneau,* G *un groupe fini d'automorphismes de* B.

Soit $\{u_s\}_{s\in G}$ *la base canonique du* B*-module libre* $B^{(G)}$.

On définit que $B^{(G)}$ *une structure de* B*-algèbre* $\Delta(B;G)$ *en définissant le produit* $(bu_s)(b'u_{s'})$, *où* $b,b' \in B$, $s,s' \in G$, *comme étant* $bs(b')u_{s\circ s'}$ (algèbre non commutative) *et une autre strcuture de* B*-algèbre* $\nabla(B;G)$ *en définissant le produit* $(bu_s)(b'u_{s'})$ *comme étant* $bb'\delta_{ss',u_s}$, *où, dans la suite,* $\delta_{ss'} = 0$ *si* $s \neq s'$ *et* $=1$ *si* $s = s'$.

On définit un homomorphisme j *de* A*-algèbres de* $\Delta(B;G)$ *dans* $\mathrm{Hom}_A(B,B)$ *par* $(j(bu_s))(x) = bs(x)$ $(x \in B)$ *et un homomorphisme* l *de* B*-algèbres de* $B \underset{A}{\otimes} B$ *dans* $\nabla(B;G)$ *par*

$l(b \otimes b') = \Sigma_{s\in G} bs(b')u_s$.

1. Démontrer que les conditions (i), (ii), (iii), (iv), (v) ci-des-

sous sont équivalentes :

(i) 1. $B^G = A$ (où $B^G = \{x \in B / \forall s \in G,\ s(x) = x\}$)

2. pour tout idempotent $e \in B$ et tout couple (s,t) d'éléments distincts de G, il existe $x \in B$ tel que $s(x)e \neq t(x)e$

3. B est une A-algèbre séparable

(ii) 1. $B^G = A$

2. il existe $x_1,\dots,x_b,\ y_1,\dots,y_n \in B$ tel que $\Sigma_{i=1}^{n} x_i s(y_i) = \delta_{s1_B}$ (avec la signification donnée plus haut de δ)

(iii) 1. Le A-module B est projectif de type fini

2. l'homomorphisme j de $\Delta(B,G)$ dans $\mathrm{Hom}_A(B,B)$ est un isomorphism

(iv) 1. $B^G = A$

2. l'homomorphisme $\iota : B \underset{A}{\otimes} B \longrightarrow \nabla(B;G)$ est un isomorphisme

(v) 1. $B^G = A$

2. pour tout idéal maximal m de B et tout élément s de G, distin de 1_B, il existe $x \in B$ tel que $s(x)-x$ n'appartienne pas à m.

((i) $\Longrightarrow$ (ii). Soit $e = \Sigma_{i=1}^{n} x_i \otimes y_i$ un idempotent comme dans l'exercice 5 1.(iii).

Calculer $x\,\varepsilon(1\otimes s(e)) = s(x)(1\otimes s(e))$.

(ii) $\Longrightarrow$ (iii). Définir $f_i \in \mathrm{Hom}_A(B,A)$ par $f_j(x) = \Sigma_{s\in G}\, s(xy_i)$. Démontrer l'égalité $x = \Sigma_{i=1}^{n} f_i(x)x_i$ pour $x \in B$ et utiliser une caractérisati des modules projectifs.

Démontrer ensuite que si $h \in \mathrm{Hom}_A(B,B)$, $h = j(w)$ où $w = \Sigma_{s\in G}\Sigma_{i=1}^{n} h(x_i)s(y_i)u_s$.

(iii) $\Longrightarrow$ (iv). Remarquer que B^G est contenu dans le centre de $\Delta(B;G$ Utiliser le fait que A est le centre de $\mathrm{Hom}_A(B,B)$. Soit t l'élément $\Sigma_{s\in G} u_s$ de $\Delta(B;G)$.

Démontrer que $j(tB) = \mathrm{Hom}_A(B,A)$. Construire alors une suite d'isomorphismes de A-modules :

$$B \underset{A}{\otimes} B \longrightarrow B \underset{A}{\otimes} tB \longrightarrow B \underset{A}{\otimes} \mathrm{Hom}_A(B,A) \longrightarrow \mathrm{Hom}_A(B,B) \longrightarrow \Delta(B;G) \downarrow \nabla(B;G)$$

dont le composé est ι.

(iv) $\Longrightarrow$ (ii). Poser $\iota^{-1}(u_{1_B}) = \Sigma_{i=1}^{n} x_i \otimes y_i$.

(ii) $\Longrightarrow$ (i). Poser $e = \Sigma_{i=1}^{n} x_i \otimes y_i$. Démontrer que e satisfait aux conditions de l'exercice 1.(iii).

(ii) $\Longrightarrow$ (v). Démontrer que, si pour $s \in G$ distinct de 1_B, $(1_B - s)B$ est contenu dans B, 1 appartient à m.

(v) $\Longrightarrow$ (ii). Démontrer d'abord l'existence pour tout s fixé de G distinct de 1_B d'éléments $x_1,\dots,x_n$, $y_1,\dots,y_n$ dépendants de s ainsi que n satisfaisant aux égalités de (ii).2.: choisir $x_1,\dots,x_{n-1},y_1,\dots,y_{n-1}$ tels que $\Sigma_{i=1}^{n-1} x_i(1_B - s)(y_i) = 1$ et poser $x_n = -\Sigma_{i=1}^{n-1} x_i s(y_i)$ et $y_n = 1$.

Remarquer ensuite que si l'on a *l'un des groupes* d'égalités :

$$\Sigma_{i=1}^{n} x_i t(y_i) = \delta_{t,1_B}$$

$$\Sigma_{j=1}^{m} x'_j t(y'_j) = \delta_{t,1_B}$$

on a l'égalité $\Sigma_{(i,j)} x_i x'_j t(y_i y'_j) = \delta_{t,1_B}$).

Si le couple (A,B) satisfait aux conditions équivalentes ci-dessus, on dit que B est une *extension galoisienne de* A *de groupe de Galois* G.

Comment se transforme la condition (i), si on suppose de plus l'anneau B connexe ?

Comment se transforme la condition (v) si B est un corps ?

(7). Soit B une extension galoisienne de A de groupe de Galois G.

1. On note $\mathrm{Tr}_{B/A}$ l'élément $j(\Sigma_{s\in G} u_s)$ de $\mathrm{Hom}_A(B,A)$ (avec les notations de l'exercice précédent).

Démontrer l'existence de $c \in B$ tel que $\mathrm{Tr}_{B/A}(c) = 1$.

(Démontrer, au préalable, que si M est un A-module projectif et si a_M est l'idéal de A engendré par les éléments f(x) où $x \in M$, $f \in \mathrm{Hom}_A(M,A)$, $A = a_M \oplus \mathrm{Ann}(M)$.

En déduire l'existence de $x_1,\dots,x_n \in B$ et $f_1,\dots,f_n \in \mathrm{Hom}_A(B,A)$ tels que $\Sigma_{i=1}^{n} f_i(x_i) = 1$.

Poser $c = \Sigma_{i=1}^{n} c_i x_i$ où c_i est défini par la condition $f_i(x) = \mathrm{Tr}_{B/A}(c_i x)$ pour tout $x \in B$).

2. Déduire de la surjectivité de $\mathrm{Tr}_{B/A}$ que A est facteur direct du A-module B.

3. Soit C une A-algèbre. On fait opérer G sur $C \underset{A}{\otimes} B$ par $s(c \otimes b) = c \otimes s(b)$.

Démontrer que $C \underset{A}{\otimes} B$ est une extension galoisienne de C de groupe de Galois G.

En déduire, que si $p \in \mathrm{Spec}(A)$, B_p est une extension galoisienne de A_p de groupe de Galois G.

4. Démontrer que le A-module projectif B est de rang égal à l'ordre de G.

(Se ramener au cas où A est local. Ecrire alors l'égalité $rg(Hom_A(B,B)) = rg(\Delta(B,G))$.

(8). Soient A un anneau, B une A-algèbre *séparable*, $\Sigma_{i=1}^{n} x_i \otimes y_i$ un idempotent de $B \underset{A}{\otimes} B$ comme dans l'exercice 5.1.(iii), h un homomorphisme de A-algèbres de B dans A.

1. Démontrer que $\Sigma_{i=1}^{n} h(x_i)y_i$ est l'unique idempotent e de B tel que, pour tout $b \in B$, $h(b)e = be$ et $h(e) = 1$.

2. On suppose, de plus, A *connexe*.

Soient $h_1,\ldots,h_n$ des homomorphismes distincts de A-algèbres de B dans A, $e_1,\ldots,e_n$ les idempotents correspondants. Démontrer les égalités $e_i e_j = e_i\,\delta_{i,j}$ et $h_i(e_j) = \delta_{i,j}$.

(9). Soient A un anneau, B une A-algèbre de type fini séparable, C une A-algèbre *connexe*.

1. Démontrer qu'il n'existe qu'un nombre fini d'homomorphismes de A-algèbres de B dans C.

(Remarquer que, si $s_1,\ldots,s_m$ sont des homomorphismes distincts de A-algèbres de B dans C, les homomorphismes $h_1,\ldots,h_m$ de $C \underset{A}{\otimes} B$ dans C, définis par $h_i(c \otimes b) = cs_i(b)$, sont distincts. Considérer des idempotents $e_1,\ldots,e_m$ associés à ces homomorphismes comme dans l'exercice. Démontrer $(C \underset{A}{\otimes} B)e_i \simeq C$. En déduire, $C \underset{A}{\otimes} B = C^m \oplus (C \underset{A}{\otimes} B)f$ où $f = 1-e_1-\ldots-e_m$, puis le fait que si B peut être engendré en tant que A-algèbre par r éléments, alors $m \leqslant r$).

2. Démontrer que, si, de plus, le A-module B est *projectif et possède un rang*, il existe au plus rg(B) homomorphismes de A-algèbres de B dans C.

3. Démontrer que, si B est une extension *galoisienne* de A de groupe G et, si f et g sont des homomorphismes de A-algèbres de B dans C, il existe un élément s de G et un seul tel que $g = f \circ s$.

En déduire que, si B est une extension galoisienne *connexe* de groupe G, tout homomorphisme de A-algèbres de B dans B est un élément de G.

(10). Soient B un anneau connexe, A un sous-anneau de B tel que B soit fini sur A.

On suppose que B est une extension galoisienne de A, de groupe de Galois G.

1. Démontrer que le groupe de Galois G de B/A est fini d'ordre égal au rang $rg_A(B)$. (Utiliser l'exercice 7).

2. Démontrer que si H est un sous-groupe de G, l'extension B/B^H est galoisienne et déduire de 1. le fait que l'application : $H \longmapsto B^H$ est injective.

3. Démontrer que l'extension B^H/A est séparable.

(Utiliser l'élément $u = \Sigma_{s\in H} s$ de $\mathrm{Hom}_{B^H}(B,B^H)$, l'élément c de B tel que $u(c) = 1$, puis l'élément e de $B^H \underset{A}{\otimes} B^H$ égal à $\Sigma_{i=1}^{n} u(x_i) \otimes u(y_i c)$, où les éléments x_i, y_i sont ceux de (ii) de l'exercice 6, en démontrant que, pour tout $x \in B^H$, on a l'égalité $(x\otimes 1)e = (1\otimes x)e$).

4. Soit C un sous-anneau de B contenant A et séparable sur A. Démontrer l'égalité $C = B^H$ où H est le sous-groupe de G des automorphismes de B laissant invariants les éléments de C.

(Considérer un ensemble $\{s_1,\dots,s_r\}$ de représentants des classes à gauche de G modulo H avec $s_1 = 1$ et les homomorphismes h_i de $B \underset{A}{\otimes} C$ dans B définis par $h_i(x\otimes y) = xs_i(y)$ $(i = 1,\dots,r)$. Prendre un idempotent $e_1 = \Sigma_{j=1}^{m} u_j \otimes v_j$ de $B \underset{A}{\otimes} C$ tel que, pour tout $w \in B \underset{A}{\otimes} C$, $h_1(w)e_1 = we_1$ et $h_i(e_1) = \delta_{i,1}$.

Démontrer que si $a \in B^H$, $a = \Sigma_{i=1}^{m} (\Sigma_{s\in G} s(u_j)ca)v_j)$. En déduire l'inclusion $B^H \subset C$ et l'égalité $B^H = C$).

5. Démontrer que si le sous-groupe H est *normal*, $A = (B^H)^K$ où K est le groupe de Galois de B^H sur A.

Soient $A \longrightarrow B \longrightarrow C$ une suite d'homomorphismes d'anneaux, M un C-module.

On a des suites exactes :

$$\Omega_{B/A} \underset{B}{\otimes} M \longrightarrow \Omega_{C/A} \underset{C}{\otimes} M \longrightarrow \Omega_{C/B} \underset{C}{\otimes} M \longrightarrow 0$$

$$0 \longrightarrow \mathrm{Der}_B(C,M) \longrightarrow \mathrm{Der}_A(C,M) \longrightarrow \mathrm{Der}_A(B,M)$$

Le but des exercices 11-17 est de définir des foncteurs $T_i(B/A,M)$ et $T^i(B/A,M)$ $(i = 0,1,2)$ tels que $T_0(B/A,M) = \Omega_{B/A} \underset{B}{\otimes} M$, $T^0(B/A,M) = \mathrm{Der}_A(B,M)$ et que les suites exactes ci-dessus se complètent en suites exactes à 9 termes :

$$T_2(B/A,M) \longrightarrow T_2(C/A,M) \longrightarrow T_2(C/B,M) \longrightarrow T_1(B/A,M) \longrightarrow T_1(C/A,M) \longrightarrow T_1(C/B,M$$

$$\downarrow$$

$$0 \longleftarrow T_0(C/B,M) \longleftarrow T_0(C/A,M) \longleftarrow T_0(B/A,M)$$

et suite analogue avec indices supérieurs au lieu d'indices inférieurs.

Le lecteur se reportera à l'article :

The cotangent complex of a morphism. S. Lichtenbaum et M. Schlessinger. Trans. Amer. math. soc. 41,70.

(11). *Soit* $A \longrightarrow B$ *un homomorphisme d'anneaux.*

Une *extension* (à deux termes) *de* B *sur* A est une suite exacte de A-modules

$$(\mathcal{E}) \qquad 0 \longrightarrow E_2 \xrightarrow{e_2} E_1 \xrightarrow{e_1} R \xrightarrow{e_o} B \longrightarrow 0$$

où R est une A-algèbre, e_o un homomorphisme de A-algèbres, E_1 et E_2 des R-modules, e_1 et e_2 des applications R-linéaires telles que, $\forall x,y \in E_1$, $e_1(x)y = e_1(y)x$.

1. Soit $I = \ker(e_o)$. Démontrer que $IE_2 = 0$ et donc que E_2 est un B-module.

A $(\mathcal{E})$ on associe la suite :

$$L_\bullet(\mathcal{E}) \qquad 0 \longrightarrow E_2 \xrightarrow{d_2} E_1 \underset{R}{\otimes} B \xrightarrow{d_1} \Omega_{R/A} \underset{R}{\otimes} B \longrightarrow 0$$

où $d_2(x) = e_2(x) \otimes 1$ et d_1 est le composé de $e_1 \otimes B : E_1 \underset{R}{\otimes} B \longrightarrow I \underset{R}{\otimes} B$ et de l'homomorphisme canonique $d : I/I^2 \longrightarrow \Omega_{R/A} \underset{R}{\otimes} B$ (on remarquera que $\mathrm{im}(e_1) = I$).

2. Démontrer que $L_\bullet(\mathcal{E})$ est un complexe.

Soient $R \xrightarrow{e_o} B$ *un homomorphisme surjectif de* A*-algèbres*, $I = \ker(e_o)$, $0 \longrightarrow U \xrightarrow{i} F \xrightarrow{j} I \longrightarrow 0$ une suite exacte de R-modules, ϕ l'application de $F \underset{R}{\otimes} F$ dans F telle que $\phi(x \otimes y) = j(x)y - j(y)x$, $U_o = \mathrm{im}(\phi)$.

3. Démontrer que U_o est contenu dans U et que, si e_1 est l'application naturelle de F/U_o dans R et e_2 l'application naturelle de U/U_o dans F/U_o, la suite :

$$0 \longrightarrow U/U_o \xrightarrow{e_2} F/U_o \xrightarrow{e_1} R \xrightarrow{e_o} B \longrightarrow 0$$

est une extension de B sur A.

Démontrer que toute extension de B sur A peut être obtenue par ce procédé.

Une extension $(\mathcal{E})$ de B sur A est dite *libre* si elle est de la forme

$$0 \longrightarrow U/U_o \longrightarrow F/U_o \longrightarrow R \longrightarrow B \longrightarrow 0$$

où R est une *algèbre de polynômes sur* A et F un R-*module libre*.

(12). *Soit* R *une* A*-algèbre.*

On dit qu'elle possède la *propriété de relèvement* si pour toute A-algèbre S, tout S-module M, toute application S-linéaire $u : M \longrightarrow S$ telle que, $\forall x,y \in M$, $u(x)y = u(y)x$ et tout couple (f,g) d'homomorphismes de A-al-

gèbres de R dans S tel que $\mathrm{im}(f-g) \subset \mathrm{im}(u)$, il existe une application A-linéaire $\lambda : R \longrightarrow M$ telle que :

$$\forall x,y \in R,\ \lambda(xy) = f(x)\lambda(y) + g(y)\lambda(x) \text{ et que } u\circ\lambda = f-g$$

Démontrer que si R est une algèbre de polynômes sur A, R possède la propriété de relèvement.

(13). Soient $\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow b \\ A' & \longrightarrow & B' \end{array}$ un diagramme commutatif d'anneaux, ($\mathcal{C}$) et ($\mathcal{C}'$) des extensions respectives de B sur A et B' sur A'.

Un morphisme de ($\mathcal{C}$) *dans* ($\mathcal{C}'$) *compatible avec* b est un triplet $(\alpha_o, \alpha_1, \alpha_2)$ où α_o est un homomorphisme de A-algèbres, α_1 et α_2 des homomo phismes de R-modules rendant commutatif me diagramme :

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & E_2 & \xrightarrow{e_2} & E_1 & \xrightarrow{e_1} & R & \longrightarrow & B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_o} & & \downarrow{\scriptstyle b} & & \\ 0 & \longrightarrow & E'_2 & \xrightarrow[e'_2]{} & E'_1 & \xrightarrow[e'_1]{} & R' & \xrightarrow[e'_o]{} & B' & \longrightarrow & 0 \end{array}$$

1. Démontrer qu'un tel morphisme définit un morphisme du complexe $L_\bullet(\mathcal{C}) \underset{B}{\otimes} B'$ dans le complexe $L_\bullet(\mathcal{C}')$.

2. Démontrer que, si la A-algèbre R possède la propriété de relèvement, deux morphismes de ($\mathcal{C}$) dans ($\mathcal{C}'$) définissent des morphismes homotopes de $L_\bullet(\mathcal{C}) \underset{B}{\otimes} B'$ dans $L_\bullet(\mathcal{C}')$. ((FFAC) chap. 6. II.2).

3. Démontrer que si l'extension ($\mathcal{C}$) est libre, il existe un morphis me de ($\mathcal{C}$) dans ($\mathcal{C}'$) compatible avec b.

(14). *Soit* $A \longrightarrow B$ *un homomorphisme d'anneaux.*

On appelle *complexe cotangent de* B *sur* A un complexe $L_\bullet(\mathcal{C})$ où ($\mathcal{C}$) est une extension *libre* de B sur A.

Déduire de ce qui précède que deux complexes cotangents de B sur A sont homotopiquement équivalents et que pour tout diagramme commutatif

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow b \\ A' & \longrightarrow & B' \end{array}$$

il existe *un* morphisme, et *un seul à homotopie près*, du tensorisé par B' sur B d'un complexe cotangent à B sur A dans un complexe cotangent à B' sur A'.

(15). *Soient* $A \longrightarrow B \longrightarrow C$ *une suite d'homomorphisme d'anneaux,* $(\mathcal{E})$ *et* $(\mathcal{G})$ *des extensions libres de* B *sur* A *et* C *sur* B *respectivement.*

1. Démontrer l'existence d'une extension libre $(\mathcal{F})$ de C sur A et de morphismes $(\mathcal{E}) \longrightarrow (\mathcal{F}) \longrightarrow (\mathcal{G})$ compatibles avec les homomorphismes $A \longrightarrow B \longrightarrow C$ telle que la suite :

$$0 \longrightarrow L_\cdot(\mathcal{E}) \underset{B}{\otimes} C \longrightarrow L_\cdot(\mathcal{F}) \longrightarrow L_\cdot(\mathcal{G}) \longrightarrow 0$$

soit exacte à l'exception éventuelle près que l'application $L^2(\mathcal{E}) \underset{B}{\otimes} C \longrightarrow L^2(\mathcal{F})$ n'est pas forcément injective.

Soit M *un* B*-module.* On pose $T_i(B/A,M) = H_i(L_\cdot(\mathcal{E}) \underset{B}{\otimes} M)$, $T^i(B/A,M) = H^i(\mathrm{Hom}_B(L_\cdot(\mathcal{E}),M)$ où $(\mathcal{E})$ est une *extension libre* de B sur A. $(i = 0, 1, 2)$.

2. Démontrer l'existence des suites exactes à neuf termes annoncées dans la présentation des exercices.

(16). *Soit*

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ A' & \longrightarrow & B' \end{array}$$

un carré cocartésien(*). *Soit* M' *un* B'*-module.*

Démontrer que si B est plat sur A ou si A' est plat sur A, les homomorphismes naturels $T_i(B/A,M') \longrightarrow T_i(B'/A',M')$ et $T^i(B/A/M') \longrightarrow T^i(B'/A',M)$ sont des isomorphismes.

Soit M *un* B*-module.*

Démontrer que si A' est plat sur A, l'homomorphisme naturel $T_i(B/A,M) \underset{B}{\otimes} B' \longrightarrow T_i(B'/A',M \underset{B}{\otimes} B')$ est un isomorphisme.

(17). *Soient* $A \longrightarrow B$ *un homomorphisme d'anneaux,* S *une partie multiplicative de* B, M *un* B*-module.*

Démontrer l'existence d'un isomorphisme $T_i(B/A,M) \underset{B}{\otimes} S^{-1}B \longrightarrow T_i(S^{-1}B/A,S^{-1}M)$.

(18). Soient k un anneau, $\rho : k \longrightarrow A$ une k-algèbre.

Une k-dérivation de Hasse de A est une suite infinie $\{D_n\}_{n\in\mathbb{N}}$ d'éléments de $\mathrm{Hom}_k(A,A)$ telle que :

(*) i.e. tel que B' soit somme amalgamée $B \underset{A}{\otimes} A'$ du diagramme

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \\ A' & & \end{array}$$

1. $D_o = 1_A$
2. $\forall x,y \in A,\ D_n(xy) = \sum_{\substack{(m,p)\\ m+p=n}} D_m(x)D_p(y)$
3. $\forall x \in A,\ D_n(D_m(x)) = \binom{n+m}{n} D_{n+m}(x)$

1. Que peut-on dire de D_1?

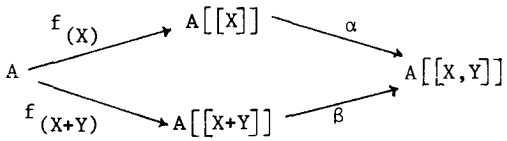
A quelle condition D_1 détermine-t-il la dérivation de Hasse de A?

2. Soit X une indéterminée.

Démontrer que l'application : $x \longmapsto \sum_{n\in N} D_n(x)X^n$ de A dans $A[[X]]$ est un homomorphisme $f_{(X)}$ de k-algèbres possédant les propriétés suivantes

1. Si g est l'homomorphisme $v(X) \longmapsto v(o)$ de $A[[X]]$ dans A, $g \circ f_{(X)} = 1_A$.

2. Le diagramme :



où Y est une autre indéterminée, α est le prolongement de $f_{(Y)}$ tel que $\alpha(X) = X$ et β est l'injection canonique, est commutatif.

Démontrer la réciproque.

APPENDICE

Espaces spectraux

par M. L. Mascle et Mme M.L. Pham
(d'après l'article de M. Höchster (49))

Un espace topologique X est dit *spectral* s'il est T_o, quasi-compact, si toute intersection finie d'ouverts quasi-compacts est quasi-compacte, si l'ensemble des ouverts quasi-compacts est une base des ouverts de la topologie et si toute partie fermée irréductible de X a un point générique.

Le spectre d'un anneau est un espace spectral. Dans (49), M. Höchster démontre, en particulier, la réciproque : un espace spectral est homéomorphe au spectre d'un anneau.

§1. LA TOPOLOGIE CONSTRUCTIBLE

Dans tout ce paragraphe, X désignera un espace spectral, Ω l'ensemble des ouverts quasi-compacts de X, Φ l'ensemble des fermés de X. On dit qu'un sous-ensemble $\mathcal{E}$ de $\Omega \cup \Phi$ à la propriété d'intersection finie si toute intersection finie d'éléments de $\mathcal{E}$ est non vide.

Lemme 1

Avec les notations ci-dessus, si $\mathcal{E}$ a la propriété d'intersection finie, l'intersection des éléments de $\mathcal{E}$ est non vide.

Démonstration

Il est immédiat que l'ensemble des parties de $\Omega \cup \Phi$ ayant la propriété d'intersection finie et contenant $\mathcal{E}$, ordonné par l'inclusion, est un ensemble ordonné inductif ; il possède donc un élément maximal $\mathcal{M}$. On va montrer que l'intersection des éléments de $\mathcal{M}$ est non vide. On pose $\mathcal{M} \cap \Phi = \{\phi_i / i \in I\}$, et $F = \bigcap_{i \in I} \phi_i$.

a) F *appartient à* $\mathcal{M}$:

comme F est un fermé et $\mathcal{M}$ est maximal, il suffit de démontrer que $\mathcal{M} \cup \{F\}$ a la propriété d'intersection finie. Pour tout $i \in I$, ϕ_i contient F ; il suffit donc de démontrer que pour tous $\omega_1, \ldots, \omega_p \in \Omega \cap \mathcal{M}$, $\omega_1 \cap \ldots \omega_p \cap F \neq \emptyset$. Mais X étant spectral, $\omega = \omega_1 \cap \ldots \cap \omega_p \in \Omega$ et $\emptyset = F \cap \omega = \cap (\phi_i \cap \omega)$ impliquerait qu'il existe $i_1, \ldots, i_s \in I$ tels que $\emptyset = \phi_{i_1} \cap \ldots \cap \phi_{i_s} \cap \omega_1 \cap \ldots \cap \omega_p$, ce qui est impossible.

b) F *est irréductible* :

F est non vide d'après a).

Supposons $F = \phi_1 \cup \phi_2$, ϕ_1 et $\phi_2 \in \Phi$; on va démontrer que ceci implique $\phi_1 = F$ ou $\phi_2 = F$, ce qui est équivalent à $\phi_1 \in \mathcal{M}$ (ou encore à $\mathcal{M} \cup \{\phi_1\}$ ou $\mathcal{M} \cup \{\phi_2\}$ a la propriété d'intersection finie).

Supposons $\phi_1 \notin \mathcal{M}$; il existe donc $\pi_1, \ldots, \pi_k \in \mathcal{M}$ tels que $\phi_1 \cap \pi_1 \cap \ldots \cap \pi_k = \emptyset$. On a alors, pour tous $\xi_1 \ldots \xi_s \in \mathcal{M}$, $\phi_2 \cap \xi_1 \cap \ldots \cap \xi_s \neq \emptyset$ car $\phi_2 \cap \xi_1 \cap \ldots \cap \xi_s = \emptyset$ impliquerait $F \cap \xi_1 \cap \ldots \cap \xi_s \cap \pi_1 \cap \ldots \cap \pi_k = \emptyset$ ce qui est impossible d'après a). Donc, $\phi_2 \in \mathcal{M}$.

c) Conclusion :

comme X est spectral, F possède un point générique, qui appartient à tout ouvert rencontrant F, donc à tous les éléments de $\mathcal{M}$, ce qui achève la démonstration du lemme 1.

Définitions

Les éléments de $\Omega \cup \Phi$ constituent une sous-base de fermés d'une nouvelle topologie sur X ; c'est la topologie constructible sur X. Un ensemble pro-constructible est par définition un fermé pour cette topologie.

Un ensemble pro-constructible est donc intersection de sous-ensembles de la forme $\omega \cup \phi$, où $\omega \in \Omega$ et $\phi \in \Phi$.

Par passage au complémentaire, un ouvert pour la topologie constructible est réunion de sous-ensembles de la forme $U \cap \complement V$, où U et $V \in \Omega$.

La topologie constructible est plus fine que la topologie initiale sur X.

Théorème 1

Un espace spectral X est compact pour la topologie constructible.

Démonstration

L'espace X est séparé : soient x et y deux points distincts de X ; comme X est T_0 ; il existe un voisinage V de l'un ne contenant pas l'autre; on peut supposer $V \in \Omega$ car Ω est une base des ouverts de X. Alors V et $\complement V$ sont des voisinages des points de x et de y pour la topologie constructible.

L'espace X est quasi-compact: ceci est une conséquence du lemme 1, car on sait qu'un espace topologique quasi-compact est caractérisé par l'existence d'une sous-base de fermés ayant la propriété suivante : toute partie $\mathcal{C} = \{\pi_i / i \in I\}$ de cette sous-base qui a la propriété d'intersection finie, vérifie $\cap \pi_i \neq \emptyset$.

Corollaire 1

Soient X *un espace spectral et* Y *un sous-ensemble pro-constructible de* X. *Un élément* x *de* X *est adhérent à* Y *si et seulement si il est adhérent à un élément de* Y.

Démonstration

Soit x un élément de X adhérent à Y. Soit $E = \{\omega\in\Omega \ / \ x\in\omega\} \cup \{Y\}$*. Les éléments de E sont des fermés pour la topologie constructible, et E a la propriété d'intersection finie. Comme X est compact, l'intersection A des éléments de E est non vide, et x est adhérent à tout élément de A.

La réciproque est évidente.

§2. SOURCES

Le but de la construction que l'on va faire est, étant donné un espace spectral X, *d'obtenir un anneau* A *dont le spectre soit homéomorphe à* X.

Dans tout ce paragraphe, X *désignera un espace spectral,* $\{A_x\}_{x\in X}$ *une famille d'anneaux intègres indexée par* X, *et* A *un sous-anneau de* $\prod_{x\in X} A_x$. *Pour tout* $y\in X$, *on note* pr_y *la projection de* $\prod_{x\in X} A_x$ *sur* A_y.

Définition

Une source est un triplet $(X,\{A_x\}_{x\in X},A)$ *notée quelquefois* (X,A) *dans la suite qui vérifie les conditions suivantes :*

(p_1) *pour tout* $x\in X$, $pr_x(A) = A_x$.

(p_2) *pour tout* $a\in A$, *l'ensemble* $d(a) = \{x\in X \ / \ pr_x(a) \neq 0\}$ *est ouvert et quasi-compact dans* X.

(p_3) *l'ensemble* $\{d(a) \ / \ a\in A\}$ *est une base d'ouverts de* X.

Exemple 1

Soit B *un anneau réduit. On note* ϕ *l'homomorphisme :*

$b \longrightarrow (b(x))_{x\in Spec(B)}$ *de* B *dans* $\prod_{x\in Spec(B)} B/x$.

Alors le triplet $(Spec(B), \{B/x\}_{x\in Spec(B)}, \phi(B))$ *est une source :*

(p_1) est vraie par construction ; pour (p_2) et (p_3) il suffit de remarquer que pour tout $b\in B$, $d(\phi(b)) = D(b)$.

* $\{\omega\in\Omega \ / \ x\in\omega\}$ est non vide car X est spectral.

L'anneau B étant réduit, l'homomorphisme ϕ est injectif. Alors Spec ϕ est un homéomorphisme de Spec(ϕ(B)) sur Spec(B), dont l'application réciproque est Spec ϕ^{-1} ; on l'explicite :

pour tout $x \in$ Spec B, (Spec ϕ^{-1})(x) = $\phi(x) = \ker(pr_x) \cap \phi(B)$.

Plus généralement, *étant donné une source* $(X,\{A_x\}_{x\in X},A)$, *les anneaux* A_x *étant intègres, il existe une application* ψ *de* X *dans* Spec A *telle que pour tout* $x\in X$, $\psi(x) = \ker(pr_x) \cap A$.

Définition

On dit que la source $(X,\{A_x\}_{x\in X},A)$ *est affine si* $\psi(X)$ = Spec(A).

C'est le cas dans l'exemple 1.

Exemple 2

Soient X *un espace spectral et* Ω *l'ensemble des ouverts quasi-compacts de* X. A tout $\omega\in\Omega$, on associe une déterminée T_ω, en sorte que l'application $\omega \longmapsto T_\omega$ soit injective. Soit k un corps et $K = k\left[T_\omega\right]$. On désigne par t_ω l'application de X dans K telle que $t_\omega(x) = T_\omega$ si $x\in\omega$ et $t_\omega(x) = 0$ si $x \notin \omega$.

Soit $A = k\left[t_\omega\right]_{\omega\in\Omega}$ *la sous-algèbre de la* k*-algèbre* K^X *des applications de* X *dans* K, *engendrée par* $\{t_\omega\}_{\omega\in\Omega}$. On remarque que si $a\in A$ et $x\in X$ la valeur a(x) de a en x est un élément de $k\left[T_\omega\right]_{\omega\in\Omega_x}$ où $\Omega_x = \{\omega\in\Omega \ / \ x\in\omega\} = \{\omega\in\Omega \ / \ t_\omega(x) = T_\omega\}$. Soit $A_x = k\left[T_\omega\right]_{\omega\in\Omega_x} = k\left[T_\omega\right]_{x\in\omega}$.

C'est un anneau intègre. L'application $a \longmapsto (a(x))_{x\in X}$ est un homomorphisme de l'anneau A dans l'anneau produit $\prod_{x\in X} A_x$. Il est évidemment injectif car a(x) = 0, pour tout $x\in X$, signifie que l'application a est nulle. On identifie A à son image au moyen de cet homomorphisme. Alors $pr_x(a) = a(x)$.

Le triplet $(X,\{A_x\}_{x\in X},A)$ *que l'on vient de construire est une source :*

(p_1) il suffit de remarquer que pour tout T_ω dans A_x, on a $x\in\omega$ et $T_\omega = t_\omega(x) = pr_x(t_\omega)$.

(p_2) soit $a = \sum_{i=1}^{n} a_i s_i$ où les s_i sont des monômes distincts en les t_ω et les a_i des éléments de k - {0}. Il est clair que $d(a) = \bigcup_{i=1}^{n} d(s_i)$; or tout monôme s_i est de la forme $t_{\omega_1} t_{\omega_2} \dots t_{\omega_p}$, et $d(s_i)=\omega_1\cap\omega_2\cap\dots\cap\omega_p$ est un ouvert quasi-compact de X, cqfd.

(p_3) pour tout $\omega\in\Omega$, $\omega = d(t_\omega)$; donc $\{d(a) \ / \ a\in A\} \supset \Omega$ qui est une base d'ouverts de X.

La source que l'on vient de construire n'est en général pas affine: il suffit pour le voir de prendre pour X l'espace réduit à un point, et pour k le corps des complexes. L'anneau A est alors l'anneau des polynomes $\mathbb{C}[T]$, et Spec A contient plus d'un point ! On a $\psi(X) = \{(0)\}$, et on remarque que (0) étant l'unique point générique de Spec $\mathbb{C}[T]$, $\{(0)\}$ est un sous-ensemble pro-constructible dense de Spec $\mathbb{C}[T]$; il est clair qu'il est homéomorphe à X. Ce résultat se généralise :

Proposition I

Soit $(X,\{A_x\}_{x\in X},A)$ *une source. L'application* ψ *définie plus haut est un homéomorphisme de* X *sur un sous-ensemble pro-constructible dense de* Spec(A).

Démonstration

a) ψ *est injective :*

soient x et y deux éléments distincts de X ; X étant T_0, et d'après (p_3) il existe $a\in A$ tel que par exemple $x\in d(a)$ et $y \notin d(a)$. On a alors $a\notin\psi(x)$ et $a\in\psi(y)$, donc $\psi(x) \neq \psi(y)$, cqfd.

b) ψ *est continue :*

d'après (p_2), il suffit de remarquer que, pour tout $a\in A$, $\psi^{-1}(D(a)) = d(a)$.

c) ψ *est une application ouverte :*

d'après (p_3), il suffit de montrer que, pour tout $a\in A$, $\psi(d(a))$ est ouvert ce qui est vrai car $\psi(d(a)) = D(a) \cap \psi(X)$.

ψ est donc un homéomorphisme de X sur $\psi(X)$.

d) $\psi(X)$ *est dense dans* Spec A :

ceci revient à montrer que $D(a) \cap \psi(X) = \emptyset$ est équivalent à $D(a) = \emptyset$; cette dernière condition équivaut à $a = 0$ (car A est réduit comme sous-anneau de $\prod A_x$). Supposons $D(a) \cap \psi(X) = \emptyset$. Alors pour tout $x\in X$, $a\in\psi(x)$, donc $a \in \bigcap \ker(pr_x)$, donc $a = 0$. cqfd.

c) $\psi(X)$ *est un sous-ensemble pro-constructible de* Spec A :

de la remarque faite en b), on déduit également que ψ est continue pour les topologies constructibles sur X et sur Spec A. Comme ce sont des espaces compacts (th. 1), $\psi(X)$ est fermé pour la topologie constructible sur Spec A.

Le problème posé au début de ce paragraphe est donc équivalent, étant donné un espace spectral X, *à la recherche d'une source affine*

dont X *soit le premier terme* : il suffit de remarquer que, si f est un homéomorphisme de X sur le spectre d'un anneau A, le triplet $(X,\{A/f(x)\}_{x\in X},\phi_1(A))$ est une source affine où ϕ_1 est l'application : $a \longmapsto (a(f(x))_{x\in X}$ de A dans $\prod_{x\in X} A/f(x)$.

Pour tout $a\in A$, *on note* $v(a) = X - d(a) = \psi^{-1}(V(a))$. *Pour tout sous-ensemble* B *de* A, $R_A(B)$ *désignera l'intersection des idéaux premiers de* A *contenant* B ; *c'est aussi la racine de l'idéal engendré par* B.

Avec ces notations, on a la caractérisation suivante des sources affines :

Théorème 2

Une source $(X,\{A_x\}_{x\in X},A)$ *est affine si et seulement si pour tout sous-ensemble fini* B *de* A, *et pour tout* $a\in A$, *on a* :

(*) $\bigcap_{b\in B} v(b) \subset v(a)$ *implique* $a \in R_A(B)$

Démonstration

Il est clair que si la source est affine, la condition (*) est satisfaite.

Réciproquement, on suppose la condition (*) vérifiée, et on démontre $\psi(X) = \mathrm{Spec}\ A$; $\psi(X)$ est un sous-ensemble pro-constructible de Spec A (prop. 1), donc intersection de sous-ensembles de la forme $U_{a,B} = V(a) \cup D(B)$, où $a\in A$ et B est un sous-ensemble fini de A. De plus, $\psi(X) \cap V(B) \subset U_{a,B} \cap V(B) \subset V(a)$ implique d'après (*) $a \in R_A(B)$, c'est à dire $V(B) \subset V(a)$. On en déduit $\mathrm{Spec}(A) = V(B) \cup D(B) = V(a) \cup D(B) = U_{a,B}$, donc $\psi(X) = \mathrm{Spec}(A)$.

Etant donné un espace spectral X, *on a construit une source dont* X *est le premier terme* (exemple 2). *Il est plus difficile de trouver une source qui de plus vérifie* (*). *C'est dans ce but que l'on introduit la notion d'extension.*

Définition

On dit que la source $(X',\{A'_{x'}\}_{x'\in X'},A')$ *est une extension de la source* $(X,\{A_x\}_{x\in X},A)$ *si* X = X', *et si pour tout* $x\in X$, A'_x *est un sous-anneau de* $k_A(x)$ *et contient* A_x ($k_A(x)$ *désigne le corps des fractions de* A_x)

Exemple 3

Soient $(X,\{A_x\}_{x\in X},A)$ *une source, et* B *un sous-ensemble de* $\prod k_A(x)$;

on note $A[B]$ *le sous-anneau de* $\prod_{x\in X} k_A(x)$ *engendré par* A *et* B, *et on suppose que pour tout* $c \in A[B]$, $d(c)$ *soit un ouvert quasi-compact de* X. *Alors* $(X,\{pr_x(A[B])\}_{x\in X},A[B])$ *est une source extension de la source* $(X,[A_x]_{x\in X},A)$; *elle est dite induite par* B.

Définition

Soit X *un espace topologique. On désigne par* $\sigma(X)$ *le sous-ensemble de* X^2 *des couples* (y,x) *d'un point* y *de* X *et d'une spécialisation* x *de* y.

Un indice sur la source $(X,\{A_x\}_{x\in X},A)$ *est la donnée* w, *pour tout* $p = (y,x) \in \sigma(X)$, *d'une valuation discrète* $w_p : k_A(y) \longrightarrow \mathbb{Z}$ (chap. 12)* *satisfaisant aux axiomes suivants :*

(I_1) *pour tout* $a\in A$ *tel que* $pr_y(a) \neq 0$, $w_p(pr_y(a)) \geq 0$ *et* $w_p(pr_y(a)) = 0$ *si et seulement si* $pr_x(a) \neq 0$.

(I_2) *pour tout* $a\in A$, *il existe* $n\in\mathbb{N}^*$ *tel que pour tout* $p = (y,x)$ *de* $\sigma(X)$, *tel que* $pr_y(a) \neq 0$, *on a* $w_p(pr_y(a)) \leq n$.

Une source (X,A) munie d'un indice w est appelée une source indexée et notée (X,A,w). Si (X,A') est une extension de la source indexée (X,A,w) on dit que (X,A') est une w-extension de (X,A) si w définit un indice sur (X,A').

Soient (X,A,w) une source indexée, a et $b \in A$ tels que $v(b) \subset v(a)$, $a \# b$ l'élément de $\prod_{x\in X} k_A(x)$ tel que $pr_x(a\#b)=0$ (resp.$=pr_x(a)/pr_x(b)$) si $pr_x(b) = 0$ (resp. $\neq 0$) et $r = \sum_{i=0}^{m} \alpha_i (a\neq b)^i$ *un élément de* $A[a\#b]$; *alors l'élément* $c = b^m r$ *de* $A[a\#b]$ *appartient à* A *et l'on a* $c = b^m r = \sum_{i=0}^{m} \alpha_i a^i b^{n-i}$.

Démonstration

Si $x \in d(b)$, on a : $pr_x(b^m r) = \sum_{i=0}^{m} pr_x(\alpha_i) pr_x(b^m) pr_x(a\neq b)^i = \sum_{i=0}^{m} pr_x(\alpha_i a^i b^{m-i})$; si $x \in v(b)$, x est élément de v(a), et $pr_x(b^m r) = pr_x(\sum_{i=0}^{m} \alpha_i a^i b^{m-i}) = 0$. Par conséquent, pour tout $x\in X$, on a $pr_x(b^m r) = pr_x(\sum_{i=0}^{m} \alpha_i a^i b^{m-i})$.

Théorème 3

Soient (X,A,w) *une source indexée,* a *et* b *deux éléments de* A *tels que* $v(b) \subset v(a)$, (alors $a\neq b$ est défini). *Les conditions suivantes sont*

* Application telle que $w_p(ab) = w_p(a)+w_p(b)$, $w_p(a+b) \geq \inf(w_p(a),w_p(b))$

équivalentes :

(i) $a \neq b$ *induit une w-extension de* (X,A,w).

(ii) pour tout $p = (y,x) \in \sigma(X)$ *tel que* $pr_y(a) \neq 0$, $w_p(pr_y(a)) \geqslant w_p(pr_y(b))$ *et on a l'égalité si et seulement si* $pr_x(a) \neq 0$.

Démonstration

(i) $\Longrightarrow$ (ii) :

Par hypothèse, $pr_y(a) \neq 0$ implique $pr_y(b) \neq 0$, d'où $pr_y(a \neq b) = pr_y(a)/pr_y(b) \neq 0$. Par conséquent, $w_p(pr_y(a \neq b)) = w_p(pr_y(a)) - w_p(pr_y(b)) \geqslant 0$ d'après (i) et I_1. D'autre part, $w_p(pr_y(a)) = w_p(pr_y(b))$ équivaut à $w_p(pr_y(a \neq b)) = 0$, et d'après (i), à $pr_x(a \neq b) \neq 0$, donc à $pr_x(a) \neq 0$.

(ii) $\Longrightarrow$ (i) :

a) $a \neq b$ *induit une extension de la source* (X,A) :

soit $r = \sum_{i=0}^{m} \alpha_i (a \neq b)^i$ un élément de $A[a \neq b]$, alors l'élément $c = b^m r = \sum_{i=0}^{m} \alpha_i a^i b^{m-i}$ appartient à A, et on remarque que $d(r) = (d(c) \cap d(a)) \cup (d(\alpha_o) \cap v(a))$, ce qui démontre que $d(r)$ est pro-constructible, et donc quasi-compact.

Il reste à montrer que $v(r)$ est fermé. On a les égalités :

$$v(r) = (v(c) \cap d(b)) \cup (v(\alpha_o) \cap v(b))$$

$$v(r) = (v(c) \cap d(a)) \cup (v(\alpha_o) \cap v(a))$$

Donc, $v(r)$ est pro-constructible, et d'après le corollaire 1, il suffit de montrer que tout élément de X adhérent à un élément de $v(r)$ est dans $v(r)$.

Soient $y \in v(r)$ et $x \in X$ tels que $x \in \{\overline{y}\}$; si $y \in v(\alpha_o) \cap v(a)$, alors x appartient aussi à $v(\alpha_o) \cap v(a)$ car c'est un fermé ; si $y \in v(c) \cap d(a)$ et si $x \in d(b)$, il suffit de remarquer que x est élément de $v(c)$ car $\{\overline{y}\} \subset v(c)$, et par conséquent x appartient à $v(r)$; il reste le cas où y appartient à $v(c) \cap d(a)$, et x est élément de $v(b)$. Comme y appartient à $v(c)$, on a $pr_y(c) = 0$, et en remplaçant c par $\sum_{i=0}^{m} \alpha_i a^i b^{m-i}$, on obtient :

$$-pr_y(\alpha_o) pr_y(b^m) = \sum_{i=0}^{m} pr_y(\alpha_i) pr_y(a^i) pr_y(b^{m-i})$$

Si l'on pose $p = (y,x)$, on a :

$$w_p(-pr_y(\alpha_o) pr_y(b^m)) = w_p(pr_y(\alpha_o)) + m w_p(pr_y(b))$$

tandis que :

$$w_p(\sum_{i=o}^{m} pr_y(\alpha_i)pr_y(a^i)pr_y(b^{m-i})) \geqslant \inf(w_p(pr_y(\alpha_i)pr_y(a^i)pr_y(b^{m-i}))$$

En remarquant que $pr_y(a) \neq 0$ et $pr_x(b) = 0 = pr_x(a)$ impliquent, d'après (ii), $w_p(pr_y(a)) > w_p(pr_y(b))$, on a :

$$w_p(\sum_{i=o}^{m} pr_y(\alpha_i)pr_y(a^i)pr_y(b^{m-i}) > mw_p(pr_y(b)).$$

D'où $w_p(pr_y(\alpha_o)) > 0$ et $pr_x(\alpha_o)$ est nul d'après I_1. Par conséquent x appartient à $v(\alpha_o)$, et comme x appartient à v(b), on a $x \in v(r)$. cqfd.

b) w *définit un indice sur* $(X, A[a \neq b])$:

Soient $p = (y,x)$ un élément de $\sigma(X)$, et $r = \sum_{i=o}^{m} \alpha_i (a \neq b)^i$ un élément de $A[a \neq b]$ tel que $pr_y(r) \neq 0$. On va démontrer que, si $pr_x(r) = 0$ alors $w_p(pr_y(r)) > 0$, et que si $pr_x(r) \neq 0$ alors $w_p(pr_y(r)) = 0$.

1) $pr_x(r) = 0$

- si $pr_x(a) \neq 0$, alors $pr_x(b) \neq 0$, d'où $pr_y(b) \neq 0$ (car $x \in \{\bar{y}\}$) et $w_p(pr_y(b)) = 0$; d'autre part, $pr_y(r) \neq 0$ et $pr_y(b) \neq 0$ entraînent $pr_y(b^m r) \neq 0$, et $pr_x(b^m r) = 0$ entraîne $w_p(pr_y(b^m r)) > 0$, d'où $w_p(pr_y(r)) = w_p(pr_y(b^m r)) - mw_p(b)) > 0$.
- si $pr_x(a) = 0$ et $pr_y(a) = 0$, alors $w_p(pr_y(r)) = w_p(pr_y(\alpha_o)) > 0$ car $pr_x(r) = pr_x(\alpha_o) = 0$.
- si $pr_x(a) = 0$ et $pr_y(a) \neq 0$, on a $pr_x(\alpha_o) = pr_x(r) = 0$, donc $w_p(pr_y(\alpha_o)) > 0$; d'autre part, $w_p(pr_y(a)) > w_p(pr_y(b))$ d'après (ii), et pour tout $i > 0$, $w_p(pr_y(\alpha_i(a \neq b)^i) = w_p(pr_y(\alpha_i) + i[w_p(pr_y(b)) - w_p(pr_y(a))] > 0$; et par conséquent $w_p(pr_y(r)) = \inf_{i \geqslant o}(w_p(pr_y(\alpha_i(a \neq b)^i))) > 0$.

2) $pr_x(r) \neq 0$

- si $pr_x(b) \neq 0$, on a $pr_y(b) \neq 0$ (car $x \in \{\bar{y}\}$), et $w_p(pr_y(b) = 0$, de même, $pr_x(b^m r) \neq 0$ entraîne $pr_y(b^m r) \neq 0$, et $w_p(pr_y(b^m r)) = 0$. Par conséquent $w_p(pr_y(r)) = w_p(pr_y(b^m r)) - mw_p(pr_y(b)) = 0$.
- si $pr_x(b) = 0$, on a d'une part $pr_x(r) = pr_x(\alpha_o) \neq 0$, d'où $w_p(pr_y(\alpha_o)) = 0$; d'autre part,
  - si $pr_y(a) = 0$, on a $pr_y(r) = pr_y(\alpha_o)$, et $w_p(pr_y(r)) = 0$
  - si $pr_y(a) \neq 0$, comme $pr_x(b) = 0 = pr_x(a)$, on a, d'après (ii), $w_p(pr_y(a \neq b) = w_p(pr_y(a)) - w_p(pr_y(b)) > 0$, donc $w_p(pr_y(r)) = \inf_{i \geqslant o}(w_p(pr_y(\alpha_i(a \neq b)^i))) = w_p(pr_y(\alpha_o)) = 0$.

Ceci achève la démonstration de (I_1), celle de (I_2) est évidente.

Notation

Soit (X,A,w) *une source indexée. On désigne par* (G(X,A,w) *l'ensemble* {(a,b) ε A^2/v(b) ⊂ v(a), *et* a ≠ b *induit une w-extension de* (X,A,w)}.

On remarque que, dans la condition (ii) du théorème 3, on peut remplacer (X,A,w) par n'importe quelle w-extension de (X,A,w). On en déduit que, si (X,A',w) est une w-extension de (X,A,w), on a $G(X,A',w) \cap A^2 = G(X,A,w)$.

Lemme

Pour toute partie finie H *de* G(X,A,w), *l'ensemble* {a≠b/(a,b) ε H} *induit une w-extension de* (X,A,w).

Démonstration

Si (a,b) appartient à G(X,A,w), a≠b induit une w-extension de (X,A,w).

Soit n > 1, supposons la propriété vérifiée pour tout sous-ensemble de G(X,A,w) ayant n éléments. Soit $H = \{(a_1,b_1),\ldots,(a_{n+1},b_{n+1})\}$ un sous-ensemble de G(X,A,w) ayant n+1 éléments ; pour tout $i = 1,2,\ldots,n+1$, posons $p_i = a_i \neq b_i$. Par hypothèse de récurrence, $(X,A[p_1,\ldots,p_n],w)$ est une w-extension de (X,A,w). Puisque (a_{n+1},b_{n+1}) appartient à $G(X,A,w) = A^2 \cap G(X,A[p_1,\ldots,p_n],w)$, la source $(X,A[p_1,\ldots,p_n][p_{n+1}],w) = (X,A[p_1,\ldots,p_{n+1}],w)$ est une w-extension de $(X,A[p_1,\ldots,p_n],w)$ et par conséquent de (X,A,w).

On en déduit que l'ensemble {a≠b / (a,b) ε G(X,A,w)} *induit une w-extension de* (X,A,w), *que l'on note* (X,A_1,w). *De proche en proche, on définit* (X,A_{n+1},w) *comme la w-extension de* $X,A_n,w)$ *induite par l'ensemble* {a≠b / (a,b) ε $G(X,A_n,w)$}. *La réunion* $M(A) = \bigcup_{n\in\mathbb{N}} A_n$ *induit une w-extension de* (X,A,w), *que l'on désigne par* M(X,A,w).

On remarque que, si a et b sont deux éléments de M(A) tels que a ≠ b induise une w-extension de M(X,A,w), alors il existe n ε *N* tel que a et b appartiennent à A_n; a ≠ b appartient donc à A_{n+1}, et la w-extension de M(X,A,w) induite par a ≠ b est M(X,A,w).

Proposition 4

Soit (X,A,w) *une source indexée, alors*

(**) *pour tout* (a,b) ε $M(A)^2$ *tel que* v(b) ⊂ v(a), *on a* $a\varepsilon R_{M(A)}(b)$.

Démonstration

Si a et b sont deux éléments de M(A), il existe un entier n tel que a et b appartiennent à A_n ; w étant un indice sur A_n, il existe un entier $N > 0$ tel que, pour tout $y \in d(b)$ et tout $p = (y,x) \in \sigma(X)$, on ait $w_p(pr_y(b)) \geqslant N$. On va démontrer que, si $v(b) \subset v(a)$, alors (a^{N+1},b) appartient à $G(X,A_n,w)$.

D'après le théorème 3, il suffit de montrer que, pour tout $p = (y,x) \in \sigma(X)$ tel que $pr_y(a) \neq 0$, si $pr_x(a) \neq 0$ alors $w_p(pr_y(b)) = w_p(pr_y(a))$, et si $pr_y(a) = 0$ alors $w_p(pr_y(a)) > w_p(pr_y(b))$:

1) $pr_x(a) \neq 0$

Alors $w_p(pr_y(a)) = 0$, d'où $w_p(pr_y(a^{N+1})) = 0$. D'autre part, $pr_x(b) \neq 0$ (car $v(b) \subset v(a)$) implique $pr_y(b) \neq 0$ (car $x \in \{\bar{y}\}$) d'où $w_p(pr_y(b)) = 0$.

2) $pr_x(a) = 0$

Alors $w_p(pr_y(a)) > 0$, donc $w_p(pr_y(a)) \geqslant 1$ et $w_p(pr_y(a^{N+1})) \geqslant N+1$. D'autre part, $pr_y(a) \neq 0$ implique $pr_y(b) \neq 0$, donc $w_p(pr_y(b)) \leqslant N$. Par conséquent, $w_p(pr_y(a^{N+1})) > w_p(pr_y(b))$.

Puisque (a^{N+1},b) appartient à $G(X,A_n,w)$, $a^{N+1} \neq b$ appartient à A_{N+1} et par conséquent à M(A). On en déduit que $a \in R_{M(A)}(b)$.

Définition

Une source (X,A) *est dite simple s'il existe un anneau* R *tel que pour tout* $x \in X$, A_x *soit un sous-anneau de* R, *et tel que, pour tout* $a \in A$, *l'ensemble* $\{pr_x(a) \ / \ x \in X\}$ *soit un sous-ensemble fini de* R.

La source construite dans l'exemple 2 est simple.

Théorème 4

Si la source (X,A,w) *est simple, alors la source* M(X,A,w) *est simple.*

Démonstration

Soit (X,A,w) une source simple. Pour tout $x \in X$, A_x est un sous-anneau d'un anneau R, et $(A_1)_x$ est un sous-anneau de l'anneau total des fractions de R. D'autre part, pour tout élément (a,b) de G(X,A,w), si les ensembles $\{pr_x(a) \ / \ x \in X\}$ et $\{pr_x(b) \ / \ x \in X\}$ sont finis, alors l'ensemble $\{pr_x(a \neq b) \ / \ x \in X\}$ est fini.

Par conséquent la source (X,A_1,w) est simple, et par induction, pour tout $n \in N$, la source (X,A_n,w) est simple. On en déduit que d'une

part $(M(A)_x$ est un sous-anneau total des fractions de R, et d'autre part pour tout $a \in M(A)$, il existe $n \in N$ tel que $a \in A_n$, et l'ensemble $\{pr_x(a) \mid x \in X\}$ est fini.

Théorème 5

Soit (X,A,w) *une source indexée simple. Alors les assertions suivantes sont équivalentes :*

(*) *Pour tout sous-ensemble fini* B *de* A, *et pour tout* $a \in A$ $\bigcap_{b\in B} v(b) \subset v(a)$ *implique* $a \in R_A(B)$.

(**) *Pour tout* $(a,b) \in A^2$ *tel que* $v(b) \subset v(a)$, *on a* $a \in R_A(B)$.

Démonstration

Il suffit de montrer que, pour tout sous-ensemble fini B de A, il existe un élément c de l'idéal de A engendré par B tel que $v(c) = \bigcap_{b\in B} v(b)$ Par induction on peut supposer que B a deux éléments, $B = \{b_1,b_2\}$, et en passant aux omplémentaires, chercher c tel que $d(c) = d(b_1) \cup d(b_2)$. Appelons $W_j(1),\ldots,W_j(m_j)$, $j = 1,2$, les sous-ensembles de $d(b_j)$ sur lesquels $x \longmapsto pr_x(b_j)$ est constante. Choisissons un point $y(W)$ dans chaque ensemble W, et un point $y(W_1,W_2)$ dans chaque intersection non vide d'un W_1 et d'un W_2. Soit Y l'ensemble de ces points ; Y est un sous-ensemble fini de $d(b_1) \cup d(b_2)$. On remarque que pour tout élément c du sous-anneau $[b_1,b_2]$ de A engendré par b_1 et b_2 ,

$$\{pr_x(c) \mid x \in d(b_1) \quad d(b_2)\} = \{pr_y(c) \mid y \in Y\}.$$

Il suffit donc de trouver c élément de $I = (b_1,b_2) \cap [b_1,b_2]$ tel que pour tout $y \in Y$, on ait $pr_y(c) \neq 0$, ou, ce qui est équivalent, tel que c n'appartienne à aucun des éléments de $\psi(Y)$. Or les éléments de $\psi(Y)$ sont des idéaux premiers, et aucun ne contient I, donc leur réunion ne contient pas I.

Corollaire 2

Pour toute source simple indexée (X,A,w), *la source* M(X,A,w) *est affine.*

Démonstration

En effet, si (X,A,w) est simple, M(X,A,w) est simple (th. 4) ; d'autre part M(X,A,w) vérifie (**) (prop. 4), donc M(X,A,w) vérifie (*) (th. 5) et M(X,A,w) est affine (th. 2).

§3. CONCLUSION

On revient à la situation considérée dans l'exemple 2, et on munit la source simple qu'y est construite d'un indice σ, de la manière suivante :

Proposition 5

Pour tout $p = (y,x) \in \sigma(X)$, *soit* w_p *l'unique valuation discrète de* $k_A(y)$ *telle que :*

(i) pour tout $\omega \in \Omega_y$, $w_p(T_\omega) = 0$ *si* $x \in \omega$ *et* $w_p(T_\omega) = 1$ *si* $x \notin \omega$.

(ii) si $S_1,\dots,S_n$ *sont des monômes distincts de* A_y *en les indéterminées* T_ω, *et si* $a_1,\dots,a_n$ *sont des éléments de* $k - \{0\}$,
$w_p(\sum_{i=1}^{n} a_i S_i) = \inf_i(w_p(S_i))$.

Alors l'application $p \longmapsto w_p$ *est un indice sur la source* (X,A).

Démonstration

(I_1) Soit $a = \sum_{i=1}^{n} a_i s_i$ un élément de A, tel que $pr_y(a) \neq 0$; alors $w_p(pr_y(a)) = \inf_i(w_p(s_i(y)) \geqslant 0$;

$w_p(pr_y(a)) = 0$ signifie qu'il existe i tel que $w_p(s_i(y)) = 0$. On remarque que s_i est de la forme $s_i = t_{\omega_1} \dots t_{\omega_2}$, avec $y \in \omega_1 \cap \dots \cap \omega_n$, et $w_p(T_{\omega_1}) = \dots = w_p(T_{\omega_n}) = 0$. D'où $x \in \omega_1 \cap \dots \cap \omega_n$ et $pr_x(a) \neq 0$. Réciproquement, si $pr_x(a) \neq 0$, il existe i tel que $s_i(x) \neq 0$. On remarque que s_i est de la forme $s_i = t_{\omega_1} \dots t_{\omega_n}$, et que $x \in \omega_1 \cap \dots \cap \omega_n$. Or $x \in \{\overline{y}\}$, d'où $y \in \omega_1 \cap \dots \cap \omega_n$, et $s_i(y) \neq 0$. Par conséquent $w_p(s_i(y)) = 0$ et $w_p(pr_y(a)) = 0$.

(I_2) Soit $a = \sum_{i=1}^{n} a_i s_i$ un élément de A ; soit n_i le degré de s_i. Pour tout $p \in \sigma(X)$, tel que $pr_y(a) \neq 0$, $w_p(pr_y(a)) \leqslant \sup(n_i)$.

Théorème 6

Soit X *un espace spectral, alors il existe un anneau* B *tel que* X *soit homéomorphe à* Spec(B).

Démonstration

On associe à l'espace X la source indexée simple (X,A,w) que l'on vient de construire (prop. 5). On sait alors (cor. 2) que la source M(X,A,w) est affine, et X est homéomorphe à Spec(M(A)).

On peut à titre d'exercice faire explicitement la construction de la source (X,A) dans le cas où X est un ensemble fini $\{x_1,\dots,x_n\}$ muni de

la topologie discrète et $k = \mathbb{C}$.

Alors Ω est l'ensemble des parties de X, et A est l'ensemble des $(a_1,\ldots,a_n)$ tels que

- a_i est un polynôme en les indéterminées $T(\omega)$ pour $x_i \in \omega$,
- si $\omega_1,\ldots, \omega_q$ sont toutes les parties de X contenant x_i et x_j , alors $a_i(T_{\omega_1},\ldots,T_{\omega_q},0,\ldots,0) = a_j(T_{\omega_1},\ldots,T_{\omega_q},0,\ldots,0)$.

L'ensemble $\sigma(X)$ est l'ensemble des couples (x_i,x_i), et G(X,A,w) est l'ensemble des couples $(a,b) \in A^2$ tels que pour tout $i = 1,2,\ldots,n$, $b_i = 0$ entraîne $a_i = 0$.

On vérifie alors que tout élément de A_1 est de la forme $a \not\equiv b$ où $(a,b) \in G(X,A,w)^2$, et que $M(A) = A_1$.

En particulier (cf. p.4) si $n = 1$, M(A) est le corps des fractions de A, et Spec $M(A) = \{(0)\}$.

Bibliographie

OUVRAGES GENERAUX

ALGEBRE COMMUTATIVE

(1) Atiyah-Mac Donald. Introduction to commutative Algebra. Addison-Wesle 1969.

(2) Bourbaki N. Algèbre commutative. chap. 1. Modules plats. Chap. 2. Localisation. Hermann 1961.

(3) Bourbaki N. Algèbre commutative. chap. 3. Graduations, Filtrations et Topologies, chap. 4. Idéaux premiers associés et décomposition primaire. Hermann 1961.

(4) Bourbaki N. Algèbre commutative. chap.5. Entiers chap.6. Valuations. Hermann 1964.

(5) Dieudonné J. Topics in local Algebra. Notre Dame Mathematical Lecture n° 60, 1967.

(6) Grothendieck-Dieudonné. Eléments de géométrie algébrique. Springer-Verlag. 166, 1971.

(7) Iversen B. Generic Local Structure in Commutative Algebra. Lecture Notes. n° 310, Springer-Verlag, 1970.

(8) Kaplansky I. Commutative Rings. Queen Mary College Mathematics Notes.

(9) Krull W. Ideal theorie. Ergebnisse der mathematik und ihrer grenzgebeite. Springer-Verlag 1935.

(10) Lang S. Algebra Addison-Wesley. 1965.

(11) Macaulay F.S. Algebraic Theory of Modular Systems. Cambridge Tracts n° 19. Cambridge 1916.

(12) Matsumura H. Commutative Algebra. Mathematics Lecture Note Series. Benjamin. 1970.

(13) Nagata M. Local Rings. Interscience Publishers. 13, 1962.

(14) Northcott D.G. Ideal Theory Cambridge at the University Press, 1953.

(15) Northcott D.G. Lessons on Rings, Modules and Multiplicities. Cambridge University Press. 1968.

(16) Raynaud M. Anneaux locaux henséliens. Lecture notes. n° 169, Springer-Verlag. 1970.

(17) Samuel P. Algèbre locale. Mémorial des Sciences mathématiques.

(18) Samuel P. Algèbre commutative. Secrétariat mathématique de l'Ecole Normale Supérieure, Paris, 1969.

(19) Serre J.P. Algèbre locale. Multiplicités. Lecture Notes n° 11, Springer-Verlag, 1965.

(20) Van der Waerden. Modern Algebra.

(21) Zariski-Samuel. Commutative Algebra. I et II. Van-Nostrand, 1960.

THEORIE DES NOMBRES

(22) Borevitch-Schafarevitch. Number theory. Academic Press, 1964.

(23) Hardy-Wright. An introduction to the theory of numbers. Oxford at the Clarendon Press, 1938.

(24) Ribenboim P. Algebraic Numbers. Pure and Applied Mathematics n° 27. Wiley Interscience, 1972.

(25) Serre J.P. Corps locaux. Hermann, 1962.

(26) Samuel P. Théorie algébrique des nombres. Hermann, 1971.

GEOMETRIE ALGEBRIQUE

(27) Demazure-Gabriel. Groupes algébriques. Amsterdam. North Holland Paris Masson, 1970.

(28) Dieudonné J. Cours de géométrie algébrique 1 et 2. Presses Universitaires de France, 1974.

(29) Fulton W. Algebraic Curves. Mathematical Lecture Notes. Benjamin, 196

(30) Mumford D. Introduction to Algebraic Geometry. Harvard lecture notes, 1967.

(31) Samuel P. Méthodes d'algèbre abstraite en géométrie algébrique. Ergebnisse der Mathematik. Springer-Verlag.

(32) Seidenberg A. Elements of the theory of algebraic Curves. Addison-Wesley, 1968.

(33) Walker R. Algebraic Curves. Dover, 1962.

(34) Weil A. Foundations of Algebraic Geometry. Amer. Math. Soc. Coll. Publ. XXIX, 1946.

GEOMETRIE ANALYTIQUE

(35) Cartan H. Famille d'Espaces complexes et fondements de la géométrie analytique. Séminaire 1960/61. Exposés 18-21 par C. Houzel. Secrétariat mathématique, 11, rue P. Curie, Paris (5ème).

(36) Grauert-Remmert. Analytische Stellenalgebren. Die Grundlehren der Mat Wiss., 176, Springer-Verlag, 1971.

(37) Hörmander L. An introduction to complex Analysis in several Variables The University Press in higher Mathematics, Van Nostrand, 1966

(38) Abhyankar S. Local Analytic geometry. Pure and Applied Maths. Academic Press, 1964.

ARTICLES

(39) Bass H. Injective Dimension in noetherian Rings. Trans Amer. Math. Soc 102. 1962, 18-29.

(40) Bass H. Descending chains and the Krull ordinal of commutative Rings. Journal of pureand applied Algebra. 1, n° 4, 1971, 347-360.

(41) Chase S.U. Direct Products of Modules. Trans. Amer. Math. Soc., 97, 1960, 457-473.

(42) De Meyer F.-Ingraham E. Separable Algebras over commutative Rings. Lecture Notes in maths. 181. Springer-Verlag.

(43) Eakin P.U. The converse to a well known theorem on noetherian Rings Math. Annalen, 177, 1968, 278-282.

(44) Eisenbud D. Subrings of artinian and noetherian Rings. Math. Annalen, 185, 1970, 247-249.

(45) Evans E.G. Zero Divisors in noetherian-like Rings. Trans. Amer. Math. Soc., 155, n° 2, 505-512.

(46) Formanek E. Faithful noetherian Modules. Proccedings of the Amer. Math Soc., 41, n° 2, 1973, 381-383.

(47) Gabriel P. Des catégories abéliennes. Bull. Soc. Math. France, 90, 1962, 323-348.

(48) Heinzer W.-Ohm J. Locally noetherian commutative Rings. Trans. Amer. Math. Soc., 158, n° 2, 273-274.

(49) Höchster M. Prime Ideal structure in commutative Rings. Trans. Amer. Math. Soc., 142, 1969, 43-60.

(50) Lasker E. Zur theorie der Moduln und Ideale, Math. Ann. LX, 1905, 20-116.

(51) Lichtenbaum S.-Schlessinger M. The cotangent complex of a Morphism. Trans. Amer. Math. Soc., , , 41-70.

(52) Matlis E. Modules with descending chain conditions. Trans. Amer. Math. Soc., 97, 1960, 495-508.

(53) Micali A. Sur les algèbres universelles. Ann. Inst. Fourier, 14,2,1964.

(54) Noether E. Ideal theorie in Ringbereichen. Math. Annalen, 83, 1921, 24-66.

(55) Samuel P. On unique factorization Domains. Illinois J. Math. 5,

1961, 1-17.

(56) Samuel P. Anneaux factoriels. Publications da Sociedade de Mathematica de São Paulo, 1963.

(57) Samuel P. About Euclidean Rings. Journal of Algebra, 19, 1971, 282-301.

(58) Soublin J.P. Anneaux et modules cohérents. Journal of Algebra. Vol. 15, n° 4, 1970, 455-472.

(59) Stark H.M. A complete determination of the complex quadratic fields of class number one.

(60) Traverso C. Semi normality and Picard Group. Annali della scuola normale superiore di Pisa. Classe di Scienze. XXIV, IV, 1970, 585-595.

Index