SCIENCES SUP

Cours et exercices corrigés

Licence 3 • CAPES • Agrégation

ALGÈBRE POUR LA LICENCE 3

Groupes, anneaux, corps

Jean-Jacques Risler
Pascal Boyer

DUNOD

ALGÈBRE POUR LA LICENCE 3

Groupes, anneaux, corps

Jean-Jacques Risler
Professeur à l'université Paris 6
Pierre-et-Marie-Curie

Pascal Boyer
Maître de conférences à l'université Paris 6
Pierre-et-Marie-Curie

DUNOD

Table des matières

Chapitre **1**

L'anneau $\mathbb{Z}$

Ce chapitre, après une section qui rassemble les définitions de base, traite de l'arithmétique classique : factorialité de $\mathbf{Z}$, groupes cycliques, petit théorème de Fermat, lemme chinois, etc.

1.1 DÉFINITIONS DE BASE

Cette section est conçue comme une sorte de lexique dans lequel sont répertoriées les définitions de base (groupes, sous-groupes, anneaux, morphismes, quotients, etc.) utilisées tout au long du livre, de façon à ce que le lecteur puisse s'y référer commodément.

1.1.1. Notations, conventions

- Un objet mathématique (par exemple une application entre deux ensembles, ou un morphisme de groupes) est dit *canonique* si sa définition ne nécessite pas de choix arbitraire (elle ne dépend que des données).
- La notation : « $:=$ » au cours de la description d'un algorithme doit être lue comme « doit être remplacé par ».
- Le symbole : ■ signifie la fin d'une démonstration.
- Certains paragraphes sont précédés d'une astérisque ; ces astériques indiquent des résultats qui, bien que traitant de questions classiques qui s'insèrent naturellement dans les développements de ce livre, nous semblent dépasser le programme de Licence de mathématiques, et peuvent donc être omis en première lecture.

1.1.2. Généralités

Définition 1.1. *Un* groupe $(G, *)$ *est un ensemble G muni d'une loi de composition interne $G \times G \longrightarrow G$, $(a, b) \mapsto a * b$, telle que :*

1. *il existe un élément neutre e, i.e. tel que pour tout $a \in G$, $e * a = a * e = a$;*
2. *la loi est associative : pour tous $a, b, c \in G$, on a $a * (b * c) = (a * b) * c$;*
3. *tout élément $a \in G$ a un inverse a' tel que $a * a' = a' * a = e$.*

La notation $(G, *)$ pour un groupe précise que la loi de groupe est notée $*$. Si la loi de groupe est notée multiplicativement, le groupe est noté $(G, \times)$ ou simplement G car on omet en général le symbole $\times$. L'élément neutre se note alors 1, et l'inverse de a se note a^{-1}. Pour un groupe $(G, +)$ l'élément neutre se note 0, et l'inverse d'un élément a se note $-a$; par convention, la notation additive est réservée aux groupes commutatifs (*cf.* la définition ci-dessous).

Définition 1.2.

- *Soient G et H deux groupes. On dit d'une application $\phi : G \longrightarrow H$ qu'elle est un* morphisme de groupes *si elle est compatible avec les lois de groupes (notées ici multiplicativement), i.e. pour tous x et y dans G, $\phi(xy) = \phi(x)\phi(y)$. Cela entraîne que $\phi(1) = 1$ et $\phi(x^{-1}) = (\phi(x))^{-1}$. S'il n'y a pas d'ambiguïté possible, on dira simplement morphisme au lieu de morphisme de groupes.*
- *Si G est un groupe fini, le cardinal de G, noté $|G|$, s'appelle* l'ordre *de G.*
- *Si pour tous $a, b \in G$ on a $ab = ba$, on dit que le groupe est commutatif ou* abélien.
- *Un* sous-groupe *d'un groupe G est un sous-ensemble qui contient l'unité et qui est stable pour la loi de groupe et pour l'opération de passage à l'inverse, autrement dit, un sous-ensemble $H \subset G$ d'un groupe G est un sous-groupe si et seulement si $1 \in H$ et $\forall x, y \in H,\ xy^{-1} \in H$.*
- *Soient $x_i,\ (i \in I)$ des éléments d'un groupe G noté multiplicativement. Le sous-groupe engendré par les éléments x_i est l'ensemble des produits finis $x_{i_1}^{\lambda_{i_1}} \dots\ x_{i_k}^{\lambda_{i_k}}$, les λ_{i_j} parcourant $\mathbf{Z}$. Ce sous-groupe est noté $< (x_i)_{i \in I} >$.*

Si $\phi : G \to H$ est un morphisme, il est immédiat de voir que l'image de ϕ (notée $\operatorname{Im} \phi$) est un sous-groupe de H, et que le noyau $\phi^{-1}(e)$ de ϕ (noté $\ker \phi$) est un sous-groupe de G.

Définition 1.3. *Soit G un groupe, $g \in G$. L'ordre de g, noté $\operatorname{ord}(g)$, est le cardinal $| < g > |$ du groupe $< g >$ si $| < g > |$ est fini, sinon $\operatorname{ord}(g) = +\infty$ (cf. le lemme 1.34 plus bas).*

Définition 1.4.

- *Un* anneau *(commutatif et unitaire) A est un groupe commutatif $(A, +)$ muni d'une deuxième loi de composition interne (notée multiplicativement et appelée multiplication) vérifiant les conditions suivantes :*

1. *la multiplication est associative, commutative, et possède un élément neutre noté 1 ;*
2. *la multiplication est distributive par rapport à l'addition, i.e. pour tous $a, b, c \in A$ on a :*
$$a(b+c) = ab + bc.$$

- *Si A et B sont deux anneaux (commutatifs et unitaires), une application*
$$\phi : A \longrightarrow B$$
est un morphisme d'anneaux *si elle est compatible avec les opérations des deux anneaux, i.e. si :*
  1. *ϕ est un morphisme des groupes additifs $(A, +)$ et $(B, +)$;*
  2. *$\phi(1) = 1$ et pour tous $a, b \in A$, $\phi(ab) = \phi(a)\phi(b)$.*

Dans tout le livre, « anneau » signifiera « anneau commutatif unitaire » (un anneau non commutatif est tel que sa multiplication ne soit pas commutative ; l'addition est toujours commutative).

Définition 1.5. *Un corps (commutatif) K est un anneau tel que tout élément non nul soit inversible pour la multiplication.*

> ***Remarque 1.6.*** Soient A et B deux groupes (resp. deux anneaux). Il existe un structure naturelle de groupe (resp. d'anneau) sur le produit cartésien $A \times B$ en définissant les opérations coordonnée par coordonnée. En revanche, si A et B sont des corps commutatifs, l'anneau produit $A \times B$ n'est pas un corps (par exemple les éléments $(1, 0)$ et $(0, 1)$ ne sont pas inversibles pour la multiplication).

Définition 1.7. *Un idéal I d'un anneau A est un sous-groupe de $(A, +)$ tel que I soit stable par la multiplication par les éléments de A, i.e. $x \in I$ et $\lambda \in A \Longrightarrow \lambda x \in I$.*

Il est immédiat de voir que le noyau d'un morphisme d'anneaux $\phi : A \to B$ est un idéal de A. Réciproquement, nous verrons au chapitre suivant (définition 2.3 et remarque 2.9) que tout idéal est le noyau d'un morphisme d'anneaux.

Définition 1.8. *Soient x_i $(i \in I)$ des éléments d'un anneau A (resp. d'un groupe abélien $(G, +)$). L'ensemble des combinaisons linéaires $\Sigma_{j=1}^{n_j} \lambda_{i_j} x_{i_j}$, $i_j \in I$, $\lambda_{i_j} \in A$ (resp. $\lambda_{i_j} \in \mathbf{Z}$) est un idéal de A (resp. un sous-groupe de G). On dit que c'est l'idéal (ou le sous-groupe) engendré par les x_i ; c'est aussi le plus petit idéal de A (resp. sous-groupe de G) contenant les x_i.*

Si $x_i \in A$ $(i \in I)$, on note $\big((x_i)_{i\in I}\big)$ l'idéal engendré par les éléments x_i. Cet idéal est aussi l'intersection de tous les idéaux de A contenant tous les x_i. Si $\phi : A \to B$ est un morphisme d'anneaux et $I \subset B$ un idéal, $\phi^{-1}(I)$ est un idéal de A.
Le cas des groupes non commutatifs sera traité au chapitre 4.

Exemple 1.9. Un sous-ensemble $I \subset \mathbf{Z}$ est un idéal de $\mathbf{Z}$ si et seulement si c'est un sous-groupe de $(\mathbf{Z}, +)$.

1.1.3. Divisibilité dans un anneau

Rappelons que dans tout le livre les anneaux considérés sont commutatifs et unitaires.

Définition 1.10. *Soit A un anneau.*

- *On dit que A est* intègre *s'il n'a pas de diviseur de 0, i.e. si pour a et b dans A, la relation $ab = 0$ implique $a = 0$ ou $b = 0$.*
- *L'ensemble des éléments inversibles de A (pour la multiplication) se note A^*. L'ensemble $(A^*, \times)$ est un groupe abélien.*
- *Soient $a \in A$ et $b \in A$. On dit que a divise b (notation $a \mid b$) s'il existe $c \in A$ tel que $b = ac$. Si A est intègre et $b \neq 0$, c est unique s'il existe.*
- *Deux éléments a et b de A sont dits* associés *si $a = \lambda b$ avec $\lambda \in A^*$.*
- *Un élément $a \in A$ est* irréductible *s'il n'est pas inversible et si la relation $a = bc$ implique b ou c inversible (« a n'a pas de diviseur strict »).*
- *Soient $a \in A$ et $b \in A$. On dit que $d \in A$ est un PGCD de a et b si :*
  1. *$d \mid a$ et $d \mid b$ (« d divise a et b ») ;*
  2. *tout $x \in A$ qui divise a et b divise d.*

  Autrement dit, si l'on note $\mathcal{D}(x)$ l'ensemble des diviseurs d'un élément $x \in A$, on a $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(d)$.
- *On dit que $p \in A$ est un PPCM de a et b si :*
  1. *$a \mid p$ et $b \mid p$;*
  2. *pour tout élément $x \in A$ tel que $a \mid x$ et $b \mid x$, alors $p \mid x$.*

> ***Remarque 1.11.*** Si A est intègre, il est immédiat de voir que si le PGCD (resp. le PPCM) de deux éléments existe, il est unique à multiplication par un élément de A^* près.

Définition 1.12. *Un anneau A est dit* euclidien *si :*

- *A est intègre ;*
- *il existe une fonction $\phi : A \setminus \{0\} \longrightarrow \mathbf{N}$ (appelée «* sthasme euclidien *») telle que :*

$$\forall a, b \in A \setminus \{0\},\ \textit{il existe } q \textit{ et } r \textit{ tels que } a = bq + r, \quad \phi(r) < \phi(b) \textit{ ou } r = 0.$$

L'opération ci-dessus s'appelle la division euclidienne de a par b ; q est le quotient *et r le* reste *(avec ici un léger abus de langage, puisque dans la définition 1.12 on n'exige pas l'unicité du quotient et du reste).*

Définition 1.13. *Un anneau A est dit* principal *s'il est intègre et si tout idéal est engendré par un élément (un tel idéal est dit* principal*).*

Définition 1.14.

- *On dit qu'un ensemble $\mathcal{P}$ d'éléments irréductibles de A est un* « système représentatif d'éléments irréductibles » *si pour tout $\tilde{p} \in A$ irréductible il existe un unique $p \in \mathcal{P}$ tel que $\tilde{p} = \lambda p$ avec $\lambda \in A^*$.*
- *On dit qu'un anneau A est* factoriel *s'il vérifie les trois conditions suivantes :*
  1. *A est intègre ;*
  2. *(existence de la factorisation) : tout $a \in A$, $a \neq 0$, s'écrit $a = \lambda p_1 \dots p_s$ avec p_i irréductibles et $\lambda \in A^*$;*
  3. *(unicité de la factorisation) : soit $\mathcal{P}$ un système représentatif d'éléments irréductibles. Si on prend les p_i dans $\mathcal{P}$, l'écriture ci-dessus est unique (à permutation près).*

Signalons que tout anneau principal est factoriel (théorème 1.30 dans le cas de **Z** ; la démonstration est la même pour tout anneau principal).

Exemple 1.15. Nous verrons plus loin que **Z** et $K[X]$ sont principaux (et donc factoriels). Dans le cas de **Z**, on prend en général pour $\mathcal{P}$ l'ensemble des nombres premiers > 0, et dans le cas de $K[X]$ l'ensemble des polynômes irréductibles unitaires.

Définition 1.16. *Soit A un anneau intègre. On considère sur le produit $A \times A \setminus \{0\}$ la relation d'équivalence suivante :*

$$(a, b) \sim (a', b') \Longleftrightarrow ab' = ba'.$$

Le quotient de $A \times A \setminus \{0\}$ par cette relation d'équivalence s'appelle le corps de fractions *de A et se note $K(A)$. La classe d'équivalence d'un couple (a, b) se note $\frac{a}{b}$. On définit sur $K(A)$ une structure de corps commutatif en posant :*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad et \quad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

1.1.4. Structure quotient

Les propriétés des quotients seront revues et développées au chapitre suivant dans le cadre des modules sur un anneau, et au chapitre 4 pour les groupes non nécessairement commutatifs.

Définition 1.17. *Soit $(G, +)$ un groupe commutatif, $H \subset G$ un sous-groupe. On note G/H l'ensemble des classes pour la relation d'équivalence $x \sim y \Longleftrightarrow x - y \in H$. La classe de x se note $\overline{x}$. On a donc :*

$$\overline{x} = x + H = \{x + h | h \in H\}.$$

Même définition pour A/I dans le cas où A est un anneau et I un idéal.

L'ensemble G/H est alors muni canoniquement d'une structure de groupe abélien « propagée » par celle de G, *i.e.* telle que l'application :

$$\pi : G \longrightarrow G/H$$

qui à x fait correspondre sa classe $\overline{x}$ (on dit aussi classe modulo H) soit un morphisme (surjectif) de groupes.

De même, si $I \subset A$ est un sous-groupe (additif) d'un anneau A, le groupe A/I est muni d'une structure d'anneau commutatif propagée par celle de A si et seulement si I est un idéal.

Voici une application de ce qui précède connue sous le nom de « théorème de Lagrange ». Ce théorème est vrai aussi dans le cas non commutatif (chapitre 4).

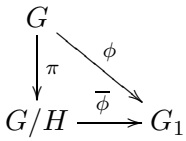
Proposition 1.18. *Soit $(G,+)$ un groupe abélien fini d'ordre n, $H \subset G$ un sous-groupe. Soit h l'ordre de H. Alors l'ordre de G/H est n/h. En particulier h divise n : l'ordre d'un sous-groupe d'un groupe fini G divise l'ordre de G.*

Démonstration. Soit $a \in G$. L'application τ_a (« translation par a ») de G dans G définie par $\tau_a(g) = a + g$ est une bijection, la bijection inverse étant τ_{-a}. Cette application envoie le sous-groupe H sur l'ensemble $a + H$, classe de a modulo H, qui est donc de cardinal h. Les classes modulo H formant une partition de G, on en déduit immédiatement la proposition. ■

Le quotient G/H est caractérisé par la propriété suivante, appelée « propriété universelle du quotient » :

Proposition 1.19. *Soit ϕ un morphisme de G dans un groupe (abélien) G_1. Alors ϕ se factorise en un morphisme $\overline{\phi} : G/H \to G_1$ (tel que $\phi = \overline{\phi} \circ \pi$) si et seulement si $H \subset \ker \phi$. Si $\overline{\phi}$ existe, il est unique.*

Démonstration. Supposons $H \subset \ker \phi$. On a alors $\phi(x + h) = \phi(x)$ pour tout $x \in G$ et tout $h \in H$, puisque $\phi(h) = 0$. Le morphisme ϕ est donc constant sur les classes d'équivalence $x + H$ modulo H. On peut ainsi définir $\overline{\phi} : G/H \longrightarrow G_1$ par $\overline{\phi}(\overline{x}) = \phi(x)$, x étant un élément quelconque de la classe $\overline{x}$, (car $\phi(x)$ ne dépend que de la classe $\overline{x}$ de x modulo H). Il est immédiat de voir que $\overline{\phi}$ est bien un morphisme de groupes, et on a par construction $\phi = \overline{\phi} \circ \pi$.
Autrement dit, le diagramme suivant est commutatif :



Réciproquement, si $\overline{\phi}$ existe avec $\phi = \overline{\phi} \circ \pi$, on a pour $h \in H$: $\phi(h) = \overline{\phi}(\pi(h)) = \overline{\phi}(\overline{0}) = 0$, et donc $H \subset \ker\phi$. Enfin la relation $\phi = \overline{\phi} \circ \pi$ implique $\overline{\phi}(\overline{x}) = \phi(x)$ pour tout $x \in G$, ce qui montre l'unicité de $\overline{\phi}$. ■

Corollaire 1.20. *Sous les hypothèses de la proposition 1.19 les conditions suivantes sont équivalentes :*

1. $H = \ker \phi$;
2. $\overline{\phi}$ est injectif.

De plus ϕ est surjectif si et seulement si $\overline{\phi}$ l'est.

La démonstration, immédiate, est laissée au lecteur.

> ***Remarque 1.21.*** La proposition 1.19 est encore vraie dans le cas du quotient d'un anneau A par un idéal I : Soit ϕ un morphisme de A dans un anneau B. Alors ϕ se factorise en un morphisme $\overline{\phi} : A/I \to B$ (tel que $\phi = \overline{\phi} \circ \pi$) si et seulement si $I \subset \ker \phi$. Si $\overline{\phi}$ existe, il est unique. De plus, $\overline{\phi}$ est injectif si et seulement si $\ker \phi = I$.

1.2 L'ANNEAU Z. DIVISION EUCLIDIENNE

Rappelons comment on définit une structure d'anneau sur le groupe $(\mathbf{Z}, +)$.

La structure de groupe de $\mathbf{Z}$ permet de définir canoniquement la multiplication : si a et n sont des nombres positifs, on pose :

$$na = an = \underbrace{a + \cdots + a}_{n \text{ fois}} = \underbrace{n + \cdots + n}_{a \text{ fois}},$$

et on étend aux éléments de $\mathbf{Z}$ en utilisant la règle des signes. Un sous-groupe de $\mathbf{Z}$ est ainsi toujours stable pour la multiplication par tout entier : c'est donc un idéal de l'anneau $\mathbf{Z}$ comme indiqué en remarque 1.6.

Théorème 1.22. *L'anneau* $\mathbf{Z}$ *est un anneau euclidien* (définition 1.12).

Démonstration. Il est clair que $\mathbf{Z}$ est intègre. On prend pour sthasme ϕ la valeur absolue : $\phi(b) = |b|$. Soient a et b donnés avec $b \neq 0$. On cherche (q, r) tels que $a = bq + r$; $\quad 0 < |r| < |b|$ ou $r = 0$. On va en fait pouvoir imposer que $r \geqslant 0$, ce qui entraînera l'unicité. L'algorithme suivant donne la réponse :

- initialisation : $(0, a)$;
- si $0 \leqslant r < |b|$, fin ;
- si $r \geqslant |b|$, $(q, r) := (q + 1, r - |b|)$,
- si $r < 0$, $(q, r) := (q - 1, r + |b|)$.

Comme l'on suppose $r \geqslant 0$, q et r sont uniques (démonstration immédiate). ■

Proposition 1.23. *Un anneau euclidien est principal (et donc en particulier* $\mathbf{Z}$ *est un anneau principal).*

Démonstration. Soient A un anneau euclidien, $I \subset A$ un idéal non réduit à $\{0\}$. Soit ϕ le sthasme de A. Celui-ci étant à valeurs dans $\mathbf{N}$, il atteint son minimum sur I. Il existe donc un élément $x \in I \setminus \{0\}$ tel que $\phi(x)$ soit minimal parmi tous les éléments (non nuls) de I. Montrons que $I = (x)$, *i.e.* que I est engendré par x. Soit $y \in I,\ y \neq 0$; On peut diviser y par x dans A : $y = qx + r$ avec $\phi(r) < \phi(x)$ ou $r = 0$. Mais I étant un idéal, $r \in I$, ce qui implique $r = 0$ à cause de l'hypothèse sur $\phi(x)$. On a donc $y = qx$. ■

Remarque 1.24. Dans le cas de $\mathbf{Z}$, les notions de sous-groupe et d'idéal se confondent comme il a été vu plus haut, et donc tout sous-groupe est de la forme $< n >$ (on notera plutôt $n\mathbf{Z}$), engendré par un élément $n \in \mathbf{Z}$. Inversement l'ensemble $n\mathbf{Z}$ des multiples de n est un sous-groupe et un idéal.

1.3 ALGORITHME D'EUCLIDE

Proposition 1.25. *Deux éléments a et b de $\mathbf{Z}$ (et plus généralement d'un anneau principal A) ont un PGCD et un PPCM (définition 1.10). Si d est un PGCD de a et b, il existe deux éléments u et v de A tels que*

$$d = au + bv \tag{1}$$

(relation de Bézout).

Démonstration. Tout générateur d de l'idéal (a, b) est un PGCD de a et b. ■

Remarques 1.26.

1. Rappelons (Remarque 1.11) que deux PGCD de a et b sont associés. Dans le cas de $\mathbf{Z}$, les inversibles sont $+1$ et -1 ; le PGCD dans $\mathbf{Z}$ est donc défini au signe près.
2. On dit que a et b sont *premiers entre eux* si $(a, b) = (1)$.
3. Dans le cas de $\mathbf{Z}$, si a et b sont deux entiers, on note $a \wedge b$ le PGCD *positif* de a et b, *i.e.* le générateur positif de l'idéal (a, b).
4. Dans la relation (1) il n'y a pas unicité des nombres u et v. Remarquons que si l'on pose $a_1 = a/d$ et $b_1 = b/d$, la relation (1) devient $1 = a_1u + b_1v$. Le lecteur vérifiera à titre d'exercice (en utilisant le lemme de Gauss ci-dessous) que :
   a) si on part de la relation (1) $d = au + bv$, toute les autres relations sont de la forme $d = au' + bv'$ avec
   $$\begin{cases} u' &= u + kb_1 \\ v' &= v - ka_1 \end{cases}$$
   pour k parcourant $\mathbf{Z}$.
   b) Il y a unicité de u et v dans (1) si on impose par exemple que $0 \leqslant u < |b_1|$ (*cf.* l'exercice 1.7)

Lemme 1.27. *(dit « Lemme de Gauss »). Soient a, b et c des éléments de* $\mathbf{Z}$ *(ou plus généralement d'un anneau principal) tels que a divise bc et $a \wedge b = 1$ (i.e. a et b premiers entre eux). Alors a divise c.*

Démonstration. La relation de Bézout (1) s'écrit $1 = au + bv$, d'où $c = cau + bcv$. L'élément a divise le second membre par hypothèse, il divise donc c. ■

> ***Remarque 1.28.*** Si on supprime l'hypothèse $a \wedge b = 1$, le lemme est évidemment faux : le nombre 6 divise $12 = 3 \times 4$ mais ne divise ni 3 ni 4 !

Signalons le corollaire suivant dont la démonstration est immédiate par récurrence :

Corollaire 1.29. *Soient $a_1, \ldots, a_n, b$ des entiers tels que $a_i \wedge b = 1$ pour $1 \leqslant i \leqslant n$. Alors $(a_1 \ldots a_n) \wedge b = 1$.*

Passons maintenant au point de vue « effectif », *i.e.* algorithmique, pour calculer dans le cas de $\mathbf{Z}$ le PGCD de deux nombres a et b, que l'on suppose > 0 pour simplifier. On remarque d'abord que si $a = bq + r$, alors $(a, b) = (b, r)$, d'où l'algorithme (dit « algorithme d'Euclide ») pour calculer le PGCD > 0 $a \wedge b$, utilisant celui de la division euclidienne décrit plus haut :

- initialisation : $r_0 = a, r_1 = b$;
- si $r_i \neq 0$, alors $r_{i-1} = r_i q_i + r_{i+1}$;
- si $r_i = 0$, alors $a \wedge b = r_{i-1}$.

Le PGCD est donc le dernier reste non nul dans l'algorithme d'Euclide.
On peut aussi calculer les coefficients u et v de la relation de Bézout (1) par l'algorithme d'Euclide « étendu » qui calcule récursivement u_i et v_i tels que :

$$r_i = au_i + bv_i. \tag{2}$$

L'algorithme utilise deux triplets (u, v, r) et (u', v', r') :

- initialisation : $(u, v, r)(u', v', r') := (1, 0, a)(0, 1, b)$;
- tant que $r' \neq 0$, $(u, v, r)(u', v', r') := (u', v', r')(u - qu', v - qv', r - qr')$, q étant défini par la division euclidienne de r par r' : $r = qr' + (r - qr')$;
- si $r' = 0$, alors (u, v) est le couple cherché.

Justification : si à l'étape i on a les triplets $(u_{i-1}, v_{i-1}, r_{i-1})(u_i, v_i, r_i)$ tels que $r_{i-1} = au_{i-1} + bv_{i-1}$ et $r_i = au_i + bv_i$, alors on a
$r_{i+1} = r_{i-1} - q_i r_i = (u_{i-1} - q_i u_i)a + (v_{i-1} - q_i v_i)b = u_{i+1}a + v_{i+1}b$.

Le « théorème fondamental de l'arithmétique » (pour l'anneau $A = \mathbf{Z}$) dit que $\mathbf{Z}$ est factoriel (définition 1.14) :

Théorème 1.30. *Soit $\mathcal{P}$ l'ensemble des nombres premiers > 0 (le nombre 1 n'est pas un nombre premier par convention). Alors :*

1. *Tout $a \in \mathbf{Z}$, $a \neq 0$ s'écrit $a = \lambda p_1 \ldots p_r$ avec λ inversible dans $\mathbf{Z}$ ($\lambda = \pm 1$) et $p_i \in \mathcal{P}$ (non nécessairement distincts deux à deux) ;*
2. *cette écriture est unique à permutation près des p_i.*

On peut aussi écrire la condition *1.* sous la forme $a = \lambda \prod_{p_i \in \mathcal{P}} p_i^{v_{p_i}(a)}$ où les $v_{p_i}(a) \in \mathbf{N}$ sont nuls sauf au plus un nombre fini.

Démonstration. Si $n \in \mathbf{Z}$, l'existence d'une décomposition $n = \pm p_1 \dots p_r$ (où les p_i sont des nombres premiers > 1) est évidente. Pour l'unicité, on peut supposer $n > 0$. On raisonne alors par récurrence sur r.

Supposons que l'on ait deux décompositions d'un nombre entier $n > 0$:

$$n = p_1 \dots p_r = p'_1 \dots p'_s$$

les p_i et les p'_j n'étant pas nécessairement distincts deux à deux. Si $r = 1$, le corollaire 1.29 du lemme de Gauss 1.27 (et une récurrence immédiate sur l'entier s) implique qu'il existe $i,\ 1 \leqslant i \leqslant s$ tel que $p'_i = p_1$. On a alors $s = 1$, d'où l'unicité dans ce cas. Dans le cas général, si pour tout $i,\ 1 \leqslant i \leqslant s$ on a $p'_i \neq p_1$, le corollaire 1.29 implique que p_1 ne divise pas le produit $p'_1 \dots p'_s$, ce qui est absurde. Il existe donc i tel que $p_1 = p'_i$, on peut diviser les deux membres par p_1 et appliquer l'hypothèse de récurrence. ■

> ***Remarque 1.31.*** La démonstration ci-dessus (et donc le théorème 1.30) est valable pour tout anneau principal en prenant pour $\mathcal{P}$ un système représentatif d'éléments irréductibles.

1.4 L'ANNEAU $\mathbf{Z}/N\mathbf{Z}$

1.4.1. Groupes cycliques

Le groupe $\mathbf{Z}/n\mathbf{Z}$ est le quotient du groupe $\mathbf{Z}$ par le sous-groupe $n\mathbf{Z}$. Le morphisme canonique $\pi : \mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z}$ fait correspondre à un entier x sa classe $\overline{x}$ modulo n (on a par définition $\overline{x} = x + n\mathbf{Z}$). Si $n = 0$, on retrouve le groupe $\mathbf{Z}$. Si $n \neq 0$, on a $n\mathbf{Z} = (-n)\mathbf{Z}$. Le groupe $\mathbf{Z}/n\mathbf{Z}$ est fini d'ordre n. Ses n éléments sont $\overline{0}, \overline{1}, \dots, \overline{n-1}$.

Définition 1.32. *Soit G un groupe. On dit que G est* monogène *s'il est engendré par un élément g. On dit que G est* cyclique *s'il est monogène et de cardinal fini.*

Commençons par le cas d'un groupe $(G, +)$. Soit $g \in G$ un élément de G. Considérons le morphisme ϕ :

$$\mathbf{Z} \longrightarrow G, \quad m \mapsto mg \quad = \quad \underbrace{g + \dots + g}_{m \text{ fois}}.$$

Son image est le sous-groupe monogène $< g >$ de G engendré par g. Son noyau est un sous-groupe de $\mathbf{Z}$ donc de la forme $n\mathbf{Z}$ pour $n \in \mathbf{Z}$. Le morphisme ϕ se factorise alors par un morphisme injectif $\tilde{\phi} : \mathbf{Z}/n\mathbf{Z} \longrightarrow G$ (corollaire 1.20) d'image $< g >$ qui donne un isomorphisme de $\mathbf{Z}/n\mathbf{Z}$ sur $< g >$.

De même, pour un groupe $(G, \times)$ (noté multiplicativement, et donc non nécessairement commutatif) et $g \in G$, on pose

$$\psi : \mathbf{Z} \longrightarrow G, \quad m \mapsto g^m,$$

dont l'image est le sous-groupe de G engendré par g, aussi noté $< g >$, encore isomorphe à un groupe $(\mathbf{Z}, +)$ ou $(\mathbf{Z}/n\mathbf{Z}, +)$ (suivant que ψ est injectif ou non). On a donc :

Proposition 1.33. *Tout groupe monogène est isomorphe soit à* $(\mathbf{Z}, +)$ *soit à* $(\mathbf{Z}/n\mathbf{Z}, +)$ *pour un entier* $n > 0$*. En particulier tout groupe cyclique est isomorphe à un groupe* $(\mathbf{Z}/n\mathbf{Z}, +)$ *avec* $n > 0$*.*

On remarque donc que le sous-groupe $< g >$ est commutatif, même si le groupe G ne l'est pas. Rappelons (définition 1.3) que l'ordre d'un élément $g \in G$ est l'ordre du sous-groupe $< g >$ engendré par g.

Lemme 1.34. *Soit* $g \in G$ *un élément d'ordre fini* r*. Alors si la loi de groupe est notée additivement, on a :*

$$r = \inf\{n \in \mathbf{N} \setminus \{0\}, ng = 0\},$$

et si la loi de groupe est notée multiplicativement,

$$r = \inf\{n \in \mathbf{N} \setminus \{0\}, g^n = 1\}.$$

Démonstration. Considérons par exemple le cas additif. Le sous-groupe $< g >$ est d'ordre r par hypothèse, donc isomorphe à $\mathbf{Z}/r\mathbf{Z}$ par la proposition 1.33. Le morphisme $\phi : \mathbf{Z} \to < g >$, $1 \mapsto g$ est par hypothèse surjectif. Il se factorise par un morphisme $\overline{\phi} : \mathbf{Z}/r\mathbf{Z} \to < g >$ qui est injectif (proposition 1.19), donc bijectif. Il suffit donc de voir que :

$$r = \inf\{n \in \mathbf{N}^*, n\overline{1} = 0\}$$

dans $\mathbf{Z}/r\mathbf{Z}$, ce qui est évident. ■

Étudions maintenant les sous-groupes et les groupes quotients d'un groupe cyclique. Considérons d'abord le cas des sous-groupes.

Tout sous-groupe de $\mathbf{Z}$ non réduit à $\{0\}$ est isomorphe à $\mathbf{Z}$ (*cf.* la remarque 1.24 : un sous-groupe de $\mathbf{Z}$ est de la forme $n\mathbf{Z}$, et la multiplication par n donne un isomorphisme de groupes de $\mathbf{Z}$ sur $n\mathbf{Z}$ si $n \neq 0$). Pour les groupes cycliques, on a la proposition suivante :

Proposition 1.35. *Tout sous-groupe d'un groupe cyclique est cyclique. Plus précisément, soit* n *un entier* > 1*.*

1. *Tout sous-groupe de* $\mathbf{Z}/n\mathbf{Z}$ *est cyclique engendré par la classe* $\overline{b}$ *d'un diviseur* b *de* n*. Ce sous-groupe est d'ordre* $a = n/b$*.*
2. *Soit* $a > 0$ *un diviseur de* n*,* $b = n/a$*. Il existe alors un et un seul sous-groupe de* $\mathbf{Z}/n\mathbf{Z}$ *d'ordre* a*. Ce sous-groupe est engendré par la classe de* b *modulo* n *; il est formé de l'ensemble des éléments de* $\mathbf{Z}/n\mathbf{Z}$ *dont l'ordre divise* a*.*

Démonstration. *1.* Soient $\pi : \mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z}$ le morphisme canonique, et $H \subset \mathbf{Z}/n\mathbf{Z}$ un sous-groupe. L'ensemble $\pi^{-1}(H) \subset \mathbf{Z}$ est un sous-groupe contenant $\ker \pi = n\mathbf{Z}$; il est donc de la forme $b\mathbf{Z}$ avec $b|n$ (remarque 1.24) ; H est donc engendré par $\overline{b} = \pi(b)$. Soit k l'ordre de l'élément $\overline{b}$. On a $a\overline{b} = \overline{ab} = \overline{n} = 0$ ce qui montre que $k \leqslant a$; d'autre part, si a_1 est un nombre tel que $0 < a_1 < a$, on a $a_1 b < n$ et donc $\overline{a_1 b} \neq 0$, d'où $k \geqslant a$.

2. L'élément $\overline{b}$ est d'ordre a (*cf.* la démonstration de *1.*). Il engendre donc un sous-groupe H d'ordre a. Donc si $\overline{g} \in H$, son ordre divise a (proposition 1.18). Réciproquement si un élément $\overline{g} \in \mathbf{Z}/n\mathbf{Z}$ a un ordre qui divise a, on a $a\overline{g} = 0$, soit $ag \in n\mathbf{Z}$, d'où $g \in b\mathbf{Z}$ et $\overline{g} \in H$, ce qui montre l'unicité de H. ■

Considérons maintenant la cas des groupes quotients.

Proposition 1.36. *Tout quotient d'un groupe cyclique est cyclique. Plus précisément, soit $G \simeq \mathbf{Z}/n\mathbf{Z}$. Tout groupe quotient de G est cyclique, isomorphe à $\mathbf{Z}/b\mathbf{Z}$ avec $b|n$. Réciproquement, si $b|n$, il existe un et un seul groupe quotient de G de cardinal b, isomorphe à $\mathbf{Z}/b\mathbf{Z}$.*

Démonstration. Soit H un groupe quotient de $\mathbf{Z}/n\mathbf{Z}$. Considérons le diagramme ci-dessous :

$$\mathbf{Z} \xrightarrow{\pi_1} \mathbf{Z}/n\mathbf{Z} \xrightarrow{\pi_2} H$$

où π_1 et π_2 sont les morphismes canoniques. Posons $\phi = \pi_2 \circ \pi_1 : \mathbf{Z} \to H$. Le morphisme ϕ est surjectif ; son noyau est donc de la forme $b\mathbf{Z}$, avec $\ker \pi_1 = n\mathbf{Z} \subset b\mathbf{Z}$, soit $b|n$. On a donc bien $H \simeq \mathbf{Z}/b\mathbf{Z}$.

Réciproquement soit b un entier tel que $b|n$, $\overline{b} \in \mathbf{Z}/n\mathbf{Z}$ sa classe modulo n. Il y a un et un seul quotient de $\mathbf{Z}/n\mathbf{Z}$ de cardinal b : c'est le quotient de $\mathbf{Z}/n\mathbf{Z}$ par l'unique sous-groupe $<\overline{b}>$ d'ordre $a = n/b$. Soit H ce sous-groupe. On considère comme ci-dessus le diagramme :

$$\mathbf{Z} \xrightarrow{\pi_1} \mathbf{Z}/n\mathbf{Z} \xrightarrow{\pi_2} H$$

avec $H = (\mathbf{Z}/n\mathbf{Z})/<\overline{b}>$. Il est immédiat de voir que le morphisme $\phi = \pi_2 \circ \pi_1$ est surjectif de noyau $b\mathbf{Z}$, ce qui montre que $H \simeq \mathbf{Z}/b\mathbf{Z}$. ■

Remarques 1.37.

1. On a ainsi une bijection entre les diviseurs > 0 de n et les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$.
2. Soit x un entier $\geqslant 0$, $\overline{x}$ sa classe modulo n. Il résulte de la relation de Bézout (1) que dans l'anneau $\mathbf{Z}/n\mathbf{Z}$ on a la relation :

$$<\overline{x}> = <\overline{x \wedge n}> .$$

3. Rappelons que si $(G,+)$ est un groupe commutatif, on définit pour $g \in G$ et $m \in \mathbf{N}$ l'élément mg comme :

$$mg \quad = \quad \underbrace{g+\cdots+g}_{m \text{ fois}}$$

et on prolonge à $\mathbf{Z}$ en posant $(-m)g = -(mg)$ pour $m \geqslant 0$.
Si a et b sont dans $\mathbf{Z}$, on alors dans le groupe $\mathbf{Z}/n\mathbf{Z}$:

$$\overline{ab} = a\overline{b} = b\overline{a}$$

comme on le voit immédiatement.

1.4.2. Inversibles de $\mathbf{Z}/n\mathbf{Z}$, applications arithmétiques

Le sous-groupe $n\mathbf{Z}$ de $\mathbf{Z}$ étant aussi un idéal, le groupe $(\mathbf{Z}/n\mathbf{Z},+)$ est muni canoniquement d'une structure d'anneau propagée par celle de $\mathbf{Z}$: si on note $\overline{a}$ la classe d'un entier a modulo n, on pose pour a et b dans $\mathbf{Z}$, $\overline{a}.\overline{b} = \overline{ab}$. Cette opération est bien définie et fait de $\mathbf{Z}/n\mathbf{Z}$ un anneau commutatif avec unité $\overline{1}$. La notation $((\mathbf{Z}/n\mathbf{Z})^*,\times)$ (ou simplement $(\mathbf{Z}/n\mathbf{Z})^*$) désigne le groupe (multiplicatif) des éléments inversibles pour la multiplication de l'anneau $\mathbf{Z}/n\mathbf{Z}$. Cet ensemble n'est pas stable pour l'addition (en particulier il ne contient pas 0), mais constitue un groupe (abélien) pour la multiplication.

Proposition 1.38. *Soient $n > 1$ et a deux entiers, $\overline{a}$ la classe de a modulo n. Les conditions suivantes sont équivalentes :*
1. $a \wedge n = 1$;
2. $\overline{a} \in (\mathbf{Z}/n\mathbf{Z})^*$;
3. $\overline{a}$ engendre le groupe $(\mathbf{Z}/n\mathbf{Z},+)$.

Démonstration. Pour tout élément $x \in \mathbf{Z}$, on note ici $\overline{x}$ sa classe modulo n.

1. $\Rightarrow$ 2. Si $a \wedge n = 1$, il existe deux nombres u et v tels que $au + nv = 1$ (1). On a donc $au \equiv 1 \bmod n$, soit $\overline{au} = \overline{1}$, d'où *2.*

2. $\Rightarrow$ 3. Il existe par hypothèse un élément $\overline{u}$ tel que $\overline{a} \cdot \overline{u} = \overline{1}$. Pour $1 \leqslant k \leqslant n-1$, les classes $k\overline{a}$ sont alors toutes distinctes (car $k\overline{a} = k'\overline{a}$ pour $1 \leqslant k' < k < n$ implique $(k-k')\overline{a} = \overline{0}$, ce qui est absurde car en multipliant par $\overline{u}$, on trouve $(k-k')\overline{1} = \overline{k-k'} = \overline{0}$). Cela implique que tout élément de $\mathbf{Z}/n\mathbf{Z}$ est de la forme $k\overline{a}$.

3. $\Rightarrow$ 1. Si $\overline{a}$ engendre $\mathbf{Z}/n\mathbf{Z}$, l'élément $\overline{1}$ est dans le groupe engendré par $\overline{a}$. Il existe donc $u \in \mathbf{Z}$ tel que $\overline{1} = \overline{ua}$, soit $1 = ua + vn$ pour $v \in \mathbf{Z}$, et donc $a \wedge n = 1$. ■

Corollaire 1.39. *L'anneau $\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si l'entier n est un nombre premier p. Le corps $\mathbf{Z}/p\mathbf{Z}$ se note alors $\mathbf{F_p}$.*

Démonstration. Rappelons d'abord que par définition, l'entier 1 n'est pas un nombre premier. Si $p > 0$ est premier, on a $a \wedge p = 1$ pour tout a, $0 < a < p$, et donc tout élément $\overline{a} \neq 0$ de $\mathbf{Z}/p\mathbf{Z}$ est inversible, ce qui veut dire que $\mathbf{Z}/p\mathbf{Z}$ est un corps.

Réciproquement, si $q = 1$, l'anneau $\mathbf{Z}/q\mathbf{Z}$ n'ayant qu'un élément ne peut être un corps (par définition tout corps K possède un élément neutre 0 pour l'addition et $(K \setminus \{0\}, \times)$ étant un groupe possède au moins un élément neutre $1 \neq 0$).

Si $q > 1$ n'est pas premier, on a $q = ab$ avec $1 < a < q$, $1 < b < q$, d'où $\overline{a}\overline{b} = 0$ dans $\mathbf{Z}/q\mathbf{Z}$, avec $\overline{a} \neq 0$ et $\overline{b} \neq 0$ (on note toujours 0 l'élément neutre pour l'addition), et donc $\mathbf{Z}/q\mathbf{Z}$ n'est pas un corps. ■

Définition 1.40. *Pour $n \geqslant 2$, on note $\varphi(n)$ le nombre de générateurs distincts du groupe $\mathbf{Z}/n\mathbf{Z}$. C'est aussi d'après la proposition 1.38 le nombre d'entiers a tels que $1 \leqslant a < n$ et $a \wedge n = 1$ ou encore l'ordre du groupe $((\mathbf{Z}/n\mathbf{Z})^*, \times)$. On pose par convention $\varphi(1) = 1$. La fonction φ s'appelle la* fonction d'Euler *(on dit aussi* indicatrice d'Euler*).*

Exemple 1.41. Si p est un nombre premier, $\varphi(p) = p - 1$ puisque $\mathbf{F_p}$ étant un corps, $|\mathbf{F_p}^*| = \varphi(p) = p - 1$.

Plus généralement, si $n = \prod_{i=1}^{k} p_i^{\nu_i}$, les p_i étant des nombres premiers et les ν_i des nombres entiers > 0, on a

$$\varphi(n) = \prod_{i}^{k} (p_i - 1) p_i^{\nu_i - 1}$$

(remarque 1.56 ci-après).

Proposition 1.42. *Soit G un groupe cyclique d'ordre n. Alors pour tout $d > 0$ tel que $d|n$, il y a dans G exactement $\varphi(d)$ éléments d'ordre d.*

Démonstration. On peut supposer que $G = \mathbf{Z}/n\mathbf{Z}$ (proposition 1.33). Soit $d \geqslant 1$ tel que $d|n$. Il existe d'après la proposition 1.35, *2.*un et un seul sous-groupe $H \subset \mathbf{Z}/n\mathbf{Z}$ d'ordre d, et l'on a $H \simeq \mathbf{Z}/d\mathbf{Z}$. De plus, H contient tous les éléments de $\mathbf{Z}/n\mathbf{Z}$ d'ordre d (unicité de H). Par définition de φ, il y a donc $\varphi(d)$ éléments d'ordre d dans H donc dans G. On notera que l'unique élément d'ordre 1 est l'élément neutre 0, ce qui justifie la convention $\varphi(1) = 1$. ■

Corollaire 1.43. *Soit $n \in \mathbf{N} \setminus \{0\}$. La fonction φ vérifie la relation suivante :*

$$\sum_{d|n} \varphi(d) = n. \tag{3}$$

Démonstration. On considère les n éléments de $\mathbf{Z}/n\mathbf{Z}$. Chaque élément non nul a un ordre d qui divise n, et pour chaque $d|n$, il y a $\varphi(d)$ éléments d'ordre d. ■

Exemple 1.44. Si p est un nombre premier, on a $\varphi(p) = p - 1$ (exemple 1.41) et $\sum_{d|p} \varphi(d) = \varphi(1) + \varphi(p) = 1 + p - 1 = p$.

Voici maintenant quelques résultats arithmétiques classiques, conséquences immédiates de ce qui précède. Rappelons que par le théorème de Lagrange (théorème 1.18), dans le groupe $((\mathbf{Z}/n\mathbf{Z})^*, \times)$ l'ordre (multiplicatif) de tout élément divise $\varphi(n)$.

Notons tout d'abord que nous démontrerons au chapitre 6 (Proposition 6.1) que pour p premier le groupe multiplicatif $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique, donc isomorphe à $(\mathbf{Z}/(p-1)\mathbf{Z}, +)$.

Pour la structure de $(\mathbf{Z}/n\mathbf{Z})^*$ avec n quelconque, *cf.* le problème 2.2.

Proposition 1.45. *(« théorème d'Euler ») Soient a et n deux éléments non nuls de* $\mathbf{N}$ *tels que $a \wedge n = 1$. Alors :*

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Démonstration. Soit $\overline{a}$ la classe de a modulo n ; on a $\overline{a} \in (\mathbf{Z}/n\mathbf{Z})^*$ par la proposition 1.38 et donc l'ordre de $\overline{a}$ divise $\varphi(n)$, d'où $\overline{a}^{\varphi(n)} = \overline{1}$, ce qui est équivalent à $a^{\varphi(n)} \equiv 1 \bmod n$. ■

Proposition 1.46. *(« petit théorème de Fermat »). Soient p un nombre premier et $a \in \mathbf{N} \setminus \{0\}$ non divisible par p. Alors :*

$$a^{p-1} \equiv 1 \bmod p.$$

Démonstration. C'est une conséquence immédiate de la proposition 1.45 puisque si p est un nombre premier, on a $\varphi(p) = p - 1$ (exemple 1.41). ■

Proposition 1.47. *(« théorème de Wilson ») Soit p un nombre premier. On a alors :*

$$(p-1)! \equiv -1 \bmod p.$$

Démonstration. Le cas $p = 2$ étant évident, on suppose $p > 2$. Considérons les $p-1$ éléments de $(\mathbf{Z}/p\mathbf{Z})^*$ (en notant avec l'abus de langage habituel encore 1 la classe de 1 modulo p) :

$$1, \overline{2}, \ldots, \overline{p-1}.$$

Leur produit vaut $\overline{(p-1)!}$; un de ces éléments x est égal à son inverse si et seulement si $x^2 = 1$. Or, comme $p \neq 2$, $1 \not\equiv -1 \bmod p$ et l'équation $X^2 = 1$ a exactement deux solutions dans le corps $\mathbf{Z}/p\mathbf{Z}$ qui sont 1 et $\overline{p-1} = \overline{p} - 1 = -1$; on a en effet la factorisation $X^2 - 1 = (X-1)(X+1)$, et si $x \in \mathbf{Z}/p\mathbf{Z}$, $x \neq \pm 1$, $(x-1)(x+1)$ est non nul puisque l'anneau $\mathbf{Z}/p\mathbf{Z}$ étant un corps, il est intègre. On peut donc dans le produit $1.\overline{2}\ldots\overline{(p-1)}$ grouper chaque élément $\overline{x_i}$ avec son inverse, sauf 1 et -1 qui sont chacun égaux à leur inverse ; on a ainsi :

$$1.\overline{2}.\ldots.(\overline{p}-1) = \overline{(p-1)!} = 1.(\overline{p}-1)\prod\left(\overline{x_i} \times \frac{1}{\overline{x_i}}\right) = \overline{p} - 1 = -1.$$

On a donc bien $(p-1)! \equiv -1 \bmod p$. ■

1.4.3. Théorème chinois

Théorème 1.48. « Lemme chinois »
Soit n un entier tel que $n = m_1 m_2$, avec $m_1 \wedge m_2 = 1$. Alors l'application ψ :

$$\mathbf{Z}/n\mathbf{Z} \longrightarrow \mathbf{Z}/m_1\mathbf{Z} \times \mathbf{Z}/m_2\mathbf{Z} \tag{4}$$

*qui à la classe $\overline{k}$ modulo n d'un entier $k \in \mathbf{Z}$ fait correspondre l'élément $(\overline{k}_1, \overline{k}_2)$ ($\overline{k}_i$ étant la classe de k modulo m_i) est un isomorphisme d'anneaux. (*cf. la remarque 1.6).

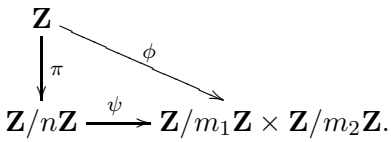
Démonstration. Soient ϕ le morphisme d'anneaux :

$$\mathbf{Z} \longrightarrow \mathbf{Z}/m_1\mathbf{Z} \times \mathbf{Z}/m_2\mathbf{Z} \qquad x \mapsto (\overline{x}_1, \overline{x}_2)$$

($\overline{x}_i$ est la classe x dans $\mathbf{Z}/m_i\mathbf{Z}$), π le morphisme canonique : $\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$. On a les inclusions suivantes d'idéaux puisque $n = m_1 m_2$: $n\mathbf{Z} \subset m_1\mathbf{Z}$ et $n\mathbf{Z} \subset m_2\mathbf{Z}$, d'où $n\mathbf{Z} \subset m_1\mathbf{Z} \cap m_2\mathbf{Z}$. Cela implique que le morphisme ϕ se factorise pour donner un morphisme d'anneaux ψ :

$$\mathbf{Z}/n\mathbf{Z} \longrightarrow \mathbf{Z}/m_1\mathbf{Z} \times \mathbf{Z}/m_2\mathbf{Z}.$$

tel que $\phi = \psi \circ \pi$ (car $n\mathbf{Z} \subset \ker\phi = m_1\mathbf{Z} \bigcap m_2\mathbf{Z}$; *cf.* la proposition 1.19). Autrement dit, le diagramme suivant est commutatif :



Montrons que ψ est bijectif.
Pour montrer que ψ est injectif, il faut montrer que $\ker\phi = n\mathbf{Z}$ (corollaire 1.20), soit $m_1\mathbf{Z} \bigcap m_2\mathbf{Z} = n\mathbf{Z}$. On a déjà vu que $n\mathbf{Z} \subset m_1\mathbf{Z} \bigcap m_2\mathbf{Z}$. Réciproquement, soit $x \in m_1\mathbf{Z} \bigcap m_2\mathbf{Z}$; on peut écrire $x = \lambda m_1 = \mu m_2$; si $x = 0$, on a $x \in n\mathbf{Z}$, et si $x \neq 0$, m_1 divise μ par le lemme de Gauss 1.27, d'où $x \in m_1 m_2\mathbf{Z} = n\mathbf{Z}$; le morphisme ψ est donc injectif. Il est aussi surjectif, puisque les deux ensembles $\mathbf{Z}/n\mathbf{Z}$ et $\mathbf{Z}/m_1\mathbf{Z} \times \mathbf{Z}/m_2\mathbf{Z}$ ont même cardinal n. ■

On a en fait le même résultat pour plusieurs entiers m_i premiers deux à deux :

Corollaire 1.49. *Soit n un entier tel que $n = m_1 \dots m_s$ avec $m_i > 1$, $m_i \wedge m_j = 1$ pour $i \neq j$. Alors l'application ψ :*

$$\mathbf{Z}/n\mathbf{Z} \longrightarrow \mathbf{Z}/m_1\mathbf{Z} \times \cdots \times \mathbf{Z}/m_s\mathbf{Z}$$

qui à la classe $\overline{k}$ modulo n d'un entier $k \in \mathbf{Z}$ fait correspondre l'élément $(\overline{k}_1, \dots, \overline{k}_s)$ ($\overline{k}_i$ étant la classe de k modulo m_i) est un isomorphisme d'anneaux.

Démonstration. Immédiate par récurrence sur s, en remarquant que si les m_i sont premiers entre eux deux à deux, $m_1 \dots m_{s-1}$ et m_s sont premiers entre eux par le corollaire 1.29, et en utilisant le théorème 1.48 pour ces deux entiers. ■

Par exemple, si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ est la décomposition de n en facteurs premiers, on a $\mathbf{Z}/n\mathbf{Z} \simeq \prod_{i=1}^{k} \mathbf{Z}/p_i^{\alpha_i}\mathbf{Z}$.

Corollaire 1.50. *Soit n un entier tel que $n = m_1 \dots m_s$ avec $m_i > 1$, $m_i \wedge m_j = 1$ pour $i \neq j$. Alors pour deux entiers a et b, on a $a \equiv b \bmod n$ si et seulement si $a \equiv b \bmod m_i$ $(1 \leqslant i \leqslant s)$.*

Démonstration. Si $a - b \equiv 0 \bmod n$, on a évidemment $a - b \equiv 0 \bmod m_i$ pour tout i. Réciproquement, si $a - b \equiv 0 \bmod m_i$ pour tout i, l'injectivité du morphisme ψ (corollaire 1.49) montre que $a - b \equiv 0 \bmod n$. ■

Remarques 1.51. 1) Pour avoir une version « constructive » du théorème chinois, il faut construire l'application g inverse de ψ. De plus la démonstration n'utilisera alors plus que $\mathbf{Z}/n\mathbf{Z}$ est de cardinal fini, et pourra s'appliquer à tout anneau principal, en particulier à l'anneau $K[X]$, comme nous le verrons au chapitre 3.

Considérons le cas général où $n = m_1 \dots m_s$ avec $m_i \wedge m_j = 1$ pour $i \neq j$. Soit ψ le morphisme d'anneaux du corollaire 1.49. La construction de l'inverse g du morphisme ψ se fait de la manière suivante :

- on détermine par l'algorithme d'Euclide étendu des nombres u_i et v_i tels que :
$$u_i m_i + v_i n/m_i = 1 \quad (cf.(2))$$
ce qui est possible car les entiers m_i et $n/m_i = m_1 \dots m_{i-1} m_{i+1} \dots m_s$ sont premiers entre eux (corollaire 1.29) ;
- on pose $e_i = 1 - u_i m_i = v_i n/m_i$;
- on a donc :
$$e_i \equiv 1 \pmod{m_i},$$
$$e_i \equiv 0 \pmod{m_j} \quad (\forall\, j \neq i);$$
- si $\overline{x}_i \in \mathbf{Z}/m_i\mathbf{Z}$ est la classe de $x_i \in \mathbf{Z}$, on pose $g(\overline{x}_1, \dots, \overline{x}_s) = \sum e_i x_i$ (mod n).

Le fait que g est l'inverse de ψ est alors immédiat.

2) Le cas où $n \wedge m \neq 1$ est traité dans l'exercice 1.24.

Exemple 1.52. Soit x un nombre entier tel que $x \equiv 3 \bmod 13$ et $x \equiv 7 \bmod 19$. Si on veut trouver sa classe modulo $247 = 13 \times 19$, on cherche la relation de Bézout par l'algorithme d'Euclide : $19 = 13 \times 1 + 6$, $13 = 2 \times 6 + 1$, d'où $1 = 13 - 2(19 - 73) = 3 \times 13 - 2 \times 19$. On a alors :

$$x \equiv 7.3.13 - 3.2.19 \bmod 247,$$

soit $x \equiv 159 \bmod 247$.

Corollaire 1.53. *Si $n = m_1 m_2$ avec $m_1 \wedge m_2 = 1$, on a alors, en appliquant* (4) *:*

$$(\mathbf{Z}/n\mathbf{Z})^* \simeq (\mathbf{Z}/m_1\mathbf{Z})^* \times (\mathbf{Z}/m_2\mathbf{Z})^* \tag{5}$$

Démonstration. L'isomorphisme ψ :

$$\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/m_1\mathbf{Z} \times \mathbf{Z}/m_2\mathbf{Z}$$

étant un isomorphisme d'anneaux, induit un isomorphisme

$$(\mathbf{Z}/n\mathbf{Z})^* \simeq (\mathbf{Z}/m_1\mathbf{Z} \times \mathbf{Z}/m_2\mathbf{Z})^*;$$

il suffit alors de montrer que

$$(\mathbf{Z}/m_1\mathbf{Z} \times \mathbf{Z}/m_2\mathbf{Z})^* = (\mathbf{Z}/m_1\mathbf{Z})^* \times (\mathbf{Z}/m_2\mathbf{Z})^*,$$

ce qui est évident, car un élément $(x, y) \in \mathbf{Z}/m_1\mathbf{Z} \times \mathbf{Z}/m_2\mathbf{Z}$ est inversible si et seulement si x et y le sont (on a alors $(x, y)^{-1} = (x^{-1}, y^{-1})$). ■

Remarque 1.54. Notons que le corollaire 1.49 donne par la même méthode un isomorphisme d'anneaux

$$(\mathbf{Z}/n\mathbf{Z})^* \simeq (\mathbf{Z}/m_1\mathbf{Z})^* \times \cdots \times (\mathbf{Z}/m_s\mathbf{Z})^*.$$

Le corollaire 1.53 va nous permettre de calculer la fonction $\varphi(n)$ pour tout entier $n > 1$.

Corollaire 1.55. *Soient m et n deux entiers > 0 tels que $m \wedge n = 1$. Alors $\varphi(mn) = \varphi(m)\varphi(n)$.*

Démonstration. Si $m > 1, n > 1$ il suffit d'appliquer le corollaire 1.53 en remarquant que pour tout entier $k > 0$ la fonction $\varphi(k)$ est le cardinal de $(\mathbf{Z}/k\mathbf{Z})^*$. Si $m = 1$ ou $n = 1$, la formule est vraie à cause de la convention $\varphi(1) = 1$. ■

On en déduit par récurrence que si n est un entier > 0, $n = p_1^{\nu_1} \dots p_k^{\nu_k}$ sa décomposition en facteurs premiers, on a

$$\varphi(n) = \prod_{1 \leqslant i \leqslant k} \varphi(p_i^{\nu_i}).$$

Remarque 1.56. Le lecteur vérifiera facilement à titre d'exercice que si p est un nombre premier,

$$\varphi(p^\nu) = (p-1)p^{\nu-1}$$

ce qui, avec le corollaire 1.53, permet de calculer $\varphi(n)$ pour tout entier $n > 0$.

EXERCICES

Les solutions des exercices et problèmes sont données en fin d'ouvrage.

ANNEAUX

Exercice 1.1. Soit E un espace compact et $A = \mathcal{C}(E)$ l'ensemble des fonctions réelles continues sur E, muni de la topologie de la convergence uniforme. Soit ϕ l'application qui à un ensemble $G \subset E$ associe l'ensemble $V(G) = \{f \in A,\ f_{|G} = 0\}$.

1. Déterminer A^*.
2. Montrer que $V(G)$ est un idéal fermé de A.
3. Montrer que les idéaux maximaux de A sont les $V(\{a\})$ avec $a \in E$ (un idéal $\mathfrak{m} \neq A$ est dit maximal s'il est maximal pour la relation d'inclusion, *i.e.* si le seul idéal qui le contient strictement est l'anneau tout entier).
4. Montrer que $V(G) = V(H) \iff \overline{G} = \overline{H}$.

L'ANNEAU $\mathbf{Z}$

Exercice 1.2. Montrer que $\forall\ n \geqslant 0$, $(2^n + 3^n)$ et $(2^{n+1} + 3^{n+1})$ sont premiers entre eux.

Exercice 1.3. Trouver les sous-groupes de $\mathbf{Z}$ contenant $48\mathbf{Z}$ et donner leurs relations d'inclusion.

Exercice 1.4. Soient $a, b, c \in \mathbf{N}$. Montrer que si $a \wedge b = 1$ alors :

1. $(ac) \wedge b = c \wedge b$
2. $(ab) \wedge c = (a \wedge c)(b \wedge c)$.

Dans le cas où l'on ne suppose plus $a \wedge b = 1$, donner des contre-exemples aux égalités précédentes.

Exercice 1.5.

1. Déterminer $(n^2 + 2n - 2) \wedge 6$ en fonction de n
   (appliquer le 2. de l'exercice 1.4 et montrer que
   $$n^2 + 2n - 2 \equiv 0 \bmod 3 \iff n \equiv 2 \bmod 3).$$
2. Déterminer $(n^3 + n^2 + 1) \wedge (n^2 + 2n - 1)$ en fonction de n ;
   (en remarquant que les coefficients dominants sont inversibles dans $\mathbf{Z}$, utiliser des divisions euclidiennes successives afin de faire descendre les degrés).

Exercice 1.6. Soient a et b des entiers premiers entre eux tels que leur produit soit une puissance k-ième d'un entier pour $k \geqslant 2$ entier. Montrer alors que a et b sont eux-mêmes des puissances k-ièmes d'entiers.

Exercice 1.7. *Variations sur le théorème de Bézout*

1. En utilisant l'algorithme d'Euclide, trouver toutes les relations de Bézout $650u + 66v = 650 \wedge 66$ (*cf.* (1)).
2. Soient a et b des entiers premiers entre eux, on cherche à savoir si un entier n peut s'écrire sous la forme $ua + vb$ avec u et v entiers positifs.
   (i) Si on n'impose pas à u et v d'être positifs, quels sont les n qui peuvent s'écrire sous la forme $ua + vb$?
   (ii) Montrer que pour tout $n \in \mathbf{Z}$, il existe un unique couple $(u_0, v_0) \in \mathbf{Z}^2$ tel que $n = u_0a + v_0b$ et $0 \leqslant u_0 < b$.
   (iii) Montrer que pour $n > ab - a - b$ il existe u et v positifs tels que $n = ua + vb$.
   (iv) Soit m un entier et soit $(u_0, v_0) \in \mathbf{Z}$ comme dans (ii), *i.e.* $m = u_0a + v_0b$ avec $0 \leqslant u_0 < b$. Montrer qu'il existe des entiers positifs u et v tels que $m = ua + vb$ si et seulement si $v_0 \geqslant 0$.
   (v) Soit m et n des entiers relatifs tels que $m + n = ab - a - b$. On écrit $m = u_0a + v_0b$ et $n = u'_0a + v'_0b$ avec $0 \leqslant u_0, u'_0 < b$. Montrer que $v_0 + v'_0 = -1$ et en déduire que parmi m et n un et un seul peut s'écrire sous la forme $ua + vb$ avec u et v positifs ou nuls.
   (vi) Montrer que $ab - a - b$ ne peut pas s'écrire sous la forme $ua + vb$ avec u et v positifs ou nuls.
   (vii) Montrer que l'ensemble des entiers n tels que $0 \leqslant n \leqslant ab - a - b$ et qu'il existe $u, v \geqslant 0$ avec $n = au + bv$ a pour cardinal $\frac{ab-a-b}{2}$.
3. On suppose que dans un pays n'existent que deux sortes de pièces, de valeurs a et b entières avec $(a \wedge b) = 1$.
   (i) Quelles sont les sommes qui peuvent être payées si on dispose d'un stock infini de pièces et qu'on autorise le rendu de monnaie ?
   (ii) Montrer que $ab - a - b$ est la somme la plus grande qu'il est impossible de payer si le rendu de monnaie n'est pas autorisé.
   (iii) Étudier le cas de 3 pièces de valeur 15, 20 et 48, et montrer que 217 est la plus grande somme que l'on ne peut pas payer sans rendu de monnaie (se ramener au cas précédent en écrivant :
   $$48x + 20y + 15z = 3(16x + 5z) + 20y).$$
4. On considère un jeu de fléchettes où le centre de la cible rapporte 7 points et son extérieur 3 points. Quels sont les scores atteignables ?

L'ANNEAU $\mathrm{Z}/N\mathrm{Z}$, CONGRUENCES

Exercice 1.8. Montrer que pour tout entier $n \geqslant 1$,

$$4^{2^n} + 2^{2^n} + 1 \equiv 0 \bmod 7.$$

(Distinguer les cas n pair et n impair).

Exercice 1.9. Donner les sous-groupes de $\mathbf{Z}/24\mathbf{Z}$ ainsi que leurs relations d'inclusion (cf. 1.36). Quels sont les sous-groupes engendrés par la classe de 18 (resp. 16) ?

Exercice 1.10. Calculer $2\,005^{2\,005} \mod 14$.

Exercice 1.11. Calculer 10^{100} modulo $247 = 13 \times 19$.

Exercice 1.12. Donner la congruence modulo 17 de $(1\,035\,125)^{5\,642}$.

Exercice 1.13. Donner la congruence de $1\,823^{242}$ modulo 18 puis celle de $2\,222^{321}$ modulo 20.

Exercice 1.14. Montrer que pour $n \geqslant 1$, on a $n^7 \equiv n \mod 42$.

Exercice 1.15. Montrer que 429 est inversible dans $\mathbf{Z}/700\mathbf{Z}$ et donner son inverse.

Exercice 1.16. Résoudre dans $\mathbf{Z}$ les congruences suivantes :

(i) $3x \equiv 4 \mod 7$;
(ii) $9x \equiv 12 \mod 21$;
(iii) $103x \equiv 612 \mod 676$.

Exercice 1.17. Soient $p \neq 2$ un nombre premier impair, $a, b \in \mathbf{N}$ non divisibles par p. Montrer que si p divise $a^2 + b^2$, alors $p \equiv 1 \mod 4$.

Exercice 1.18. Soient a et b deux entiers premiers entre eux, $n = a^4 + b^4$, p un diviseur premier de n, $p \neq 2$.

1. Montrer que $n \equiv 1$ ou $2 \bmod 16$.
2. Montrer que les classes $\overline{a}$ et $\overline{b}$ de a et $b \bmod p$ sont dans $(\mathbf{Z}/p\mathbf{Z})^*$.
3. Calculer l'ordre de $\overline{a}/\overline{b}$ dans $(\mathbf{Z}/p\mathbf{Z})^*$.
4. En déduire que $p \equiv 1 \bmod 8$.

Exercice 1.19. *« Un test de primalité »*. Soient a et p deux entiers tels que $a \wedge p = 1$. Montrer que les conditions suivantes sont équivalentes :

(i) l'entier p est premier ;
(ii) on a $(X - a)^p \equiv X^p - a \bmod p$ dans l'anneau $\mathbf{Z}[X]$.

Exercice 1.20. Soient p et q des nombres premiers distincts.

1. Quel est le cardinal de $(\mathbf{Z}/pq\mathbf{Z})^*$? Combien y a-t-il d'éléments de $(\mathbf{Z}/pq\mathbf{Z})^*$ égaux à leur inverse ?
2. Montrer la congruence :

$$\frac{(pq-1)!}{(q-1)!p^{q-1}(p-1)!q^{p-1}} \equiv 1 \bmod pq$$

(même méthode que pour le théorème de Wilson).

MORPHISMES

Exercice 1.21.

1. Montrer que tout homomorphisme de groupes
$$\phi : \mathbf{Z}/a\mathbf{Z} \to \mathbf{Z}/b\mathbf{Z}$$
est déterminé par $\phi(1)$ et que $\phi(1)$ est un élément dont l'ordre divise a.
Réciproquement, montrer que si l'ordre de $x \in \mathbf{Z}/b\mathbf{Z}$ divise a, il existe un morphisme ϕ tel que $\phi(1) = x$.
2. Montrer que les conditions suivantes sont équivalentes :
   (i) $a \wedge b = 1$
   (ii) tout homomorphisme $\phi : \mathbf{Z}/a\mathbf{Z} \to \mathbf{Z}/b\mathbf{Z}$ est l'homomorphisme nul.

Exercice 1.22. Déterminer les morphismes de groupes $\mathbf{Z}/3\mathbf{Z} \to \mathbf{Z}/4\mathbf{Z}$ puis ceux de $\mathbf{Z}/12\mathbf{Z} \to \mathbf{Z}/15\mathbf{Z}$.

Exercice 1.23. On fixe un nombre premier p. Soit a un entier > 0.

1. Trouver la condition nécessaire et suffisante que doit satisfaire n pour qu'il existe un morphisme de groupes non nul :
$$\mathbf{Z}/p^a\mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z}.$$
2. On suppose maintenant $n = p^b$, b étant un nombre entier > 0. Caractériser les éléments $x \in \mathbf{Z}/p^b\mathbf{Z}$ tels qu'il existe un morphisme
$$\phi : \mathbf{Z}/p^a\mathbf{Z} \longrightarrow \mathbf{Z}/p^b\mathbf{Z}$$
avec $\phi(1) = x$.
3. Calculer le nombre de morphismes distincts : $\mathbf{Z}/p^a\mathbf{Z} \longrightarrow \mathbf{Z}/p^b\mathbf{Z}$ (on pourra supposer $a \leqslant b$).

Exercice 1.24. Soit $\pi : \mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ le morphisme qui à $k \in \mathbf{Z}$ associe ses classes modulo n et m (cf. 1.48). Montrer que le noyau de π est engendré par le PPCM de m et n et que l'image de π est $\{(\overline{a}, \overline{b})$ tels que $(n \wedge m)|(b - a)\}$.

Application : que peut-on dire de la congruence de k modulo 10 sachant que $k \equiv 3 \bmod 6$?

PROBLÈMES

Problème 1.1. *Un test de primalité*
Soient n un entier > 1, p un nombre premier tels que $n - 1 = p^r m$, avec $r \geqslant 1$, $m \geqslant 1$.

1. On suppose qu'il existe un entier a tel que $a^{n-1} \equiv 1 \bmod n$ et $(a^{\frac{n-1}{p}} - 1) \wedge n = 1$. Soit q un diviseur premier de n. Montrer que $(a^m - 1) \wedge q = 1$.

2. Soit $b \in \mathbf{Z}/q\mathbf{Z}$ la classe de a^m. Montrer que $b \in (\mathbf{Z}/q\mathbf{Z})^*$ et calculer son ordre (multiplicatif).
3. Montrer que $q \equiv 1 \bmod p^r$.
4. On écrit maintenant $n-1 = uv$ (sans hypothèse particulière sur u, v). On suppose que pour tout facteur premier p de u, il existe un entier a_p tel que $a_p^{n-1} \equiv 1 \bmod n$ et $(a_p^{\frac{n-1}{p}} - 1) \wedge n = 1$. Montrer que tout facteur premier q de n vérifie $q \equiv 1 \bmod u$.
5. On suppose en plus des hypothèses de 4. que $v \leqslant u+1$. Montrer que n est premier.

Problème 1.2. *Une généralisation du petit théorème de Fermat*

1. Soit n un entier $\geqslant 2$. Montrer que les conditions suivantes sont équivalentes :
   (i) n est sans facteurs carrés et pour tout nombre premier p, $p|n \Rightarrow (p-1)|(n-1)$;
   (ii) $\forall a \in \mathbf{Z}, a^n \equiv a \bmod n$;
   (iii) $\forall a \in \mathbf{Z}$ tel que $(a, n) = (1)$, $a^{n-1} \equiv 1 \bmod n$.
2. On considère les conditions suivantes (pour n impair) :
   (i) n est sans facteurs carrés et pour tout nombre premier p, $p|n \Rightarrow (p-1)|(n-1)/2$;
   (ii) $\forall a \in \mathbf{Z},\ (a, n) = (1),\ a^{(n-1)/2} \equiv 1 \bmod n$.
   Montrer que (i) $\Leftrightarrow$ (ii).
3. Soit m un entier > 0. On suppose que les nombres $6m+1,\ 12m+1,\ 18m+1$ sont premiers. Montrer que $n = (6m+1)(12m+1)(18m+1)$ vérifie les propriétés de 1. Montrer que si m est impair, alors n vérifie les propriétés de 2.

Problème 1.3. *Étude des premiers nombres de Fermat*

On pose pour tout $n \in \mathbf{N}$, $F_n = 2^{2^n} + 1$; F_n est par définition le n-ième nombre de Fermat.

1. Soit $m \in \mathbf{N}\backslash\{0\}$. Prouver que si $2^m + 1$ est premier alors m est une puissance de 2.
2. Calculer F_n pour $n \leqslant 4$ et vérifier qu'ils sont tous premiers.
3. Montrer qu'*a priori*, un diviseur premier potentiel de F_5 est de la forme $64k + 1$.
4. Montrer que F_5 est divisible par $641 = 1 + 5.2^7 = 5^4 + 2^4$.
5. Montrer que pour $n \neq m$, F_n et F_m sont premiers entre eux et en déduire l'existence d'une infinité de nombres premiers.

Problème 1.4. *Utilisation des entiers de Gauss, théorème des deux carrés*

On note $A = \mathbf{Z}[i] = \{a + ib \,|\, (a, b) \in \mathbf{Z}^2\}$ l'anneau des entiers de Gauss. Pour $z = a + ib \in A$, on pose $N(a + ib) = a^2 + b^2$.

1. Montrer que N est multiplicative, *i.e.* $N(zz') = N(z)N(z')$; en déduire que $A^* = \{\pm 1, \pm i\}$ ainsi que l'identité de Lagrange :

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

2. En remarquant que tout nombre complexe peut s'écrire comme la somme d'un élément de $\mathbf{Z}[i]$ et d'un nombre complexe de module strictement plus petit que 1, en déduire que A est euclidien mais que la division euclidienne n'est pas unique.
3. Soit S l'ensemble des entiers > 0 somme de deux carrés. Montrer que S est stable par multiplications.
4. Soit p un nombre premier. Montrer l'équivalence des points suivants :
   - p est irréductible dans A ;
   - $p \equiv 3 \bmod (4)$;
   - $p \notin S$.
5. En déduire que les éléments irréductibles de A modulo les éléments inversibles sont les p premiers congrus à 3 modulo 4 et les $a + ib$ tels que $a^2 + b^2$ est premier.
6. Montrer que si $n \geqslant 2$, alors $n \in S$ si et seulement si la multiplicité $v_p(n)$ de p dans n est paire pour tout $p \equiv 3 \bmod 4$ (« théorème des deux carrés ») .

Problème 1.5. *Un anneau non factoriel*
Soit $A := \mathbf{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \,/\, (a, b) \in \mathbf{Z}^2\}$. On introduit l'application « norme » : $N(a + ib\sqrt{5}) = a^2 + 5b^2 \in \mathbf{N}$. On rappelle (1.10) qu'un élément $z \in A$ est dit irréductible si et seulement s'il vérifie la propriété suivante :

$$z = z_1 z_2 \text{ et } z_1 \notin A^* \Longrightarrow z_2 \in A^*$$

1. Montrer que $z \in A^*$ si et seulement si $N(z) = 1$ puis que si $N(z)$ est un nombre premier alors z est irréductible.
2. Montrer que tout élément $z \in A$ tel que $N(z) = 9$ est irréductible. En étudiant alors l'égalité :
$$3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$
montrer que $\mathbf{Z}[i\sqrt{5}]$ n'est pas factoriel (*cf.* 1.14).
3. Étudier de même l'égalité $2.3 = a.b$ avec $a = 1 + i\sqrt{5}$ et $b = 1 - i\sqrt{5}$; montrer avec cet exemple que le lemme de Gauss n'est pas vérifié et que $2a$ et ab n'ont pas de PGCD.

Chapitre 2

Modules de type fini

Tous les groupes considérés dans ce chapitre sont commutatifs (on dit aussi abéliens). Nous allons voir que tout groupe abélien peut-être considéré comme un $\mathbf{Z}$-module. Or les propriétés fondamentales des $\mathbf{Z}$-modules sont en fait valables sans changement pour les modules sur les anneaux principaux. Comme nous utiliserons ces propriétés au chapitre suivant pour les modules de type fini sur un anneau de polynômes $K[X]$ (sur un corps K), nous les avons énoncées et démontrées dans le cadre plus général des modules sur un anneau principal A.

D'autre part, certaines démonstrations sont présentées dans ce livre sous forme d'algorithmes utilisant l'algorithme d'Euclide et l'algorithme d'Euclide « étendu » (et donc l'algorithme de division). Si l'on veut que ces algorithmes soient « effectifs » (*i.e.* programmables), il faut se placer sur un anneau A dans lequel il existe un algorithme pour la division euclidienne, ce qui est le cas de $A = K[X]$, à condition que l'on sache programmer les additions et multiplications dans K comme par exemple pour $K = \mathbf{Q}$.

2.1 LE LANGAGE DES MODULES

Pour cette introduction, A est un anneau (donc pour nous commutatif et unitaire) quelconque dont l'élément unité pour la multiplication est noté 1.

2.1.1. Généralités

Définition 2.1. *Soit $(M, +)$ un groupe commutatif. On dit que M est un A-module s'il est muni d'une application $A \times M \to M$, où l'on note ax l'image de (a, x), telle que :*

1. $\forall a \in A$ *et* $x, y \in M$, $a(x+y) = ax + ay$ *;*

2. $\forall a, b \in A$ *et* $x \in M$, $(a+b)x = ax + bx$ *;*

3. $\forall a, b \in A$ *et* $x \in M$, $1x = x$ *et* $a(bx) = (ab)x$.

Remarques 2.2.

1. La définition de A-module est ainsi formellement la même que celle de K-espace vectoriel. Cependant lorsque A n'est pas un corps, nous verrons qu'il y a des grandes différences ; en particulier un A-module ne possède pas nécessairement une base. Les définitions de sous-modules, systèmes de générateurs, familles libres, bases, morphismes, images, noyaux, etc. sont les mêmes que dans le cas des espaces vectoriels ; elles ne seront pas toutes répétées ici. Les propriétés des modules quotients sont aussi analogues à celles des espaces vectoriels quotients ; cependant elles sont souvent moins bien connues et nous avons pensé qu'il était nécessaire de les exposer en détails dans le cadre de ce livre (paragraphe 2.1.2.).
2. Soient M et N deux A-modules. Un morphisme de A-modules $M \to N$ est un morphisme de groupes additifs $(M, +) \to (N, +)$ qui est de plus A-linéaire. Sauf mention du contraire, dans ce chapitre le mot « morphisme » signifiera « morphisme de A-modules ». Dans le cas où A est un corps, on retrouve la notion classique d'application linéaire entre espaces vectoriels.
3. Si $(G, +)$ est un groupe commutatif, il est canoniquement muni d'une structure de $\mathbf{Z}$-module, en définissant (pour $n > 0$) ng comme $g + g + \cdots + g$ n fois, et $(-1)g$ comme $-g$. On dira plutôt « groupe » (sous-entendu commutatif) que « $\mathbf{Z}$-module ».
4. L'anneau A est lui-même un A-module engendré par 1. Les sous-A-modules (on dit simplement sous-modules) de A sont les *idéaux*.
5. Soit M un A-module, $M_i \subset M$ $(1 \leqslant i \leqslant n)$ des sous-modules. Alors, comme pour les espaces vectoriels, on a $M = M_1 \oplus \cdots \oplus M_n$ si et seulement si chaque élément $m \in M$ peut s'écrire de manière unique $m = m_1 + \cdots + m_n$ avec $m_i \in M_i$.
6. Soit M un A-module, $M_i \subset M$ $(1 \leqslant i \leqslant n)$ des sous-modules tels que $M = M_1 \oplus \cdots \oplus M_n$. On a alors un isomorphisme canonique ψ entre M et $\prod_{i=1}^n M_i = M_1 \times \cdots \times M_n$ (si $m_i \in M_i$, on pose $\psi(m_1 + \cdots + m_n) = (m_1, \ldots, m_n)$). Inversement, si on pose $\prod_{i=1}^n M_i = M_1 \times \cdots \times M_n$, chaque M_i s'identifie à un sous-module $f_i(M_i)$ de $\prod_{i=1}^n M_i$ par le morphisme $f_i : m \in M_i \mapsto (0, \ldots, 0, m, 0, \ldots, 0)$ avec m à la i-ième place. On a alors :

$$\prod_{i=1}^{n} M_i = \bigoplus_{i=1}^{n} f_i(M_i) \simeq \bigoplus_{i=1}^{n} M_i.$$

Notons qu'un isomorphisme analogue n'existe pas dans le cas des produits infinis.

7. Un A-module M est de *type fini* s'il admet un nombre fini de générateurs $(m_1, \ldots, m_k)$. Le fait que $(m_1, \ldots, m_k)$ soit un système de générateurs est équivalent au fait que le morphisme :
$$\phi : \ A^k \to M, \quad \phi(\lambda_1, \ldots, \lambda_k) = \sum_{i=1}^{k} \lambda_i m_i$$
est surjectif.
8. Soit M un A-module. L'ensemble des éléments $\lambda \in A$ qui annulent M (*i.e.* tels que $\forall m \in M$ on ait $\lambda m = 0$) est un idéal appelé *annulateur* de M et noté ann(M). Par exemple, si $M = A/I$, on a ann$(M) = I$.

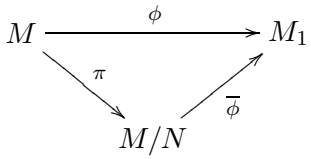
2.1.2. Quotients

Définition 2.3. *Soient M un A-module, $N \subset M$ un sous-module. On définit une relation d'équivalence sur M de la manière suivante : on dit que deux éléments m_1 et m_2 de M sont équivalents si $m_1 - m_2 \in N$. L'ensemble quotient pour cette relation d'équivalence se note M/N et est muni d'une structure de A-module propagée par celle de M, i.e. telle que l'application canonique $\pi : M \to M/N$ soit un morphisme surjectif de noyau N (appelé morphisme canonique).*

Si l'on note $\overline{m} = \pi(m)$ la classe d'un élément $m \in M$, la structure de module sur M/N est définie par $\overline{m_1} + \overline{m_2} = \overline{m_1 + m_2}$ et pour $\lambda \in A$ et $m \in M$, $\lambda\overline{m} = \overline{\lambda m}$. Il est immédiat de vérifier que ces opérations définissent une structure de module sur M/N telle que l'application π soit un morphisme surjectif.
Le quotient est caractérisé par la propriété suivante (appelée « propriété universelle du quotient », *cf.* 1.19) :

Proposition 2.4. *Soient $N \subset M$ deux modules, $\pi : M \to M/N$ le morphisme canonique, $\phi : M \to M_1$ un morphisme tel que $N \subset \ker \phi$; il existe alors un morphisme unique $\overline{\phi} : M/N \to M_1$ tel que $\overline{\phi} \circ \pi = \phi$. Réciproquement l'existence d'un tel morphisme implique $N \subset \ker\phi$. De plus le morphisme $\overline{\phi}$ est injectif si et seulement si $N = \ker \phi$.*

On a donc sous l'hypothèse $N \subset \ker \phi$ un « diagramme commutatif » :



La démonstration est la même que celle de la proposition 1.19.
On utilise cette proposition de la manière suivante : pour définir un morphisme $\overline{\phi} : M/N \longrightarrow M_1$, il est équivalent de définir un morphisme $\phi : M \longrightarrow M_1$ tel que $N \subset \ker \phi$.

Voici quelques propriétés classiques des quotients, toutes conséquences directes de la proposition 2.4 :

Corollaire 2.5. « Décomposition canonique d'un morphisme ».
Soient M et M_1 deux A-modules, $\phi : M \to M_1$ un morphisme, $\pi : M \to M/\ker\phi$ le morphisme canonique. On a alors une décomposition de ϕ dite « décomposition canonique » *: $\phi = i \circ \overline{\phi} \circ \pi$ où i est l'injection canonique : $\phi(M) = \mathrm{Im}(M) \to M_1$, et $\overline{\phi}$ un isomorphisme : $M/\ker\phi \to \phi(M)$.*

$$\begin{array}{ccc} M & \xrightarrow{\phi} & M_1 \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ M/\ker\phi & \xrightarrow{\overline{\phi}} & \phi(M) \end{array}$$

Corollaire 2.6. *Soient M, N, P trois A-modules tels que $N \subset P \subset M$. Alors l'injection canonique $f : P \to M$ « passe aux quotients » pour donner une injection : $\overline{f} : P/N \to M/N$ ce qui permet d'identifier P/N et son image par $\overline{f}$. On a alors avec cette identification :*

$$(M/N)/(P/N) \simeq M/P.$$

Exemple 2.7. Prenons $M = \mathbf{Z}$, $P = a\mathbf{Z}$, $N = ab\mathbf{Z}$, a et b étant deux entiers. On a alors $(\mathbf{Z}/ab\mathbf{Z})/(a\mathbf{Z}/ab\mathbf{Z}) \simeq \mathbf{Z}/a\mathbf{Z}$. Notons que $\mathbf{Z}/b\mathbf{Z} \simeq a\mathbf{Z}/ab\mathbf{Z}$ (exercice).

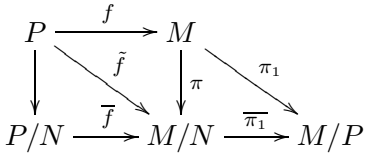
Corollaire 2.8. *Soient $N_i, M_i \ \ (1 \leqslant i \leqslant n), M$ des A-modules tels que $\forall i$, $N_i \subset M_i \subset M$, $M = \bigoplus_{i=1}^n M_i$. Posons $N = \bigoplus_{i=1}^n N_i$ $(N \subset M)$. On a alors un isomorphisme canonique :*

$$M/N \simeq \bigoplus_{i=1}^{n} (M_i/N_i).$$

Un cas particulier du corollaire précédent est le suivant : soient M_1 et M_2 deux sous-modules d'un A-module M tels que $M = M_1 \oplus M_2$, alors $M/M_1 \simeq M_2$ (on applique le corollaire précédent avec $N_1 = M_1,\ N_2 = \{0\}$).

Le corollaire 2.5 résultant d'un simple changement de notations dans la proposition 2.4, nous allons démontrer le corollaire 2.6 (la démonstration du corollaire 2.8, immédiate, est laissée au lecteur).

Démonstration. (du corollaire 2.6) : soit π le morphisme canonique : $M \to M/N$, $\tilde{f} = \pi \circ f$. Le morphisme $\tilde{f}$ se factorise par un morphisme injectif $\overline{f} : P/N \to M/N$ d'après la proposition 2.4. Toujours d'après la proposition 2.4, le morphisme canonique $\pi_1 : M \to M/P$ se factorise par un morphisme (encore surjectif) : $\overline{\pi_1} : M/N \to M/P$ (car $N \subset \ker\pi_1 = P$) dont le noyau est l'image de $f(P)$ par π égale à l'image de $\overline{f}$ (*cf.* le diagramme commutatif ci-dessous) identifiée à P/N.



On peut alors appliquer le corollaire 2.5 au morphisme (surjectif) $\overline{\pi_1}$. ■

Remarque 2.9. Soit I un idéal de A. Le A-module quotient A/I est alors naturellement muni d'une structure d'anneau propagée par celle de A via le morphisme canonique $\pi : A \to A/I$: si $x, y \in A/I$, il existe a et b dans A tels que $\pi(a) = x, \pi(b) = y$. On pose alors $xy = \pi(ab)$, et il est immédiat de voir que cette multiplication est bien définie et fait de A/I un anneau avec unité $\pi(1)$ (que l'on note aussi 1 en général).

2.2 CALCUL MATRICIEL SUR UN ANNEAU PRINCIPAL

Dans toute la suite de ce chapitre, A désignera un anneau euclidien pour lequel il existe un algorithme pour la division euclidienne. Nous utiliserons le calcul matriciel seulement pour les anneaux $A = \mathbf{Z}$ et au chapitre suivant pour $A = K[X]$, K étant un corps.

Rappelons quelques propriétés d'un tel anneau A.

1. Un élément $p \in A$ est irréductible si et seulement si l'anneau quotient $A/(p)$ est un corps (*cf.* le corollaire 1.39 pour le cas $A = \mathbf{Z}$; la preuve est la même pour tout anneau principal).
2. L'anneau A est contenu dans son corps des fractions $K(A)$ (définition 1.12).
3. L'anneau A est factoriel (théorème 1.30).

2.2.1. Trigonalisation

La présentation de cette section est inspirée de [**3**]. On note $\mathcal{M}_{n,m}(A)$ l'ensemble des matrices de taille $n \times m$ (n lignes et m colonnes) à coefficients dans A. On note $\mathcal{M}_n(A)$ l'ensemble des matrices de taille $n \times n$ à coefficients dans A, $SL_n(A)$ le sous-ensemble de $\mathcal{M}_n(A)$ formé des matrices de déterminant 1.

Lemme 2.10. *Une matrice $M \in \mathcal{M}_n(A)$ est inversible si et seulement si $\det M \in A^*$. En particulier $M \in \mathcal{M}_n(\mathbf{Z})$ est inversible si et seulement si $\det M = \pm 1$.*

Démonstration. Si la matrice M est inversible, il est clair que son déterminant aussi (dans l'anneau A). Inversement, on a la formule suivante pour une matrice à coefficients dans un anneau :

$$^t\mathrm{co}(M) \times M = \det M \times I_n$$

($\mathrm{co}(M)$ est la matrice des cofacteurs, et I_n la matrice identité de taille (n,n)). Si $\det M$ est inversible dans A, on peut diviser par $\det M$, et l'on a :

$$(\det M)^{-1}({}^t\mathrm{co}(M) \times M) = I_n,$$

d'où

$$M^{-1} = {}^t\mathrm{co}(M)(\det(M))^{-1}.$$

■

En particulier toute matrice $M \in SL_n(A)$ est inversible.

Le lemme suivant est le lemme technique essentiel pour tout ce qui concerne la calcul matriciel sur A.

Lemme 2.11. *Soient x et y deux éléments de A, z un PGCD de x et y (défini à multiplication par un élément de A^* près). Il existe alors une matrice :*

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(A)$$

telle que :

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} z \\ 0 \end{pmatrix} \tag{1}$$

Démonstration. On peut supposer que $(x\ y) \neq (0\ 0)$ (sinon, tout est nul). Il existe alors deux éléments u et v dans A tels que $z = ux + vy$ (formule (1) du chapitre 1) (si $x = 0$ (resp. $y = 0$), on prend $u = 0$ (resp. $v = 0$) par convention). Alors la matrice

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} u & v \\ -y/z & x/z \end{pmatrix} \tag{2}$$

convient, car z étant un PGCD de x et y, il les divise. ■

Remarques 2.12.

1. La multiplication à gauche d'une matrice $M \in \mathcal{M}_{n,m}(A)$ par un élément de $SL_n(A)$ revient à effectuer des manipulations sur les lignes de M. Si on veut manipuler les colonnes, il faut multiplier à droite par un élément de $SL_m(A)$, ce que nous ferons au paragraphe suivant ; dans le cas du lemme 2.11, cela donnerait l'égalité suivante (obtenue en transposant (1)) :

$$(x \quad y) \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} = (z \quad 0) \tag{3}$$

2. Dans le cas où $x = 0$, on pose $u = 0$ par convention et l'on obtient :

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

3. Dans le cas où $x|y$, on a $(x,y) = (x)$, donc un PGCD de x et y est x, et l'on pose :

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -y/x & 1 \end{pmatrix}.$$

Nous allons utiliser la matrice de taille (n, n) suivante :

$$L_{j,k} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}_{j,k} = \begin{pmatrix} 1 & 0 & \dots & & & & & & \dots & 0 \\ 0 & \ddots & & & & & & & 0 & \vdots \\ & & 1 & & & & & & & \\ \vdots & 0 & \dots & \alpha & 0 & \dots & & \beta & \vdots & \\ & \vdots & & & 1 & & & & & \\ & & & & & \ddots & & & & \\ & & & & & & 1 & & & \\ & & & \gamma & 0 & \dots & & \delta & & \\ & & & & & & & & 1 & \\ & & & & & & & & & \ddots \\ 0 & \dots & & & & & & & & 1 \end{pmatrix} \tag{4}$$

α étant à la place (j, j) (sur la j-ième ligne et la j-ième colonne), β à la place (j, k), γ à la place (k, j) et δ à la place (k, k). Notons l_i la ligne d'indice i d'une matrice M.

Lemme 2.13. *La multiplication à gauche d'une matrice $M \in \mathcal{M}_{n,m}(A)$ par la matrice $L_{j,k}$ remplace l_j et l_k par $\alpha l_j + \beta l_k$ et $\gamma l_j + \delta l_k$ respectivement. De plus,* $\det L_{j,k} = \alpha\delta - \beta\gamma$.

Démonstration. Exercice laissé au lecteur sur la multiplication des matrices. ■

Proposition 2.14. *Soit $M \in \mathcal{M}_{n,m}(A)$. Il existe alors une matrice $L \in SL_n(A)$ telle que $LM = M'$ soit triangulaire supérieure (i.e. avec des zéros sous la diagonale principale).*

Démonstration. La démonstration consiste à appliquer plusieurs fois les lemmes 2.11 et 2.13 pour faire apparaître des zéros sous la diagonale principale.

a) Soit $M = (a_{ij})$ $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m)$. Multiplions M à gauche par la matrice $L_1 = L_{1,2}$ (*cf.* (4)), avec α, β, γ et δ choisis de façon à ce que la première colonne de $M_1 = L_1 M$ commence par $\begin{pmatrix} d \\ 0 \end{pmatrix}$ avec $(d) = (a_{11}, a_{21})$ (*i.e.* d est un PGCD de a_{11} et a_{21}) ; on a donc (d'après le lemme 2.11) :

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} u & v \\ -a_{21}/d & a_{11}/d \end{pmatrix},$$

u et v vérifiant $d = ua_{11} + va_{21}$. On a en particulier $\alpha\delta - \beta\gamma = 1$ et donc $L_1 \in SL_n(A)$ et la matrice $M_1 = L_1 M$ a un zéro à la place $(2, 1)$.

b) On multiplie ensuite M_1 à gauche par une matrice L_2 de la forme $L_{1,3}$ pour faire apparaître un zéro à la place $(3, 1)$ (ce qui remplace d par d_1 tel que $(d_1) = (d, a_{31})$, et ainsi de suite jusqu'à ce que l'on obtienne la matrice $M_{n-1} = L_{n-1} \cdots L_1 M$ dont la première colonne est de la forme ${}^t(d_{n-1}\, 0 \dots 0)$, d_{n-1} étant un PGCD de tous les éléments de la première colonne de M.

c) On continue de même avec la seconde colonne, en commençant par multiplier à gauche par une matrice $L_{2,3}$ de façon à laisser la première ligne inchangée et de ne « manipuler » que les lignes $l_2, \dots, l_n$, ce qui implique aussi que la première colonne des nouvelles matrices reste égale à ${}^t(d_{n-1}\, 0 \dots 0)$ (les coefficients de $L_{2,3}$ étant choisis pour faire apparaître un zéro à la place $(3,2)$).

d) Une récurrence immédiate achève la preuve. ■

Si $v := (a_1 \dots a_n)$ est un vecteur ligne, on dit que v est de *longueur* $n - p$ si p est le plus grand entier tel que $a_1 = \dots = a_p = 0$ (si tous les a_i sont nuls, la longueur de v est 0). On a alors :

Corollaire 2.15. *Soit $M \in \mathcal{M}_{n,m}(A)$. Il existe $L \in SL_n(A)$ telle que la longueur des lignes de la matrice LM décroisse strictement (en particulier LM est triangulaire supérieure dans le cas où $n = m$).*

Démonstration. Par une facile récurrence sur m (nombre de colonnes) :

a) si la première colonne n'est pas constituée que de zéros, on applique la méthode précédente pour obtenir une nouvelle matrice dont la première colonne est de la forme ${}^t(x_1\, 0 \dots 0)$, x_1 étant un PGCD (donc non nul) des éléments de la première colonne de M. On applique ensuite l'hypothèse de récurrence à la matrice M' formée des éléments a_{ij}, avec $i \geqslant 2$ et $j \geqslant 2$;

b) si la première colonne est nulle, on applique l'hypothèse de récurrence à la matrice M'' formée des éléments a_{ij} avec $j \geqslant 2$ (et i quelconque, *i.e.* toutes les lignes). ■

2.2.2. Échelonnement

Rappelons que pour deux éléments a et b de A, la notation $a \mid b$ signifie que a divise b. Par convention, tout élément de A divise 0.

Définition 2.16. *Soit M une matrice de taille (n, m) à coefficients entiers. On dit que M est* réduite *(ou* échelonnée*) si :*

$$M = \begin{pmatrix} a_{1,1} & 0 & \dots & & 0 \\ 0 & a_{2,2} & 0 & \dots & \vdots \\ \vdots & & \ddots & & \\ & & & a_{n,n} & \dots\ 0 \end{pmatrix} \tag{5}$$

avec

$$a_{i,i} \mid a_{i+1,i+1}, \quad 1 \leqslant i \leqslant \inf(n,m) - 1.$$

Sur la figure, on a représenté une matrice M avec $n < m$. Il est à noter que les derniers $a_{i,i}$ peuvent être nuls et que tous les éléments non sur la diagonale sont nuls.

Théorème 2.17. *Soit M une matrice de taille (n, m) à coefficients dans A. Il existe alors $L \in SL_nA$ et $R \in SL_m(A)$ telles que :*

$$M' = LMR$$

soit réduite.

> ***Remarque 2.18.*** L'énoncé analogue sur un corps K est que toute matrice $M \in \mathcal{M}_{n,m}(K)$ est équivalente à une matrice M' de la forme
>
> $$M' = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix},$$
>
> I_r désignant la matrice identité de taille r, équivalente signifiant que $M' = LMR$ avec $L \in \mathrm{GL}_n(K)$ et $R \in \mathrm{GL}_m(K)$. L'entier r est le *rang* de M.

Comme pour la proposition 2.14, la démonstration du théorème 2.17 se fait en plusieurs étapes, en appliquant à chaque fois le lemme 2.13 pour manipuler les lignes, et en transposant (et multipliant à droite) pour manipuler aussi les colonnes. La démonstration est présentée comme un algorithme qui utilise des sous-algorithmes que nous appellerons procédures.

Définition 2.19. *Soit $a \in A$, $a \neq 0$, $a = \lambda p_1 \dots p_k$ sa décomposition en éléments irréductibles de A ($\lambda \in A^*$) distincts ou non. L'entier k s'appelle la* longueur *de a et se note $l(a)$.*

L'entier k est bien déterminé puisque l'écriture $a = \lambda p_1 \dots p_k$ est unique à l'ordre des p_i près si l'on prend les p_i dans un système représentatif fixé $\mathcal{P}$ d'éléments irréductibles (définition 1.14). Par exemple, si $A = \mathbf{Z}$, le nombre -120 est de longueur 5, car on a $-120 = -2^3.3.5 = -(2 \times 2 \times 2 \times 3 \times 5)$.

Décrivons maintenant la première étape de l'algorithme.

Proposition 2.20. *Soit $M \in \mathcal{M}_{n,m}$, $M = (a_{i,j})$. Il existe une matrice $L \in SL_n(A)$ telle que dans $M' = LM$ la première colonne soit de la forme*

$$c'_1 = \begin{pmatrix} a'_{1,1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

avec les conditions suivantes :

1. *si $a_{1,1}$ divise chaque $a_{i,1}$ $(i > 1)$, la ligne l_1 de M est inchangée (en particulier $a'_{1,1} = a_{1,1}$),*
2. *sinon, $l(a'_{1,1}) < l(a_{1,1})$.*

Démonstration. (procédure « ASC » pour « Annulation d'une sous-colonne ») Appliquons l'algorithme de la proposition 2.14 à la matrice colonne :

$$\begin{pmatrix} a_{1,1} \\ \vdots \\ a_{n,1} \end{pmatrix};$$

il existe une matrice $L \in SL_n(A)$ telle que

$$L \begin{pmatrix} a_{1,1} \\ a_{2,1} \\ \vdots \\ a_{n,1} \end{pmatrix} = \begin{pmatrix} a'_{1,1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

avec $a'_{1,1} = \mathrm{PGCD}(a_{1,1}, a_{2,1}, \ldots, a_{n,1})$. Alors,

1. si $a_{1,1}$ divise tous les $a_{i,1}$ $(i > 1)$, les matrices de passage successives sont de la forme :
$$\begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}$$
(remarque 2.12), et donc la ligne l_1 est inchangée ;
2. sinon l'élément $a'_{1,1}$ est un diviseur strict de $a_{1,1}$ puisque c'est le PGCD des $a_{i,1}$ $(1 \leqslant i \leqslant n)$; on a donc $l(a'_{1,1}) < l(a_{1,1})$.

■

> ***Remarque 2.21.*** En échangeant les lignes et les colonnes, la même démonstration définit une procédure « ASL » (annulation d'une sous-ligne) qui annule une sous-ligne dans les mêmes conditions que ci-dessus, en multipliant à droite par un élément de $SL_m(A)$.

Lemme 2.22. *Il existe deux matrices $L \in SL_n(A)$ et $R \in SL_m(A)$ telles que dans la matrice LMR, la colonne d'indice* 1 *soit de la forme :*

$$\tilde{c}_1 = \begin{pmatrix} \tilde{a}_{1,1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

et la ligne d'indice 1 *de la forme :*

$$\tilde{l}_1 = (\tilde{a}_{1,1}\, 0 \ldots 0).$$

Démonstration. Procédure « ASCSL » (« Annulation d'une sous-colonne et d'une sous-ligne à la fois »).

On applique la procédure ASL pour obtenir une matrice M' avec dans la ligne l'_1, $a'_{1,j} = 0$ pour les indices $j > 1$, puis la procédure ASC à cette matrice M' pour obtenir $M'' = (a''_{ij})$. Alors :

– soit l'élément $a'_{1,1}$ divise tous les éléments $a'_{i,1},\ i > 1$ de la sous-colonne d'indice 1, et la ligne l'_1 est inchangée (proposition 2.20) ; on a donc annulé à la fois la sous-ligne et la sous-colonne d'indice 1 (et $a''_{11} = a'_1$) ;
– soit ce n'est pas le cas, et la ligne l'_1 est éventuellement modifiée (et donc les zéros de la sous-ligne peuvent disparaître). Mais dans ce cas on a $l(a''_{1,1}) < l(a'_{1,1})$, et on refait la procédure ASL pour la matrice M''.

Comme la longueur de l'élément $a_{1,1}$ est finie, disons égale à k, au bout de k étapes au plus la longueur ne baisse plus, et la procédure s'arrête. ■

Lemme 2.23. *Il existe deux matrices $L \in SL_n(A)$ et $R \in SL_m(A)$ telles que dans la matrice LMR le résultat soit le même que dans le lemme* 2.22*, mais que en plus l'élément $\tilde{a}_{1,1}$ divise tous les éléments de la sous-matrice $(\tilde{a}_{i,j})_{i>1,j>1}$.*

Démonstration. Procédure « RSCSL » (« Réduction d'une sous-colonne et d'une sous-ligne à la fois »).
Si après la procédure ASCSL l'élément $\tilde{a}_{1,1}$ ne divise pas un élément $\tilde{a}_{i,j}$ avec $i > 1, j > 1$, on remplace la ligne $\tilde{l}_1$ par $\tilde{l}_1 + \tilde{l}_i$. Cela se fait en multipliant à gauche par un élément de $SL_n(A)$ (lemme 2.13). Dans la matrice M^1 obtenue, l'élément $\tilde{a}_{1,1}$ n'a pas changé, mais cette fois ne divise pas l'élément $a^1_{1,j} = \tilde{a}_{i,j}$. On réapplique alors la procédure ASLSC pour annuler la sous-ligne et la sous-colonne de M^1, ce qui fait baisser la longueur de l'élément d'indice $(1, 1)$ (proposition 2.20). Au bout d'un nombre fini de telles étapes, la procédure s'arrête. ■

Démonstration. **(du théorème 2.17)**.
Appliquons la dernière procédure RSCSL à la matrice M. On obtient alors une matrice $M_1 = LMR$ de la forme

$$M_1 = \begin{pmatrix} a'_{1,1} & 0 \\ 0 & Y \end{pmatrix}$$

l'élément $a'_{1,1}$ divisant tous les éléments de la matrice Y. On répète alors la même procédure à la matrice Y ce qui donne un matrice $Y_1 = \tilde{L}_1 Y \tilde{R}_1$ avec $\tilde{L}_1 \in SL_{n-1}(A)$ et $\tilde{R}_1 \in SL_{m-1}(A)$. Comme $a'_{1,1}$ divise tous les éléments $y_{i,j}$ de Y, il divise tous les éléments de Y_1 puisque ceux-ci sont combinaisons linéaires d'éléments de Y.
On pose alors $L_1 = \begin{pmatrix} 1 & 0 \\ 0 & \tilde{L}_1 \end{pmatrix} \in SL_n(A)$ et $R_1 = \begin{pmatrix} 1 & 0 \\ 0 & \tilde{R}_1 \end{pmatrix} \in SL_m(A)$ et on continue récursivement. ■

2.3 MODULES LIBRES DE TYPE FINI

Dans ce paragraphe (et les suivants), l'anneau A est toujours un anneau principal (en fait $A = \mathbf{Z}$ ou $A = K[X]$), bien que certaines des notions étudiées ci-dessous aient un sens pour un anneau plus général.

2.3.1. Rang

Définition 2.24. *On dit qu'un A-module M est libre de type fini s'il possède une base finie $(f_1, \ldots, f_n)$.*

Exemples 2.25.

1. Posons $e_1 = (1, 0 \ldots, 0), \ldots, e_n = (0, \ldots, 1)$. Le module produit A^n est libre de base $(e_1, \ldots, e_n)$. Cette base est dite « *base canonique* ».
2. Le $\mathbf{Z}$-module $\mathbf{Z}/n\mathbf{Z}$ n'est pas libre pour $n \neq 0$.

Proposition 2.26. *Soit L un A-module libre ayant une base $(f_1, \ldots, f_n)$.*

1. Le morphisme $\phi : L \to A^n$ défini par $\phi(f_i) = e_i$ est un isomorphisme.

2. L'entier n ne dépend pas de la base choisie. On l'appelle le rang *de L.*

Démonstration. Le fait que le morphisme ϕ soit défini par ses valeurs aux éléments f_i vient de la définition d'une base. Le fait que ce soit un isomorphisme est évident (considérer le morphisme inverse ψ défini par $\psi(e_i) = f_i$).

Pour montrer *2.*, il faut montrer que si l'on a un isomorphisme $\phi : A^n \to A^m$, alors $n = m$. Nous allons nous ramener au cas des espaces vectoriels, et utiliser l'invariance de la dimension. Soit $p \in A$ un élément irréductible (donc non inversible). Le quotient $A/(p)$ est alors un corps k (proposition 1.39). Pour un A-module M, notons pM l'image de la multiplication par p (ensemble des éléments de M de la forme pm pour $m \in M$). Dans le cas du module libre A^n, On a $pA^n \simeq (pA)^n$, et $A^n/pA^n \simeq (A/pA)^n = k^n$ (corollaire 2.8).

Si maintenant $\phi : M \to M'$ est un morphisme de modules, on a $\phi(pM) \subset pM'$, ce qui implique que ϕ « passe aux quotients », *i.e.* que l'on a un diagramme commutatif :

$$\begin{array}{ccc} M & \xrightarrow{\phi} & M' \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ M/pM & \xrightarrow{\overline{\phi}} & M'/pM' \end{array}$$

π et π' étant les morphismes canoniques de passage au quotient. Appliquant ce fait aux modules $M = A^n$, $M' = A^m$ et à l'isomorphisme ϕ, on voit que le morphisme $\overline{\phi}$ est un morphisme surjectif $k^n \to k^m$. On a donc $n \geqslant m$ puisque k est un corps. En échangeant les rôles de n et m, on voit que $n = m$. ■

2.3.2. Sous-modules d'un module libre

Nous allons tout d'abord donner des conséquences de la proposition 2.14.

Proposition 2.27. *Soit G un sous-module de type fini de A^n. Alors G est libre de rang $m \leqslant n$.*

Démonstration. Soit $(v_1, \ldots, v_p)$ un système de générateurs de G, avec $v_i \in A^n$. On peut former une matrice M à coefficients dans A et de taille (p, n) (les lignes de M sont les v_i exprimés dans la base canonique de A^n). En appliquant le corollaire 2.15, on obtient une matrice $M_1 = LM$ avec m lignes non nulles $w_1, \ldots, w_m$ de longueur strictement décroissante (on a donc $m \leqslant n$ et $m \leqslant p$). Les vecteurs w_i $(1 \leqslant i \leqslant m)$ sont dans G (car combinaisons linéaires à coefficients dans A des v_i), libres (car la longueur des w_i est strictement décroissante), et générateurs car la matrice $L \in SL_p(A)$ étant inversible, la relation $M = L^{-1}M_1$ exprime les v_i comme combinaisons linéaires des w_j à coefficients dans A. ■

Théorème 2.28. *Soient L un A-module libre de rang n, $N \subset L$ un sous-module. Alors N est libre de rang $m \leqslant n$.*

Démonstration. On peut supposer que $L = A^n$ (proposition 2.26). D'après la proposition 2.27, il suffit alors de montrer que N est de type fini. Raisonnons par récurrence sur n.

a) $n = 1$. Dans ce cas, N est un idéal de A, donc engendré par un élément a puisque A est supposé principal. On a alors $N = aA$ et la multiplication par a donne un isomorphisme $A \simeq Aa$.

b) Passage de $n-1$ à n. Soit π_1 le morphisme $N \longrightarrow A$ défini par $\pi_1(a_1, \ldots, a_n) = a_1$ (restriction à N de la première projection $A^n \rightarrow A$). L'ensemble $\pi_1(N)$ est alors un sous-module de A, donc un idéal engendré par un élément b_1. On suppose $b_1 \neq 0$, sinon N est contenu dans le sous-module engendré par $(e_2, \ldots, e_n)$ ($(e_1, \ldots, e_n)$ est la base canonique de A^n), isomorphe à A^{n-1} et on peut appliquer l'hypothèse de récurrence. Soit $g_1 \in N$ un élément tel que $\pi_1(g_1) = b_1$. Posons $N_1 = N \cap (Ae_2 \oplus \cdots \oplus Ae_n)$. Montrons que l'on a alors :

$$N = g_1 A \oplus N_1$$

En effet si $x \in g_1 A \cap N_1$, on a $x = \lambda g_1$ ($\lambda \in A$), $\pi_1(x) = \lambda a_1$ et $\pi_1(x) = 0$ puisque $x \in N_1$; on a donc $\lambda = 0$ puisque $a_1 \neq 0$ par hypothèse (A étant principal, il est intègre). On a ainsi $g_1 A \cap N_1 = (0)$.

D'autre part on a $N = g_1 A + N_1$, car si $x \in N$, posons $\pi_1(x) = \mu b_1$ avec $\mu \in A$. On écrit alors $x = \mu g_1 + (x - \mu g_1)$, et comme $\pi_1(x) = \mu \pi_1(g_1)$, on a $x - \mu g_1 \in N_1 = \ker \pi_1$. On a donc bien $N = g_1 A \oplus N_1$ et on applique l'hypothèse de récurrence à N_1 (contenu dans $Ae_2 \oplus \cdots \oplus Ae_n$). ■

2.3.3. Bases adaptées

Donnons maintenant une conséquence du théorème 2.17.

Théorème 2.29. *Soit $N \subset A^n$ un sous-module de A^n. Il existe alors une base $(f_1, \ldots, f_n)$ de A^n et des éléments $a_i \in A$, $1 \leqslant i \leqslant n$ tels que :*

$$\begin{cases} a_1 \mid a_2 \mid \cdots \mid a_n, \\ \text{les } (a_i f_i) \text{ tels que } a_i \neq 0 \text{ forment une base de } N. \end{cases}$$

De plus, la suite des idéaux (a_i) satisfaisant ces conditions est unique (les (a_i) ne dépendent que de N et non de son plongement dans A^n).

Démonstration. On sait que N est libre de rang $m \leqslant n$ (théorème 2.28) ; soit $(g_1, \ldots, g_k)$ un système de générateurs de N avec $m \leqslant k \leqslant n$. En écrivant les vecteurs g_i (développés sur la base canonique de A^n) en colonnes, et en complétant par $n - k$ colonnes de 0 placées au début, on obtient une matrice $M \in \mathcal{M}_n(A)$ (« matrice de passage » dans le cas où $m = n$). Appliquons le théorème 2.17 à la matrice M. Il existe donc $L \in SL_n A$ et $R \in SL_n(A)$ telles que $M' = LMR$ soit réduite avec des éléments $a_{i,i}$ sur la diagonale que l'on note simplement a_i.

Si l'on fixe la base de A^n (qui sauf mention du contraire est la base canonique), une matrice $B \in \mathcal{M}_n(A)$ s'interprète comme une application linéaire de A^n dans A^n que nous noterons encore B. L'application correspondant à la matrice M' se décompose alors en trois applications linéaires :

$$A^n \xrightarrow{R} A^n \xrightarrow{M} A^n \xrightarrow{L} A^n$$

telles que L et R soient inversibles et que l'image de M soit le sous-module N de A^n. Si on note $(e_i)_{1 \leqslant i \leqslant n}$ la base canonique de A^n, on définit $(f_i)_{1 \leqslant i \leqslant n}$ comme l'image inverse de (e_i) par L : $L(f_i) = e_i$ $(1 \leqslant i \leqslant n)$. La famille $(f_i)_{1 \leqslant i \leqslant n}$ est bien une base de A^n puisque L est inversible, et comme $LMR(e_i) = a_i e_i$, on a $MR(e_i) = a_i f_i$, $1 \leqslant i \leqslant n$ (ce qui est une autre façon de définir les f_i), et donc les $(a_i f_i)$ tels que $a_i \neq 0$ forment une base de $\mathrm{Im} M = N$ satisfaisant aux conditions de l'énoncé.

L'unicité des idéaux (a_i) sera démontrée au paragraphe suivant (remarque 2.38). ■

Définition 2.30. *La base $(f_1, \ldots, f_n)$ s'appelle une* base adaptée *au sous-module N de A^n.*

2.4 MODULES DE TYPE FINI SUR UN ANNEAU PRINCIPAL

Définition 2.31. *Soit M un A-module. On dit que $m \in M$ est un* élément de torsion *s'il existe $\lambda \in A, \lambda \neq 0$, tel que $\lambda m = 0$. L'ensemble des éléments de torsion de M est noté M_t. Si $M_t = \{0\}$, on dit que M est sans torsion. Si $M = M_t$, on dit que M est un* module de torsion.

Il est clair que M_t est un sous-module de M : on dit que M_t est le *sous-module de torsion* de M.

Exemple 2.32. Un module libre est sans torsion. Si $a \in A,\ a \neq 0$, le module $A/(a)$ est un module de torsion (tous ses éléments sont annulés par a). En revanche, si $a = 0$, le module $A/(a)$ est isomorphe à A donc libre de rang 1.

Nous allons démontrer le théorème de structure fondamental suivant :

Théorème 2.33. *Soit M un A-module de type fini, M_t son sous-module de torsion. Alors :*

1. *le sous-module M_t est de type fini ;*
2. *il existe un sous-module $L \subset M$ libre de rang r tel que*
$$M = M_t \oplus L;$$
3. *il existe des éléments $a_1, \ldots, a_q$ de A tels que :*
   - *les a_i sont non nuls et non inversibles,*
   - $a_1 | a_2 | \ldots | a_q$,
   - $M_t \simeq A/(a_1) \times \cdots \times A/(a_q)$
   (et donc il existe des sous-modules M_i de M_t tels que $M_i \simeq A/(a_i)$ et que
$$M_t = M_1 \oplus \cdots \oplus M_q);$$
4. *l'entier r et les idéaux $(a_1), \ldots, (a_q)$ sont uniques (ils ne dépendent que du module M).*

Définition 2.34. *L'entier $r = \dim L$ est le* rang *de M. Les idéaux non nuls (a_i) $(1 \leqslant i \leqslant q)$ sont les* facteurs invariants *de M.*

Le théorème 2.33 entraîne immédiatement la réciproque du fait qu'un module libre est sans torsion (dans le cas d'un module de type fini) :

Corollaire 2.35. *Soit M un A-module de type fini sans torsion. Alors M est libre.*

> ***Remarque 2.36.*** Le corps des rationnels $\mathbf{Q}$ est un exemple de $\mathbf{Z}$-module sans torsion et non libre (si $q_1 = a/b$ et $q_2 = c/d$ sont deux rationnels non nuls, on a la relation $bcq_1 - adq_2 = 0$). $\mathbf{Q}$ n'est donc pas un $\mathbf{Z}$-module de type fini, car sinon cela contredirait le corollaire 2.35.

Démontrons maintenant le théorème 2.33.

a) *Existence*. Le module M est par hypothèse de type fini. Soit $(m_1, \ldots, m_n)$ un système (fini) de générateurs de M. Posons $L_1 = A^n$, on peut alors définir un morphisme :
$$f :\ L_1 \to M$$
tel que $f(e_i) = m_i,\ 1 \leqslant i \leqslant n$; ce morphisme est surjectif par définition d'un système de générateurs (remarque 2.2). Soit $N = \ker f$. On peut appliquer le théorème 2.29 au sous-module N de L_1 : il existe une base $(f_1, \ldots, f_n)$ de L_1 et des éléments

$b_i \in A$ tels que $b_1|b_2|\dots|b_n$ et que les $(b_i f_i)$ tels que $b_i \neq 0$ forment une base de N. Supposons que :

- $b_1, \dots, b_k$ soient inversibles,
- $b_{k+1}, \dots, b_{k+q}$ soient non inversibles et non nuls,
- $b_{k+q+1} = \dots = b_n = 0$.

Posons alors $a_i = b_{k+i}$ $(1 \leqslant i \leqslant q)$ et $r = n - q - k$. Le passage au quotient de L_1 par $\ker f$ (en appliquant le corollaire 2.8) donne l'existence de la décomposition de M en $\prod A/(a_i) \times A^r$. Le passage à l'écriture en somme directe des $M_i \simeq A/(a_i)$ et L est alors automatique : *cf.* la remarque 2.2.

b) *Unicité*. Comme $L \simeq M/M_t$, son rang ne dépend que du module M (proposition 2.26).

Il faut montrer maintenant l'unicité des idéaux (a_i) tels que $1 \leqslant i \leqslant q$, *i.e.* la proposition suivante :

Proposition 2.37. *Soit A un anneau principal. On considère un A-module M tel que :*

$$M \simeq \frac{A}{(a_1)} \times \dots \times \frac{A}{(a_q)} \tag{6}$$

où les a_i sont des éléments non nuls et non inversibles de A tels que $a_1|a_2|\dots|a_q$. Alors les idéaux (a_i) sont uniquement déterminés.

Démonstration. Supposons que l'on ait deux décompositions pour le A-module M :

$$M \simeq \frac{A}{(a_1)} \times \dots \times \frac{A}{(a_q)} \simeq \frac{A}{(a'_1)} \times \dots \times \frac{A}{(a'_s)} \tag{7}$$

vérifiant les hypothèses de la proposition.

Rappelons que l'annulateur de M (remarque 2.2), noté ann(M), est l'idéal de A formé des éléments λ qui annulent M. On voit alors immédiatement que ann(M) $= (a_q) = (a'_s)$. On déduit de (7) qu'il existe des sous-modules M_i (resp. M'_j) de M tels que $M_i \simeq \frac{A}{(a_i)}$ (resp. $M'_j \simeq \frac{A}{(a'_j)}$) et

$$M = M_1 \oplus \dots \oplus M_q = M'_1 \oplus \dots \oplus M'_s.$$

Posons $\tilde{M} = M_1 \oplus \dots \oplus M_{q-1}$ et $\tilde{M}' = M'_1 \oplus \dots \oplus M'_{s-1}$; on a $M = \tilde{M} \oplus M_q$ et $M' = \tilde{M}' \oplus M'_s$ avec de plus $M_q \simeq M'_s \simeq \frac{A}{\text{ann}(M)}$. Si on note ϕ un isomorphisme : $M_q \to M'_s$, tout $x \in M$ s'écrit de manière unique comme

$$x = \tilde{x} + x_1 = \tilde{x}' + \phi(x_1)$$

avec $\tilde{x} \in \tilde{M}$, $x_1 \in M_q$, $\tilde{x}' \in \tilde{M}'$.

L'application ψ de $\tilde{M}$ dans $\tilde{M}'$ définie par $\psi(\tilde{x}) = \tilde{x}$‘ est un isomorphisme comme on le voit immédiatement.

On a donc $\tilde{M} \simeq \tilde{M}'$; une récurrence immédiate sur l'entier q achève la preuve. ■

Remarque 2.38. Cette dernière démonstration prouve aussi l'unicité des idéaux (a_i) dans la définition d'une base adaptée (définition 2.30). Soit en effet $N \subset A^n$ un sous-module, $(f_1, \dots f_n)$ une base de A^n et $a_i \in A$ tels que $a_1 | \dots | a_n$, $a_{q+1} = \cdots = a_n = 0$, $a_q \neq 0$ et que les $(a_i f_i)$ $(i \leqslant q)$ forment une base de N. Supposons $a_1, \dots, a_k$ inversibles, a_{k+1} non inversible. Posons $M = A^n/N$. Alors :

$$M \simeq \bigoplus_{i=k+1}^{n} A/(a_i);$$

d'après la proposition 2.37, les idéaux (a_i) , $k+1 \leqslant i \leqslant q$, sont uniquement déterminés. Il en est de même de l'entier $n-q$ qui est le rang du module libre M/M_t, et donc des entiers k et q (puisque n, rang du module libre A^n, fait partie des données).

2.5 MODULES INDÉCOMPOSABLES

Soit M un A-module de torsion de type fini. Nous allons montrer un deuxième « théorème de structure », à savoir que M peut se décomposer en une somme directe de modules « indécomposables ».

Définition 2.39. *Un A-module M est dit* indécomposable *s'il n'est pas isomorphe à la somme directe de deux A-modules non nuls.*

Proposition 2.40. *Soit M un A-module de type fini ; les conditions suivantes sont équivalentes :*

1. *le module M est indécomposable ;*
2. *$M \simeq A$, ou il existe un élément irréductible $p \in A$ et un entier $\alpha > 0$ tels que :*

$$M \simeq A/(p^\alpha).$$

Démonstration. *1.* $\Rightarrow$ *2.* D'après le théorème 2.33 on peut supposer $M = A/(a)$; si l'élément a possède au moins deux facteurs irréductibles, il résulte du lemme chinois que M n'est pas indécomposable.

2. $\Rightarrow$ *1.* L'anneau A étant intègre, il est clair que le A-module A est indécomposable.

Si $\alpha > 0$, les sous-modules de $\tilde{M} = A/(p^\alpha)$ sont engendrés par les images dans $\tilde{M}$ des éléments p^γ pour $\gamma \leqslant \alpha$ (proposition 1.36 ; la démonstration est la même dans tout anneau principal). Si M_1 et M_2 sont deux tels sous-modules, on a toujours $M_1 \subset M_2$ ou $M_2 \subset M_1$; ils ne peuvent donc pas être en somme directe. ■

Définition 2.41. *Soient M un A-module, $p \in \mathcal{P}$ un élément irréductible. On note $M(p)$ l'ensemble des éléments $x \in M$ annulés par une puissance de p, i.e. tels qu'il existe un entier α avec $p^\alpha x = 0$. Un tel x est appelé* élément de p-torsion.

Il est clair que $M(p)$ est un sous-module de M.

Avant d'énoncer le deuxième théorème de structure, rappelons que l'annulateur de M (remarque 2.2) se note ann(M). Si M est un A-module de torsion de type fini, on a ann$(M) \neq (0)$, car si $(e_1, \dots, e_k)$ est un système de générateurs de M et $\lambda_i \in A$ sont des éléments non nuls tels que $\lambda_i e_i = 0$, l'élément non nul $\lambda = \prod_{i=1}^{k} \lambda_i$ appartient à ann(M).

Pour les résultats d'unicité, nous aurons besoin de fixer un système représentatif $\mathcal{P}$ d'éléments irréductibles de A (par exemple les polynômes irréductibles unitaires si $A = K[X]$).

Théorème 2.42. *Soit M un A-module de torsion de type fini, $(a) = \mathrm{ann}(M)$ son annulateur. Alors :*

1. $$M = \bigoplus_{p_i \in \mathcal{P},\ p_i | a} M(p_i)$$
   et $M(p_i) \neq (0)$ pour chaque élément irréductible p_i tel que $p_i | a$;
2. *Il existe une suite d'entiers $\nu_{i1} \leqslant \nu_{i2} \leqslant \cdots \leqslant \nu_{ik}$ unique telle que, pour chaque élément irréductible $p_i \in \mathcal{P},\ p_i | a$:*
   $$M(p_i) \simeq \prod_{j=1}^{k} A/(p_i^{\nu_{ij}}))$$
   (ce qui est équivalent à l'existence de sous-modules $M_{ij} \subset M(p_i)$ tels que $M(p_i) = \bigoplus M_{ij}$ et $M_{ij} \simeq A/(p_i^{\nu_{ij}}))$;
3. *la décomposition :*
   $$M \simeq \prod_{i,j} A/(p_i^{\nu_{ij}})$$
   est l'unique décomposition de M en produit de modules indécomposables (à isomorphisme près et à l'ordre près des facteurs).

Démonstration. Le théorème 2.33 donne une décomposition :

$$M \simeq \bigoplus_{j=1}^{q} M_j \tag{8}$$

en somme directe de sous-modules monogènes $M_j \simeq A/(a_j)$, avec $a_1 | \dots | a_q$. Comme l'annulateur d'un module $A/(a_j)$ est (évidemment) l'idéal (a_j), on voit que l'annulateur de M est l'idéal $(a) = (a_q)$ puisque $a_j | a_q$ pour tout j.
Le lemme suivant est une version du « lemme chinois ». ■

Lemme 2.43. *Soit $a \in A$ un élément non nul, $a = \lambda \prod_{i=1}^{s} p_i^{\nu_i}$ sa décomposition en facteurs irréductibles ($\lambda \in A^*, p_i \in \mathcal{P}$). On a alors une décomposition en somme directe :*

$$A/(a) = \bigoplus_{i=1}^{s} M_i$$

avec $M_i \simeq A/(p_i^{\nu_i})$.

Démonstration. La démonstration est la même que celle du théorème chinois (théorème 1.48). ■

On déduit de (8) et du lemme précédent une décomposition de M en somme directe :

$$M = \bigoplus M_{ij} \text{ avec } M_{ij} \simeq A/(p_i^{\nu_{ij}})$$

les p_i étant des diviseurs de a_q, les p_i et les ν_{ij} étant déterminés de manière unique (car les idéaux (a_i) sont déterminés de manière unique et la décomposition du lemme 2.43 est unique à l'ordre près des facteurs). Les M_{ij} étant indécomposables, il suffit maintenant pour démontrer le théorème de montrer le lemme suivant :

Lemme 2.44. *Avec les notations ci-dessus, on a* $M(p_i) = \bigoplus_j M_{ij}$.

Démonstration. Pour $p_i \neq p_j$, p_i et $p_j^{\nu_{jk}}$ sont premiers entre eux ; l'image de p_i dans $A/(p_j^{\nu_{jk}}) = M_{jk}$ est donc inversible ce qui implique $M(p_i) \cap M_{jk} = (0)$. On a donc $M(p_i) = \bigoplus_j M_{ij}$. ■

Cela achève la démonstration du théorème.

Remarques 2.45. Pour la commodité du lecteur, nous allons récapituler les théorèmes de structure pour un module M de type fini sur un anneau principal.

1. Si $M_t \subset M$ est le sous-module de torsion de M, il est de type fini et l'on a :

   $$M = M_t \oplus L$$

   où L est un module libre de rang fini.
2. Il existe des éléments $a_1, \ldots, a_q$ de A tels que
   - les a_i sont non nuls et non inversibles ;
   - $a_1 | a_2 | \ldots | a_q$,

   tels que :

   $$M_t \simeq A/(a_1) \times \cdots \times A/(a_q)$$

   (théorème 2.33) ; l'annulateur de M_t est alors l'idéal (a_q) ; les idéaux (a_i) ne dépendent que du A-module M_t.
3. Soit M_t un module de torsion de type fini,(a) son annulateur, $\mathcal{P}$ un système représentatif d'éléments extrémaux de A ; on a :

   $$M_t = \bigoplus_{p_i \in \mathcal{P},\, p_i | a} M_t(p_i),$$

   $M_t(p_i)$ désignant l'ensemble des éléments de p_i-torsion de M_t (théorème 2.42).

4. Si $p_i \in \mathcal{P}, p_i | a$, il existe une suite croissante d'entiers $\nu_{i1} \leqslant \nu_{i2} \leqslant \cdots \leqslant \nu_{ik}$ unique telle que :
$$M_t(p_i) \simeq \prod_{j=1}^{k} A/(p_i^{\nu_{ij}})$$
(théorème 2.42).

Exemple 2.46. Prenons $A = \mathbf{Z}$, $M = M_t = \mathbf{Z}/96\mathbf{Z} \times \mathbf{Z}/72\mathbf{Z} \times \mathbf{Z}/10\mathbf{Z}$. On a $96 = 2^5 \times 3$, $72 = 2^3 \times 3^2$, d'où :
$$M \simeq \mathbf{Z}/32\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$$
par le théorème chinois. On a donc :
$$\begin{array}{lcccccc} M(2) & \simeq & \mathbf{Z}/32\mathbf{Z} & \times & \mathbf{Z}/8\mathbf{Z} & \times & \mathbf{Z}/2\mathbf{Z} \\ M(3) & \simeq & \mathbf{Z}/9\mathbf{Z} & \times & \mathbf{Z}/3\mathbf{Z} & & \\ M(5) & \simeq & \mathbf{Z}/5\mathbf{Z}\,. & & & & \end{array} \tag{9}$$
Pour trouver la décomposition du théorème 2.42, on lit le tableau ci-dessus « en lignes », et on trouve $M = M(2) \oplus M(3) \oplus M(5)$.

Pour trouver la décomposition du théorème 2.33, on lit le tableau ci-dessus « en colonnes » (en commençant par la fin si on veut suivre l'ordre de l'énoncé), et on regroupe les facteurs de chaque colonne en utilisant le théorème chinois. On trouve donc ici $a_3 = 32 \times 9 \times 5 = 1\,440$ (annulateur de M), $a_2 = 8 \times 3 = 24$, $a_1 = 2$, d'où la décomposition $M \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/24\mathbf{Z} \times \mathbf{Z}/1\,440\mathbf{Z}$.

2.5.1. Cas des groupes abéliens

Comme nous l'avons remarqué plus haut, tout groupe abélien G est canoniquement muni d'une structure de $\mathbf{Z}$-module. Nous allons reformuler certains des résultats précédents dans le cas particulier des groupes abéliens.

Lemme 2.47. *Soit G un groupe abélien de type fini. Les conditions suivantes sont équivalentes :*
1. G est un groupe de torsion (i.e. $G = G_t$) ;
2. G est de cardinal fini (on dit que G et un groupe fini).

Démonstration. On a $G = G_t \oplus L$ avec L libre d'après le théorème 2.33. Si G est de cardinal fini, on a nécessairement $L = (0)$.

Réciproquement, le théorème 2.33 (ou le théorème 2.42) montre que si G est de torsion, il est somme directe finie de groupes finis, donc il est de cardinal fini égal au produit des cardinaux de ces groupes. ■

Les résultats suivants sont des conséquences directes des propriétés ci-dessus. Leur démonstration est laissée en exercice.

Rappelons que si G est un groupe abélien et $p \in \mathbf{Z}$ un nombre premier, on note $G(p)$ l'ensemble des $g \in G$ annulés par une puissance de p (éléments de p-torsion).

Proposition 2.48. *Soit G un groupe abélien fini d'ordre n.*

1. *L'annulateur de G est engendré par un diviseur de n qui a les mêmes diviseurs premiers ;*
2. *si p est un diviseur premier de n, G contient un élément d'ordre p ;*
3. *supposons $G = G(p)$. Alors il existe une suite unique de nombres entiers $(\alpha_1, \ldots, \alpha_q)$ telle que $1 \leqslant \alpha_1 \leqslant \cdots \leqslant \alpha_q$ et*
$$G \simeq \prod_{i=1}^{q} \mathbf{Z}/p^{\alpha_i}\mathbf{Z};$$
4. $$G = \bigoplus_{p_i | n} G(p_i);$$
5. *cas particulier $G = \mathbf{Z}/n\mathbf{Z}$: si $G = \mathbf{Z}/n\mathbf{Z}$ et $n = p_1^{\nu_1} \ldots p_s^{\nu_s}$ on a $G(p_i) \simeq \mathbf{Z}/p_i^{\nu_i}\mathbf{Z}$;*
6. *si G est d'ordre n, $G(p) \neq (0)$ si et seulement si p divise n, $G = G(p)$ si et seulement si n est une puissance de p.*

Cette proposition permet de classer à isomorphisme près tous les groupes abéliens finis d'ordre n donné. On procède de la manière suivante. Soit G un groupe d'ordre n.

1. On écrit $n = p_1^{\nu_1} \ldots p_s^{\nu_s}$ avec p_i premiers, ν_i entiers ;
2. on a alors $G \simeq G(p_1) \oplus \cdots \oplus G(p_s)$;
3. pour chaque entier i, $1 \leqslant i \leqslant s$ il existe une suite croissante (ν_{ij}) unique d'entiers > 0 tels que $\sum_j \nu_{ij} = \nu_i$ et $G(p_i) \simeq \bigoplus_j \mathbf{Z}/p_i^{\nu_{ij}}\mathbf{Z}$;
4. deux groupes d'ordre n sont isomorphes si et seulement si tous les p_i et les entiers ν_{ij} sont les mêmes.

> ***Remarque 2.49.*** Soient p un nombre premier, ν un nombre entier. L'ensemble des classes d'isomorphismes des groupes d'ordre ν de la forme $G(p)$ correspond donc bijectivement à l'ensemble des suites (ν_j) croissantes telles que $\sum \nu_j = \nu$.

L'ensemble des groupes $G = G(p_i))$ d'ordre ν_i (à isomorphisme près) correspond donc bijectivement à l'ensemble des suites (ν_{ij}) croissantes en j telles que $\Sigma_j \nu_{ij} = \nu_i$.

Exemple 2.50. Classement à isomorphisme près de tous les groupes abéliens d'ordre 108.

On a $108 = 2^2 \times 3^3$. Si G est d'ordre 108, on $G = G(2) \oplus G(3)$ avec $G(2)$ d'ordre 4 et $G(3)$ d'ordre 27. Il y a à isomorphisme près deux possibilités pour $G(2)$: $\mathbf{Z}/4\mathbf{Z}$ et $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (qui correspondent aux suites (2) et $(1,1)$), et trois pour $G(3)$: $\mathbf{Z}/27\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z}$ et $(\mathbf{Z}/3\mathbf{Z})^3$ (qui correspondent respectivement aux suites (3), $(1,2)$ et $(1,1,1)$) ; il y a donc à isomorphisme près six groupes abéliens d'ordre 108.

EXERCICES

Les solutions des exercices et problèmes sont données en fin d'ouvrage.

ANNEAUX – CALCUL MATRICIEL

Exercice 2.1. On considère les sous-groupes de $\mathbf{Z}^2$ suivants :

$G_1 =< 2e_1, 3e_2 >$, $G_2 =< 2e_1, 3e_1 + 4e_2 >$ et $G_3 =< 2e_1 + 2e_2, 2e_1 + 6e_2 >$, (e_1, e_2) désignant la base canonique de $\mathbf{Z}^2$. On explicitera dans chacun des cas une base adaptée de $\mathbf{Z}^2$ au sous-groupe G_i et l'on déterminera les facteurs invariants de $\mathbf{Z}^2/G_i$.

Exercice 2.2. Soit (e_1, e_2, e_3) la base canonique de $\mathbf{Z}^3$ et soit $L \subset \mathbf{Z}^3$ le sous-groupe engendré par les vecteurs

$$e'_1 := 2e_1 - e_2 + e_3, \quad e'_2 := e_1 + 4e_2 - e_3, \quad e'_3 := 3e_1 - e_2 - e_3.$$

Trouver une base adaptée au sous-module L de $\mathbf{Z}^3$ et décrire $\mathbf{Z}^3/L$.

Exercice 2.3. Soit $x = (n_1, \ldots, n_p) \in \mathbf{Z}^p$.

1. Montrer que les conditions suivantes sont équivalentes :
   (i) PGCD $(n_1, \ldots, n_p) = 1$.
   (ii) Le vecteur x fait partie d'une base de $\mathbf{Z}^p$.
   (iii) Il existe $A \in SL_p(\mathbf{Z})$ telle que $A^t x = {}^t(1, 0, \ldots, 0)$.
2. On pose $p = 4$ et $x = (10, 6, 7, 11)$. Compléter x en une base de $\mathbf{Z}^4$.

Exercice 2.4. Résoudre dans $\mathbf{Z}^4$ le système :

$$\begin{pmatrix} 3 & 2 & 3 & 4 \\ 1 & -2 & 1 & -1 \end{pmatrix} X = \begin{pmatrix} -8 \\ -3 \end{pmatrix}$$

STRUCTURE DES GROUPES ABÉLIENS FINIS

Exercice 2.5. Montrer qu'il y a (à isomorphisme près) trois groupes abéliens d'ordre 8.

Exercice 2.6. Déterminer (à isomorphisme près) tous les groupes abéliens d'ordre 72 ainsi que leurs facteurs invariants.

Exercice 2.7. Donner les facteurs invariants ainsi que la décomposition en modules indécomposables du $\mathbf{Z}$-module :

$$M = \mathbf{Z}/20\mathbf{Z} \times \mathbf{Z}/18\mathbf{Z} \times \mathbf{Z}/12\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$$

Exercice 2.8. Déterminer tous les groupes abéliens de cardinal $2^4 3^2 5$ sous forme de produits de modules indécomposables ainsi que leurs facteurs invariants.

PROBLÈMES

Problème 2.1. *Sous-groupes de* $\mathbf{Z}^n$

Soient n un entier positif et $G \subset \mathbf{Z}^n$ un sous-groupe de rang n. Soit $(g_1, \cdots, g_n)$ une base de G ; on note M la matrice de passage de cette base dans la base canonique de $\mathbf{Z}^n$ (*i.e.* la matrice ayant pour colonnes les g_i développés dans la base canonique).

1. Montrer que le groupe $\mathbf{Z}^n/G$ est fini.
2. Montrer que card$((\mathbf{Z}^n/G)) = |\det M|$.
3. Soit H un groupe abélien engendré par trois éléments h_1, h_2, h_3 soumis aux relations :

$$3h_1 + h_2 + h_3 = 0$$

$$25h_1 + 8h_2 + 10h_3 = 0$$

$$46h_1 + 20h_2 + 11h_3 = 0$$

   Montrer que card$(H) = 19$ puis que $H \simeq \mathbf{Z}/19\mathbf{Z}$.
4. Trianguliariser la matrice

$$\begin{pmatrix} 3 & 1 & 1 \\ 25 & 8 & 10 \\ 46 & 20 & 11 \end{pmatrix}$$

   en multipliant à droite par une matrice de $SL_3(\mathbf{Z})$ que l'on précisera.
5. En déduire un isomorphisme $\varphi : H \simeq \mathbf{Z}/19\mathbf{Z}$ et préciser les valeurs de $\varphi(h_1), \varphi(h_2), \varphi(h_3)$.

Problème 2.2. *Étude de* $U_n := (\mathbf{Z}/n\mathbf{Z})^*$

1. Montrer que le groupe Aut$(\mathbf{Z}/n\mathbf{Z})$ des automorphismes du groupe $\mathbf{Z}/n\mathbf{Z}$ est isomorphe à U_n. Noter en particulier que Aut$(\mathbf{Z}/n\mathbf{Z})$ est abélien.
2. Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Prouver que $U_n \simeq \prod_{i=1}^r U_{p_i^{\alpha_i}}$.
3. Soit p premier impair et $\alpha \geqslant 2$.
   (i) Montrer que pour tout $k \in \mathbf{N}$, il existe $\lambda_k \in \mathbf{N}\backslash\{0\}$ premier avec p tel que $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$. Quel est alors l'ordre de $1+p$ dans U_{p^α} ?
   (ii) Montrer que $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique d'ordre $p-1$.
   (iii) En considérant le morphisme naturel $\psi : U_{p^\alpha} \to U_p$, montrer que U_{p^α} contient un élément x d'ordre $p-1$.
   (iv) Montrer alors en utilisant le théorème de structure des groupes abéliens finis que U_{p^α} est cyclique et donc isomorphe à

$$\mathbf{Z}/\varphi(p^\alpha)\mathbf{Z} \simeq \mathbf{Z}/p^{\alpha-1}(p-1)\mathbf{Z}.$$

   Construire explicitement un tel isomorphisme en utilisant l'élément x.

(v) De manière indépendante, soit $g \in U_{p^\alpha}$ tel que $\psi(g)$ soit un générateur de U_p et tel que $g^{p-1} \neq 1 \mod p^2$. Montrer alors que g est un générateur de U_{p^α}. Dans le cas où $g^{p-1} \equiv 1 \mod p^2$, montrer que $g+p$ est un générateur de U_{p^α}.

4. Le cas $p = 2$.

(i) Déterminer U_2 et U_4.

(ii) Soit $\alpha \geqslant 3$ et $k \in \mathbf{N}$. Montrer que $5^{2^k} = 1 + {}_k 2^{k+2}$ avec ${}_k$ impair. En déduire l'ordre de 5 dans U_{2^α}.

(iii) En utilisant le théorème de structure des groupes abéliens finis et en comptant les éléments d'ordre 2, montrer que U_{2^α} est isomorphe à $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2^{\alpha-2})$. Construire explicitement un tel isomorphisme.

5. Caractériser alors les entiers n tels que U_n soit cyclique.

Chapitre **3**

Réduction des endomorphismes

Ce chapitre utilise les résultats du chapitre 2 (avec l'anneau de polynômes $K[X]$ comme anneau de base) pour étudier les endomorphismes d'un espace vectoriel de dimension finie. On arrive ainsi facilement à la définition des invariants de similitude, au théorème de Cayley-Hamilton, à la forme réduite de Jordan, etc.

3.1 L'ANNEAU $K[X]$

Soit K un corps (commutatif). On note $K[X]$ l'anneau des polynômes sur le corps K. Si $P \in K[X]$, $P \neq 0$, on note $\deg(P)$ son degré, et $\mathrm{dom}(P)$ son coefficient dominant (coefficient du terme de plus haut degré). On a donc $\mathrm{dom}(P) \neq 0$ par définition. Rappelons que le degré d'un polynôme P n'est défini que si $P \neq 0$. On identifie K avec l'ensemble des polynômes de degré 0 (auquel on ajoute l'élément 0). Le groupe multiplicatif des éléments inversibles de $K[X]$ est alors K^*.

Proposition 3.1. *L'anneau $K[X]$ est euclidien pour le sthasme $\phi(P) := \deg(P)$.*

Démonstration. Les propriétés du degré montrent immédiatement que $K[X]$ est un anneau intègre.

Soient C et D deux polynômes donnés avec $D \neq 0$. On cherche (Q, R) tels que $C = DQ + R, \quad R = 0 \text{ ou } \deg(R) < \deg(D)$.

L'algorithme suivant donne la réponse :

– si $\deg(R) \geqslant \deg(D)$ (et donc $R \neq 0$), on fait :
$(Q, R) := (Q + E, R - ED)$ avec $E = \dfrac{\mathrm{dom}(R)}{\mathrm{dom}(D)} X^{\deg(R)-\deg(D)}$;

– sinon, l'algorithme est terminé. ■

Remarques 3.2.

1. Il est immédiat de voir que dans la division euclidienne définie plus haut, il y a unicité du quotient et du reste.
2. Si les polynômes C et D sont à coefficients dans un anneau A intègre (par exemple $\mathbf{Z}$) et si $\mathrm{dom}(D)$ est inversible, l'algorithme produit des polynômes à coefficients dans A.
3. L'anneau $\mathbf{Z}[X]$ n'est pas principal (vérifier que l'idéal $(2, X)$ n'est pas principal).

La proposition 3.1 implique que l'anneau $K[X]$ est principal donc factoriel. On définit $\mathcal{P}$ comme l'ensemble des polynômes irréductibles unitaires de degré > 0. On a alors :

Proposition 3.3. *Tout $Q \in K[X]$ non nul s'écrit de manière unique (à l'ordre près des facteurs) :*

$$Q = \lambda \prod_{i=1}^{s} P_i^{\nu_i}$$

avec $\lambda \in K^*$, $P_i \in \mathcal{P}$ et ν_i des entiers positifs.

Étudions maintenant le quotient de l'anneau $K[X]$ par un idéal (Q).

Proposition 3.4. *Soit $Q \in K[X]$ un polynôme de degré d. Alors l'anneau quotient $E = K[X]/(Q)$ est un espace vectoriel de dimension d sur le corps K (la structure d'espace vectoriel est propagée par celle de $K[X]$ de façon à ce que le morphisme canonique $\pi : K[X] \to E$ soit une application K-linéaire). Si on pose $x = \pi(X)$, et si l'on note encore 1 l'élément $\pi(1)$, une base du K-espace E est $(1, x, \ldots, x^{d-1})$.*

Démonstration. Immédiate, laissée au lecteur. ■

Cette proposition sera réénoncée au chapitre 6 (proposition 6.8).

3.2 POLYNÔME MINIMAL

Soient E un espace vectoriel de dimension finie n sur un corps K. Nous noterons A l'anneau $K[X]$. Fixons $u \in \mathrm{End}_K(E)$ un endomorphisme de E ; cette donnée fait de E un A-module (avec $A = K[X]$) de la manière suivante : E est déjà un groupe abélien pour l'addition ; pour définir l'opération de multiplication d'un élément $x \in E$ par un polynôme $P = a_0 + \cdots + a_p X^p$, on considère l'endomorphisme

$P(u) = a_0 I + a_1 u + \cdots + a_p u^p$ (I est l'identité et u^p est l'endomorphisme $u \circ u \circ \cdots \circ u$ p fois). On pose $P.x = P(u)(x)$ (image de x par l'endomorphisme $P(u)$). Il est immédiat que ces opérations satisfont les axiomes des modules. La multiplication par les constantes a_i est définie par la structure d'espace vectoriel de E. Il s'en suit que la structure de module de E prolonge celle d'espace vectoriel : si $a_0 \neq 0 \in K$, la multiplication par a_0 d'un élément de E (définie car E est un espace vectoriel) est la même si on considère E comme un A-module et a_0 comme un polynôme de degré 0. Nous noterons E_u l'espace vectoriel E muni de la structure de A-module que nous venons de décrire (cette structure dépend de l'endomorphisme u).

Lemme 3.5.

1. Le A-module E_u est un module de torsion de type fini.
2. Les sous-modules de E_u sont les sous-espaces vectoriels de E stables par u.

Démonstration. Un système de générateurs de E en tant qu'espace vectoriel est *a fortiori* un système de générateurs de E_u, car si $(e_1, \ldots, e_n)$ engendrent E sur K, ils engendrent *a fortiori* E_u sur A (tout $x \in E$ peut s'écrire $\sum \lambda_i e_i$, et les λ_i non nuls peuvent être considérés comme des polynômes de degré zéro). E_u est donc un A module de type fini, évidemment de torsion car on peut appliquer à E_u le théorème 2.33 : $E_u \simeq E_{u_t} \oplus L$, L étant un A-module libre. Mais $L = 0$, puisque E_u est de dimension finie sur K. Le point *2.* est évident. ■

Le A-module de type fini E_u étant de torsion, il a un annulateur non réduit à 0.

Définition 3.6. *On appelle* polynôme minimal *de u le polynôme unitaire générateur de l'idéal annulateur de E_u ; on note ce polynôme q_u.*

On a alors :

Lemme 3.7. *Tout polynôme Q tel $Q(u) = 0$ est divisible par q_u.*

Démonstration. $Q(u) = 0$ est équivalent au fait que $Q \in (q_u) = \mathrm{ann}(E_u)$. ■

Rappelons qu'à l'endomorphisme u est attaché un autre polynôme, son polynôme caractéristique $\chi_u(X)$ qui est de degré n. Pour le calculer, on fixe une base (e) de E, et on considère la matrice $M_{(e)}(u)$ qui représente u dans la base (e). On a alors $\chi_u(X) = \det(XI - M_{(e)}(u))$ (ce déterminant ne dépend pas de la base choisie).

Remarques 3.8.

1. L'idéal (q_u), annulateur de E_u, est le dernier facteur invariant du A-module E_u (définition 2.34).
2. Tout endomorphisme du A-module E_u est en particulier K-linéaire et est donc un endomorphisme du K-espace vectoriel E. Réciproquement, un endomorphisme K-linéaire $E \to E$ est aussi un endomorphisme du A-module E_u si et seulement s'il commute avec u, comme on le voit immédiatement.

3.3 ESPACES CYCLIQUES

Définition 3.9. *Soit E un espace vectoriel de dimension n sur K, muni d'un endomorphisme u. On dit que E_u est* monogène *(on dit aussi* cyclique *par analogie avec les groupes cycliques) s'il existe un élément $v \in E$ qui engendre le A-module E_u.*

Proposition 3.10. *Soit E un espace vectoriel de dimension n, u un endomorphisme. Alors les conditions suivantes sont équivalentes :*

1. *le A-module E_u est cyclique ;*
2. *il existe un polynôme unitaire (donc non nul) Q tel que $E_u \simeq A/(Q)$. On a alors $Q = q_u$;*
3. *il existe une base $(e) = (e_1, \dots, e_n)$ de E dans laquelle la matrice de u est de la forme :*
$$M_e(u) = \begin{pmatrix} 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & \dots & 0 & a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & a_{n-1} \end{pmatrix}.$$
4. *$q_u(X) = \chi_u(X)$.*

Si ces conditions sont réalisées, on a :
$$q_u(X) = \chi_u(X) = X^n - a_{n-1}X^{n-1} - \dots - a_1X - a_0.$$

Définition 3.11. *La matrice ci-dessus s'appelle la* matrice compagnon *du polynôme $X^n - a_{n-1}X^{n-1} - \dots - a_1X - a_0$ qui est son polynôme caractéristique.*

Démonstration.
1. $\Rightarrow$ 2. Supposons E_u cyclique, et soit $v \in E$ qui engendre E_u (sur A). On a donc un morphisme surjectif $\phi : A \to E_u$ qui à un polynôme $P \in A$ fait correspondre $P(u)(v) \in E$, que l'on note aussi $P.v$. Le noyau de ϕ est engendré par un polynôme unitaire $Q(X)$ (on a alors $A/(Q) \simeq E_u$, *cf.* le corollaire 2.5). Montrons que $Q = q_u$. On a $q_u.y = 0 \ \forall \ y \in E$ par définition du polynôme minimal et donc en particulier $q_u.v = 0$, et donc $Q|q_u$ puisque Q engendre par hypothèse l'idéal des polynômes qui annulent l'élément v. Réciproquement, si $y \in E$, on a $y = R.v$ pour un polynôme $R \in A$ par hypothèse, et $Q.y = QR.v = RQ.v = 0$ puisque par hypothèse $Q.v = 0$, et donc $q_u|Q$ puisque q_u est l'annulateur de E et que Q annule tout $y \in E$. On a donc bien $Q = q_u$ (car ils sont tous les deux unitaires), ce qui implique que $A/(q_u) \simeq E_u$.
2. $\Rightarrow$ 3. On a $n = \dim E = \deg(Q)$ (proposition 3.4). Soit $v \in E$ l'image de 1 par l'isomorphisme $A/(Q) \to E_u$. On voit immédiatement que les vecteurs $v, u.v, u^2.v, \dots, u^{n-1}.v$ forment une base de E (proposition 3.4). Dans cette base, la matrice de l'endomorphisme u a bien la forme décrite.

3. $\Rightarrow$ *1.* Soit $(e) = (e_1, \ldots, e_n)$ la base dans laquelle u est représenté par la matrice de l'énoncé. Alors si l'on pose $v = e_1$, on voit tout de suite que
$e_i = u(e_{i-1}) = u^{i-1}(v) = X^{i-1}.v$ pour $2 \leqslant i \leqslant n$ et donc que E est cyclique.
3. $\Rightarrow$ *4.* Le polynôme $\chi_u(X)$ annule $v = e_1$ (on exprime que $u(e_n) = u^n(v) = X^n.v$ est donné par la dernière colonne de la matrice), donc il est divisible par q_u (qui est aussi l'annulateur de e_1). Comme il est de plus unitaire et de même degré n, il est égal à q_u.
L'implication *4.* $\Rightarrow$ *1.* sera montrée au paragraphe suivant (corollaire 3.15). ■

Supposons les conditions ci-dessus réalisées. Le calcul du déterminant de $XI - M_e(u)$ montre que $\chi_u(X) = X^n - a_{n-1}X^{n-1} - \cdots - a_1X - a_0$.

3.4 INVARIANTS DE SIMILITUDE

Avec les hypothèses ci-dessus, appliquons le théorème 2.33 au A-module E_u. On a alors l'énoncé suivant :

Théorème 3.12. *Il existe une décomposition de E_u en sous-modules (i.e. une décomposition de E en sous-espaces stables par u) :*

$$E_u = E_1 \oplus E_2 \oplus \cdots \oplus E_n$$

telle que :

1. E_i est cyclique, isomorphe à $\frac{K[X]}{(P_i)}$ (avec $P_i \in K[X]$ unitaire),

2. $P_1 | P_2 | \ldots | P_n$.

Alors le polynôme minimal de u est P_n et le polynôme caractéristique de u est $\chi_u(X) = \prod_{1 \leqslant i \leqslant n} P_i(X)$.
De plus la suite des P_i est uniquement déterminée (i.e. pour toute décomposition de E_u en sous-modules vérifiant 1. et 2., les polynômes P_i sont les mêmes).

> ***Remarque 3.13.*** Si $d_i = \deg P_i$, on a $d_1 + \cdots + d_n = n = \deg \chi_u(X)$ (rappelons que l'espace vectoriel E est de dimension n). Les premiers d_i sont donc en général nuls (et les premiers polynômes P_i égaux à 1).

Démonstration. **(du théorème)**.
On va appliquer le théorème 2.33 au $K[X]$-module E_u en prenant un système de générateurs avec n éléments (qui existe toujours puisque un système de générateurs du K-espace vectoriel E est *a fortiori* un système de générateurs du $K[X]$-module E_u).
Supposons que $P_1 = P_2 = \cdots = P_q = 1,\ P_{q+1} \neq 1$. Le théorème 2.33 appliqué au A-module E_u donne alors une décomposition

$$E_u = E_{q+1} \oplus \cdots \oplus E_n$$

en sous-modules cycliques (ou monogènes), $E_i \simeq A/(P_i)$, avec $P_{q+1}|P_{q+2}|\dots|P_n$ déterminés de manière unique (car on les suppose unitaires). On a donc $P_n = q_u$ puisque P_n est l'annulateur (unitaire) de E_u. Cette décomposition est en particulier une décomposition de l'espace vectoriel E en somme directe : $E = \bigoplus_{i=q+1}^{n} E_i$. Choisissons dans chaque E_i une base $(e)_i$ dans laquelle la matrice de $u|_{E_i}$ soit représentée par la matrice compagnon $C_i = M_{e_i}(u_{|E_i})$ de la proposition 3.10. La matrice de u dans la base $(e) = \Big((e)_{q+1}, \dots, (e)_n\Big)$ est alors la matrice diagonale par blocs :

$$M_e(u) = \begin{pmatrix} C_{q+1} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & C_n \end{pmatrix} \tag{1}$$

Son polynôme caractéristique est donc le produit des polynômes caractéristiques des matrices C_i : on a $\chi_u(X) = \prod_{q+1\leqslant i\leqslant n} P_i(X) = \prod_{1\leqslant i\leqslant n} P_i(X)$. ■

Nous dirons qu'une base (e) vérifiant la propriété précédente est une *base adaptée* à u. Nous venons en particulier de démontrer les deux résultats suivants :

Corollaire 3.14. *(« Théorème de Cayley-Hamilton ») Soit u un endomorphisme d'un espace vectoriel E de dimension finie sur un corps K. Alors :*

1. $q_u(X)|\chi_u(X)$,
2. *ces deux polynômes ont les mêmes facteurs irréductibles.*

Corollaire 3.15. *L'espace E_u est cyclique si et seulement si $\chi_u(X) = q_u(X)$.*

Définition 3.16. *Les polynômes unitaires P_i sont appelés les* invariants de similitude *de l'endomorphisme u.*

Les invariants de similitude de l'endomorphisme u sont donc par définition les générateurs unitaires des facteurs invariants du $K[X]$-module E_u, avec cette différence que si $n = \dim_K E$, il y a n invariants de similitude dont certains peuvent être égaux à 1.

Cette définition est justifiée par la proposition suivante :

Proposition 3.17. *Soient u_1 et u_2 deux endomorphismes de l'espace vectoriel de dimension finie E sur le corps K. Les conditions suivantes sont équivalentes :*

1. *Les endomorphismes u_1 et u_2 ont les mêmes invariants de similitude.*
2. *Les A-modules E_{u_1} et E_{u_2} sont isomorphes.*
3. *Les endomorphismes u_1 et u_2 sont conjugués.*

Rappelons que deux endomorphismes u_1 et u_2 sont *conjugués* s'il existe un endomorphisme G de E inversible tel que $u_1 = G^{-1}u_2G$, et que deux matrices M_1 et M_2 sont semblables s'il existe une matrice inversible Q telle que $M_1 = Q^{-1}M_2Q$.

Démonstration. Remarquons tout d'abord que deux endomorphismes sont conjugués si et seulement s'ils sont représentés par la même matrice dans deux bases (éventuellement) différentes.

1. $\Rightarrow$ *2.* Il existe deux bases $(e)_1$ et $(e)_2$ telles que dans chaque base $(e)_i$ $(1 \leqslant i \leqslant 2)$ l'endomorphisme u_i soit représenté par la même matrice (1) du théorème 3.12. L'application K-linéaire ϕ telle que $\phi(e_{1i}) = (e_{2i})$ $(1 \leqslant i \leqslant n)$ est un isomorphisme des A-modules E_{u_1} et E_{u_2} comme on le vérifie immédiatement.

2. $\Rightarrow$ *3.* Soit ϕ un isomorphisme $E_{u_1} \rightarrow E_{u_2}$. Si $x \in E_{u_1}$ (resp. E_{u_2}) on a par définition $X.x = u_1(x)$ (resp. $X.x = u_2(x)$), d'où $u_2(\phi(x)) = X.\phi(x) = \phi(X.x) = \phi(u_1(x))$ ce qui se traduit par l'égalité $u_1 = \phi^{-1} \circ u_2 \circ \phi$ et donc u_1 et u_2 sont conjugués.

3. $\Rightarrow$ *1.* Si u_1 et u_2 sont conjugués, soit $(e)_1$ une base de E adaptée à u_1 (théorème 3.12). Il existe alors par hypothèse une autre base $(e)_2$ dans laquelle la matrice de u_2 est égale à $M_{(e)_1}(u_1)$; elle est donc adaptée à u_2 et les endomorphismes u_1 et u_2 ont les mêmes invariants de similitude calculés avec la matrice $M_{(e)_1}(u_1)$. ■

On définit les invariants de similitude d'une matrice $M \in \mathcal{M}_n(K)$ comme les invariants de similitude de l'endomorphisme de K^n représenté par M dans la base canonique de K^n.

Corollaire 3.18.

1. *Deux matrices M_1 et $M_2 \in \mathcal{M}_n(K)$ sont semblables si et seulement si elles ont mêmes invariants de similitude.*
2. *Soient $K \subset K'$ deux corps tels que K soit un sous-corps de K'. Alors deux matrices de $\mathcal{M}_n(K)$ sont semblables (sur K) si et seulement si elles sont semblables sur K'.*

Démonstration. La condition *1.* est conséquence directe de la proposition 3.17 puisque deux matrices M_1 et M_2 sont semblables si et seulement si les endomorphismes u_1 et u_2 qu'elles représentent dans la base canonique sont conjugués.

2. Si M_1 et M_2 sont semblables sur K, il existe $Q \in GL_n(K)$ telle que $M_1 = Q^{-1}M_2Q$. Elles sont donc semblables sur K' puisque $K \subset K'$.
Réciproquement si M_1 et $M_2 \in \mathcal{M}_n(K)$ sont semblables sur K', elles ont les mêmes invariants de similitude par *1.* Mais ces invariants de similitude (uniques par le théorème 3.12) sont des polynômes $P_i \in K[X]$. Les matrices sont donc semblables sur K par *1.* ■

3.5 FORME RÉDUITE DE JORDAN

Soit u un endomorphisme d'un espace vectoriel E de dimension finie n sur un corps K. Supposons que $q_u(X) = (X-\alpha)^d$ avec $\alpha \in K$ et $d \geqslant 1$; il existe alors un élément $v \in E$ tel que $(u - \alpha I)^{d-1}.v \neq 0$, puisque par hypothèse le polynôme $(X - \alpha)^{d-1}$ n'annule pas E_u. Soit $F \subset E_u$ le sous-module engendré par v ; F est alors monogène,

et le polynôme minimal de $u|_F$ est encore q_u (car il divise $q_u = (X-\alpha)^d$ qui est le polynôme minimal de u et donc annule $u_{|F}$ et ne divise pas $(X-\alpha)^{d-1}$ puisque par hypothèse $(X-\alpha)^{d-1}$ n'annule pas F). On a donc :

$$F \simeq \frac{K[X]}{(X-\alpha)^d}$$

par la proposition 3.10. Posons :

$$x_1 = v,\ x_2 = (X-\alpha).v = uv - \alpha v,\ x_d = ux_{d-1} - \alpha x_{d-1}.$$

On a $x_i = (X-\alpha)^{i-1}.v$ pour $1 \leqslant i \leqslant d$ et l'on voit immédiatement que $(x_1, \ldots, x_d)$ est une famille libre, car une relation linéaire entre les x_i s'interprète comme l'existence d'un polynôme de degré $\leqslant d-1$ qui annule v, ce qui est impossible car l'annulateur de v et l'annulateur de F coïncident, puisque F est monogène engendré par v. La famille $(x_1, \ldots, x_d)$ est donc une base de F (en tant qu'espace vectoriel). De plus F est stable par u, et la matrice de $u_{|F}$ dans cette base est :

$$\begin{pmatrix} \alpha & 0 & \ldots & & \\ 1 & \alpha & 0 & \ldots & \\ 0 & 1 & \ddots & & \\ \vdots & 0 & \ddots & & \\ 0 & & & 1 & \alpha \end{pmatrix} \tag{2}$$

Remarque 3.19. En prenant pour base de F la famille $(x_d, x_{d-1}, \ldots, x_1)$, la matrice de l'endomorphisme $u_{|F}$ dans cette base devient :

$$\begin{pmatrix} \alpha & 1 & 0 & \ldots & 0 \\ 0 & \alpha & 1 & 0 & \vdots \\ 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & & 1 \\ 0 & \ldots & \ldots & 0 & \alpha \end{pmatrix} \tag{3}$$

Une matrice comme (2) ou (3) est appelée *bloc de Jordan*. Nous ne considérerons dans la suite que des blocs de Jordan de la forme (3).

3.5.1. Réduction d'un endomorphisme sur le corps $\mathbf{C}$

Supposons maintenant que $K = \mathbf{C}$. Les polynômes irréductibles unitaires de $\mathbf{C}[X]$ sont alors les $P_i = X - \alpha_i$, avec $\alpha_i \in \mathbf{C}$ (« Théorème de d'Alembert-Gauss » 5.1). Soit donc u un endomorphisme du $\mathbf{C}$-espace vectoriel de dimension finie E. Le module E_u est un $\mathbf{C}[X]$-module de torsion. Il est donc isomorphe (en tant que $\mathbf{C}[X]$-module) à $\bigoplus_i E(P_i)$, avec $P_i = X - \alpha_i$ et

$$E(P_i) \simeq \prod_j \frac{\mathbf{C}[X]}{((X-\alpha_i)^{\beta_{ij}})} \tag{4}$$

d'après le théorème 2.42. Comme les sous-espaces images dans E_u des $F_{ij} = \frac{\mathbf{C}[X]}{((X-\alpha_i)^{\beta_{ij}})}$ sont des $\mathbf{C}[X]$-modules, ils sont stables par l'endomorphisme u, cycliques, et le polynôme minimal de $u|_{F_{ij}}$ est $(X-\alpha_i)^{\beta_{ij}}$ par la proposition 3.10 ; il existe donc une base de F_{ij} dans laquelle la matrice de la restriction de u à cet espace est un bloc de Jordan de la forme (3) (ou (2)). Si l'on prend une base de E réunion de telles bases pour tous les F_{ij}, la matrice de u dans cette base est donc une matrice diagonale par blocs, chaque bloc étant un bloc de Jordan, les tailles des blocs de Jordan étant les β_{ij}. On a ainsi montré le théorème de Jordan :

Théorème 3.20. *Soit u un endomorphisme de $\mathbf{C}^n$ représenté par une matrice $M \in \mathcal{M}_n(\mathbf{C})$. Alors M est semblable à une matrice de Jordan :*

$$\begin{pmatrix} M_1 & 0 & \dots & 0 \\ 0 & M_2 & \dots & \vdots \\ \vdots & & \ddots & \\ 0 & \dots & & M_k \end{pmatrix} \tag{5}$$

où chaque M_i est un bloc de Jordan avec une valeur propre α_i de M sur sa diagonale.

Remarquons qu'il peut y avoir plusieurs blocs avec la même valeur propre et qu'il résulte de l'unicité dans le théorème 2.42 que à l'ordre près des blocs la matrice de Jordan est unique.

> ***Remarque 3.21.*** Avec les notations ci-dessus, on voit que les α_i sont les valeurs propres de M, que son polynôme caractéristique est $\chi_M(X) = \prod_{i,j}(X-\alpha_i)^{\beta_{ij}}$ (produit des polynômes caractéristiques des M_i), et que son polynôme minimal est $q_M(X) = \prod_{i,j}(X-\alpha_i)^{\sup_j(\beta_{ij})}$. On retrouve donc que le polynôme minimal divise le polynôme caractéristique, et que ces deux polynômes ont les mêmes racines (et donc les mêmes facteurs irréductibles). Noter qu'il peut y avoir plusieurs facteurs avec la même valeur propre α_i, et que donc la multiplicité de la valeur propre α_i dans $\chi_u(X)$ est $\sum_j \beta_{ij}$.

3.5.2. Applications

Le théorème 3.20 montre en particulier que toute matrice à coefficients complexes est semblable à une matrice triangulaire (au choix : supérieure ou inférieure).

Définition 3.22.

1. *Soit $u \in End_K(E)$ un endomorphisme. On dit que u est* nilpotent *s'il existe un entier k tel que $u^k = 0$;*
2. *on dit que u est* diagonalisable *s'il existe une base (e) de E dans laquelle la matrice $M_{(e)}(u)$ est une matrice diagonale.*

On a alors la proposition suivante :

Proposition 3.23. *Les deux conditions suivantes sont équivalentes :*

1. L'endomorphisme u est diagonalisable ;

2. les racines de $q_u(X)$ sont simples (i.e. tous les β_{ij} sont égaux à un).

Démonstration. *2. $\Rightarrow$ 1.* par le théorème 3.20, car alors tous les blocs de Jordan sont de taille (1,1), réduits à un terme α_i (éventuellement répété plusieurs fois), et la matrice de Jordan est diagonale.

1. $\Rightarrow$ 2. Si u est diagonalisable avec valeurs propres α_i, $1 \leqslant i \leqslant n$, chaque α_i étant de multiplicité ν_i, et $\alpha_i \neq \alpha_j$ pour $i \neq j$, il est annulé par le polynôme $Q = \prod_{1 \leqslant i \leqslant n}(X - \alpha_i)$. Son polynôme minimal divise Q, il est donc aussi à racines simples (en fait on a $q_u(X) = Q(X)$ puisque on a vu que $q_u(X)$ avait les mêmes facteurs irréductibles que le polynôme caractéristique $\chi_u(X) = \prod(X - \alpha_i)^{\nu_i}$). ■

On voit en particulier qu'un bloc de Jordan est diagonalisable si et seulement s'il est de taille (1,1).

Rappelons (théorème 2.42) que le $\mathbf{C}[X]$-module E_u est égal à $\bigoplus_i E(P_i)$ avec $P_i = X - \alpha_i$ et

$$E(P_i) \simeq \prod_j \frac{\mathbf{C}[X]}{((X - \alpha_i)^{\beta_{ij}})} \quad .$$

Définition 3.24. *Les sous-espaces $E(P_i)$ de E sont appelés* sous-espaces caractéristiques *de l'endomorphisme u.*

> ***Remarque 3.25.*** Posons $d_i = \sup_j \beta_{ij}$. L'annulateur de $E(P_i)$ est l'idéal engendré par $(X - \alpha_i)^{d_i}$. Si on pose $\nu_i = \sum_j \beta_{ij}$, ν_i est la multiplicité de la valeur propre α_i de u (exposant de $(X - \alpha_i)$ dans le polynôme caractéristique $\chi_u(X)$) comme remarqué plus haut, et $d_i \leqslant \nu_i$. Cela entraîne que l'espace $E(P_i)$ est aussi le noyau de l'endomorphisme $(u - \alpha_i Id)^{\nu_i}$ (démonstration aisée, laissée au lecteur), ce qui est la définition classique des sous-espaces caractéristiques.

Remarquons que si l'endomorphisme u est nilpotent, il est annulé par le polynôme X^k. On a alors nécessairement $q_u(X) = X^d$ (avec $d \leqslant k$, et aussi $d \leqslant n$ par le théorème de Cayley-Hamilton 3.14) ; l'endomorphisme u est donc annulé par X^n. D'autre part, u est nilpotent si et seulement si la matrice $M_{(e)}(u)$ est nilpotente, (e) étant une base quelconque de E.

Exemples 3.26.

1. Soit T une matrice triangulaire avec des zéros sur la diagonale. Alors T est nilpotente.
2. Toute matrice semblable à une matrice nilpotente est nilpotente.
3. Une matrice $A \in \mathcal{M}_n(\mathbf{C})$ est nilpotente si et seulement si sa seule valeur propre est 0.

On a alors :

Théorème 3.27. *(« Décomposition de Dunford ») Soit $u \in End_{\mathbf{C}}(E)$. Alors il existe un endomorphisme diagonalisable D et un endomorphisme nilpotent N tels que :*

1. $u = D + N$

2. $DN = ND$

De plus les endomorphismes N et D sont uniques et s'expriment comme des polynômes en u.

Démonstration.

1. Existence. Elle est donnée par la réduction de Jordan de l'endomorphisme u : si J est la matrice de Jordan de l'endomorphisme u, on a $J = D+N$, D étant la matrice diagonale qui a la même diagonale que J, et N la matrice $J - D$ qui est nilpotente (exemple 3.26). Il est alors clair que D et N commutent, car la multiplication se fait par blocs, et que pour un bloc

$$\begin{pmatrix} \alpha & 1 & 0 & \dots & 0 \\ 0 & \alpha & 1 & 0 & \vdots \\ 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & & 1 \\ 0 & \dots & \dots & 0 & \alpha \end{pmatrix}$$

on a $J_i = D_i + N_i$ avec $D_i = \alpha_i \mathrm{Id}_{\nu_j}$ et donc évidemment $N_i D_i = D_i N_i$.

2. Unicité. Considérons une décomposition $u = D + N$ avec $N^k = 0$ pour un certain entier k. Soit α une valeur propre de D, F_α l'espace propre correspondant, $v \in F_\alpha$ un vecteur propre. On a $D.v = \alpha v$ d'où $(u - \alpha I)v = Nv$, $(u - \alpha I)^2 v = (u - \alpha I)Nv = N(u - \alpha I)v = N^2 v$, et de proche en proche $(u - \alpha I)^s v = N^s v$ pour tout entier s. On a donc $F_\alpha \subset \ker(u - \alpha I)^k$ (puisque par hypothèse $N^k = 0$). Si on note α_i les valeurs propres de u, α est donc l'un des α_i (car $\ker(u - \alpha I)^k \neq (0)$ implique que $u - \alpha I$ n'est pas inversible, donc que α est valeur propre de u). Si $\alpha = \alpha_i$, on a ainsi $F_{\alpha_i} \subset E_i$, E_i étant le sous-espace caractéristique (de l'endomorphisme u) correspondant à α_i (définition 3.24). Comme E est somme directe des E_i et aussi des F_{α_i} (puisque D est diagonalisable), on en déduit que $F_{\alpha_i} = E_i$ pour tout i.

L'espace E_i est donc stable par D (et N) et $D_{|E_i} = \alpha_i$ Id. Cela montre l'unicité de D (les E_i ne dépendent que de u) et donc de N puisque $N = u - D$.

Montrons maintenant que D et N s'expriment comme des polynômes en u ; le théorème chinois montre qu'il existe un polynôme $P(X)$ tel que $P \equiv \alpha_i \bmod (X - \alpha_i)^{\nu_i}$ pour tout i. On a alors $P(u)_{|E_{\alpha_i}} = \alpha_i \mathrm{Id}$ car il existe par hypothèse un polynôme $R_i(X)$ tel que $P(X) = \alpha_i + R_i(X)(X - \alpha_i)^{\nu_i}$, et $(X - \alpha_i)^{\nu_i}$ annule le sous-module E_{α_i} de E_u. Cela implique que $D = P(u)$ et $N = u - P(u) = Q(u)$ avec $Q(X) = X - P(X)$. ■

Exemple 3.28. Considérons la matrice $B = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}$ de $\mathcal{M}_2(\mathbf{R})$. On a $B = D + N$ avec $D = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ et $N = \begin{pmatrix} 0 & 3 \\ 0 & 0 \end{pmatrix}$, mais cette décomposition n'est pas celle du théorème 3.27 car D et N ne commutent pas.

En fait B est diagonalisable (puisque à valeurs propres simples) et l'on a donc $D = B$, $N = 0$ dans la décomposition de Dunford.

EXERCICES

Les solutions des exercices et problèmes sont données en fin d'ouvrage.

POLYNÔME MINIMAL

Exercice 3.1. Soit E un espace vectoriel sur $\mathbf{R}$ de dimension n, u un endomorphisme de polynôme minimal q_u. On suppose que $q_u = P_1P_2$, P_1 et P_2 étant des polynômes unitaires non constants premiers entre eux. On note E_u l'espace E muni de la structure de $\mathbf{R}[X]$-module définie par l'endomorphisme u.

1. Montrer que pour $i = 1, 2$,
$$E_i = \{x \in E \mid P_i(u)(x)) = 0\}$$
est un sous-module de E_u.
2. Montrer que $E_u = E_1 \oplus E_2$.
3. Montrer que pour $i = 1, 2$, P_i est le polynôme minimal de $u_{|E_i}$.

INVARIANTS DE SIMILITUDE

Exercice 3.2. Soit V un $\mathbf{C}$ espace vectoriel de dimension finie $n \geqslant 1$ et $u \in \mathrm{End}_{\mathbf{C}}(V)$. On munit V de sa structure de $\mathbf{C}[X]$-module associée à u.

1. On suppose que V ne possède aucun sous-module non trivial. Montrer que $n = 1$. On remplace maintenant $\mathbf{C}$ par $\mathbf{R}$. L'énoncé est-il encore vrai ?
2. On note $\chi_u = R_1.R_2^2 \cdots R_l^l$ le polynôme caractéristique de u, où les R_i sont deux à deux premiers entre eux, sans facteurs carrés et unitaires. Vérifier qu'une telle écriture est possible et est unique.
3. Avec les notations du (b), on suppose de plus que V est somme directe de sous-$\mathbf{C}[X]$-modules de dimension 1 (en tant que $\mathbf{C}$-espaces vectoriels). Calculer les invariants de similitude de u.

Exercice 3.3. Soit V un $\mathbf{C}$ espace vectoriel de dimension finie $n \geqslant 1$ et $u \in \mathrm{End}_{\mathbf{C}}(V)$. On suppose que pour toute paire W, W' de sous-espaces vectoriels de V stables par u, on a soit $W \subset W'$ soit $W' \subset W$.

Déterminer les invariants de similitude de u, son polynôme minimal en fonction de son polynôme caractéristique.

Exercice 3.4. Soient K un corps et E un K-espace vectoriel de dimension 3. Montrer que deux endomorphismes de E sont semblables si et seulement s'ils ont le même polynôme minimal et le même polynôme caractéristique.

Exercice 3.5. Soient K un corps, λ un élément de K et M le bloc de Jordan de taille (n, n) associée à λ.

1. Montrer que M possède une unique valeur propre et déterminer la dimension du sous-espace propre associé.
2. Quel est le polynôme minimal de M ?

Exercice 3.6. Soient E un espace vectoriel sur $\mathbf{C}$ de dimension finie et u un endomorphisme de E. On note I l'identité de E.

1. Montrer que si le $\mathbf{C}[X]$-module E associé à u est cyclique, alors pour tout $\lambda \in \mathbf{C}$ la dimension du noyau de $u - \lambda I$ est $\leqslant 1$.
2. En déduire que le maximum des dimensions des sous-espaces propres de u est égal au nombre d'invariants de similitude non constants de u.

Exercice 3.7. Soit u un endomorphisme de $\mathbf{C}^n$. Montrer que le nombre d'invariants de similitude de u est égal au maximum des dimensions de ses sous-espaces propres.

Exercice 3.8. Soit u un endomorphisme de $\mathbf{C}^n$ ayant une seule valeur propre α. On pose $d^i = \dim \ker(u - \alpha Id)^i$; on note r_α l'entier à partir duquel la suite (d^i) stationne (*i.e.* $d^{r_\alpha - 1} < d^{r_\alpha} = d^{r_\alpha + 1} = \cdots$). Montrer que le polynôme minimal de u est $q_u = (X - \alpha)^{r_\alpha}$.

Exercice 3.9. Pour $n > 1$, on note $J_n \in \mathcal{M}_n(\mathbf{C})$ la matrice nilpotente dont tous les coefficients sont nuls, sauf ceux de la première sur-diagonale $j_{i,i+1}$ pour $1 \leqslant i < n$ qui sont égaux à 1. On considère les matrices suivantes, écrites par blocs :

1. $M_1 = \mathrm{diag}(aI_3, bI_2, cI_1)$;
2. $M_2 = \mathrm{diag}(I_3, I_2 + J_2, I_2 + J_2, I_3 + J_3, I_3 + J_3, 2I_2, 2I_3 + J_3, 3I_2, 3I_2 + J_2)$;
3. $M_3 = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \ddots & \vdots & a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & a_{n-1} \\ 0 & \cdots & 0 & 0 & a_n \end{pmatrix}$.

Déterminer dans chaque cas :

(i) les invariants de similitudes ;

(ii) les polynômes minimaux et caractéristiques ;

(iii) les dimensions des sous-espaces caractéristiques.

Exercice 3.10. Soit u un endomorphisme de $\mathbf{C}^n$, dont les valeurs propres sont 0 et 1 ; on note K_0^i (resp. K_1^i) le noyau de u^i (resp $(u-\mathrm{Id})^i$) et soit d_0^i (resp. d_1^i) sa dimension. On suppose que la suite (d_0^i) (resp. (d_1^i)) est égale à $(4,7,9,10,10,\dots)$ (resp. $(3,4,5,5,\dots)$). Déterminer alors les invariants de similitudes de u.

Exercice 3.11. Écrire sous la forme de Jordan les endomorphismes u dont les invariants de similitudes non constants sont :

(a) $P_1(X) = X$;

(b) $P_1(X) = X(X-1)$;

(c) $P_1(X) = X$ et $P_2(X) = X^2$;

(d) $P_1(X) = X$ et $P_2(X) = X(X-1)$;

(e) $P_1(X) = X^2(X-1)$, $P_2(X) = X^2(X-1)(X-2)$, $P_3(X) = X^3(X-1)^2(X-2)$ et $P_4(X) = X^4(X-1)^3(X-2)^4$.

PROBLÈMES

Problème 3.1. *Un algorithme pour la décomposition de Dunford*
On se propose dans ce problème de donner un algorithme pour calculer la décomposition de Dunford sans calculer les valeurs propres (le calcul des valeurs propres ne peut en général se faire que de manière approchée).

Soit $n \geqslant 1$ et $A \in \mathcal{M}_m(K)$ une matrice carrée à coefficients dans le corps $K \subset \mathbf{C}$. On note χ_A le polynôme caractéristique de A. Dans $\mathbf{C}$, $\chi_A(X)$ se décompose sous la forme $\prod_i (X-\lambda_i)^{n_i}$ avec $\sum_i n_i = m$. On introduit alors le polynôme $P(X) = \prod_i (X-\lambda_i)$.

1. Montrer que
$$P(X) = \frac{\chi_A(X)}{\chi_A(X) \wedge \chi_A'(X)},$$
où $\chi_A(X) \wedge \chi_A'(X)$ désigne le PGCD unitaire de χ_A avec son polynôme dérivé. En déduire alors que $P(X)$ est un polynôme à coefficients dans K.

2. Soient U et N deux matrices de $\mathcal{M}_n(K)$ respectivement inversible et nilpotente qui commutent entre elles. Montrer que $U-N$ est inversible. Montrer alors que $P'(A)$ est une matrice inversible de $\mathcal{M}_m(K)$ dont l'inverse commute avec A.

3. On considère alors la suite suivante : $A_0 := A$ et $A_{n+1} := A_n - P(A_n).(P'(A_n))^{-1}$. On veut montrer par récurrence sur n que la suite est bien définie, *i.e.* que $P'(A_n)$ est une matrice inversible.
   (i) Montrer que pour tout polynôme $Q \in K[X]$, il existe $\tilde{Q} \in K[X, Y]$ tel que $Q(X + Y) = Q(X) + YQ'(X) + Y^2\tilde{Q}(X, Y)$.
   (ii) En supposant la suite A_n définie jusqu'au rang n, montrer que $P(A_n)$ s'écrit sous la forme $P(A)^{2^n} B_n$ où B_n est une matrice de $\mathcal{M}_n(K)$ qui est un polynôme en A.
   (iii) En utilisant une formule de Taylor pour le polynôme P', écrire $P'(A_{n+1})$ comme la somme d'une matrice inversible $P'(A_n)$ et d'une matrice nilpotente qui commutent entre elles.
4. Montrer que la suite A_n est stationnaire de limite D avec D diagonalisable sur $\mathbf{C}$ et $N := A - D$ nilpotente vérifiant $DN = ND$.

Chapitre **4**

Groupes

Nous allons dans ce chapitre étudier les groupes non nécessairement commutatifs, en nous concentrant sur le groupe symétrique, et sur quelques exemples de groupes liés à la géométrie.

4.1 GÉNÉRALITÉS

Pour un groupe G non nécessairement commutatif (*cf.* 1.1), nous noterons la loi multiplicativement. L'élément neutre est donc noté 1, et l'inverse d'un élément g est noté g^{-1}.

Définition 4.1. *Soit H un sous-groupe d'un groupe G. Si $a \in G$, le sous-ensemble :*

$$aH = \{g \in G \mid g = ah, \quad h \in H\}$$

est par définition la classe à gauche *de l'élément a relativement à H. De même le sous-ensemble Ha est appelé* classe à droite.

Remarques 4.2.

1. En général les classes à gauche et les classes à droite ne coïncident pas, sauf si G est commutatif, ou pour certains sous-groupes H appelés distingués (*cf.* plus bas).
2. Deux éléments g_1 et g_2 de G sont dans la même classe à gauche relativement à H si et seulement si $g_1^{-1}g_2 \in H$; les classes à gauche

sont donc les classes d'équivalence pour la relation d'équivalence $g_1 \sim g_2 \Leftrightarrow g_1^{-1}g_2 \in H$ (il est immédiat de voir que cette relation est une relation d'équivalence).

3. Les classes à gauche forment donc une partition de G (*cf.* la remarque précédente) ; l'ensemble des classes à gauche est noté G/H (contrairement au cas commutatif, il n'existe pas en général de structure de groupe sur G/H propagée par celle de G). Le cardinal de G/H s'appelle *l'indice* de H dans G.

Si G est fini, on en déduit le « théorème de Lagrange » (*cf.* le lemme 1.18 pour le cas commutatif) :

Théorème 4.3. *Soit H un sous-groupe d'un groupe fini G d'ordre n. Notons $|G/H|$ le cardinal de G/H (indice de H dans G). Alors*

$$|G| = n = |H||G/H|.$$

Donc l'ordre de tout sous-groupe de G divise l'ordre de G ; en particulier, l'ordre d'un élément $g \in G$ divise l'ordre de G.

Démonstration. Soit $a \in G$. L'application de G dans lui-même τ_a de multiplication à gauche par a ($\tau_a(g) = ag$) est bijective, son inverse étant la multiplication par a^{-1} ; elle envoie H (la classe de 1) sur aH. Toutes les classes à gauche aH ont donc le même cardinal h =card(H). Comme ces classes constituent une partition de G, le théorème est démontré. ■

Définition 4.4. *Soit A une partie d'un groupe G. Il existe un plus petit sous-groupe H de G contenant A : on l'appelle le sous-groupe* engendré *par A. On note $H =< A >$.*

L'existence de H se voit en prenant l'intersection de tous les sous-groupes contenant A (l'intersection de sous-groupes est un sous-groupe).

À titre d'exercice, le lecteur pourra montrer que H est l'ensemble des éléments qui peuvent s'écrire $\{a_1 \dots a_n, |n \in \mathbf{N}, a_i \in A \text{ ou } a_i^{-1} \in A\}$.

Il faut noter que le sous-groupe engendré par un élément $g \in G$ est commutatif, même si G n'est pas commutatif (proposition 1.33).

Enfin, nous allons donner la condition sur un sous-groupe H pour que l'ensemble G/H des classes à gauche ait une structure de groupe propagée par celle de G : cette condition est que les classes à gauche et à droite coïncident.

Définition 4.5. *Un sous-groupe H d'un groupe G est dit* distingué *si :*

$$\forall\, a \in G, \quad aH = Ha.$$

La condition s'écrit aussi $aHa^{-1} = H$ pour tout a dans G. La notation $H \triangleleft G$ signifie que H est un sous-groupe distingué de G.

Proposition 4.6. *Soit $H \subset G$ un sous-groupe. Les conditions suivantes sont équivalentes :*

1. *il existe un groupe G' et un homomorphisme $\phi : G \longrightarrow G'$ tels que $H = \ker \phi$;*
2. *$H \triangleleft G$ (H est distingué dans G) ;*
3. *l'ensemble G/H est muni d'une structure de groupe (« groupe quotient ») propagée par celle de G, i.e. telle que l'application $\pi : G \to G/H$ définie par $\pi(a) = \{aH\}$ soit un morphisme de groupes.*

Démonstration.
1. $\Rightarrow$ 2. Soit $a \in G$. Montrons que $a^{-1}Ha = H$: si $h \in \ker \phi$, posons $h' = a^{-1}ha$; on a alors $\phi(h') = 1$ et donc $h' \in H$, d'où $a^{-1}Ha \subset H$, et de même dans l'autre sens.
2. $\Rightarrow$ 3. Nous allons définir sur G/H une structure de groupe telle que $\pi : G \to G/H$ soit un morphisme de noyau H et poser $G' = G/H$. Par définition, on pose $aH.bH = abH$ pour a et b dans G. Pour voir que cette opération est bien définie et que π (défini par $\pi(g) = gH$) est un morphisme de groupes, il faut voir que si $aH = a'H$, $bH = b'H$, alors $abH = a'b'H$. Montrons par exemple que $abH \subset a'b'H$, *i.e.* $ab \in a'b'H$. On a $a = a'h_1$, $b = b'h_2$ par hypothèse (avec $h_i \in H$), donc $ab = a'h_1b'h_2$. Mais il existe $h_3 \in H$ tel que $h_1b' = b'h_3$ puisque H est distingué ; on a donc $ab = a'b'h_3h_2 \in a'b'H$.
3. $\Rightarrow$ 1. Il suffit de prendre $G' = G/H$ et $\phi = \pi$. ■

Définition 4.7. *On dit qu'un groupe G est* simple *s'il ne contient aucun sous-groupe distingué non trivial (i.e. différent de G et $\{e\}$).*

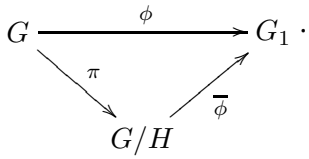
Remarques 4.8.

1. Si G est commutatif, tous les sous-groupes sont distingués.
2. Si H est distingué, le noyau du morphisme $\phi : G \to G/H$ est le sous-groupe H. Donc un sous-groupe est distingué si et seulement si c'est le noyau d'un morphisme.
3. Si G est fini d'ordre n, et H un sous-groupe distingué d'ordre h, l'ordre du groupe quotient G/H est n/h par le théorème 4.3.
4. Comme dans le cas des groupes abéliens, le quotient satisfait la « propriété universelle » de la proposition 4.9 ci-dessous, dont la démonstration est la même que dans le cas commutatif.
5. Nous allons rencontrer deux familles de groupes simples : d'abord les groupes $(\mathbf{Z}/p\mathbf{Z}, +)$ où p est un nombre premier (ce sont les seuls groupes commutatifs simples, comme on le voit facilement : proposition 1.35), puis les groupes alternés A_n pour $n \neq 4$ (*cf.* ci-dessous) ; de plus nous verrons que le groupe des rotations $S\mathcal{O}(\mathbf{R}^3)$ est simple.

Proposition 4.9. *Soient G un groupe, $H \triangleleft G$ un sous-groupe distingué, $\phi : G \to G_1$ un morphisme tel que $H \subset \ker \phi$; il existe alors un morphisme unique $\overline{\phi} : G/H \to G_1$ tel que $\overline{\phi} \circ \pi = \phi$. Réciproquement l'existence d'un tel morphisme implique $H \subset \ker \phi$. De plus le morphisme $\overline{\phi}$ est injectif si et seulement si $H = \ker \phi$.*

La démonstration est la même que celle de la proposition 2.4.

On a donc sous l'hypothèse $H \subset \ker \phi$ un « diagramme commutatif » :



Nous verrons des exemples dans les paragraphes suivants.

4.2 LE GROUPE SYMÉTRIQUE

Définition 4.10. *On appelle groupe symétrique d'indice n le groupe S_n des permutations de l'ensemble $E = \{1, 2, \ldots, n\}$.*

S_n est un groupe fini avec $n!$ éléments. Par définition de la loi de groupe sur S_n, si g et g' sont des éléments de S_n, l'élément gg' est la permutation qui consiste à effectuer d'abord la permutation g', puis la permutation g.

> ***Remarque 4.11.*** Si E' est un ensemble quelconque à n éléments, toute bijection ϕ de E sur E' induit un isomorphisme entre S_n et le groupe des permutations de E' : on fait correspondre à $\sigma \in S_n$ la bijection $\phi \circ \sigma \circ \phi^{-1}$ de E' dans lui-même.

Définition 4.12. *1) La permutation qui à $1, 2 \ldots, n$ fait correspondre $i_1, \ldots, i_n$ se note* $\begin{bmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{bmatrix}$;

2) soient $i_1, \ldots, i_k$ ($1 < k \leqslant n$) des éléments deux à deux distincts de $\{1, 2, \ldots, n\}$. La notation $(i_1 \ldots i_k)$ désigne la permutation σ telle que $\sigma(i_l) = i_{l+1}$ ($1 \leqslant l \leqslant k-1$), $\sigma(i_k) = i_1$, et $\sigma(i_s) = i_s$ pour $i_s \notin \{i_1, \ldots, i_k\}$. Une telle permutation est une permutation circulaire, *ou* cycle. *L'entier k est la* longueur *du cycle, et l'ensemble $\{i_1, \ldots, i_k\}$ le* support *du cycle. Un cycle de longueur deux est une* transposition.

Toutes les assertions qui suivent doivent être soigneusement vérifiées à titre d'exercice.

> ***Remarques 4.13.***
>
> 1. Les cycles $(i_1 \ldots i_k), (i_2 \ldots i_k\ i_1), \ldots, (i_k\ i_1 \ldots i_{k-1})$ sont identiques.
> 2. Deux cycles à supports disjoints commutent.
> 3. Soient σ une permutation et $c = (i_1 \ldots i_k)$ un cycle. Alors $\sigma c \sigma^{-1} = (\sigma(i_1) \ldots \sigma(i_k))$.
> 4. Inversement deux cycles de même longueur sont conjugués (*i.e.* si c_1 et c_2 sont deux tels cycles, il existe $\sigma \in S_n$ tel que $c_2 = \sigma c_1 \sigma^{-1}$).

5. Si $n = 2$, le groupe S_2 a deux éléments : l'identité et le cycle (12). Il est isomorphe à $(\mathbf{Z}/2\mathbf{Z}, +)$.
6. Si $n = 3$, S_3 a six éléments : l'identité et les cycles (123) et (132) (qui forment un sous-groupe isomorphe à $\mathbf{Z}/3\mathbf{Z}$), et les trois transpositions $(12), (13)$ et (23). S_3 s'identifie au groupe des isométries du plan qui laissent globalement invariant un triangle équilatéral. Ces isométries se caractérisent en effet par les permutations qu'elles induisent sur les sommets du triangle. S_3 n'est pas commutatif car par exemple $(12)(123) = (32) = (23)$ alors que $(123)(12) = (13)$.
7. Pour le cas $n = 4$, *cf.* l'exemple 4.20 ci-dessous.

Nous allons maintenant « dévisser » les éléments de S_n, c-à-d. les exprimer comme produit de permutations « simples ».

Proposition 4.14. *Tout élément σ de S_n est produit de cycles dont les supports sont deux à deux disjoints, et cela de manière unique, à l'ordre près des cycles (qui commutent par la remarque* 4.13*).*

Démonstration. Si $i \in \{1, \ldots, n\}$, soit l le plus petit entier tel que $\sigma^l(i) = i$ (un tel l existe puisque $\sigma^{n!} = Id$ par le théorème de Lagrange ; en fait $l \leqslant n$ comme il résulte immédiatement des considérations qui suivent). La famille $\mathcal{A} = (i, \sigma(i), \sigma^2(i), \ldots, \sigma^{l-1}(i))$ vérifie les propriétés (immédiates) suivantes :

1. $\mathcal{A}$ définit un cycle c de longueur l de la manière suivante : $c(j) = \sigma(j)$ si $j \in \mathcal{A}$, et $c(j) = j$ si $j \notin \mathcal{A}$;
2. deux tels cycles ont des supports disjoints ou confondus ;
3. la permutation σ est le produit de tous les cycles à supports disjoints ainsi déterminés.

Cela démontre l'existence et l'unicité de la décomposition de σ en produit de cycles de supports disjoints deux à deux. ■

Exemple 4.15. Soit $n = 8$ et σ la permutation $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 5 & 1 & 8 & 7 & 2 \end{bmatrix}$. Alors on a $\sigma = (1345)(268)(7)$ (que l'on note en général $(1345)(268)$ en omettant les cycles de longueur 1).

Corollaire 4.16. *Le groupe S_n est engendré par les transpositions (i.e. les cycles de longueur 2).*

Démonstration. D'après la proposition 4.14, il suffit de montrer qu'un cycle est produit de transpositions. Mais il est facile de voir que

$$(i_1\ i_2 \ldots i_k) = (i_1\ i_2)(i_2\ i_3) \ldots (i_{k-2}\ i_{k-1})(i_{k-1}\ i_k)$$

(on reporte i_k à la première place en le faisant successivement « sauter » $i_{k-1}, \ldots, i_1$). ■

Proposition 4.17. *Soit* $(G, \times) = \{1, -1\} \simeq (\mathbf{Z}/2\mathbf{Z}, +)$. *Il existe un (unique) morphisme de groupes surjectif appelé* signature *:*

$$\varepsilon \ : \quad S_n \longrightarrow G.$$

Ce morphisme vérifie la propriété suivante :
Si σ est un cycle de longueur k, sa signature vaut $\varepsilon(\sigma) = (-1)^{k-1}$
(en particulier, si τ est une transposition, sa signature vaut -1).

Démonstration. Montrons d'abord l'existence du morphisme ε vérifiant les propriétés de l'énoncé ; le morphisme ε est défini sur les cycles par la formule de la proposition ; si σ est une permutation exprimée comme un produit de cycles $c_1 c_2 \dots c_k$ dont les supports sont disjoints deux à deux, on pose $\varepsilon(\sigma) = \varepsilon(c_1) \dots \varepsilon(c_k)$, ce qui définit ε pour toute permutation σ. Il faut alors montrer que si σ et τ sont deux permutations, on a $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$. D'après le corollaire 4.16, il existe $s > 0$ tel que l'on puisse écrire τ comme le produit de s transpositions τ_i. Par une récurrence immédiate sur l'entier s, il suffit de montrer que si σ est une permutation exprimée comme un produit de cycles $c_1 c_2 \dots c_k$ dont les supports sont disjoints deux à deux et τ une transposition, on a $\varepsilon(\sigma\tau) = -\varepsilon(\sigma)$. Il y a trois cas à considérer :

1. Les supports de σ et τ sont disjoints. Dans ce cas on a $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau) = -\varepsilon(\sigma)$ puisque par définition de ε on a $\varepsilon(\tau) = -1$;
2. le support de τ est contenu dans le support d'un cycle c_i. Posons $c_i = (i_1 \dots i_k)$ et $\tau = (i_j\, i_l),\ j < l$. On a alors :

   $$c_i\tau = (i_1 \dots i_j\, i_{l+1} \dots i_k)(i_{j+1} \dots i_l)$$

   et $c_i\tau$ est produit de deux cycles à supports disjoints de longueurs k_1 et k_2 avec $k_1 + k_2 = k$. On a bien $\varepsilon(c_i\tau) = -\varepsilon(c_i)$, puisque

   $$\varepsilon(c_i\tau) = (-1)^{k_1-1} \times (-1)^{k_2-1} = (-1)^{k-2} = -(-1)^{k-1}.$$

3. Le support de τ fait partie des supports de deux cycles disjoints c_i et c_j (on inclut ici les cycles de longueur 1). Alors si $c_i = (i_1 \dots i_k)$, $c_j = (j_1 \dots j_s)$ et $\tau = (i_j\, j_l)$, on a :

   $$c_i c_j \tau = (i_1 \dots i_j\, j_{l+1} \dots j_1 \dots j_l\, i_{j+1} \dots i_k)$$

   et la conclusion est la même que pour le cas précédent.

L'unicité de ε est immédiate ; il suffit de montrer que si $\varepsilon : S_n \to G$ est surjectif, on a $\varepsilon(\tau) = -1$ pour toute transposition τ (corollaire 4.16). Mais deux transpositions τ et τ' sont conjuguées (remarque 4.13, 4.) ; on a donc $\varepsilon(\tau) = \varepsilon(\tau')$ pour toute transposition τ' ; si on avait $\varepsilon(\tau) = 1$, on aurait $\varepsilon(\tau') = 1$ pour toute transposition τ', donc pour toute permutation σ et ε ne serait pas surjectif. ■

Il résulte en particulier de ce résultat que si l'on écrit une permutation σ comme un produit de transpositions de plusieurs manières différentes, la parité du nombre de ces transpositions est toujours la même.

Remarque 4.18. Le lecteur pourra montrer à titre d'exercice que si σ une permutation de l'ensemble $E = \{1, \ldots, n\}$, la signature $\varepsilon(\sigma)$ est égale à la parité $(-1)^k$ du nombre k de couples $(i, j) \in E^2$ tels que $i < j$ et $\sigma(i) > \sigma(j)$.

Définition 4.19. *Le noyau de ε est un sous-groupe (distingué) de S_n appelé* groupe alterné *et noté A_n. Les éléments de A_n sont appelés des* permutations paires *(car elles sont produit d'un nombre pair de transpositions), les autres des* permutations impaires.

Le sous-groupe A_n est distingué d'après la proposition 4.6, et de cardinal $n!/2$ d'après le théorème 4.3. C'est le sous-groupe de S_n formé des permutations de signature +1. Le quotient S_n/A_n est isomorphe à $(\mathbf{Z}/2\mathbf{Z}, +)$ (le sous-groupe A_n est donc d'indice 2 dans S_n).

Exemples 4.20.

1. Dans le groupe S_3, le sous-groupe A_3 est le groupe $(\mathrm{Id}, (123), (132))$ isomorphe à $(\mathbf{Z}/3\mathbf{Z}, +)$: *cf.* la remarque 4.13 ; si l'on identifie comme dans cette remarque S_3 et les isométries qui fixent un triangle équilatéral, A_3 s'identifie aux rotations qui fixent ce triangle.
2. Le groupe S_4 s'identifie aux isométries de $\mathbf{R}^3$ qui fixent un tétraèdre régulier. Il a $4! = 24$ éléments, et donc $|A_4| = 12$. Les 12 éléments de A_4 sont : l'identité, les 3-cycles (il y en a huit), et les trois éléments $(1\,3)(2\,4),\ (1\,4)(2\,3),\ (1\,2)(3\,4)$. Ces trois éléments plus l'identité constituent un sous-groupe H de A_4 commutatif et distingué (vérification facile). Le groupe H est isomorphe au « groupe de Klein » $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Parmi les groupes A_n, A_4 est le seul qui possède un sous-groupe distingué non trivial (*i.e.* non égal a lui-même ou à $\{1\}$) ; autrement dit pour $n \neq 4$, A_n est *simple* : *cf.* la section 4.3.2. plus bas.

Remarques 4.21. Notons les faits suivants, qui seront proposés en exercices :

1. Les transpositions $(1\,2),\ (1\,3), \ldots, (1\,n)$ engendrent S_n.
2. Les cycles $(1\,2)$ et $(1\,2 \ldots n)$ engendrent S_n.
3. Pour $k < n$ on a : $(k\ k+1) = (1\,2 \ldots n)^{k-1}(1\,2)(1\,2 \ldots n)^{1-k}$.
4. Pour $n \geqslant 3$, les 3-cycles engendrent A_n.

4.3 OPÉRATION D'UN GROUPE SUR UN ENSEMBLE

Définition 4.22. *Soient G un groupe, X un ensemble. On dit que G* opère à gauche *sur X s'il existe une application (on dit aussi une «* action *» de G sur X) :*

$$G \times X \longrightarrow X : \quad (g, x) \mapsto g.x$$

telle que :
1. $\forall\, g, g' \in G$, $x \in X$, $g.(g'.x) = (gg').x$
2. $\forall\, x \in X$, $1.x = x$.

Sauf mention explicite du contraire, nous supposerons toujours que les actions se font à gauche (l'action à droite se définit comme $(g, x) \mapsto x.g$, ce qui change l'axiome *1.* de la définition 4.22).

Exemples 4.23.

1. Le groupe orthogonal $O_2(\mathbf{R})$ opère sur $\mathbf{R}^2$ (*cf.* le paragraphe suivant).
2. Si G est un groupe, on peut le faire opérer sur lui-même de plusieurs façons, par exemple :
   a) Par translations à gauche : si $g, x \in G$, on pose $g.x = gx$ que l'on note aussi $\tau_g(x)$ (*cf.* la démonstration de la proposition 4.24 ci-dessous).
   b) Par *automorphismes intérieurs* : si $g, x \in G$, on pose $g.x = gxg^{-1}$ (le lecteur vérifiera que cette opération est bien une opération à gauche ; la formule $g.x = g^{-1}xg$ définit une opération à droite).
3. Le groupe S_n opère (par définition) sur l'ensemble $E = \{1, 2, \ldots, n\}$ par permutations.

On déduit de l'exemple 2. ci-dessus la proposition suivante (« théorème de Cayley ») :

Proposition 4.24. *Soit G un groupe fini d'ordre n. Alors G est isomorphe à un sous-groupe de S_n.*

Démonstration. La « translation à gauche » τ_g (multiplication à gauche par l'élément g) est une bijection de G sur lui-même, et deux éléments distincts g et g' induisent des bijections distinctes. Dautre part on a :

$$\forall x \in G : (\tau_{g'} \circ \tau_g).x = \tau_{g'}.gx = g'gx, \text{ et donc } \tau_{g'} \circ \tau_g = \tau_{g'g};$$

l'application $g \mapsto \tau_g$ est donc un morphisme injectif de G dans le groupe $S(G)$ (groupe des permutations de G), qui est isomorphe à S_n puisque $|G| = n$. ■

Définition 4.25. *Soit G un groupe opérant sur l'ensemble X.*

1. Si $x \in X$, l'orbite *de x est l'ensemble des $g.x$ pour $g \in G$. On la note $\omega(x)$.*

2. Si $x \in X$, l'ensemble $S_x \subset G$ formé des éléments $g \in G$ tels que $g.x = x$ est un sous-groupe de G appelé le stabilisateur *de x.*

La vérification du fait que S_x est un sous-groupe est évidente.

Exemples 4.26.

1. Dans l'opération de S_n sur l'ensemble $\{1, 2, \ldots, n\}$, le stabilisateur d'un élément i est isomorphe à S_{n-1} (il s'identifie de manière évidente au groupe des permutations de l'ensemble à $n - 1$ éléments $\{1, 2, \ldots, n\} \setminus \{i\}$).
2. Si $\sigma \in S_n$, on peut restreindre l'action de S_n sur $E = \{1, 2, \ldots, n\}$ au sous-groupe $< \sigma >$ de S_n engendré par σ. Soit $\omega \subset E$ une orbite de $< \sigma >$; il existe

donc un entier k et un élément $i \in E$ tels que $\omega = \{i, \sigma(i), \ldots, \sigma^{k-1}(i)\}$ (ω est l'orbite de l'élément i). L'action de σ sur ω est donc un cycle $(i_0, \ldots, i_{k-1})$ (avec $i_0 = i$ et $i_j = \sigma^j(i)$) de la décomposition de la proposition 4.14 : on voit donc que la partition de E en orbites disjointes sous l'action de $< \sigma >$ est équivalente à la décomposition de σ en cycles à supports disjoints deux à deux.

3. Si G opère sur lui-même par automorphismes intérieurs (exemple 4.23), l'orbite d'un élément $x \in G$ s'appelle la *classe de conjugaison* de x : c'est l'ensemble des $x' \in G$ tels qu'il existe $g \in G$ avec $x' = gxg^{-1}$. S'il existe $g \in G$ tel que $x' = gxg^{-1}$, on dit que x et x' sont *conjugués* (ou que x' est un conjugué de x).
   En particulier, si $G = S_n$:
   - le conjugué d'un k-cycle est un k-cycle (remarque 4.13) ;
   - deux k-cycles σ_1 et σ_2 sont conjugués ;
   - plus généralement, deux permutations sont conjuguées si et seulement si, dans leur décomposition canonique en cycles, apparaissent le même nombre de k-cycles pour tout entier $k,\ 2 \leqslant k \leqslant n$ (remarques 4.11) ;
   - deux transpositions τ_1 et τ_2 sont conjuguées par un élément de A_n.

Proposition 4.27. *Soit G un groupe opérant sur l'ensemble X. Pour $x \in X$, l'application $\phi_x : G \to \omega(x)$ définie par $g \mapsto g.x$ se factorise par l'application $\pi : G \to G/S_x$ en une application $\overline{\phi}_x : G/S_x \to \omega(x)$ qui est une bijection.*

Démonstration. L'application ϕ_x est surjective par définition d'une orbite, et donc $\overline{\phi}_x$ aussi.

Pour montrer l'injectivité de $\overline{\phi}_x$, on remarque que deux éléments g_1 et g_2 de G ont même image par ϕ_x si et seulement si

$$g_1.x = g_2.x \iff g_2^{-1}g_1.x = x \iff g_2^{-1}g_1 \in S_x \iff g_1S_x = g_2S_x.$$

L'application ϕ_x est donc constante sur les classes à gauche suivant S_x, ce qui donne une application surjective $\overline{\phi}_x : G/S_x \to \omega(x)$ dont on vient de montrer qu'elle est aussi injective. ■

4.3.1. Quelques applications

Définition 4.28. *Le* centre $Z(G)$ *d'un groupe G est le sous-ensemble de G formé des éléments $x \in G$ qui commutent à tous les éléments de G :*

$$Z(G) = \{x \in G \mid xg = gx, \quad \forall\, g \in G\}.$$

Le centre $Z(G)$ est un sous-groupe distingué (et commutatif) de G (immédiat), et $Z(G) = G$ si et seulement si G est commutatif.

Exemples 4.29. 1) Pour $n \geqslant 3$, on a $Z(S_n) = \{1\}$. En effet, prenons $\sigma \in S_n$, $\sigma \neq \mathrm{Id}$. Il existe donc un indice i tel que $\sigma(i) \neq i$. Comme $n \geqslant 3$, il existe j (dans $\{1, 2, \ldots, n\}$) tel que $j \neq i$ et $j \neq \sigma(i)$. Soit τ la transposition $(j\,\sigma(i))$. Alors on a $\sigma\tau(i) = \sigma(i)$ et $\tau\sigma(i) = j$, donc σ et τ ne commutent pas et $\sigma \notin Z(S_n)$.

2) Considérons l'action d'un groupe G sur lui-même par automorphismes intérieurs (exemple 4.23). Le centre est alors caractérisé comme l'ensemble des $x \in G$ tels que $\omega(x) = \{x\}$. Soient ω_i les orbites de l'action de G sur lui-même (par automorphismes intérieurs) telles que $|\omega_i| > 1$. Notons que si $|G|$ est fini, $|\omega_i|$ divise $|G|$ (proposition 4.27) ; on a alors avec ces notations :

Proposition 4.30.

1. Soit G un groupe fini. Alors :

$$|G| = |Z(G)| + \sum_i |\omega_i| \tag{1}$$

(« équation aux classes »).

2. Soit $p \in \mathbf{N}$ un nombre premier.

(a) Si $|G| = p$, G est cyclique ($G \simeq (\mathbf{Z}/p\mathbf{Z}, +)$), donc abélien.

(b) Si $|G| = p^k$ pour $k \geqslant 1$, alors $|Z(G)| = p^s$ pour un entier s tel que $1 \leqslant s \leqslant k$ (en particulier $|Z(G)| \geqslant p$).

(c) Si $|G| = p^2$, G est abélien.

Démonstration. *1.* traduit simplement le fait que G est réunion disjointe des orbites. Notons que $|Z(G)| \geqslant 1$ puisque l'on a toujours $1 \in Z(G)$.

2. (a) Si $|G| = p$, soit $g \in G$, $g \neq 1$. Alors l'ordre $|<g>|$ de $<g>$ est > 1 et doit diviser p : on a donc $|<g>| = p$ d'où $|<g>| = G$ et G est cyclique.

(b) Dans la formule (1), chaque $|\omega_i|$ est une puissance de p car il divise $|G|$, et $|Z(G)| \geqslant 1$. Le nombre $|Z(G)|$ est donc une puissance non nulle de p puisqu'il est $\geqslant 1$, qu'il est divisible par p et qu'il doit diviser $|G| = p^k$.

(c) D'après (*b*), $|Z(G)| = p$ ou p^2. Soit $x \neq 1$ un élement de $Z(G)$; le sous-groupe $< x >$ est contenu dans $Z(G)$ et x est d'ordre p ou p^2. Si x est d'ordre p^2, G est commutatif car alors $G = Z(G)$. Si x est d'ordre p, le sous-groupe $<x>$ est distingué dans G, puisque $< x > \subset Z(G)$. Le groupe quotient $G/ < x >$ est d'ordre p donc cyclique par (a). Soit $y \in G$ dont l'image $\overline{y}$ dans $G/ < x >$ engendre $G/ < x >$ (il suffit que $\overline{y} \neq 1$). Alors tout élément de G s'écrit de manière unique comme $x^a y^b$ avec $0 \leqslant a \leqslant p-1$ et $0 \leqslant b \leqslant p-1$ (comme il y a p^2 tels éléments, il suffit de voir que ces éléments sont distincts deux à deux, ce qui est un exercice facile laissé au lecteur). Comme $x \in Z(G)$, on voit que deux tels éléments commutent et donc que G est abélien. ■

3) On peut évidemment généraliser l'équation aux classes (1) au cas général d'une action d'un groupe G sur un ensemble fini E en exprimant que E est réunion disjointe des orbites.

4.3.2. *Simplicité de A_n

Théorème 4.31. *Pour $n \neq 4$, le groupe alterné A_n est simple.*

Démonstration. Les groupes $A_2 = S_2 \simeq (\mathbf{Z}/2\mathbf{Z}, +)$ et $A_3 \simeq (\mathbf{Z}/3\mathbf{Z}, +)$ sont simples. Pour $n \geqslant 5$, la stratégie est la suivante : on sait que les 3-cycles engendrent A_n pour $n \geqslant 3$ (remarque 4.18). On va montrer que pour $n \geqslant 5$, les 3-cycles sont conjugués dans A_n (on sait déjà qu'ils le sont dans S_n). Si $H \triangleleft A_n$ est un sous-groupe distingué, il suffira de montrer que H contient un 3-cycle, car alors il les contiendra tous et sera donc égal à A_n. ■

Lemme 4.32. *Pour $n \geqslant 5$, les 3-cycles sont conjugués dans A_n.*

Démonstration. Soient c_1 et c_2 deux 3-cycles ; on sait qu'il existe $\sigma \in S_n$ tel que $c_1 = \sigma^{-1} c_2 \sigma$ (remarque 4.13). Si $c_1 = (i_1\, i_2\, i_3)$, $c_2 = (j_1\, j_2\, j_3)$, σ est défini par $\sigma(i_1) = j_1,\ \sigma(i_2) = j_2,\ \sigma(i_3) = j_3$. Si $\sigma \notin A_n$ et si $n \geqslant 5$, il existe deux éléments i_4 et i_5 différents de i_1, i_2, i_3 ; si on pose alors $\tau = (i_4\, i_5)$, l'élément $\tilde{\sigma} = \sigma\tau$ est dans A_n et l'on a aussi $c_1 = \tilde{\sigma}^{-1} c_2 \tilde{\sigma}$. ■

Montrons maintenant le théorème.

Démonstration. Soit H un sous-groupe distingué de $\mathcal{A}_n$ et notons r le minimum des cardinaux des supports des éléments de $H - \{Id\}$. Le but est de montrer que $r = 3$ et donc qu'il existe un 3-cycle appartenant à H.

Soit tout d'abord $\sigma \in H$ distinct de l'identité et a tel que $b = \sigma(a) \neq a$. On considère alors $s = (a\ b\ c)$ avec $c \notin \{a, b, \sigma(b)\}$. Soit $\tau = s\sigma s^{-1}\sigma^{-1}$ qui appartient à H car, H étant un sous-groupe distingué, il contient $s\sigma s^{-1}$ et σ^{-1}. On a $\tau = (a\ b\ c) \circ (b\ \sigma(a)\ \sigma(b))$ qui est donc de support de cardinal inférieur à 5. Pour conclure que $r \leqslant 5$, il reste à vérifier que τ n'est pas l'identité. Or on a $\tau(c) \neq c$ car $c \neq \sigma(b)$.

Supposons alors que $r = 5$; un élément de $\mathcal{A}_n$ de support de cardinal 5 est forcément un 5-cycle qui quitte à renuméroter les éléments est $(1\ 2\ 3\ 4\ 5)$. On calcule à nouveau un commutateur soit

$$(1\ 2\ 3\ 4\ 5) \circ (4\ 5\ 2) \circ (1\ 2\ 3\ 4\ 5)^{-1} \circ (4\ 5\ 2)^{-1} = (1\ 2\ 3\ 4\ 5) \circ (1\ 2\ 3\ 5\ 4) = (1\ 3)(2\ 4)$$

d'où la contradiction.

Supposons donc que $r = 4$; un élément de $\mathcal{A}_n$ de support de cardinal 4 est forcément à renumérotation près, $(1\ 2)(3\ 4)$. On introduit le commutateur

$$(1\ 2)(3\ 4) \circ (4\ 5) \circ (1\ 2)(3\ 4) \circ (4\ 5) = (3\ 5\ 4)$$

On a ainsi $r \leqslant 3$ et comme $\mathcal{A}_n$ ne contient aucun élément de support de cardinal 2, on conclut que $r = 3$ et donc que H contient un 3-cycle. ■

Corollaire 4.33. *Les seuls sous-groupes distingués de S_n sont $\{0\}$ et $\{A_n\}$ pour $n = 3$ et $n \geqslant 5$.*

4.3.3. *Les théorèmes de Sylow

Définition 4.34. *Soit G un groupe fini d'ordre $n = |G|$, p un nombre premier tel que $p|n$, $r \geqslant 1$ le plus grand entier tel que $p^r|n$. Alors un* sous-groupe de Sylow *de G (on dit aussi p-Sylow) est un sous-groupe d'ordre p^r. Nous noterons $\mathcal{S}_p$ (ou plutôt $\mathcal{S}$ s'il n'y a pas d'ambiguïté) l'ensemble des p-Sylow de G.*

Théorème 4.35. *Soit G un groupe fini, p un nombre premier divisant l'ordre de G. Il existe alors un p-Sylow (autrement dit, l'ensemble $\mathcal{S}$ est non vide).*

Lemme 4.36. *Soient p un nombre premier, m et r des entiers > 0. Alors*

$$\binom{p^r m}{p^r} \equiv m \bmod p. \tag{2}$$

Démonstration. On a l'identité :

$$(1+X)^p = \sum_{i=0}^{p} \binom{p}{i} X^i$$

dans l'anneau de polynômes $\mathbf{Z}[X]$, d'où $(1+X)^p \equiv 1 + X^p \bmod p$ puisque $\binom{p}{i} = \frac{p(p-1)\ldots(p-i+1)}{i(i-1)\ldots 1} \equiv 0 \bmod p$ (p divise le numérateur et pas le dénominateur), et donc :

$$(1+X)^{p^2} = ((1+X)^p)^p \equiv (1+X^p)^p \equiv (1+X^{p^2}) \bmod p$$

On en déduit par récurrence sur r que pour tout entier $r \geqslant 0$ on a $(1+X)^{p^r} \equiv 1+X^{p^r} \bmod p$, d'où :

$$(1+X)^{p^r m} = \left((1+X)^{p^r}\right)^m \equiv (1+X^{p^r})^m \bmod p.$$

En identifiant les termes X^{p^r} dans $(1+X)^{mp^r}$ et $(1+X^{p^r})^m$, on trouve ainsi :

$$\binom{p^r m}{p^r} \equiv m \bmod p.$$

■

Démonstration. (du théorème 4.35). Posons $|G| = p^r m$ avec $r \geqslant 1$ et $p \wedge m = 1$. Soit E l'ensemble des parties de G à p^r éléments ; il faut montrer qu'il existe au moins un sous-groupe de G parmi les éléments de E.

Le groupe G opère sur E par translations à gauche (exemple 4.23). Notons $\omega(X)$ l'orbite d'un éléments $X \in E$ sous cette action (4.25). On a $|E| = \binom{n}{p^r} = \binom{p^r m}{p^r} \equiv m \bmod p$ par (2) ; il existe donc $X_0 \in E$ tel que p ne divise pas $|\omega(X_0)|$ (puisque E est la réunion disjointe des orbites $\omega(X)$ et $p \wedge m = 1$). Soit $H \subset G$ le stabilisateur de X_0 (4.25) ; on a $|G|/|H| = |\omega(X_0)|$ (proposition 4.27) et donc p^r divise $|H|$ puisque $|G| = mp^r$ avec $p \wedge m = 1$. On a donc $|H| \geqslant p^r$. Montrons que $|H| = p^r$: soit $x \in X_0$; on a $hx \in HX_0 = X_0\ \forall h \in H$, d'où $H \subset X_0 x^{-1}$; on a donc $|H| \leqslant |X_0 x^{-1}| = p^r$ et donc bien $|H| = p^r$, *i.e.* H est un p-Sylow. ■

Énonçons maintenant le second théorème de Sylow qui décrit les propriétés de l'ensemble $\mathcal{S}$ des sous-groupes de Sylow de G.

Théorème 4.37. *Sous les hypothèses du théorème 4.35, on a les propriétés suivantes :*

1. *soit $K \subset G$ un p-sous-groupe (i.e. tel que $|K|$ soit une puissance de p). Il existe un p-Sylow H tel que $K \subset H$;*
2. *si H et H' sont deux p-Sylow, ils sont conjugués dans G (il existe $g \in G$ tel que $H = g^{-1}H'g$) ;*
3. *$|\mathcal{S}| \equiv 1 \bmod p$ et $|\mathcal{S}|$ divise m.*

Démonstration. Remarquons d'abord que le conjugué d'un p-Sylow est un p-Sylow, et que donc G opère sur $\mathcal{S}$ par conjuguaison. Soit K un p-sous-groupe de G, H un p-Sylow, $\omega(H)$ l'orbite de H ; si $S \subset G$ est le stabilisateur de H, on a $H \subset S$ et donc $|\omega(H)| = |G|/|S|$ est non divisible par p (car $H \subset S$ implique que $|S|$ est divisible par p^r par le théorème de Lagrange). Si on restreint l'action de G sur $\omega(H)$ au sous-groupe K, on voit donc par la formule des classes (1) qu'il existe $H_1 \in \omega(H)$ fixé par K, puisque par hypothèse $|K|$ est une puissance de p. On a donc $k^{-1}H_1k = H_1 \ \forall \ k \in K$; l'ensemble des $l \in G$ tels que $l^{-1}H_1l = H_1$ est ainsi un sous-groupe L de G tel que $K \subset L$ (et évidemment aussi $H_1 \subset L$) ; de plus H_1 est distingué dans L par définition de L. Le sous-groupe H_1 étant un p-Sylow, $|L/H_1| = |L|/|H_1|$ n'est pas divisible par p (puisque $|L|$ est un diviseur de $n = mp^r$) ; soit $\pi : L \to L/H_1$ le morphisme canonique. Le groupe K étant un p-groupe, il en est de même pour le sous-groupe $\pi(K)$ de L/H_1 (car $|\pi(K)|$ divise $|K|$ qui est une puissance de p). Comme par le théorème de Lagrange $|\pi(K)|$ doit diviser $|L/H_1|$, on en déduit $\pi(K) = \{e\}$, *i.e.* $K \subset H_1$, d'où *1.*, et *2.* en prenant pour K un p-Sylow (on a alors $K = H_1$).

Montrons *3.* Soit $H \in \mathcal{S}$ un p-Sylow, $S \subset G$ le sous-groupe stabilisateur de H (pour l'action de G sur $\mathcal{S}$ par conjugaison). On a $H \subset S$, et $\mathcal{S}$ est l'orbite de H par la condition *2.* Donc $|\mathcal{S}| = |G|/|S| \equiv 1 \bmod p$. Enfin $|\mathcal{S}|$ divise $mp^r = |G|$ par la condition *2.* puisque $\mathcal{S}$ est l'orbite de n'importe quel p-Sylow et donc $|\mathcal{S}|$ divise m puisque $|\mathcal{S}| \equiv 1 \bmod p$. ■

Exemples 4.38.

1. Soit G un groupe abélien fini, p un nombre premier tel que p divise $|G|$. Les théorèmes 4.35 et 4.37 impliquent que $|\mathcal{S}| = 1$: il y a un et un seul p-Sylow dans G, le groupe $G(p)$. De plus G est somme directe de tous ses sous-groupes de Sylow (proposition 2.48).
2. Soit $\mathbf{F_p} = \mathbf{Z}/p\mathbf{Z}$ le corps à p éléments, $G = GL_n(\mathbf{F_p})$ (matrices inversibles à coefficients dans $\mathbf{F_p}$).
   On a
   $$|G| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1}) \tag{3}$$
   (exercice : il suffit de compter les bases de $(\mathbf{F_p})^n$). Alors le sous-groupe H formé

des matrices triangulaires supérieures avec des 1 sur la diagonale principale est un p-Sylow de G. On a en effet $|H| = p \times p^2 \times \cdots \times p^{n-1} = p^{n(n-1)/2}$ et

$$|G| = p^{n(n-1)/2}(p^n - 1)(p^{n-1} - 1)\dots(p-1) = p^{n(n-1)/2}m$$

avec $m \wedge p = 1$.

4.4 QUELQUES EXEMPLES LIÉS À LA GÉOMÉTRIE

4.4.1. Le groupe orthogonal en dimension 2

Les applications linéaires $\mathbf{R}^2 \to \mathbf{R}^2$ qui sont des isométries forment un groupe (avec comme opération la composition) noté $\mathcal{O}(\mathbf{R}^2)$. Une application linéaire f de $\mathbf{R}^2$ dans lui-même est dans $\mathcal{O}(\mathbf{R}^2)$ si et seulement si l'image $(f(e_1), f(e_2))$ de la base canonique (e_1, e_2) de $\mathbf{R}^2$ est une base orthonormale de $\mathbf{R}^2$. Si M_f est la matrice qui représente f dans la base (e_1, e_2), les vecteurs $f(e_1), f(e_2)$ développés dans la base (e_1, e_2) forment par définition les colonnes de M_f. Les matrices M représentant les éléments de $\mathcal{O}(\mathbf{R}^2)$ sont donc caractérisées par la relation :

$$M\,{}^tM = {}^tM M = I, \tag{4}$$

I représentant la matrice identité de rang deux. Cette relation implique que $\det M = \pm 1$.

Définition 4.39.

1. *Le groupe $\mathcal{O}(\mathbf{R}^2)$ s'appelle le* groupe orthogonal *(en dimension 2). Ce groupe s'identifie au groupe des matrices M de rang 2 vérifiant la relation* (4) *que nous noterons $\mathcal{O}_2(\mathbf{R})$. Les matrices $M \in \mathcal{O}_2(\mathbf{R})$ sont dites* orthogonales.
2. *On note $S\mathcal{O}(\mathbf{R}^2)$ le sous-groupe de $\mathcal{O}(\mathbf{R}^2)$ formé des isométries qui conservent l'orientation, i.e. dont la matrice M est de déterminant $+1$ (on note $S\mathcal{O}_2(\mathbf{R})$ le sous-groupe des matrices $M \in \mathcal{O}_2(\mathbf{R})$ de déterminant 1).*

Notons U le groupe (multiplicatif) des nombres complexes de module 1. Si on identifie $\mathbf{C}$ à $\mathbf{R}^2$ par $z = x + iy \mapsto (x, y)$ (notons que cette identification oriente canoniquement $\mathbf{R}^2$, *i.e.* choisit la base (e_1, e_2) comme étant directe), l'ensemble U s'identifie au cercle $S^1 \subset \mathbf{R}^2$.

Lemme 4.40. *Soit $\underline{b} = (f_1, f_2)$ une base orthonormale de $\mathbf{R}^2$.*

1. *Tout élément $f \in S\mathcal{O}(\mathbf{R}^2)$ est représenté dans la base $\underline{b}$ par une matrice de la forme $M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ avec $a^2 + b^2 = 1$.*
2. *L'application qui à $f \in SO(\mathbf{R}^2)$ fait correspondre la matrice M est un isomorphisme de $SO(\mathbf{R}^2)$ sur le groupe multiplicatif $S\mathcal{O}_2(\mathbf{R})$ des matrices de la forme $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ avec $a^2 + b^2 = 1$ (cet isomorphisme dépend de la base $\underline{b}$ choisie).*

3. L'application $S\mathcal{O}_2(\mathbf{R}) \to U$ définie comme $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mapsto a + ib$ est un isomorphisme de groupes.

Démonstration. Soit $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ une matrice de $S\mathcal{O}_2(\mathbf{R})$. On a $a^2 + b^2 = c^2 + d^2 = 1$, $ac + bd = 0$ et $ad - bc = 1$ par (4). Si $a = 0$, on trouve aussitôt $d = 0$, d'où $c = \pm 1$, $b = \pm 1$, $b = -c$, et $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ ou $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Si $a \neq 0$, on trouve en éliminant c que $d = \pm a$ et de même $b = \pm c$, d'où $a = d$ et $c = -b$ puisque $ad - bc = 1$. On a donc $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ avec $a^2 + b^2 = 1$.

La démonstration de *2.* et *3.* est immédiate. ■

> ***Remarque 4.41.*** Le lecteur vérifiera à titre d'exercice que l'application $S\mathcal{O}_2(\mathbf{R}) \to U$ ci-dessus est aussi un homéomorphisme ($S\mathcal{O}_2(\mathbf{R})$ est un sous-espace topologique de $\mathcal{M}_4(\mathbf{R}) \simeq \mathbf{R}^4$ et U est un sous-espace de $\mathbf{C} \simeq \mathbf{R}^2$).

4.4.2. Angles

Rappelons l'existence d'un morphisme de groupes surjectif :

donné par
$$\begin{aligned} \mathbf{R} &\to U \\ \theta &\mapsto e^{i\theta} = \cos\theta + i\sin\theta \end{aligned}$$

de période 2π.

On définit les *angles* comme les éléments de U. Tout angle est donc de la forme $e^{i\theta}$ avec $\theta \in \mathbf{R}$; le nombre θ est la *mesure* de l'angle (définie à $2k\pi$ près) ; on fait souvent l'abus de langage consistant à confondre l'angle et sa mesure, et à parler de « l'angle θ », bien que θ ne soit pas un angle, mais un nombre réel, que l'on prend en général compris entre 0 et 2π ou entre $-\pi$ et π puisque deux nombres qui diffèrent de $2k\pi$ définissent le même angle ; on a fait cet abus de langage dans l'énoncé de la proposition 4.42 ci-dessous.

Proposition 4.42. *Tout élément $f \in S\mathcal{O}(\mathbf{R}^2)$ est représenté par une matrice de la forme :*
$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix};$$
on dit que f est la rotation *d'angle θ.*
Tout élément de $g \in \mathcal{O}(\mathbf{R}^2) \setminus S\mathcal{O}(\mathbf{R}^2)$ est une symétrie orthogonale par rapport à une droite (passant par O), on dit aussi que g est une réflexion*. La matrice correspondant à g s'écrit :*
$$A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$
si l'axe de symétrie de g fait un angle $\theta/2$ avec l'axe des x (i.e. si l'axe de symétrie est l'image de l'axe des x par la rotation d'angle $\theta/2$).

Démonstration. D'après le lemme 4.40, l'élément $A \in S\mathcal{O}_2(\mathbf{R})$ peut s'écrire :

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

θ (défini modulo 2π) étant la mesure de l'angle de la rotation de matrice A.
Une rotation de $\mathbf{R}^2$ est donc caractérisée de trois manières : soit par sa matrice A, soit par son angle $e^{i\theta}$, soit par la mesure $\theta \in \mathbf{R}$ de cet angle (définie modulo 2π). Comme il a été noté plus haut, on fait souvent l'abus de langage qui consiste à confondre l'angle et sa mesure, et de parler de « rotation d'angle θ ».
Si maintenant $ad - bc = -1$, le même raisonnement montre que l'on peut écrire :

$$A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

Les relations $a + d = 0$ et $ad - bc = -1$ montrent alors que les valeurs propres de A sont 1 et -1, et le calcul classique montre que le sous-espace propre correspondant à la valeur propre 1 est engendré par le vecteur de coordonnées $(\cos\theta/2, \sin\theta/2)$, l'autre espace propre lui étant orthogonal (puisque A est symétrique). Dans cette base de vecteurs propres, la matrice A' de g s'écrit alors $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Cela achève la démonstration de la proposition. ■

Remarque 4.43. *Définition « géométrique » des angles*

Se donner une demi-droite D d'origine O revient à se donner le point d'intersection de D et S^1, donc un élément $e^{i\theta}$ de U.

De même, se donner un couple (ordonné) (D_1, D_2) de demi-droites d'origine O revient à se donner un couple $(e^{i\theta_1}, e^{i\theta_2})$ d'éléments de U. On définit alors l'angle $\widehat{D_1, D_2}$ comme l'élément $e^{i(\theta_2 - \theta_1)}$ de U.

Si on considère l'action de $S\mathcal{O}(\mathbf{R}^2) \simeq U$ sur les couples (D_1, D_2) de demi-droites donnée par :

$$e^{i\theta}.(e^{i\theta_1}, e^{i\theta_2}) \mapsto (e^{i(\theta_1+\theta)}, e^{i(\theta_2+\theta)}),$$

on voit que deux angles de demi-droites sont les mêmes si et seulement s'ils sont dans la même orbite pour cette action.

On peut donc aussi définir les angles comme les orbites de l'action de $S\mathcal{O}(\mathbf{R}^2)$ sur les couples (ordonnés) de demi-droites d'origine O : c'est cette définition que l'on peut appeler « définition géométrique des angles ».

Signalons quelques propriétés algébriques du groupe $\mathcal{O}(\mathbf{R}^2)$ dont la démonstration est laissée au lecteur.

Proposition 4.44.

1. *Soit r_θ la rotation d'angle θ $(-\pi < \theta \leqslant \pi)$, s une réflexion. Alors on a*
$$sr_\theta s^{-1} = r_{-\theta} = r_\theta^{-1}.$$
2. *Le groupe $\mathcal{O}(\mathbf{R}^2)$ est engendré par les réflexions. Plus précisément :*
   - *Tout élément de $\mathcal{O}(\mathbf{R}^2) \setminus S\mathcal{O}(\mathbf{R}^2)$ est un réflexion.*
   - *Toute rotation r_θ est le produit de deux réflexions dont l'angle des axes vaut $\theta/2$ (θ est défini modulo 2π ; $\theta/2$ est donc défini modulo π ; c'est l'angle de deux droites non orientées).*
   - *Réciproquement, le produit de deux réflexions par rapport à des droites qui font un angle de $\theta/2$ (modulo π) est la rotation d'angle θ.*
3. *Le groupe $S\mathcal{O}(\mathbf{R}^2)$ est commutatif ; le centre de $\mathcal{O}(\mathbf{R}^2)$ est le sous-groupe formé de $\{\mathrm{Id}, -\mathrm{Id}\}$.*

Remarquons enfin que si (f_1, f_2) est une base orthonormale directe de $\mathbf{R}^2$ (*i.e.* image de la base canonique par une rotation), la matrice de la rotation R_θ d'angle θ dans cette base est encore $A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$ puisqu'elle s'écrit $Q^{-1}AQ$, $Q \in S\mathcal{O}_2(\mathbf{R})$ étant la matrice de changement de bases, et que $S\mathcal{O}_2(\mathbf{R})$ est commutatif.

En revanche, si la base (f_1, f_2) n'est pas directe, il résulte de la proposition 4.44, *1.*, que la matrice de la rotation R_θ dans la base (f_1, f_2) est la matrice A^{-1} (obtenue en changeant θ en $-\theta$ dans A).

4.4.3. Sous-groupes finis de $\mathcal{O}(\mathbf{R}^2)$

Définition 4.45. *On appelle* groupe dihédral *d'indice n un sous-groupe de $\mathcal{O}(\mathbf{R}^2)$ formé des isométries linéaires qui laissent globalement invariant un polygône régulier $\mathcal{P}$ à n sommets (et de centre O).*

L'identité est l'élément neutre d'un tel groupe que l'on note D_n par abus de langage (en omettant la référence au polygône $\mathcal{P}$).

Si D_n et D'_n sont deux groupes dihédraux de même indice n, ils sont conjugués dans $\mathcal{O}(\mathbf{R}^2)$: il existe une rotation $\sigma \in S\mathcal{O}(\mathbf{R}^2)$ telle que $D'_n = \sigma^{-1} D_n \sigma$ (exercice facile). En particulier, les groupes D_n et D'_n sont isomorphes.

Proposition 4.46. *Soit D_n un groupe dihédral. Le groupe D_n est engendré par deux éléments r et s vérifiant les relations suivantes (en notant 1 l'élément neutre de D_n) :*
$$r^n = 1,\ s^2 = 1,\ sr = r^{n-1}s\ ; \tag{5}$$
on a $|D_n| = 2n$ et tout groupe engendré par deux éléments r et s satisfaisant ces relations est isomorphe à D_n.

Démonstration. Montrons que le groupe D_n est engendré par la rotation r d'angle $2\pi/n$, et une symétrie orthogonale s par rapport à une droite joignant O à un sommet du polygône $\mathcal{P}$. Soit $\{A_i\}$ l'ensemble des sommets de $\mathcal{P}$, s la symétrie orthogonale par rapport à la droite OA_1. Soit $\phi \in \mathcal{O}(\mathbf{R}^2)$ laissant globalement invariant $\mathcal{P}$. Supposons que $\phi(A_1) = A_k$. Il existe un entier q, $0 \leqslant q \leqslant n-1$ unique tel que $r^q(A_1) = A_k$, d'où $r^q(A_1) = \phi(A_1)$. On a donc soit $r^{-q}\phi = Id$, *i.e.* $\phi = r^q$, soit $r^{-q}\phi = s$ *i.e.* $\phi = r^q s$.

Tout élément de D_n s'écrit ainsi de manière unique comme r^q ou $r^q s$ avec $0 \leqslant q \leqslant n-1$, ce qui implique que $|D_n| = 2n$. Si on a un groupe G engendré par deux éléments r' et s' satisfaisant (5), il est alors facile de voir que l'application $\phi : G \to D_n$ définie par $\phi(r') = r$ et $\phi(s') = s$ est un isomorphisme de groupes. ■

Exemples 4.47.

1. Un groupe D_2 a quatre éléments : $\pm$ l'identité et deux réflexions s et s' (on voit facilement qu'il est isomorphe au « groupe de Klein » $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$).
2. On a $D_3 \simeq S_3$, comme il a été vu dans la remarque 4.13.

Théorème 4.48. *Soit $G \subset \mathcal{O}(\mathbf{R}^2)$ un sous-groupe d'ordre fini q. Alors G est isomorphe soit au groupe cyclique $\mathbf{Z}/q\mathbf{Z}$ (et alors $G \subset S\mathcal{O}(\mathbf{R}^2)$), soit à un groupe dihédral D_n (et $q = 2n$).*

Démonstration. a) Supposons d'abord $G \subset S\mathcal{O}(\mathbf{R}^2)$ (et donc G commutatif). Chaque élément g de G est une rotation r_g d'angle θ_g, que l'on peut supposer tel que $0 \leqslant \theta_g < 2\pi$ (*cf.* la proposition 4.42 : on identifie un angle avec sa mesure comprise entre 0 et 2π). Comme G est fini, il existe un $\theta_0 > 0$ minimal parmi les θ_g non nuls (car on suppose $G \neq \{\mathrm{Id}\}$). Montrons que G est cyclique engendré par la rotation r_0 d'angle θ_0. Si $g \in G$, il existe un entier $k > 0$ unique tel que $0 \leqslant \theta_g - k\theta_0 < \theta_0$. Mais $\theta_g - k\theta_0$ est l'angle de la rotation $(r_g)(r_0)^{-k} \in G$ (rappelons que l'application $\phi : SO_2(\mathbf{R}) \to U$ ci-dessus permet d'identifier une rotation d'angle θ avec l'élément $e^{i\theta} \in U$), ce qui implique que $\theta_g - k\theta_0 = 0$ par minimalité de θ_0, et donc $\theta_g = k\theta_0$, ou $r_g = r_0^k$. Le groupe G est ainsi cyclique, donc isomorphe à $\mathbf{Z}/q\mathbf{Z}$ pour q égal l'ordre de G.

b) Si $G \not\subset S\mathcal{O}(\mathbf{R}^2)$, soit $H = G \cap S\mathcal{O}(\mathbf{R}^2)$. H est isomorphe à $\mathbf{Z}/n\mathbf{Z}$ pour un entier n par a). Soit $s \in G$ une réflexion (*i.e.* un élément de G non dans H) ; on a alors $G = H \cup sH$ comme on le vérifie immédiatement. Le groupe G est donc engendré par les deux éléments h (générateur de H) et s, qui vérifient les relations :

$$h^n = Id,\ s^2 = Id,\ hs = sh^{-1} = sh^{n-1}$$

(la dernière résultant du fait que sh est une symétrie, donc $shsh = Id$ d'où $shs = h^{-1}$ et $hs = sh^{-1}$) ; ces relations sont les relations (5) où l'on a posé $1 = Id$. Le groupe G est donc bien isomorphe à un groupe dihédral D_n. ■

4.4.4. Le groupe orthogonal en dimension 3

Dans tout ce paragraphe, les droites (resp. les plans) seront toujours des droites (resp. des plans) contenant l'origine, *i.e.* des droites (resp. des plans) vectorielles (resp. vectoriels). L'ensemble des applications linéaires $\mathbf{R}^3 \to \mathbf{R}^3$ qui sont des isométries forme un groupe (avec comme opération la composition) noté $\mathcal{O}(\mathbf{R}^3)$. Une application linéaire f de $\mathbf{R}^3$ dans lui-même est dans $\mathcal{O}(\mathbf{R}^3)$ si et seulement si l'image $(f(e_1), f(e_2), f(e_3))$ de la base canonique (e_1, e_2, e_3) de $\mathbf{R}^3$ est une base orthonormale de $\mathbf{R}^3$. Si M_f est la matrice qui représente f dans la base (e_1, e_2, e_3), les vecteurs $f(e_1), f(e_2), f(e_3)$ développés dans la base (e_1, e_2, e_3) forment par définition les colonnes de M_f. Les matrices M représentant les éléments de $\mathcal{O}(\mathbf{R}^3)$ sont donc caractérisées par la relation :

$$M\,{}^tM = {}^tMM = I, \tag{6}$$

I représentant la matrice identité de rang trois. Cette relation implique que $\det M = \pm 1$.

Définition 4.49.

1. *Le groupe $\mathcal{O}(\mathbf{R}^3)$ s'appelle le* groupe orthogonal *(en dimension 3). Ce groupe s'identifie au groupe des matrices M de rang 3 vérifiant la relation* (6)*. Nous noterons $\mathcal{O}_3(\mathbf{R})$ ce groupe de matrices. Les matrices $M \in \mathcal{O}_3(\mathbf{R})$ sont dites* orthogonales*.*
2. *On note $S\mathcal{O}(\mathbf{R}^3)$ le sous-groupe de $\mathcal{O}(\mathbf{R}^3)$ formé des isométries qui conservent l'orientation, i.e. dont la matrice M est de déterminant $+1$. La notation $S\mathcal{O}_3(\mathbf{R})$ désigne le sous-groupe des matrices $M \in \mathcal{O}_3(\mathbf{R})$ de déterminant 1.*

> ***Remarque 4.50.*** Si $f \in \mathcal{O}(\mathbf{R}^3)$ et si M' est la matrice représentant l'application f dans une base orthonormale quelconque (pas nécessairement la base canonique), M' est aussi une matrice orthogonale (vérification immédiate : si M est la matrice qui représente f dans la base canonique, on a $M' = Q^{-1}MQ$, avec Q, M et Q^{-1} orthogonales).

Donnons maintenant quelques exemples classiques d'éléments de $\mathcal{O}(\mathbf{R}^3)$.

Exemples 4.51.

1. Soit f la symétrie orthogonale par rapport à un plan P. Alors $f \in \mathcal{O}(\mathbf{R}^3) \backslash S\mathcal{O}(\mathbf{R}^3)$ (*i.e.* $\det M_f = -1$) ; on dit que f est une *réflexion*. Dans une base orthonormale convenable (formée de deux vecteurs de P et d'un vecteur orthogonal), la matrice de f s'écrit :

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \tag{7}$$

2. Soit f la symétrie orthogonale par rapport à une droite D. Alors $f \in S\mathcal{O}(\mathbf{R}^3)$; on dit que f est un *renversement*. Dans une base orthonormale convenable, la matrice de f s'écrit $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$.
3. Soient D une droite orientée (par un vecteur unitaire V_1 porté par D), P le plan orthogonal à D. On peut choisir une base orthonormale (V_2, V_3) de P de façon à ce que la base (V_1, V_2, V_3) de $\mathbf{R}^3$ soit orthonormale directe (*i.e.*$\det(V_1, V_2, V_3) = +1$). Soit θ un angle (que l'on peut choisir par exemple tel que $-\pi < \theta \leqslant \pi$, *cf.* la proposition 4.42). On appelle rotation d'angle θ et d'axe D l'application linéaire f dont la matrice dans la base (V_1, V_2, V_3) s'écrit :

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}; \tag{8}$$

on a $f \in S\mathcal{O}(\mathbf{R}^3)$, la droite D est fixée par f (c'est l'axe de la rotation), et la restriction de f au plan P (orienté par la base (V_2, V_3)) est la rotation d'angle θ. Dans le cas où $\theta = \pi$, on retrouve les renversements.

Proposition 4.52. *Soit M une matrice (3,3) orthogonale (i.e.telle que $M \in \mathcal{O}_3(\mathbf{R})$). Alors :*

1. *M a toujours une valeur propre réelle $\lambda_1 = \pm 1$. Les valeurs propres (réelles ou complexes) de M sont de module 1.*
2. *Si $M \in S\mathcal{O}_3(\mathbf{R})$, M a une valeur propre $\lambda_1 = 1$. Si V_1 est un vecteur propre unitaire pour λ_1, l'application f de matrice M (dans la base canonique) est une rotation d'axe la droite (orientée) D définie par V_1. La matrice de f est donc de la forme* (8) *dans une base orthonormale convenable (ayant pour premier vecteur le vecteur V_1).*
3. *Si $M \in \mathcal{O}_3(\mathbf{R}) \setminus S\mathcal{O}_3(\mathbf{R})$, M a une valeur propre $\lambda_1 = -1$. Si V_1 est un vecteur propre unitaire pour la valeur propre λ_1, l'application f définie par la matrice M est la composée d'une rotation f_1 d'axe D, droite orientée définie par V_1, et d'une réflexion s par rapport au plan P orthogonal à D. Les applications s et f_1 commutent, et la matrice de f dans une base orthonormale convenable (de premier vecteur V_1) est de la forme :*

$$M = \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} \tag{9}$$

Démonstration.

1. Soit $\chi(X) \in \mathbf{R}[X]$ le polynôme caractéristique de M. Le polynôme $\chi(X)$ étant de degré 3, il a une racine réelle λ_1. Si λ est une valeur propre réelle de M, V un vecteur propre associé, notons encore V la matrice colonne de V développé dans la base canonique. On a alors $MV = \lambda V$ d'où ${}^tV\,{}^tM = \lambda\,{}^tV$ et

$$\|V\|^2 = {}^t V.V = {}^t V\,{}^tMMV = \lambda^2\,{}^tV.V = \lambda^2\|V\|^2,$$

d'où $\lambda^2 = 1$ puisque $V \neq 0$.

Si maintenant $\lambda_2 \in \mathbf{C}$ est une racine non réelle de $\chi(X)$, $\overline{\lambda_2}$ est aussi racine (proposition 5.4), et on a $|\lambda_1\lambda_2\overline{\lambda_2}| = |\det(M)| = 1$ (*cf.* la définition 5.35 ; rappelons que le terme constant de $\chi(X)$ est égal à $-\det(M)$), d'où $|\lambda_2|^2 = 1$.

2. Supposons $M \in S\mathcal{O}_3(\mathbf{R})$; on a alors $\det M = 1$. Soient λ_1, λ_2 et λ_3 les valeurs propres de M avec $\lambda_1 = \pm 1$. On a $\lambda_1\lambda_2\lambda_3 = \det M = 1$. Si $\lambda_2 \notin \mathbf{R}$, on a $\lambda_3 = \overline{\lambda_2}$ et $\lambda_2\lambda_3 = \lambda_2\overline{\lambda_2} = \|\lambda_2\|^2 = 1$, d'où $\lambda_1 = 1$.
Si λ_1, λ_2 et λ_3 sont réelles, elles ne peuvent être toutes égales à -1 puisque leur produit vaut 1. La matrice M a donc au moins une valeur propre égale à 1, que l'on note λ_1.
Soit maintenant V_1 un vecteur propre correspondant à λ_1 ; les points de la droite D définie par V_1 sont invariants par l'application linéaire f de matrice M ; il suffit alors d'appliquer les résultats du paragraphe précédent dans le plan orthogonal à V_1.

3. Si $M \in \mathcal{O}_3(\mathbf{R}) \setminus S\mathcal{O}_3(\mathbf{R})$, on a $\det M = -1$ et le même raisonnement que pour *2.* ci-dessus montre qu'il existe une valeur propre $\lambda_1 = -1$. Si V_1 est un vecteur propre correspondant à λ_1 et P le plan orthogonal à V_1, notons s la réflexion définie par P, S sa matrice dans la base canonique. On voit alors immédiatement que l'on a $SM = MS \in S\mathcal{O}_3(\mathbf{R})$, et on peut appliquer *2.* à la matrice MS. ■

4.4.5. *Générateurs et centre

Étudions maintenant quelques propriétés algébriques du groupe $\mathcal{O}(\mathbf{R}^3)$.

Proposition 4.53.

1. *Le groupe $\mathcal{O}(\mathbf{R}^3)$ est engendré par les réflexions ; plus précisément, tout élément de $\mathcal{O}(\mathbf{R}^3)$ peut s'écrire comme le produit d'au plus trois réflexions ; tout élément de $S\mathcal{O}(\mathbf{R}^3)$ peut s'écrire comme le produit de deux réflexions.*
2. *Le groupe $S\mathcal{O}(\mathbf{R}^3)$ est engendré par les renversements. Tout élément de $S\mathcal{O}(\mathbf{R}^3)$ peut s'écrire comme le produit de deux renversements.*

Démonstration.
1. Soit d'abord $f \in S\mathcal{O}(\mathbf{R}^3)$ une rotation d'axe D. Alors f est le produit de deux réflexions par des plans contenant D (on applique la proposition 4.44 dans le plan P orthogonal à D).
Soit maintenant $f \in \mathcal{O}(\mathbf{R}^3) \setminus S\mathcal{O}(\mathbf{R}^3)$. Soit s une réflexion ; on a $fs \in S\mathcal{O}(\mathbf{R}^3)$. Il existe donc deux réflexions s_1 et s_2 telles que $fs = s_1s_2$, d'où $f = s_1s_2s$.
2. Soit $f \in S\mathcal{O}(\mathbf{R}^3)$. On peut donc écrire par ce qui précède $f = s_1s_2$ où s_1 et s_2 sont des réflexions. Mais l'opposé $-s$ d'une réflexion s est un renversement, comme on le voit par exemple sur la forme matricielle (7). L'application f est donc bien le produit de deux renversements, car on a $f = (-s_1)(-s_2)$. ■

Proposition 4.54. *Le centre de $\mathcal{O}(\mathbf{R}^3)$ est $\{Id, -Id\}$, Id désignant l'identité. Le centre de $S\mathcal{O}(\mathbf{R}^3)$ est réduit à $\{Id\}$.*

Commençons par démontrer deux lemmes.

Lemme 4.55. *Soit $f \in \mathrm{GL}(\mathbf{R}^n)$ (i.e. f est une aplication linéaire inversible) qui laisse stable toutes les droites vectorielles, alors f est une homothétie.*

Démonstration. Le cas $n = 1$ est évident. Si $n \geqslant 2$, soient V_1 et V_2 deux vecteurs indépendants de $\mathbf{R}^n$. On a par hypothèse $f(V_1) = \lambda_1 V_1$, $f(V_2) = \lambda_2 V_2$, $f(V_1 + V_2) = \lambda_3(V_1 + V_2)$ avec $\lambda_i \in \mathbf{R} \setminus \{0\}$.
On a donc la relation $\lambda_3(V_1 + V_2) = \lambda_1 V_1 + \lambda_2 V_2$, ce qui implique tout de suite que $\lambda_1 = \lambda_2 = \lambda_3$ puisque V_1 et V_2 sont linéairement indépendants ; on voit donc en faisant varier V_2 que f est bien une homothétie. ■

Lemme 4.56. *Soit r_θ une rotation d'axe une droite (orientée) D et d'angle θ (on suppose $-\pi < \theta \leqslant \pi$). Alors :*

- *si $g \in S\mathcal{O}(\mathbf{R}^3)$, $gr_\theta g^{-1}$ est la rotation d'axe $g(D)$ et d'angle θ ;*
- *si $g \in \mathcal{O}(\mathbf{R}^3) \setminus S\mathcal{O}(\mathbf{R}^3)$, $gr_\theta g^{-1}$ est la rotation d'axe $g(D)$ et d'angle $-\theta$.*

Démonstration. D'après la proposition 4.53, l'élément g est produit de deux réflexions si $g \in S\mathcal{O}(\mathbf{R}^3)$ et de trois réflexions si $g \in \mathcal{O}(\mathbf{R}^3) \setminus S\mathcal{O}(\mathbf{R}^3)$. Il suffit donc de montrer le lemme dans le cas où g est une réflexion.

Il est clair que la droite $g(D)$ est fixe sous l'action de $\tilde{r} = gr_\theta g^{-1}$. Comme $\tilde{r} \in S\mathcal{O}(\mathbf{R}^3)$ (parce que le déterminant de la matrice associée vaut $+1$), c'est donc une rotation d'axe $g(D)$; pour caractériser son angle $\tilde{\theta} \in]-\pi, \pi]$, il suffit de déterminer l'angle entre un vecteur $V_1 \in g(D)^\perp$ ($g(D)^\perp$ est le plan orthogonal à la droite $g(D)$) et son image $V_2 = \tilde{r}(V_1)$ qui est aussi dans le plan $g(D)^\perp$.

Rappelons comment on peut définir l'angle $e^{i\theta}$ entre deux vecteurs W_1 et W_2 unitaires et non colinéaires de $\mathbf{R}^3$. Un angle d'un plan euclidien orienté est caractérisé par son cosinus et son sinus. On choisit un vecteur unitaire W_3 orthogonal au plan (W_1, W_2), ce qui oriente ce plan (en définissant une base directe de ce plan comme une base (f_1, f_2) telle que la base (w_3, f_1, f_2) soit une base directe de $\mathbf{R}^3$) et permet de parler de l'angle $\theta = \widehat{W_1, W_2}$. On a alors :

$$\begin{array}{rcl} \cos\theta & = & W_1.W_2 \\ \sin\theta & = & \det(W_1, W_2, W_3) \end{array} \tag{10}$$

où $W_1.W_2$ est le produit scalaire et (W_1, W_2, W_3) la matrice des W_i développés en colonnes sur la base canonique. En effet, dans la base orthonormale directe (f_1, f_2, f_3) telle que $f_1 = W_3$, $f_2 = W_1$, la matrice (W_3, W_1, W_2) s'écrit : $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \cos\theta \\ 0 & 0 & \sin\theta \end{pmatrix}$, matrice de déterminant $\sin\theta$. Or ce déterminant est égal à celui de la matrice (W_1, W_2, W_3). Remarquons d'ailleurs que le déterminant de cette matrice est le « produit mixte » des vecteurs unitaires W_1, W_2, W_3. On voit donc que choisir $-W_3$ au lieu de W_3 (ce qui change l'orientation du plan (W_1, W_2)) change $\sin\theta$ en $-\sin\theta$ et donc θ en $-\theta$ si on a supposé $-\pi < \theta \leqslant \pi$ (si $\theta = \pi$ on pose aussi $-\theta = \pi$ puisque θ est défini modulo 2π et que l'on a supposé que la mesure des angles était dans l'intervalle $]-\pi, \pi]$).

Revenons à la preuve du lemme 4.56. Soit P_g le plan invariant par la réflexion g, et prenons $V_1 \in P_g \cap g(D)^\perp$, $V_2 = gr_\theta g^{-1}(V_1) = \tilde{r}(V_1)$, $V_3 = g(W)$, W étant le vecteur unitaire qui oriente la droite D. On a par hypothèse $\det(V_1, r_\theta(V_1), W) = \sin\theta$ par (10) et de même $\det(V_1, \tilde{r}(V_1), V_3) = \sin\tilde{\theta}$. Comme V_1 est invariant par la réflexion g par hypothèse, on a $V_1 = g(V_1), \tilde{r}(V_1) = g \circ r_\theta(V_1)$ et $V_3 = g(W)$ et donc si M_g désigne la matrice de l'endomorphisme g (dans la base canonique de $\mathbf{R}^3$), on a :

$$(V_1, \tilde{r}(V_1), V_3) = M_g \times (V_1, r_\theta(V_1), W)$$

d'où $\sin\tilde{\theta} = -\sin\theta$ (*cf.* (10)) puisque $\det M_g = -1$, et donc $\tilde{\theta} = -\theta$ (car on a évidemment $\cos\theta = \cos\tilde{\theta}$). ■

Montrons maintenant la proposition 4.54. Soit Z le centre de $\mathcal{O}(\mathbf{R}^3)$. Il est clair que $\{Id, -Id\} \subset Z$. Réciproquement soient $g \in Z$, D une droite vectorielle, r_D le renversement défini par la droite D. Comme $g \in Z$, on a $gr_D g^{-1} = r_D$, et aussi $gr_D g^{-1} = r_{g(D)}$ par le lemme 4.56. On a donc $D = g(D)$ pour toute droite D, et le lemme 4.55 montre que g est une homothétie ; comme g est aussi une isométrie, on a bien $g = \pm Id$. Le cas du groupe $S\mathcal{O}(\mathbf{R}^3)$ est analogue et laissé au lecteur (noter que $-\mathrm{Id} \notin S\mathcal{O}(\mathbf{R}^3)$!). Cela achève la preuve de la proposition 4.54.

> ***Remarque 4.57.*** Réciproquement, il est immédiat de voir que deux rotations d'axes orientés D_1 et D_2 et de même angle θ sont conjuguées dans $S\mathcal{O}(\mathbf{R}^3)$: il suffit de montrer qu'il existe une rotation r telle que $r(D_1) = D_2$.

4.4.6. *Simplicité de $S\mathcal{O}(\mathbf{R}^3)$

Théorème 4.58. *Le groupe $S\mathcal{O}(\mathbf{R}^3)$ est simple.*

Démonstration. Soit G un sous-groupe distingué non réduit à l'identité. On rappelle (*cf.* la proposition 4.53) que $\mathcal{O}^+(3, \mathbf{R})$ est engendré par les renversements et que (remarque 4.57) tous les renversements sont conjugués dans $S\mathcal{O}(\mathbf{R}^3)$. Ainsi pour montrer que G est égal à $S\mathcal{O}(\mathbf{R}^3)$ tout entier, il suffit de montrer que G contient un renversement.

Soit alors $u \in G$, une rotation d'axe D et soit P le plan orthogonal à D à l'origine de sorte que la restriction de u à P est une rotation d'angle θ. Quitte à remplacer u par u^{-1}, on peut supposer $0 < \theta \leqslant \pi$, et même $0 < \theta < \pi$ car si $\theta = \pi$, u est un renversement et la démonstration est finie. ■

Soient S^2 la sphère unité de $\mathbf{R}^3$, x un point de S^2, $y = u(x)$; on note d la distance entre x et y.

Lemme 4.59. *Pour tout $0 \leqslant d' \leqslant d$, il existe x_1, x_2 des points de la sphère unité à distance d' l'un de l'autre et tels que $x_2 = u(x_1)$.*

Démonstration. Soit $a \in D$, $\|a\| = 1$. Donnons d'abord une démonstration « heuristique » de ce lemme. Il est clair (*cf.* figure 4.1) que u transforme le grand

cercle C_1 de S^2 passant par a et x en le grand cercle C_2 passant par a et $y = u(x)$. Lorsque le point x_1 parcourt C_1 de x à a, la distance $d(x_1, x_2)$ tend vers 0 de façon continue ; elle prend donc toute valeur d' $(0 \leqslant d' \leqslant d)$ par le théorème des valeurs intermédiaires.

De manière plus précise, considérons le vecteur $x + \lambda a$ $(\lambda \in \mathbf{R})$.
On a $\|x + \lambda a\|^2 = 1 + \lambda^2$ et donc $x_1 = \frac{x+\lambda a}{\sqrt{1+\lambda^2}} \in S^2$ et $u(x_1) = \frac{1}{\sqrt{1+\lambda^2}}(y + \lambda a)$ (puisque $u(a) = a$) et donc $\|u(x_1) - x_1\| = \frac{d}{\sqrt{1+\lambda^2}}$. Si l'on suppose $d' \neq 0$, il suffit de prendre λ tel que $\frac{d}{\sqrt{1+\lambda^2}} = d'$, soit $\lambda = \frac{\sqrt{d^2-d'^2}}{d'}$. ■

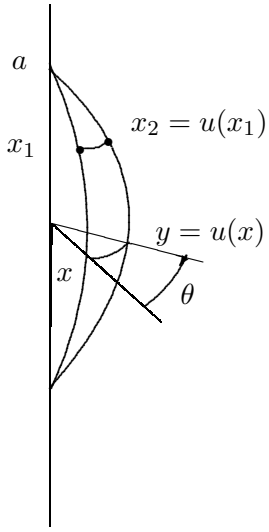


Figure 4.1

Lemme 4.60. *Étant donnés y_1, y_2 des points de S^2 distants de d' avec $0 \leqslant d' \leqslant d$, il existe $u' \in G$ tel que $u'(y_1) = y_2$.*

Démonstration. Prenons x_1 et x_2 deux points de S^2 comme dans le lemme 4.59. On a donc $d(x_1, x_2) = d' = d(y_1, y_2)$. Il existe une rotation $r \in S\mathcal{O}(\mathbf{R}^3)$ telle que $r(x_1) = y_1, r(x_2) = y_2$ (exercice 4.18). On pose alors $u' = r^{-1}ur$ ($u' \in G$ puisque G est distingué). ■

Démonstration. **(du théorème)** Considérons maintenant un point $y_1 \in S^2$ et la rotation r_n d'axe D et d'angle π/n. On a $\|r_n(x) - x\| = 2|\sin(\pi/2n)|$ et donc $\|r_n(x) - x\| < d$ (avec toujours $d = \|u(x) - x\|$).
D'après le lemme 4.60, il existe $u' \in G$ tel que $u'(x) = r_n(x)$; on a donc $u'^n(x) = -x$, ce qui entraîne que la rotation $u'^n \in G$ est un renversement. ■

EXERCICES

Les solutions des exercices et problèmes sont données en fin d'ouvrage.

GROUPES

Exercice 4.1.

1. Soit G un groupe dont tous les éléments $\neq 1$ sont d'ordre 2. Montrer que G est commutatif.
2. Montrer que l'ordre de G est alors de la forme 2^n (raisonner par récurrence sur l'ordre de G).
3. Soit G un groupe, $H \subset G$ un sous-groupe d'indice 2. Montrer que H est distingué dans G.

Exercice 4.2. Soient G un groupe et C un sous-groupe de son centre. Montrer que si le groupe quotient G/C est cyclique, alors G est abélien.

Exercice 4.3. Soient G un groupe fini et H un sous-groupe distingué de G d'ordre n. On suppose que n est premier avec l'indice de H dans G. Montrer que H est le seul sous-groupe d'ordre n de G.

Exercice 4.4. Soit G un groupe. On note e l'élément neutre de G. Étant donnés deux sous-groupes A et B de G, on désigne par AB le sous-ensemble de G formé des éléments de G de la forme ab, où a est dans A et où b est dans B.

Considérons désormais deux sous-groupes H et K de G.

1. Montrer que HK=KH si et seulement si HK est un sous-groupe de G.
2. Montrer que si H est distingué dans G on a HK=KH (et donc HK est un sous-groupe de G).
3. Montrer que si H est distingué dans G l'application $\varphi : K \to HK/H$ définie par $\varphi(k) = kH$ réalise (par passage au quotient) un isomorphisme de $K/H \cap K$ sur HK/H.
4. Montrer que si H et K sont distingués dans G et si $H \cap K = \{e\}$, l'application $\psi : H \times K \to HK$ définie par $\psi\big((h,k)\big) = hk$ est un isomorphisme de groupes.

Soit $SL_2(\mathbf{Z})$ le groupe des matrices carrées d'ordre 2 à coefficients dans $\mathbf{Z}$ dont le déterminant est 1. Posons

$$M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{et} \quad N = \begin{pmatrix} 0 & 1 \\ -1 & -1. \end{pmatrix}$$

5. Déterminer l'ordre de M, de N et de MN dans $SL_2(\mathbf{Z})$.
6. Soient H (resp. K) le sous-groupe de $SL_2(\mathbf{Z})$ engendré par M (resp. par N). Montrer que HK n'est pas un groupe.

Exercice 4.5.

1. Soit G un groupe non commutatif d'ordre 10 ; montrer que G contient un élément d'ordre 5 (utiliser la question 1. de l'exercice 4.1).
2. Montrer que G contient un sous-groupe distingué H d'ordre 5 et que tout élément $x \in G \setminus H$ est d'ordre deux (considérer le groupe quotient G/H).
3. Montrer que G est isomorphe au groupe dihédral D_5 (considérer l'ordre d'un élément xh).

Exercice 4.6. Soit p un nombre premier, G un groupe de cardinal p^k. Montrer que pour tout $s \leqslant k$, G possède un sous-groupe d'ordre p^s (raisonner par récurrence sur k en considérant le centre de G).

GROUPE SYMÉTRIQUE

Exercice 4.7. Dans le groupe symétrique $\mathcal{S}_5$, combien y a-t-il de 5-cycles distincts ? de 4-cycles distincts ?

Exercice 4.8. Soit $p \geqslant 5$ un nombre premier et $H \subset \mathcal{S}_p$ un sous-groupe tel que $1 < [\mathcal{S}_p : H] < p$.

1. Montrer que tout cycle d'ordre p est contenu dans H.
2. Montrer que tout cycle d'ordre 3 est produit de deux cycles d'ordre p.
3. Montrer que $H = \mathcal{A}_p$.
4. Montrer que $\mathcal{S}_5$ ne contient aucun sous-groupe de cardinal 30, 40.

Exercice 4.9. Soit σ l'élément de $\mathcal{S}_{11}$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 10 & 7 & 9 & 11 & 2 & 1 & 3 & 5 & 8 & 4 & 6 \end{pmatrix}.$$

Décomposer σ en un produit de cycles à supports disjoints. Préciser l'ordre de σ et la signature de σ.

Exercice 4.10. (*cf.* la remarque 4.21).

1. Montrer que $\mathcal{S}_n$ est engendré par les systèmes suivants et pas par un sous-ensemble strict :
   (i) les transpositions $(1\ i)$ pour $i = 2, \cdots, n$;
   (ii) les transpositions $(i\ i+1)$ pour $i = 1, \cdots, n-1$;
   (iii) le cycle $c_n = (1\ \cdots\ n)$ et la transposition $\tau = (1\ 2)$.
2. Montrer que $\mathcal{A}_n$ pour $n \geqslant 3$ est engendré par les 3-cycles.
3. Montrer que si un ensemble de k transpositions engendre S_n, alors $k \geqslant n-1$.

Exercice 4.11. Donner la décomposition en cycles à supports disjoints de $(1\,2\,3)(2\,4)(1\,3)$ et de $(1\,2\,\cdots\,n-1)(1\,n)$ (*cf.* la proposition 4.14).

Exercice 4.12. Quel est l'ordre maximal d'un élément de $\mathcal{S}_5$?

Exercice 4.13. Quelle est la décomposition en cycles à supports disjoints de c^k, où $c = (1 \cdots n) \in \mathcal{S}_n$?

OPÉRATION D'UN GROUPE SUR UN ENSEMBLE

Exercice 4.14. Soit $n \geqslant 5$.

1. Soit H un sous-groupe d'indice n de $\mathcal{S}_n$. Montrer que H est isomorphe à $\mathcal{S}_{n-1}$. (Le groupe $\mathcal{S}_n$ opère sur $\mathcal{S}_n/H$ par translations à gauche, ce qui donne un morphisme ϕ de $\mathcal{S}_n$ dans les permutations de $\mathcal{S}_n/H$; montrer que ϕ est injectif et déterminer l'image de H).
2. Soit H un sous-groupe d'indice k de $\mathcal{S}_n$ avec $1 < k < n$. Montrer que $k = 2$ et $H = \mathcal{A}_n$.

Exercice 4.15. Soit G un groupe fini. Soit p le plus petit facteur premier de l'ordre de G. Montrer qu'un sous-groupe H de G d'indice p est distingué dans G (faire opérer H sur l'ensemble quotient G/H des classes à gauche de G modulo H par translation à gauche).

Exercice 4.16. Soit G un groupe fini d'ordre 21 opérant sur un ensemble fini E ayant n éléments.

1. On suppose $n = 19$. On suppose aussi qu'il n'existe pas de point fixe dans E sous l'action de G. Combien y a-t-il d'orbites dans E ? Quel est le nombre d'éléments dans chacune de ces orbites ?
2. On suppose $n = 11$. Montrer qu'il existe au moins un point fixe dans E sous l'action de G.
3. Soit n un entier > 11. Montrer qu'il existe un ensemble ayant n éléments sur lequel G opère sans point fixe.

EXEMPLES LIÉS À LA GÉOMÉTRIE

Exercice 4.17. Soient E un espace vectoriel euclidien et f une isométrie de E. Montrer que les conditions suivantes sont équivalentes :

(i) f est une symétrie.

(ii) f est d'ordre 2 dans le groupe orthogonal de E.

(iii) f est diagonalisable.

Exercice 4.18. Soient a et b deux vecteurs distincts de même norme de $\mathbf{R}^3$. Montrer qu'il existe une unique symétrie par rapport à un plan de $\mathbf{R}^3$ qui transforme a en b.

Exercice 4.19. Soit u l'endomorphisme de $\mathbf{R}^3$ dont la matrice dans la base canonique est

$$M = \frac{1}{4}\begin{pmatrix} -2 & -\sqrt{6} & \sqrt{6} \\ \sqrt{6} & 1 & 3 \\ -\sqrt{6} & 3 & 1. \end{pmatrix}$$

1. Montrer que u est une isométrie. Est-elle directe ou indirecte ?
2. Trouver une base orthonormée de $\mathbf{R}^3$ dans laquelle la matrice de u soit de la forme :

$$M = \begin{pmatrix} \varepsilon & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$$

avec $\varepsilon^2 = 1$ et $\theta \in \mathbf{R}$. Déterminer ε et $\cos\theta$. Expliciter $\sin\theta$ dans la base considérée.

TROIS POLYÈDRES RÉGULIERS ET LEUR GROUPE

Exercice 4.20. *Le tétraèdre régulier*
On note $\mathcal{I}_T$ le groupe des isométries qui laissent le tétraèdre globalement invariant et $\mathcal{D}_T$ le sous-groupe de $\mathcal{I}_T$ constitué par les déplacements de $\mathcal{I}_T$.

1. Montrer que l'on peut considérer $\mathcal{I}_T$ (resp. $\mathcal{D}_T$) comme un sous-groupe de $\mathcal{O}(\mathbf{R}^3)$ (resp. $S\mathcal{O}(\mathbf{R}^3)$).
2. Montrer que $\mathcal{I}_T$ est fini de cardinal $\leqslant 24$.
3. Montrer que $\mathcal{I}_T \simeq \mathcal{S}_4$ et $\mathcal{D}_T \simeq \mathcal{A}_4$.

Exercice 4.21. *Le cube*
Avec des notations analogues à celles du tétraèdre, on introduit $\mathcal{I}_C$ et $\mathcal{D}_C$.

1. Montrer que $\mathcal{I}_C$ est fini. Quel est l'indice $[\mathcal{I}_C : \mathcal{D}_C]$?
2. En faisant opérer $\mathcal{I}_C$ sur l'ensemble Δ des 4 diagonales, montrer que $\mathcal{D}_C$ est isomorphe à $\mathcal{S}_4$.

Exercice 4.22. *L'octaèdre*
Soit S la sphère circonscrite à l'octaèdre. Étant donné un point $P \neq O$, son plan polaire est $\{M \ / \ (\vec{OM}, \vec{OP}) = 1\}$, où $(.,.)$ désigne le produit scalaire canonique. De même le point dual d'un plan H ne contenant pas O est le point P tel que $(\vec{OP}, \vec{OM}) = 1$ pour tout point M de H. On introduit le cube dont les faces sont les plans polaires aux 6 sommets de l'octaèdre par rapport à S. On l'appelle le cube dual à l'octaèdre. Montrer qu'une isométrie laisse l'octaèdre globalement invariant si et seulement s'il laisse son cube dual globalement invariant. Donner alors le groupe de l'octaèdre.

PROBLÈMES

Problème 4.1. *Le groupe dihédral d'ordre 26*

Soient p un nombre premier, n un entier positif, G un groupe d'ordre pn et $H \subset G$ un sous-groupe d'indice p.

On note G/H l'ensemble (de cardinal p) des classes à gauches xH. On identifie le groupe des permutations de l'ensemble $\{G/H\}$ avec le groupe symétrique S_p et on note :

$$\phi : \ G \to S_p$$

le morphisme défini par la multiplication à gauche des classes par les éléments de G.

1. Montrer que
$$H_1 = \ker \phi = \cap g H g^{-1},$$
l'intersection portant sur tous les éléments $g \in G$.
2. On suppose que p est le plus petit nombre premier divisant $|G|$. Montrer que H est distingué (on montrera que $H = H_1$).
3. Soit L un groupe fini dont tous les éléments sont d'ordre deux. Montrer que L est commutatif.
Dans la suite, G est un groupe non commutatif d'ordre 26.
4. Montrer que G contient un élément d'ordre 13.
5. Montrer que G contient un sous-groupe distingué H d'ordre 13, et que tout élément $x \in G$, $x \notin H$ est d'ordre deux.
6. Montrer que G est isomorphe au groupe dihédral D_{13}.

Problème 4.2. *« Jeu de taquin »*

Le jeu de taquin, dit $15 - 14$, fut commercialisé en 1873. Il s'agissait d'un carré constitué de 15 cases numérotées de 1 à 15 ainsi qu'un seizième emplacement vide :

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Une opération élémentaire consiste à faire glisser une des cases numérotées dans l'espace libre comme dans la figure dessous :

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	→

1	2	3	4
5	6	7	8
9	10	11	12
13	15		14

Le jeu suscita un engouement extraordinaire après le défi lancé par le fabricant qui avait inversé les cases 14 et 15 et proposé une fortune au premier qui parviendrait à remettre les cases dans le bon ordre.

Afin de résoudre le défi, on propose de numéroter la case vide par 16 et de noter la configuration suivante :

3	5	11	6
7	9	14	12
1	10		2
4	15	8	13

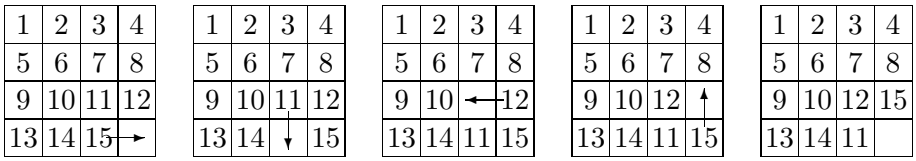
sous la forme

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 3 & 5 & 11 & 6 & 7 & 9 & 14 & 12 & 1 & 10 & 16 & 2 & 4 & 15 & 8 & 13 \end{pmatrix}$$

et de le considérer comme un élément de $\mathcal{S}_{16}$. Ainsi un mouvement élémentaire correspond à une transposition de 16 avec un de ses voisins, ici 14, 10, 8 et 2. On considère le marquage suivant :

●		●	
	●		●
●		●	
	●		●

1. Montrer que si la case 16 est sur une case marquée (resp. non marquée) alors la permutation associée est de signature 1 (resp. -1). Que penser du défi proposé à l'époque ?
2. On inverse, en démontant le jeu, les cases 14 et 15. On veut alors déterminer quelles sont exactement toutes les permutations de $\mathcal{S}_{16}$ que l'on peut obtenir. On commence par étudier celles telles que 16 est invariante, de sorte que l'on peut considérer la permutation en question comme un élément de $\mathcal{S}_{15}$ qui d'après (1) est un élément de $\mathcal{A}_{15}$.
   (i) On considère les déplacements élémentaires suivants :



   Montrer que l'on obtient un 3-cycle que l'on précisera.
   (ii) Construire d'autres 3-cycles, par exemple $(1\ 6\ 2)$, $(7\ 6\ 11)$, $(6\ 7\ 3)$, $(5\ 9\ 6)$, $(6\ 10\ 7)$, $(4\ 3\ 8)$, $(11\ 15\ 12)$, $(10\ 14\ 11)$, $(9\ 13\ 10)$.
   (iii) Montrer que $\mathcal{A}_{15}$ est engendré par les 3-cycles $(1\ 2\ i)$ pour $3 \leqslant i \leqslant 15$.
   (iv) Montrer que toute permutation de $\mathcal{A}_{15}$ peut être obtenue.
3. Déterminer alors toutes les configurations possibles. En outre en démontant et remontant le jeu de manière aléatoire, quelle est la probabilité de pouvoir, en jouant, revenir sur la position ordonnée comme précédemment ?

Chapitre **5**

Racines des polynômes

Ce chapitre est consacré aux racines des polynômes à une variable. La section 5.2, qui traite des racines réelles des polynômes à coefficients dans $\mathbf{R}$, est la plus originale en ce sens que ces questions, bien que fondamentales à notre avis, sont rarement traitées dans les ouvrages d'enseignement ; les autres parties sont plus classiques (irréductibilité des polynômes à coefficients dans $\mathbf{Q}$, résultant, discriminant, fonctions symétriques des racines, etc.).

5.1 GÉNÉRALITÉS, IRRÉDUCTIBILITÉ

Tout d'abord, fixons deux notations. Soit $P \in K[X]$ (K étant un corps). La notation $Z(P)$ désigne le nombre de racines de P (dans K) comptées avec multiplicités, et $z(P)$ le nombre de racines distinctes.

De même si $K = \mathbf{R}$ et si $I \subset \mathbf{R}$ est un intervalle, $Z_I(\mathbf{R})$ (resp. $z_I(\mathbf{R})$) désigne le nombre de racines de P dans I comptées avec multiplicités (resp. le nombre de racines distinctes dans I).

D'autre part, si $a \in \mathbf{R}$, $(a)_+$ (resp. $(a)_-$) désigne un ensemble $V \cap]a, +\infty)$ (resp. $V \cap (-\infty, a[$), où V est un voisinage de a arbitrairement petit.

5.1.1. Polynômes à coefficients complexes

Rappelons le théorème de d'Alembert-Gauss :

Théorème 5.1. *Tout polynôme $P \in \mathbf{C}[X]$ de degré $d > 0$ possède une racine dans $\mathbf{C}$.*

Ce théorème est admis. On en déduit que si P est de degré $d > 0$, il a exactement d racines complexes, comptées avec multiplicités (autrement dit, $\text{card}(Z(P)) = d$). De plus, les polynômes unitaires irréductibles sont les $X - \alpha$ pour $\alpha \in \mathbf{C}$. Tout polynôme non nul de $\mathbf{C}[X]$ s'écrit donc de manière unique à l'ordre près des facteurs (proposition 3.3) :

$$P(X) = \lambda \prod_{i=1}^{k} (X - \alpha_i)^{\nu_i} \tag{1}$$

avec $\lambda \in \mathbf{C}^*$, les ν_i étant des entiers positifs vérifiant $\sum \nu_i = d$.

Donnons maintenant une borne supérieure sur les modules des racines de P.

Proposition 5.2. *Soit $P \in \mathbf{C}[X]$, $P = a_0 + a_1 X + \cdots + a_d X^d$, avec $a_d \neq 0$. Alors, si $\alpha \in \mathbf{C}$ est une racine de P, on a :*

$$|\alpha| \leqslant 1 + \sup_{1 \leqslant i \leqslant d-1} \frac{|a_i|}{|a_d|}. \tag{2}$$

Démonstration. Posons $Q(X) = \frac{P(X)}{a_d}$, $b_i = \frac{|a_i|}{|a_d|}$ et $B = \sup(b_i)$. Le polynôme Q est unitaire, a les mêmes racines que P et vérifie :

$$|Q(x)| \geqslant |x|^d - B(|x|^{d-1} + \cdots + 1) = |x|^d - B\frac{|x|^d - 1}{|x| - 1}$$

pour tout $x \in \mathbf{C}$, $|x| \neq 1$. Si $|x| > 1 + B$, on a $1 > \frac{B}{|x|-1}$ et $|x|^d > \frac{|x|^d B}{|x|-1}$, d'où

$$|Q(x)| > \frac{B}{|x| - 1}\big(|x|^d - (|x|^d - 1)\big) = \frac{B}{|x| - 1} > 0,$$

et donc x ne peut donc être racine de Q. ■

Remarque 5.3. À titre d'exercice, le lecteur pourra montrer de manière analogue que :

$$|\alpha| \leqslant \sup_{1 \leqslant i \leqslant d-1} \Big(d\frac{|a_i|}{|a_d|}\Big)^{1/d-i}. \tag{3}$$

(*cf.* exercice 5.10).

5.1.2. Polynômes à coefficients réels

Proposition 5.4. *Soit $P \in \mathbf{R}[X]$. Soit $\alpha \in \mathbf{C}$ une racine de P de multiplicité ν. Alors $\overline{\alpha}$ (conjugué de α) est aussi racine de P de même multipicité ν.*

Démonstration. Par hypothèse, on peut écrire $P(X) = (X - \alpha)^\nu Q(X)$ avec $Q \in \mathbf{C}[X]$, $Q(\alpha) \neq 0$. Pour un polynôme $Q \in \mathbf{C}[X]$, notons $\overline{Q}$ le polynôme dont les coefficients sont les conjugués de ceux de Q. Le fait que la conjugaison $z \mapsto \overline{z}$ soit un automorphisme du corps $\mathbf{C}$, et donc en particulier que $\forall\ z_1, z_2 \in \mathbf{C}$ on ait $\overline{z_1}.\overline{z_2} = \overline{z_1 z_2}$ et $\overline{z_1} + \overline{z_2} = \overline{z_1 + z_2}$ implique que si Q_1 et Q_2 sont deux polynômes à

coefficients complexes, on a $\overline{Q_1 Q_2} = \overline{Q_1}\ \overline{Q_2}$. Comme $P \in \mathbf{R}[X]$, on a $\overline{P} = P$, et donc :

$$P(X) = (X-\alpha)^\nu Q(X) = (X-\overline{\alpha})^\nu \overline{Q}(X).$$

Comme on peut supposer que $\alpha \notin \mathbf{R}$ (sinon la proposition est triviale), les polynômes $(X-\alpha)^\nu$ et $(X-\overline{\alpha})^\nu$ sont premiers entre eux dans $\mathbf{C}[X]$ (puisque les polynômes $X-\alpha$ et $X-\overline{\alpha}$ sont irréductibles et différents). Le lemme de Gauss 1.27 implique alors que $(X-\overline{\alpha})^\nu$ divise $Q(X)$. On a donc :

$$P(X) = (X-\alpha)^\nu (X-\overline{\alpha})^\nu S(X),$$

avec $S(\alpha) \neq 0$ et *a priori* $S(X) \in \mathbf{C}[X]$. Mais en prenant le conjugué de cette relation, on voit que $S(X) = \overline{S}(X)$, *i.e.* $S(X) \in \mathbf{R}[X]$, ce qui implique aussi $S(\overline{\alpha}) \neq 0$. ■

Corollaire 5.5.

1. *Si $P \in \mathbf{R}[X]$ est de degré d, $Z(P) \leqslant d$ et $Z(P) \equiv d \bmod 2$.*
2. *Les polynômes unitaires irréductibles sur $\mathbf{R}$ sont les polynômes de la forme $X-\alpha$ ou $X^2 - bX + c$ avec $b^2 - 4c < 0$.*

Démonstration. Immédiate en groupant chaque racine non réelle avec sa conjuguée. ■

5.1.3. Polynômes à coefficients rationnels

Définition 5.6. *Soit*

$$P = a_0 + a_1 X + \cdots + a_d X^d$$

un polynôme à coefficients entiers.

1. *On définit le* contenu *de P comme le nombre*

$$c(P) = \mathrm{PGCD}(a_0, a_1, \ldots, a_d)$$

   (le PGCD étant défini au signe près, on prend par convention le PGCD positif.)
2. *Un polynôme $P \in \mathbf{Z}[X]$ est dit* primitif *si $c(P) = 1$.*
3. *Un polynôme $P \in \mathbf{Z}[X]$ est dit* irréductible *s'il n'est pas produit de deux éléments non inversibles de $\mathbf{Z}[X]$.*

Si $P \in \mathbf{Z}[X]$ on a donc $P = c(P)\tilde{P}$ avec $\tilde{P}$ primitif. En particulier tout polynôme unitaire est primitif.

Si $P \in \mathbf{Z}[X]$ est de degré > 0 et non primitif, il n'est pas irréductible au sens de la définition ci-dessus : on peut en effet écrire $P = c(P)\tilde{P}$ avec $c(P) \neq \pm 1$ donc non inversible dans $\mathbf{Z}$ (et donc dans $\mathbf{Z}[X]$) et $\tilde{P}$ non inversible puisque de degré > 0 par hypothèse.

La proposition suivante est connue sous le nom de « lemme de Gauss ». A ne pas confondre avec le lemme de Gauss 1.27 !

Proposition 5.7. *« Lemme de Gauss » Soit $P \in \mathbf{Z}[X]$ un polynôme primitif. Alors P est irréductible dans $\mathbf{Q}[X]$ si et seulement s'il est irréductible dans $\mathbf{Z}[X]$.*

Démonstration. Si $P \in \mathbf{Z}[X]$ est primitif et irréductible dans $\mathbf{Q}[X]$ (on dit aussi irréductible sur $\mathbf{Q}$), il est évidemment irréductible sur $\mathbf{Z}$ (car si $P = P_1P_2$ dans $\mathbf{Z}[X]$, P_1 ou P_2 doit être constant car P est irréductible sur $\mathbf{Q}$, et cette constante doit être ± 1 puisque P est primitif).

Il faut maintenant montrer la réciproque (qui est moins évidente), à savoir que si P est irréductible sur $\mathbf{Z}$, il est aussi irréductible sur $\mathbf{Q}$.

Lemme 5.8. *Soient $P, Q \in \mathbf{Z}[X]$. Alors*

$$c(PQ) = c(P)c(Q). \tag{4}$$

Démonstration. On peut écrire $PQ = c(P)c(Q)\tilde{P}\tilde{Q}$, où $\tilde{P}$ et $\tilde{Q}$ sont primitifs. Les coefficients du polynôme PQ sont donc divisibles par $c(P)c(Q)$, ce qui signifie que $c(P)c(Q)$ divise $c(PQ)$. Pour voir que $c(PQ) = c(P)c(Q)$, il suffit de montrer que $\tilde{P}\tilde{Q}$ est primitif, *i.e.* que le produit de deux polynômes primitifs est primitif.

Supposons donc P et Q primitifs, et posons $P = a_0 + a_1X + \cdots + a_dx^d$ et $Q = b_0 + b_1X + \cdots + b_sX^s$. Raisonnons par l'absurde et considérons un diviseur premier p de $c(PQ)$. Si on note (comme dans la preuve de la proposition 5.9 ci-dessous) $\overline{P}$ la réduction d'un polynôme P modulo p (on a ainsi $\overline{P} \in \mathbf{Z}/p\mathbf{Z}[X]$), on a donc $\overline{PQ} = 0$ par hypothèse, ce qui est absurde puisque $\overline{PQ} = \overline{P} \cdot \overline{Q}$, $\overline{P} \neq 0$, $\overline{Q} \neq 0$ et que l'anneau $\mathbf{Z}/p\mathbf{Z}[X]$ est intègre, $\mathbf{Z}/p\mathbf{Z}$ étant un corps. ■

Démontrons maintenant la proposition 5.7. Soit $P \in \mathbf{Z}[X]$ un polynôme primitif et irréductible sur $\mathbf{Z}$ tel que $P = P_1'P_2'$ dans $\mathbf{Q}[X]$, avec P_1' et P_2' non constants. En réduisant les coefficients de P_1' et P_2' au même dénominateur, on obtient une relation $kP = P_1P_2$ dans $\mathbf{Z}[X]$ (avec $k \in \mathbf{Z}$). Comme $c(P) = 1$ par hypothèse, on obtient $c(P_1)c(P_2) = c(P_1P_2) = |k|$ en utilisant (4). En posant $P_i = c(P_i)\tilde{P}_i$ $(i = 1, 2)$, on en déduit $P = \tilde{P}_1\tilde{P}_2$ dans $\mathbf{Z}[X]$ avec $\tilde{P}_1$ et $\tilde{P}_2$ non constants, ce qui est absurde puisque l'on a supposé P irréductible sur $\mathbf{Z}$. ■

Proposition 5.9. *« Critère de Eisenstein »*
Soient $P = a_0 + \cdots + a_dX_d \in \mathbf{Z}[X]$ un polynôme non constant, p un nombre premier tel que :
1. $p \nmid a_d$
2. $p | a_i$ pour $0 \leqslant i \leqslant d-1$
3. $p^2 \nmid a_0$

Alors P est irréductible dans $\mathbf{Q}[X]$.

Démonstration. En divisant par $c(P)$ on peut supposer P primitif. Il suffit alors de montrer que P est irréductible dans $\mathbf{Z}[X]$ par la proposition 5.7. Raisonnons par l'absurde : supposons que $P = P_1P_2$ dans $\mathbf{Z}[X]$, avec P_1 et P_2 non constants. Si $Q = c_0 + \cdots + c_qX^q \in \mathbf{Z}[X]$ et si p est un nombre premier, notons $\overline{Q} = \overline{c_0} + \cdots + \overline{c_q}X^q$

le polynôme de $\mathbf{F_p}[X]$ obtenu en prenant les classes des coefficients modulo p (« réduction de Q modulo p »). Rappelons que $\mathbf{F_p}$ désigne le corps premier $\mathbf{Z}/p\mathbf{Z}$. L'égalité $P = P_1P_2$ donne par réduction modulo p la relation $\overline{P} = \overline{P_1}\ \overline{P_2}$ dans $\mathbf{F_p}[X]$ (car il est immédiat de voir que $\overline{P_1P_2} = \overline{P_1} \cdot \overline{P_2}$ puisque l'application $a \mapsto \overline{a}$ de $\mathbf{Z}$ dans $\mathbf{F_p}$ est un morphisme d'anneaux). Mais par hypothèse $\overline{P} = \overline{a_d}X^d$. Notons α_0 et β_0 les coefficients constants de P_1 et P_2 ; on en déduit que $\overline{\alpha_0} = \overline{\beta_0} = 0$ dans $\mathbf{F_p}$: on a en effet $\overline{\alpha_0}\overline{\beta_0} = \overline{a_0} = 0$, d'où $\overline{\alpha_0} = 0$ ou $\overline{\beta_0} = 0$ puisque $\mathbf{F_p}$ est un corps. Si par exemple $\overline{\alpha_0} = 0$, notons $\overline{\alpha_r}X^r$ le monôme non nul de plus bas degré de $\overline{P_1}$; on alors $\overline{\beta_0}\overline{\alpha_r} = \overline{a_r} = 0$ d'où $\overline{\beta_0} = 0$. On en déduit que $p|\alpha_0$ et $p|\beta_0$, et donc que $p^2|\alpha_0\beta_0$, soit $p^2|a_0$, ce qui est contraire à l'hypothèse *3.* ■

Corollaire 5.10. *Pour tout entier $n \geqslant 2$ il existe une polynôme unitaire irréductible de degré n dans $\mathbf{Q}[X]$.*

Démonstration. Le polynôme $X^n - 2$ est irréductible sur $\mathbf{Q}$ car il satisfait aux hypothèses de la proposition 5.9 avec $p = 2$. ■

Corollaire 5.11. *Soit p un nombre premier. Alors le polynôme*

$$P = 1 + X + X^2 + \cdots + X^{p-1}$$

est irréductible sur $\mathbf{Q}$.

Démonstration. Il suffit d'effectuer le changement de variables $X = Y + 1$ et d'appliquer la proposition 5.9. ■

5.2 LES RACINES RÉELLES

Définition 5.12. *Soit $(a) = (a_0, \ldots, a_d)$ une suite finie de nombres réels. On appelle* variation $V(a)$ *de la suite (a) le nombre de changements de signes dans la suite des a_i (sans compter les zéros). Si $P(X) = a_0 + a_1X + \cdots + a_dX^d$ est un polynôme à coefficients réels, on pose $(a) = (a_0, \ldots, a_d)$, et $V(P) = V(a)$.*

Par exemple, si $(a) = (1, -3, 0, 0, 4, 0, -12, 5)$, alors $V(a) = 4$.

Proposition 5.13. *« Lemme de Descartes »*

Soient $P(X) = a_0 + a_1X + \cdots + a_dX^d$ un polynôme à coefficients réels, $Z_+(P)$ le nombre de racines > 0 de P comptées avec multiplicités. Alors

$$Z_+(P) \leqslant V(P) \quad \text{et} \quad Z_+(P) \equiv V(P) \mod 2 \tag{5}$$

Démonstration. On suppose $a_d \neq 0$ et on raisonne par récurrence sur d, le cas $d = 0$ étant évident. On peut supposer $a_0 \neq 0$, sinon on divise P par X (ce qui ne change pas les racines > 0 ni $V(P)$), et on applique l'hypothèse de récurrence. On suppose aussi $a_0 > 0$, quitte à éventuellement multiplier P par -1.

Considérons le polynôme dérivé $P'(X)$. Si $P(X) = a_0 + a_s X^s + \cdots + a_d X^d$ avec $a_s \neq 0$, on a $P' = s a_s X^{s-1} + \cdots + d a_d X^{d-1}$. Le lemme suivant est une conséquence immédiate du théorème de Rolle :

Lemme 5.14.

1. *Soit $z \in \mathbf{R}$ un zéro de P avec multiplicité ν. Alors si $\nu > 1$, c'est un zéro de P' avec multiplicité $\nu - 1$.*
2. *Soient $z_i < z_{i+1}$ deux zéros consécutifs de P (i.e. tels que P ne s'annule pas dans l'intervalle $]z_i, z_{i+1}[$). Alors $Z_{]z_i,z_{i+1}[}(P')$ est impair (en particulier $Z_{]z_i,z_{i+1}[}(P') \geqslant 1$, ce qui est l'énoncé du « Théorème de Rolle » pour les polynômes).*

Démonstration. *1.* Par hypothèse $P(X) = (X - z)^\nu Q(X)$ avec $Q(z) \neq 0$. En dérivant cette égalité, on voit immédiatement que si $\nu > 1$, z est un zéro de P' avec multiplicité $\nu - 1$.

2. Comme P ne s'annule pas dans $]z_i, z_{i+1}[$, P' a des signes opposés en $(z_i)_+$ et en $(z_{i+1})_-$. Comme un polynôme change de signe en un zéro de multiplicité ν si et seulement ν est impair, on voit que le nombre de zéros (avec multiplicités) de P' dans l'intervalle $]z_i, z_{i+1}[$ est impair. ■

Notons $z_1, \ldots, z_k$ les zéros > 0 de P, avec multiplicités $\nu_1, \ldots, \nu_k$.

On a $\sum_{i=1}^k \nu_i = Z_+(P)$. Deux cas se présentent.

a) $a_s > 0$.

On a $V(P) = V(a_0, a_s, \ldots, a_d)$ et $V(P') = V(s a_s, \ldots, d a_d) = V(a_s, \ldots, a_d)$.
On a donc $V(P) = V(P')$ dans ce cas puisque on a supposé $a_0 > 0$.

Comptons les zéros positifs de P' :

- $Z_{]0,z_1[}(P')$ est impair (donc $\geqslant 1$) par le lemme 5.14 puisque $P'(0_+) > 0$ (car $P'(X) = X^{s-1}(a_{s-1} + \cdots)$) et $P'((z_1)_-) < 0$: *cf.* Figure 5.1.
- Chaque z_i tel que $\nu_i > 1$ est un zéro de P' avec multiplicité $\nu_i - 1$.
- Chaque $Z_{]z_i,z_{i+1}[}(P')$, $1 \leqslant i \leqslant k-1$ est impair donc $\geqslant 1$ (lemme 5.14).
- Entre $(z_k)_+$ et $+\infty$, il y a un nombre pair de zéros de P' avec multiplicités (ce nombre peut être nul), car comme P ne s'annule pas entre z_k et $+\infty$, P' a le même signe en $(z_k)_+$ et au voisinage de l'infini.

On obtient donc dans ce cas :

$$Z_+(P') \geqslant 1 + \sum_{i=1}^k (\nu_i - 1) + k - 1 = \sum_{i=1}^k \nu_i = Z_+(P)$$

et aussi :

$$Z_+(P') \equiv 1 + \sum_{i=1}^k (\nu_i - 1) + k - 1 = Z_+(P) \bmod 2.$$

Comme $V(P) = V(P')$, les relations ci-dessus et l'hypothèse de récurrence appliquée à P' donnent :

$$Z_+(P) \leqslant Z_+(P') \leqslant V(P') = V(P) \text{ et } Z_+(P) \equiv Z_+(P') \equiv V(P) \bmod 2.$$

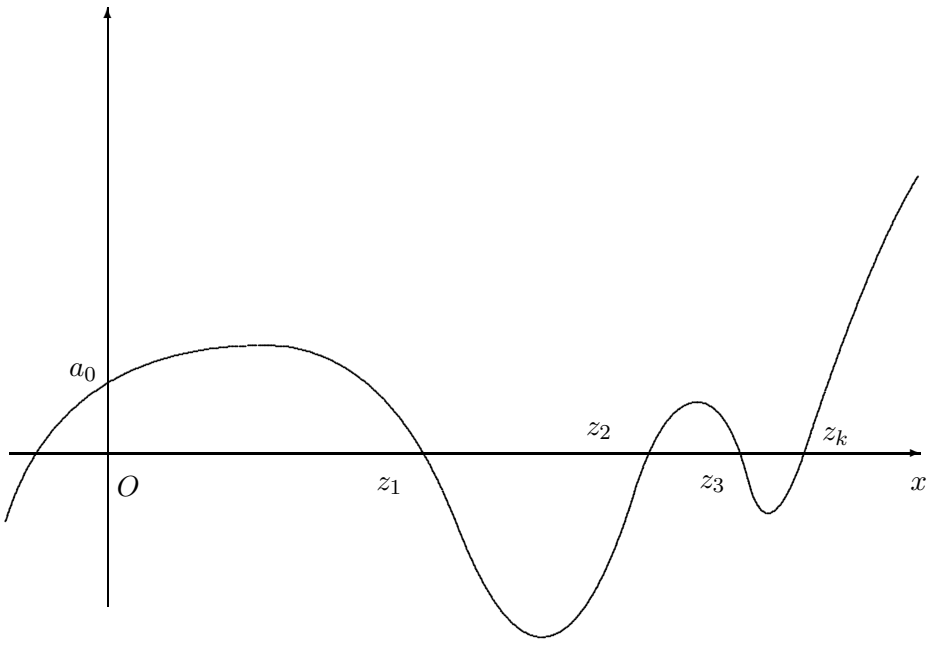


Figure 5.1 : cas $a_s > 0$

b) $a_s < 0$. On a alors $V(P') = V(P) - 1$.

La suite du raisonnement est la même que pour le cas a), sauf qu'il y a cette fois-ci un nombre pair (qui peut être nul) de zéros z' de P' (comptés avec multiplicités) tels que $0 < z' < z_1$. On en déduit donc que :

$$Z_+(P) \leqslant Z_+(P') + 1 \leqslant V(P') + 1 = V(P) \quad \text{et}$$
$$Z_+(P) \equiv Z_+(P') + 1 \equiv V(P') + 1 \equiv V(P) \bmod 2.$$

■

Corollaire 5.15. *Supposons que $P \in \mathbf{R}[X]$ ait k monômes non nuls. Alors*

$$Z_+(P) \leqslant k - 1$$

Démonstration. On a alors évidemment $V(P) \leqslant k - 1$ et on applique le lemme de Descartes. ■

> ***Remarque 5.16.*** Dans le cas où P a k monômes non nuls, on a aussi $Z_-(P) \leqslant k - 1$ (en considérant les racines > 0 du polynôme $P(-X)$), et donc P a au plus $2k - 2$ zéros réels non nuls (comptés avec multiplicités), plus éventuellement la racine 0.

5.2.1. Suites de Sturm

Définition 5.17. *Soient P et Q dans $\mathbf{R}[X]$. On définit la* suite de Sturm $St(P,Q)$ *comme la suite de polynômes $P_0, P_1, \ldots, P_m$ définis de la manière suivante : $P_0 = P,\ P_1 = Q,\ P_{i+1}$ est l'opposé du reste de la division euclidienne de P_{i-1} par P_i et P_m est au signe près le dernier reste non nul dans l'algorithme d'Euclide.*
Soit $a \in \mathbf{R}$. On définit $V(P,Q,a)$ comme la variation de la suite :

$$\big(P_0(a), P_1(a), \ldots, P_m(a)\big) \quad \textit{(définition 5.12)}.$$

On notera que

$$P_{i-1} = P_i Q_i - P_{i+1} \quad \text{pour} \quad 1 \leqslant i \leqslant m-1 \tag{6}$$

et que le polynôme P_m est un PGCD de P et Q.

Théorème 5.18. *« Théorème de Sturm »*
Avec les notations ci-dessus, supposons que $P(a)P(b) \neq 0$. On a alors :

$$z_{[a,b]}(P) = V(P,P',a) - V(P,P',b). \tag{7}$$

Démonstration.
a) *Cas où P et P' sont premiers entre eux* (et donc où P n'a pas de racine multiple).

Lorsque x parcourt l'intervalle $[a,b]$, la variation $V(P,P',x)$ ne change éventuellement que lorsque x passe une racine x_0 d'un des P_i. Notons $V(P,P',(x_0)_-)$ la variation $V(P,P',x)$ pour $x < x_0$, x très proche de x_0, et de manière analogue $V(P,P',(x_0)_+)$ pour $x > x_0$.

1. Supposons que en un point x_0 on ait $P_i(x_0) = 0$ pour un (ou plusieurs) indices $i > 0$, et $P(x_0) \neq 0$. Soit i un indice tel que $P_i(x_0) = 0$. On a par hypothèse $i \geqslant 1$, et $i < m$ puisque P_0 et P_1 étant premiers entre eux, leur PGCD P_m est une constante non nulle. La relation (6) implique que pour $0 \leqslant j \leqslant m-1$ un nombre x_0 ne peut être racine à la fois de P_j et de P_{j+1}, car sinon il serait aussi racine de P_{j-1}, et de proche en proche de tous les P_i pour $i \leqslant j$, et donc de $P' = P_1$ et $P = P_0$, ce qui est contraire à l'hypothèse a). On a donc alors $P_{i-1}(x_0) \neq 0$ et $P_{i+1}(x_0) \neq 0$. Supposons par exemple $P_{i-1}(x_0) < 0$ et donc $P_{i+1}(x_0) > 0$ (puisque (6) et le fait que $P_i(x_0) = 0$ impliquent que $P_{i-1}(x_0)P_{i+1}(x_0) < 0$).
   Considérons les signes de la suite $(P_{i-1}(x), P_i(x), P_{i+1}(x))$.
   Pour $x = (x_0)_-,\ x = x_0,\ x = (x_0)_+$ on trouve la suite $(-,*,+)$, $*$ étant un des trois signes $+,\ 0$, ou $-$. Quelle que soit la valeur du signe $*$, il y a un et un seul changement de signe dans la suite $(-,*,+)$, et donc la variation de la suite totale ne change pas lorsque x franchit la valeur x_0 : on a toujours $V(P,P',(x_0)_-) = V(P,P',(x_0)_+)$ dans le cas 1.
2. Supposons maintenant que $P(x_0) = 0$. On a les tableaux de variations ci-dessous, suivant le signe de $P_1(x_0) = P'(x_0)$ (non nul par hypothèse) :

	$(x_0)_-$	x_0	$(x_0)_+$
P_0	$-$	0	$+$
P_1	$+$	$+$	$+$

	$(x_0)_-$	x_0	$(x_0)_+$
P_0	$+$	0	$-$
P_1	$-$	$-$	$-$

   On voit que dans les deux cas la variation diminue de 1 lorsque x passe par la valeur x_0.

b) *Cas où P peut avoir des racines multiples.*

La preuve du cas a) repose sur les trois propriétés suivantes ; on se donne une suite $(Q_0, \ldots, Q_m)$, $Q_i \in \mathbf{R}[X]$ telle que :

- $P = Q_0$ et Q_m est constant ;
- si α est une racine de Q_0, le produit $Q_0 Q_1$ est négatif sur un intervalle $]\alpha - \varepsilon, \alpha[$ et positif sur un intervalle $]\alpha, \alpha + \varepsilon[$;
- si α est une racine de Q_i, $0 < i < m$, $Q_{i-1}(\alpha)Q_{i+1}(\alpha) < 0$.

Alors, si ces trois propriétés sont satisfaites, la démonstration ci-dessus montre que $z_{[a,b]}(Q_0) = V((Q_i), a) - V((Q_i), b)$.

Considérons maintenant la suite $P_0, P_1, \ldots, P_m$, avec $P_0 = P$ et $P_1 = P'$, P_m un PGCD de P et P'. Le polynôme P_m divisant $P = P_0$ et $P' = P_1$, il divise tous les P_i. Il est alors immédiat que la suite de polynômes :

$$(Q_0, \ldots, Q_m) = (P_0/P_m, P_1/P_m, \ldots, P_{m-1}/P_m, 1)$$

satisfait aux trois propriétés ci-dessus. On peut donc appliquer le théorème 5.18 au polynôme P_0/P_m qui a les mêmes racines que P, et à la suite des P_i/P_m qui en chaque point a non racine de P_m a le même nombre de changements de signes que la suite $(P_0, P_1, \ldots, P_m)$ (si on multiplie tous les termes d'une suite par un même nombre réel $\neq 0$, la variation ne change pas). ■

Définition 5.19. *On note $V(P, P', +\infty)$ la variation des coefficients dominants des polynômes P_i constituant la suite de Sturm. De même $V(P, P', -\infty)$ désigne la variation de la suite des coefficients dominants des polynômes $P_i(-X)$.*

Si on note d_i le degré du polynôme P_i et c_i son coefficient dominant, on a donc :

$$V(P, P', +\infty) = V(c_0, c_1, \ldots, c_m),$$
$$V(P, P', -\infty) = V((-1)^{d_0} c_0, (-1)^{d_1} c_1, \ldots, (-1)^{d_m} c_m).$$

Corollaire 5.20. *Soit $z(P)$ le nombre de racines réelles de P (sans compter les multiplicités). Alors*

$$z(P) = V(P, P', -\infty) - V(P, P', +\infty). \tag{8}$$

Démonstration. Soit M une borne pour les racines de tous les P_i, $0 \leqslant i \leqslant m$ (*cf.* (2)) ; on a alors $V(P, P', -M) = V(P, P', -\infty)$ et $V(P, P', +M) = V(P, P', +\infty)$ puisque chaque P_i garde un signe constant pour $x \leqslant -M$ et $x \geqslant M$. Le corollaire résulte alors du théorème 5.18. ■

Définition 5.21. *Si P et Q sont deux polynômes à coefficients réels et si $[a, b]$ est un intervalle, on note $z_{[a,b]}(P, Q > 0)$ (resp. $z_{[a,b]}(P, Q < 0)$ le nombre de racines distinctes α de P dans l'intervalle $[a, b]$ telles que $Q(\alpha) > 0$ (resp. $Q(\alpha) < 0$).*

Proposition 5.22. *Soient P et Q deux polynômes à coefficients réels n'ayant pas de racine réelle commune, $[a,b]$ un intervalle tel que $P(a)P(b) \neq 0$. Alors*

$$z_{[a,b]}(P, Q > 0) - z_{[a,b]}(P, Q < 0) = V(P, P'Q, a) - V(P, P'Q, b). \tag{9}$$

La démonstration, analogue à celle du théorème 5.18 est laissée au lecteur. Remarquons que si l'on suppose $Q = 1$, on retrouve le théorème 5.18.

Remarque 5.23. On a aussi évidemment la relation :

$$z_{[a,b]}(P) = z_{[a,b]}(P, Q > 0) + z_{[a,b]}(P, Q < 0).$$

On peut ainsi déduire de la proposition 5.22 et du théorème 5.18 les valeurs de $z_{[a,b]}(P, Q > 0)$ et $z_{[a,b]}(P, Q < 0)$.

5.3 RÉSULTANT ET DISCRIMINANT

Soient

$$P = a_0 + a_1 X + \cdots + a_p X^p, \quad a_p \neq 0$$
$$Q = b_0 + b_1 X + \cdots + b_q X^q, \quad b_q \neq 0$$

deux polynômes à coefficients dans un anneau A.

Définition 5.24. *On appelle* matrice de Sylvester*de P et Q la matrice suivante :*

$$S(P,Q) = \begin{pmatrix} a_p & \cdots & \cdots & & a_0 & & \\ & \ddots & & & & \ddots & \\ & & a_p & \cdots & \cdots & & a_0 \\ b_q & \cdots & & b_0 & & & \\ & \ddots & & & \ddots & & \\ & & \ddots & & & & \\ & & & b_q & & \cdots & b_0 \end{pmatrix} \begin{matrix} -- \\ q \\ -- \\ -- \\ \\ p \\ \\ -- \end{matrix} \begin{matrix} \\ lignes \\ \\ \\ \\ lignes \\ \\ \end{matrix} \tag{10}$$

Le résultant *de P et Q, noté $R(P,Q)$, est le déterminant de $S(P,Q)$.*

En échangeant les q premières lignes avec les p dernières, on voit que :

$$R(P,Q) = (-1)^{pq} R(Q,P). \tag{11}$$

Le lemme suivant est essentiel pour calculer le résultant et montrer ses propriétés.

Lemme 5.25. *Supposons P et Q à coefficients dans un corps K.*

1. *Si Q divise P, on a $R(P,Q) = 0$;*
2. *si Q ne divise pas P, soient R le reste de la division de P par Q, r le degré de R. Alors*

$$R(P,Q) = (-1)^{pq} b_q^{p-r} R(Q,R). \tag{12}$$

Démonstration. Multiplions la i-ième colonne de la matrice $S(P,Q)$ par X^{p+q-i}. On obtient la matrice $\tilde{S}(P,Q)(X)$ suivante :

$$\left(\begin{array}{ccccccc} a_pX^{p+q-1} & \dots & & & a_0X^{q-1} & 0 & \dots \\ & \ddots & & & & \ddots & \\ 0 & \dots & a_pX^p & \dots & & & a_0 \\ b_qX^{p+q-1} & \dots & & b_0X^{p-1} & 0 & \dots & 0 \\ 0 & \ddots & & & \ddots & & \\ \vdots & & \ddots & & & & \\ 0 & \dots & & b_qX^q & \dots & & b_0 \end{array}\right) \begin{array}{l} -- \\ q \quad lignes \\ -- \\ -- \\ \\ p \quad lignes \\ \\ -- \end{array} \tag{13}$$

telle que $\tilde{S}(P,Q)(1) = S(P,Q)$. Remarquons que dans la matrice $\tilde{S}(P,Q)(X)$, la ligne l_i est formée des monômes du polynôme $X^{q-i}P(X)$ pour $1 \leqslant i \leqslant q$, et des monômes du polynôme $X^{p+q-i}Q(X)$ pour $q+1 \leqslant i \leqslant p+q$.

Montrons maintenant (12). Si $q > p$, on a $R = P$, et le lemme est vrai par la formule (11).

Si $p \geqslant q$, considérons la division euclidienne :

$$P = QA + R, \quad \deg(R) < \deg(Q) \text{ ou } R = 0. \tag{14}$$

Posons :

$$A(X) = \alpha_0 + \alpha_1 X + \cdots + \alpha_{p-q}X^{p-q};$$

on a donc :

$$QA = \alpha_0 Q + \alpha_1(XQ) + \cdots + \alpha_{p-q}(X^{p-q}Q). \tag{15}$$

1. Si Q divise P, on voit ainsi en utilisant (15) que la relation $P = QA$ s'interprète en disant que la ligne l_q de la matrice $\tilde{S}(P,Q)(X)$ est une combinaison linéaire des lignes $l_{p+q}, l_{p+q-1}, \dots, l_{2q}$ avec coefficients $\alpha_0, \dots, \alpha_{p-q}$. Le déterminant de la matrice $\tilde{S}(P,Q)(X)$ est donc nul, ce qui implique que $R(P,Q) = 0$.

2. Dans le cas général, posons

$$R(X) = c_0 + c_1X + \cdots + c_rX^r$$

avec $c_r \neq 0$. On voit alors en utilisant (15) que la relation $P = QA + R$ s'interprète en disant que la ligne l_q de la matrice $\tilde{S}(P,Q)(X)$ est la somme de la ligne $(0, \dots, 0, c_rX^r, \dots, c_0)$ correspondant au polynôme $R(X)$, et d'une combinaison linéaire des lignes $l_{p+q}, l_{p+q-1}, \dots, l_{2q}$ avec coefficients $\alpha_0, \dots, \alpha_{p-q}$.

On peut donc remplacer la ligne l_q de $\tilde{S}(P,Q)(X)$ par la ligne $(0, \dots, 0, c_rX^r, \dots, c_0)$ sans changer son déterminant.

En procédant de même avec les relations

$$X^iP = X^iQA + X^iR$$

pour $0 \leqslant i \leqslant q-1$, on voit que l'on peut remplacer les q premières lignes de $\tilde{S}(P,Q)(X)$ par les lignes formées de zéros et des monômes des polynômes X^iR,

$0 \leqslant i \leqslant q-1$, la ligne l_{q-i} étant remplacée par la ligne $(0,\dots,0,c_rX^{r+i},\dots,c_0X^i,0,\dots,0)$, cela sans changer le déterminant.

En faisant $X=1$ on voit alors que le déterminant de $S(P,Q)$ est égal au déterminant de la matrice :

$$\left(\begin{array}{ccccccc} 0 & \dots & c_r & \dots & c_0 & 0 & \dots \\ & & & \ddots & & \ddots & \\ 0 & \dots & & & c_r & \dots & c_0 \\ b_q & \dots & & b_0 & 0 & \dots & \\ 0 & \ddots & & & \ddots & & \\ \vdots & & \ddots & & & & \\ 0 & \dots & & b_q & \dots & & b_0 \end{array}\right) \begin{array}{l} -- \\ q \quad lignes \\ -- \\ -- \\ \\ p \quad lignes \\ \\ -- \end{array}$$

d'où la relation (12). ■

Corollaire 5.26. *On peut calculer le résultant en utilisant l'algorithme d'Euclide (section 1.3), convenablement modifié.*

Corollaire 5.27. *Soit K un corps. Avec les notations ci-dessus, les conditions suivantes sont équivalentes :*

1. $R(P,Q)=0$;
2. *les polynômes P et Q ont un facteur commun de degré >0 dans $K[X]$.*

Démonstration.
1. $\Rightarrow$ *2.* Supposons que *2.* soit faux, *i.e.* que P et Q n'aient pas de facteur commun dans $K[X]$. Le PGCD de P et Q (dernier reste non nul dans l'algorithme d'Euclide) est alors une constante $c \neq 0$. Le lemme 5.25 appliqué récursivement donne :

$$R(P,Q) = \alpha R(R_s, c)$$

avec $\alpha \neq 0$, $c \neq 0$ et R_s un reste de degré $r_s > 0$. Mais on voit tout de suite (en regardant la matrice de Sylvester) que $R(R_s,c) = c^{r_s} \neq 0$, et donc que $R(P,Q) \neq 0$.

2. $\Rightarrow$ *1.* Si P et Q ont un facteur commun non trivial A dans $K[X]$, supposons d'abord que $P = QA$ avec A de degré $p-q > 0$. Alors le lemme 5.25 montre que $R(P,Q)=0$. Dans le cas général, on se retrouve (en appliquant le lemme 5.25) dans la situation ci-dessus en considérant le dernier reste non nul dans l'algorithme d'Euclide. ■

Proposition 5.28. *Supposons que dans $K[X]$, on ait :*

$$P = a_p(X-\alpha_1)\dots(X-\alpha_p)$$
$$Q = b_q(X-\beta_1)\dots(X-\beta_q).$$

Alors

$$R(P,Q) = a_p^q b_q^p \prod_{i,j}(\alpha_i-\beta_j) = a_p^q \prod_{1\leqslant i\leqslant p} Q(\alpha_i) = (-1)^{pq} b_q^p \prod_{1\leqslant j\leqslant q} P(\beta_j)\,. \quad (16)$$

Démonstration. Les égalités :

$$a_p^q b_q^p \prod(\alpha_i - \beta_j) = a_p^q \prod Q(\alpha_i) = (-1)^{pq} b_q^p \prod P(\beta_j)$$

sont immédiates.

Posons $R_2(P,Q) = a_p^q \prod Q(\alpha_i) = (-1)^{pq} b_q^p \prod P(\beta_j)$.

Pour montrer que $R_2(P,Q) = R(P,Q)$, on peut supposer $p \geqslant q > 0$ (car on a évidemment $R(P,Q) = R_2(P,Q) = b_q^p$ si $q = 0$). Il suffit alors de montrer que R_2 satisfait à la même relation de récurrence (12) que $R(P,Q)$. Si $P = QA + R$, on a $P(\beta_j) = R(\beta_j)$ pour toute racine β_j de Q, et donc :

$$R_2(P,Q) = (-1)^{pq} b_q^p \prod P(\beta_j) = (-1)^{pq} b_q^p \prod R(\beta_j) = (-1)^{pq} b_q^{p-r} R_2(Q,R),$$

ce qui est bien la même relation que (12). ■

Passons maintenant au discriminant d'un polynôme.

Définition 5.29. *Soit A un anneau intègre et $P = a_p X^p + \cdots + a_0 \in A[X]$ tel que $a_p \neq 0$. Alors on définit le* discriminant *$D(P)$ de la manière suivante :*

$$D(P) = \frac{(-1)^{\frac{p(p-1)}{2}}}{a_p} R(P,P').$$

Remarquons que cette définition a bien un sens quel que soit l'anneau intègre A, car dans la matrice de Sylvester $R(P,P')$, la première colonne est divisible par a_p, puisque $P' = pa_p X^{p-1} + \cdots + a_1$.

Proposition 5.30. *Si $P(X) = a_p(X - \alpha_1)\dots(X - \alpha_p)$, alors :*

$$D(P) = (-1)^{\frac{p(p-1)}{2}} a_p^{2p-2} \prod_{i \neq j} (\alpha_i - \alpha_j) = a_p^{2p-2} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Démonstration. On a

$$P'(X) = a_p \sum_{i=1}^{p} (X - \alpha_1)\dots(\widehat{X - \alpha_i})\dots(X - \alpha_p),$$

la notation $(\widehat{X - \alpha_i})$ signifiant que l'on omet le terme $(X - \alpha_i)$ dans le produit. La proposition 5.28 montre que $R(P,P') = a_p^{p-1} \prod_{i=1}^p P'(\alpha_i)$. Comme $P'(\alpha_i) = a_p(\alpha_i - \alpha_1)\dots(\alpha_i - \alpha_p)$ (sans le terme $(\alpha_i - \alpha_i)$), cela entraîne le résultat. ■

Exemple 5.31. 1) Si $P = aX^2 + bX + c$, $P' = 2aX + b$, on a :

$$S(P,P') = \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix},$$

d'où $R(P) = a(4ac - b^2)$ et $D(P) = b^2 - 4ac$.

2) $P = X^3 + pX + q$, $P' = 3X^2 + p$, un petit calcul de déterminant montre facilement que $D(P) = -4p^3 - 27q^2$.

Remarque 5.32. Supposons que P soit à coefficients dans $\mathbf{C}$. Alors la condition $D(P) \neq 0$ (équivalente au fait que P et P' n'ont pas de racine commune) signifie que P n'a que des racines simples.

5.3.1. *Séparation et isolation des racines réelles

Définition 5.33. *Soit $P \in \mathbf{C}[X]$, $\quad P = a_0 + a_1X + \cdots + a_dX^d$, avec $a_d \neq 0$, α_i les racines de P. On pose :*

$$\mathrm{sep}P = \inf_{\alpha_i \neq \alpha_j} |\alpha_i - \alpha_j|.$$

Proposition 5.34.
On suppose que $P \in \mathbf{Z}[X]$. Alors, en posant $C = |a_d| + \sup_{1 \leqslant i \leqslant d-1} |a_i|$, on a pour $d \geqslant 3$:

$$\mathrm{sep}P \geqslant (2C)^{-\frac{d(d-1)}{2}+1}.$$

Démonstration.
(a) Supposons d'abord que les racines de P sont simples.

On peut supposer, quitte à changer les indices, que $\mathrm{sep}P = |\alpha_1 - \alpha_2|$. Soit $D(P)$ le discriminant de P. La définition 5.29 montre que $D(P) \in \mathbf{Z}$ puisque par hypothèse $P \in \mathbf{Z}[X]$. On a donc $1 \leqslant |D(P)|$ puisque l'hypothèse (a) implique que $D(P) \neq 0$ (remarque 5.32). On a donc d'après la proposition 5.30 :

$$1 \leqslant |a_d|^{2d-2} \prod_{i<j} (\alpha_i - \alpha_j)^2, \text{ soit}$$

$$\frac{1}{(\alpha_1 - \alpha_2)^2} \leqslant |a_d|^{2d-2} \prod_{i<j,(i,j)\neq(1,2)} |\alpha_i - \alpha_j|^2.$$

Mais $|\alpha_i - \alpha_j| \leqslant |\alpha_i| + |\alpha_j| \leqslant 2\frac{C}{|a_d|}$ (*cf.* (2)), et il y a $\frac{d(d-1)}{2} - 1 = \frac{d^2-d-2}{2}$ facteurs $|\alpha_i - \alpha_j|^2$, ce qui donne :

$$\frac{1}{|\alpha_1 - \alpha_2|^2} \leqslant \frac{(2C)^{d^2-d-2}}{|a_d|^{d^2-3d}} \leqslant (2C)^{d^2-d-2}$$

(car $|a_d| \geqslant 1$ et $d^2 - 3d \geqslant 0$), d'où le résultat.

(b) Dans le cas général (*i.e.* lorsque les racines de $P \in \mathbf{Z}[X]$ ne sont pas nécessairement simples), on peut supposer P primitif (définition 5.6) quitte à le diviser par son contenu (qui est un entier). On considère le polynôme $R = \mathrm{PGCD}(P, P')$ que l'on peut supposer dans $\mathbf{Z}[X]$ et primitif ; on a alors $P = QR$ dans $\mathbf{Z}[X]$, P et R étant primitifs (conséquence immédiate du lemme 5.8). On peut alors appliquer la méthode

de (a) au polynôme Q qui a les mêmes racines que P, mais avec multiplicité 1. On trouve donc, en notant d' le degré de Q, et en utilisant que $d' \leqslant d$:

$$\frac{1}{(sepP)^2} = \frac{1}{(sepQ)^2} \leqslant (2C)^{d'^2-d'-2} \leqslant (2C)^{d^2-d-2}.$$

■

5.4 *FONCTIONS SYMÉTRIQUES DES RACINES

Définition 5.35. *Soit*

$$P(X) = (X - t_1)(X - t_2)\dots(X - t_n) = X^n - s_1X^{n-1} + \dots + (-1)^n s_n, \quad (17)$$

considéré comme un polynôme en X à coefficients dans l'anneau $\mathbf{Z}[t_1, \dots, t_n]$.
Le polynôme $s_j(t_1, \dots, t_n) \in \mathbf{Z}[t_1, \dots, t_n]$ s'appelle la j-ième fonction symétrique élémentaire *des t_i.*

On déduit immédiatement de (17) les relations suivantes :

$$\begin{aligned} s_1 &= t_1 + \dots + t_n \\ s_2 &= \sum_{i<j} t_i t_j \\ &\vdots \\ s_n &= t_1 \dots t_n. \end{aligned}$$

Soit maintenant A un anneau intègre (par exemple $A = \mathbf{Z}$ ou $A = K$, K étant un corps). Si on fait agir le groupe symétrique S_n sur les variables $(t_1, \dots, t_n)$ par permutations, cette action induit une action de S_n sur l'anneau $A[t_1, \dots, t_n]$ telle que pour $\sigma \in S_n$, $\sigma.Q(t_1, \dots, t_n) = Q(t_{\sigma(1)}, \dots, t_{\sigma(n)})$.

Définition 5.36. *Un polynôme $Q \in A[t_1, \dots, t_n]$ est dit* symétrique *s'il est invariant par cette action,* i.e. *si $\sigma.Q = Q$ pour tout $\sigma \in S_n$.*

Exemples 5.37.

1. Les polynômes s_i sont symétriques (d'où leur nom !) puisque pour tout $\sigma \in S_n$
$$P(X) = (X - t_1)\dots(X - t_n) = (X - t_{\sigma(1)})\dots(X - t_{\sigma(n)}).$$
2. Plus généralement si $G \in A[X_1, \dots, X_n]$ est un polynôme en n variables, le polynôme $G(s_1, \dots, s_n) \in A[t_1, \dots, t_n]$ est évidemment symétrique. Nous allons voir plus bas que la réciproque est vraie.
3. Les polynômes
$$N_k = t_1^k + \dots + t_n^k$$
sont symétriques pour tout entier $k \geqslant 0$. On les appelle *« sommes de Newton »*.

Nous allons rappeler la définition du degré d'un polynôme à plusieurs variables et introduire la notion de poids qui nous servira pour le prochain théorème.

Définition 5.38.

1. *Le degré d'un monôme non nul $\lambda X_1^{a_1} X_2^{a_2} \dots X_n^{a_n}$ ($\lambda \in A \setminus \{0\}$) est l'entier $a_1 + a_2 + \dots + a_n$. Le degré d'un polynôme non nul $P \in A[X_1, \dots, X_n]$ est le maximum des degrés de ses monômes.*
2. *Fixons pour chaque variable X_i un nombre $w_i \in \mathbf{N}$ que nous appellerons poids de X_i. Le poids d'un monôme non nul $\lambda X_1^{a_1} X_2^{a_2} \dots X_n^{a_n}$ est l'entier $\sum_{i=1}^n w_i a_i$; le poids d'un polynôme non nul P est le maximum des poids de ses monômes.*

Exemples 5.39.

1. Si le poids de X_i est 1 pour tout i, on retrouve la notion habituelle de degré.
2. Posons $w_i = i$, $1 \leqslant i \leqslant n$ (w_i est le poids de X_i). Alors, un monôme non nul $\lambda X_1^{a_1} X_2^{a_2} \dots X_n^{a_n}$ (avec $a_i \geqslant 0$) est de poids $p = \sum_{j=1}^n j a_j$. Si l'on remplace chaque variable X_i par la i-ième fonction symétrique élémentaire $s_i(t_1, \dots, t_n)$, on obtient le polynôme
$$P(t_1, \dots, t_n) = \lambda s_1^{a_1} \dots s_n^{a_n}$$
qui est homogène de degré $p = \sum j a_j$ en les variables $t_1, \dots, t_n$ (cet exemple est la raison de l'introduction ici de la notion de poids). Plus généralement, il est clair que si $P(X_1, \dots, X_n)$ est un polynôme de poids d, $P(s_1, \dots, s_n)$ est de degré $\leqslant d$ en $(t_1, \dots, t_n)$ puisque chaque s_i est de degré i en $(t_1, \dots, t_n)$.

Dans le théorème suivant, le poids de chaque variable X_i est par définition l'entier i (comme dans l'exemple précédent), et A est toujours un anneau intègre.

Théorème 5.40. *Soit $G \in A[t_1, \dots, t_n]$ un polynôme symétrique. Il existe alors un polynôme unique $R \in A[X_1, \dots, X_n]$ tel que :*
$$G = R(s_1, \dots, s_n).$$
De plus si G est de degré d, R est de poids d.

Exemple 5.41. Soit $G = t_1^2 + \dots + t_n^2$ ($G = N_2$, deuxième somme de Newton). Alors $R(s_1, s_2) = s_1^2 - 2s_2$. Le polynôme G est de degré 2, et $R(X_1, X_2, \dots, X_n) = X_1^2 - 2X_2$ (qui ne dépend ici que de X_1 et X_2) est homogène de poids 2 (i.e. tous les monômes sont de poids 2).

Démonstration. (du théorème). Admettons l'unicité de R, et montrons son existence. Nous allons raisonner par une double récurrence, d'abord sur le nombre de variables n puis sur le degré d, le cas $n = 1$ étant trivial (tout polynôme est alors symétrique, on a $t_1 = s_1$ d'où $G = R$), ainsi que le cas $d = 1$ (avec un nombre quelconque de variables).

Soit donc $G(t_1, \dots, t_n)$ un polynôme symétrique de degré d, et supposons le théorème montré pour les polynômes en $n - 1$ variables, ainsi que pour les polynômes en n variables de degré $\leqslant d-1$. Notons $s'_1, \dots s'_{n-1}$ les fonctions symétriques élémentaires des variables $(t_1, \dots, t_{n-1})$. Le polynôme $G(t_1, \dots, t_{n-1}, 0)$ est symétrique dans les

variables $(t_1, \ldots, t_{n-1})$ et de degré $\leqslant d$; il existe donc par hypothèse de récurrence (sur n) un polynôme $R_1(X_1, \ldots, X_{n-1})$ de poids $\leqslant d$ tel que :

$$G(t_1, \ldots, t_{n-1}, 0) = R_1(s'_1, \ldots, s'_{n-1}).$$

Posons $G_1 = G - R_1(s_1, \ldots, s_{n-1})$. Le polynôme $G_1(t_1, \ldots, t_n)$ est symétrique puisqu'il est la différence de deux polynômes symétriques, et de degré $\leqslant d$ (exemple 5.39) puisque G est de degré d et que $R_1(s_1, \ldots, s_{n-1})$ est de poids $\leqslant d$ par hypothèse de récurrence. De plus il vérifie $G_1(t_1, \ldots, t_{n-1}, 0) = 0$. Le polynôme G_1 est donc divisible par t_n, et comme il est symétrique, il est aussi divisible aussi par $t_1, \ldots, t_{n-1}$. On en déduit qu'il est divisible par le produit $s_n = t_1 \ldots t_n$ (si $G_1 = t_n \tilde{G}_1$ est divisible par t_1 par exemple, on a $G_1(0, t_2, \ldots, t_n) = t_n \tilde{G}_1(0, t_2, \ldots, t_n) \equiv 0$ d'où $\tilde{G}_1(0, t_2, \ldots, t_n) \equiv 0$ et donc $\tilde{G}_1$ est divisible par t_1, et G_1 par $t_n t_1$; on continue ainsi de proche en proche). Posons donc $G_1 = s_n G_2(t_1, \ldots, t_n)$; le polynôme G_2 est alors de degré $\leqslant d - n$ et symétrique. On peut donc lui appliquer l'hypothèse de récurrence (sur d) et écrire $G_2(t_1, \ldots, t_n) = R_2(s_1, \ldots, s_n)$, le polynôme $R_2(X_1, \ldots, X_n)$ étant de poids $\leqslant d - n$. La relation :

$$G = s_n G_2(t_1, \ldots, t_n) + R_1(s_1, \ldots, s_{n-1}) = s_n R_2(s_1, \ldots, s_n) + R_1(s_1, \ldots, s_{n-1})$$

montre alors l'existence du polynôme R :

$$R = X_n R_2(X_1, \ldots, X_n) + R_1(X_1, \ldots, X_{n-1}).$$

Il est clair que le polynôme R est de poids $\leqslant d$, et même exactement de poids d, puisque $R(s_1, \ldots, s_n)$ est par hypothèse de degré d en $t_1, \ldots, t_n$ (si R était de poids $< d$, $R(s_1, \ldots, s_n)$ serait de degré $< d$: exemple 5.39).

Montrons maintenant l'unicité du polynôme $R(X_1, \ldots, X_n)$ (lorsque les t_i sont des variables indépendantes). Raisonnons par l'absurde et par récurrence sur n. S'il existait deux polynômes différents R_1 et R_2 tels que $G(t_1, \ldots, t_n) = R_i(s_1, \ldots, s_n)$, $i = 1, 2$, on en déduirait par différence un polynôme non nul $H \in \mathbf{Z}[X_1, \ldots, X_n]$ tel que $H(s_1, \ldots, s_n) = 0$. Considérons un tel polynôme H de degré minimal d. On peut écrire H comme un polynôme en X_n :

$$H(X_1, \ldots, X_n) = h_0(X_1, \ldots, X_{n-1}) + \cdots + h_d(X_1, \ldots, X_{n-1}) X_n^d.$$

Le polynôme h_0 est alors non nul, car sinon on pourrait écrire :

$$H(X_1, \ldots, X_n) = X_n Q(X_1, \ldots, X_n)$$

avec Q de degré $d - 1$ et $Q(s_1, \ldots, s_n) = 0$, ce qui contredirait la minimalité de d. On a donc en substituant :

$$h_0(s_1, \ldots, s_{n-1}) + \cdots + h_d(s_1, \ldots, s_{n-1}) s_n^d = 0$$

dans l'anneau $\mathbf{Z}[t_1, \ldots, t_n]$. En faisant $t_n = 0$, on obtient alors $h_0(s'_1, \ldots, s'_{n-1}) = 0$ avec $h_0 \neq 0$, ce qui est absurde car contraire à l'hypothèse de récurrence sur n. ■

Il résulte en particulier du théorème 5.40 que pour n fixé les sommes de Newton N_i (exemple 5.37) sont des polynômes en les fonctions $s_1, \dots, s_i$. Les formules qui expriment les S_i en fonction des s_k sont connues sous le nom de « formules de Newton » ; on a par exemple :

$$N_0 = n, \quad N_1 = s_1, \quad N_2 = s_1^2 - 2s_2.$$

Nous allons montrer comment on peut effectivement calculer ces formules par récurrence sur n.

Lemme 5.42. *Pour $k \geqslant n$, on a :*

$$N_k - s_1 N_{k-1} + \cdots + (-1)^n s_n N_{k-n} = 0. \tag{18}$$

Démonstration. Considérons le polynôme de la définition 5.35 :

$$P(X) = (X - t_1)(X - t_2)\dots(X - t_n) = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n. \tag{19}$$

On a $P(t_i) = t_i^n + \cdots + (-1)^n s_n = 0$, d'où (18) en multipliant par t_i^{k-n} et en sommant pour $1 \leqslant i \leqslant n$. ■

La relation (18) permet ainsi de calculer N_k pour tout $k \geqslant n$ en fonction de $s_1, \dots, s_n$ si on connait les formules pour $N_0, N_1, \dots, N_{n-1}$ qui résultent du lemme suivant :

Lemme 5.43. *Pour $0 \leqslant h \leqslant n-1$ on a :*

$$N_h - s_1 N_{h-1} + s_2 N_{h-2} + \cdots + (-1)^h h s_h = 0. \tag{20}$$

Démonstration. Dérivons (19) par rapport à X. En utilisant la première égalité (et le fait que $P(t_i) = 0$), cela donne :

$$P'(X) = \sum_{i=1}^{n} \frac{P(X)}{X - t_i} = \sum_{i=1}^{n} \frac{P(X) - P(t_i)}{X - t_i} = \sum_{i=1}^{n} \Big(\sum_{j=0}^{n-1} (-1)^j s_j \frac{X^{n-j} - t_i^{n-j}}{X - t_i} \Big).$$

En écrivant : $\quad X^{n-j} - t_i^{n-j} = (X - t_i) \sum_{k=0}^{n-j-1} t_i^k X^{n-j-k-1}$

et en remplaçant, on trouve :

$$\begin{aligned}
P'(X) &= \sum_{i=1}^{n} \sum_{j=0}^{n-1} (-1)^j s_j \Big(\sum_{k=0}^{n-j-1} t_i^k X^{n-j-k-1} \Big) \\
&= \sum_{j=0}^{n-1} (-1)^j s_j \Big(\sum_{k=0}^{n-j-1} N_k X^{n-j-k-1} \Big) \\
&= \sum_{k=0}^{n-1} N_k \Big(\sum_{j=0}^{n-k-1} (-1)^j s_j X^{n-j-k-1} \Big) \\
&= \sum_{0 \leqslant k \leqslant h \leqslant n-1} (-1)^{h-k} s_{h-k} N_k X^{n-h-1}
\end{aligned} \tag{21}$$

(en ayant posé $h = j + k$ pour la dernière égalité).

Si maintenant on dérive la deuxième expression de $P(X)$ dans (19), il vient :

$$P'(X) = \sum_{h=0}^{n-1} (-1)^h (n-h) s_h X^{n-h-1},$$

d'où :

$$(n-h)s_h = \sum_{k=0}^{h} (-1)^k s_{h-k} N_k$$

en identifiant les termes en X^{n-h-1} avec (21), ce qui donne $-hs_h = \sum_{k=1}^{h} (-1)^k s_{h-k} N_k$ et (20). ■

Remarques 5.44.

1. Réciproquement les formules (20) montrent que les s_i s'expriment comme des polynômes en $N_1, \ldots, N_i$: le théorème 5.40 est donc aussi vrai en remplaçant les s_i par les N_i.
2. Considérons le polynôme en X :

   $$P(X) = (X - t_1)(X - t_2) \ldots (X - t_n)$$

   à coefficients dans l'anneau $B = \mathbf{Z}[t_1, \ldots, t_n]$, les t_i étant des indéterminées. Si K est un corps, et ϕ le morphisme : $\mathbf{Z}[t_1, \ldots, t_n] \to K$ défini par $\phi(t_i) = \alpha_i$, ϕ induit un morphisme d'anneaux : $B[X] \to K[X]$. L'image de P par ce morphisme est le polynôme unitaire de $K[X]$ ayant les α_i pour racines (*i.e.* $\phi(P) = (X - \alpha_1) \ldots (X - \alpha_n)$). Tous les calculs effectués sur les t_i se transposent ainsi aux α_i.

EXERCICES

Les solutions des exercices et problèmes sont données en fin d'ouvrage.

POLYNÔMES

Exercice 5.1. Soit $P(X) = a_n X^n + \cdots + a_0 \in \mathbf{Z}[X]$; montrer que si $p/q \in \mathbf{Q}$ est une racine de $P(X)$ alors q (resp. p) divise a_n (resp. a_0). Factoriser $3X^3 + 4X^2 + 2X - 4$ sur $\mathbf{Q}, \mathbf{R}, \mathbf{C}$.

Exercice 5.2. Soit $P(X) \in \mathbf{Q}[X]$ et x une racine de $P(X)$ de multiplicité strictement supérieure à $(\deg P)/2$; montrer que $x \in \mathbf{Q}$.

Exercice 5.3. Soit $P \in \mathbf{R}[X]$ tel que $P'(X)$ divise $P(X)$; montrer que le quotient est de la forme $a(X - \alpha)$ pour a, α réels.
En dérivant k fois ($k < \deg P$) l'égalité $P(X) = P'(X)a(X - \alpha)$, montrer que $P^{(k)}(\alpha) = 0$ et en déduire que $P(X) = \frac{P^{(n)}(\alpha)}{n!}(X - \alpha)^n$, où n est le degré de $P(X)$.

Exercice 5.4. Soit $P \in \mathbf{R}[X]$ tel que $P(x) \geqslant 0 \ \forall \ x \in \mathbf{R}$. Montrer que $P = R^2 + S^2$ dans $\mathbf{R}[X]$.

Exercice 5.5. Soient $a \in \mathbf{R}$ et P un polynôme de degré n à coefficients réels tels que $P(a) > 0$ et pour $1 \leqslant k \leqslant n$, $P^{(k)}(a) \geqslant 0$; montrer que P n'a pas de racines dans $[a, +\infty[$.

Exercice 5.6. Montrer que $\sum_{k=0}^{n} \frac{X^k}{n!}$ n'a pas de racines multiples.

Exercice 5.7. Soit $P(X) = X^6 - 6X^5 + 15X^4 - 20X^3 + 12X^2 - 4$; calculer le pgcd de P et P' puis factoriser P sur $\mathbf{R}$ et $\mathbf{C}$.

Exercice 5.8. Montrer que $X^n \sin\theta - X\sin(n\theta) + \sin(n-1)\theta$ est divisible par $X^2 - 2X\cos\theta + 1$ et donner le quotient.

Exercice 5.9. Soient $a \neq b \in \mathbf{C}$, calculer le reste de la division euclidienne de $P(X) \in \mathbf{C}[X]$ par $(X-a)(X-b)$.

RACINES DES POLYNÔMES À COEFFICIENTS COMPLEXES

Exercice 5.10. Soit $P = a_0 + a_1X + \cdots + a_dX^d \in \mathbf{C}[X]$, $a_d \neq 0$. Montrer que si α est une racine de P, on a :

$$|\alpha| \leqslant \sup_{0 \leqslant i \leqslant d-1} \Big(d\frac{|a_i|}{|a_d|} \Big)^{1/(d-i)}$$

Exercice 5.11. Soit $P = a_0 + a_1Z + \cdots + a_nZ^n \in \mathbf{C}[Z]$.

1. Montrer que les zéros (complexes) de P' sont dans l'enveloppe convexe des zéros de P.
2. Soit $K \subset \mathbf{C}$ un convexe. Montrer que l'ensemble des $w \in \mathbf{C}$ tels que les solutions de $P(Z) = w$ soient contenues dans K est un convexe de $\mathbf{C}$. (Indication : considérer $Q = (P(Z) - w_1)^{n_1}(P(Z) - w_2)^{n_2}$ où les w_i sont des nombres complexes).

RACINES DES POLYNÔMES À COEFFICIENTS RÉELS

Exercice 5.12. Soit $P(X)$ un polynôme à coefficients réels. Démontrer le lemme de Descartes par récurrence sur le nombre de racines réelles > 0 (avec multiplicités), en écrivant

$$P(X) = (X - \alpha)Q(X)$$

avec $\alpha > 0$, et en comparant les variations des coefficients de P et de ceux de Q.

Exercice 5.13. *« Théorème de Budan-Fourier »*. Soit $P(X)$ un polynôme de degré d à coefficients réels. On note $V(x)$ le nombre de changements de signes dans la suite

$$(P(x), P'(x), P >> (x), \ldots, P^{(d)}(x)).$$

Soit $[a, b]$ un intervalle tel que $P(a)P(b) \neq 0$. On rappelle que $Z_{[a,b]}(P)$ désigne le nombre de racines (comptées avec multiplicités) dans l'intervalle $[a, b]$.

Montrer que $Z_{[a,b]}(P) \leqslant V(a) - V(b)$ et $Z_{[a,b]}(P) \equiv V(a) - V(b) \bmod 2$. En déduire le lemme de Descartes.

Exercice 5.14. Soit

$$F(X) = \sum_{i=0}^{n} P_i(X) e^{\alpha_i X}$$

où $P_i(X) \in \mathbf{R}[X]$ est un polynôme de degré d_i. Montrer que le nombre $z(F)$ de zéros de F dans $\mathbf{R}$ est fini et que $z(F) \leqslant \sum d_i + n$. (Même méthode que pour le lemme de Descartes : raisonner par récurrence en utilisant le théorème de Rolle).

Exercice 5.15. On considère le polynôme $X^{14} - 7.13.X^2 - 14.6X - 13.6$. Que peut-on dire du nombre de racines réelles positives et négatives de ce polynôme en utilisant la règle de Descartes puis celle de Sturm ?

RÉSULTANT, DISCRIMINANT

Exercice 5.16. On considère la courbe paramétrée $x(t) = t^2 + t + 1$, $y(t) = \frac{t^2-1}{t^2+1}$. En donner une équation algébrique.

Exercice 5.17. Montrer que le sous-ensemble de $\mathcal{M}_n(\mathbf{C})$ constitué des matrices à n valeurs propres distinctes est un ouvert de $\mathcal{M}_n(\mathbf{C})$.

Exercice 5.18. Calculer le discriminant du polynôme $P(X) = X^3 + pX + q$

1. En appliquant la définition.
2. En calculant la suite de Sturm $S(P, P')$.

Exercice 5.19. Calculer le résultant $R_Y(P, Q)$ des polynômes $P_X(Y) = X^2 - XY + Y^2 - 1$ et $Q_X(Y) = 2X^2 + Y^2 - Y - 2$ considérés comme des éléments de $\mathbf{R}[X][Y]$, *i.e.* comme des polynômes en Y à coefficients dans $\mathbf{R}[X]$. Trouver alors les points d'intersections des ellipses d'équations $P = 0$ et $Q = 0$.

Exercice 5.20. Soient $C_X(Y) = X^2 + Y^2 + bY + c$ et $P_X(Y) = X^2 + Y + g$ où b, c, g sont des réels.

1. Calculer le résultant $R_Y(C, P)$.

2. Donner une condition sur b, c, g pour que les points d'intersection de l'ellipse C avec la parabole P aient la même abscisse (réelle ou complexe).
3. Donner des conditions sur b, c, g pour que tous les points d'intersection de P et C soient réels. Retrouver cette condition en utilisant la règle de Sturm.

Exercice 5.21.

1. Soient A et B deux polynômes de $K[X]$ où K est un corps. Construire un polynôme dont les racines sont les sommes d'une racine de A et d'une racine de B (on considèrera les Y solutions du système $A(X) = B(Y - X) = 0$).
2. Construire un polynôme à coefficients entiers qui possède $\sqrt{2} + \sqrt[3]{7}$ pour racine.

FONCTIONS SYMÉTRIQUES DES RACINES

Exercice 5.22.

1. Soient $a_1, a_2, \ldots, a_n$ des nombres strictement positifs. Montrer que
$$(a_1 \ldots a_n)^{1/n} \leqslant \frac{a_1 + \cdots + a_n}{n}.$$
2. Déterminer tous les polynômes à coefficients $+1, -1$, ou 0 ayant toutes leurs racines réelles (appliquer 1. aux carrés des racines d'un polynôme P à coefficients $+1, -1$ ou 0 ayant toutes ses racines réelles).

Exercice 5.23. Soient $\alpha, \beta, \gamma, \delta$ les racines complexes de $X^4 - 2X^3 + aX^2 + bX - 1$; trouver a, b pour que l'on ait $\alpha + \beta = \gamma + \delta$ et $\alpha\beta = -\gamma\delta$. Donner alors les racines.

Exercice 5.24. Soient a, b, c des nombres complexes ; montrer qu'une condition nécessaire et suffisante pour que les points A, B, C du plan réel, d'affixes respectives a, b, c, forment un triangle isocèle rectangle en A est
$$c^2 + b^2 - 2a(b + c) + 2a^2 = 0.$$
En déduire qu'une CNS pour que les solutions a, b, c de l'équation $x^3 + px + q$ forment un triangle rectangle isocèle est $27q^2 - 50p^3 = 0$.

Exercice 5.25. Calculer les fonctions symétriques élémentaires $s_i(x, y, z)$ $(1 \leqslant i \leqslant 3)$ des solutions du système d'équations :
$$\begin{cases} x^2 + y^2 + z^2 = 2 \\ x^3 + y^3 + z^3 = 2 \\ x^4 + y^4 + z^4 = 2 \end{cases}$$
(utiliser les relations de Newton).

PROBLÈMES

Problème 5.1. *Un analogue pour les polynômes d'une conjecture célèbre en théorie des nombres*

1. Soient $a_0, \ldots, a_n$ des nombres complexes deux à deux distincts et $b_0, \ldots, b_n$ des nombres complexes. Montrer qu'il existe un unique polynôme P, à coefficients complexes de degré au plus n tel que pour tout $0 \leqslant i \leqslant n$, $P(a_i) = b_i$ (polynôme d'interpolation de Lagrange).
2. Soient $P, Q \in \mathbf{C}[X]$ on suppose $\deg(Q) \leqslant \deg(P)$.
   (i) Si pour tout $x \in \mathbf{C}$, $P(x) = 0 \iff Q(x) = 0$, peut-on affirmer que $P = Q$?
   (ii) On suppose maintenant que $P(x) = 0$ si et seulement si $Q(x) = 0$ et $P(x) = 1$ si et seulement si $Q(x) = 1$. On note $\alpha_1, \ldots, \alpha_r$ les racines de P et $\beta_1, \ldots, \beta_s$ les racines de $P - 1$. Montrer que $r + s \geqslant \deg(P) + 1$.
   (iii) En déduire que $P = Q$.

   Remarque. On conjecture que si m et n sont deux entiers ayant les mêmes diviseurs premiers, que si de plus $m + 1, n + 1$ ont les mêmes diviseurs premiers ainsi que $m + 2, n + 2$, alors $m = n$ *(conjecture d'Erdös-Woods).*

Problème 5.2. *Partage de secret*

Soit p un nombre premier « grand » ; tous les entiers considérés dans la suite seront supposés inférieur à p. Soit s_0 un entier. On choisit alors $n - 1$ entiers $s_1, \ldots, s_{n-1}$ « au hasard » (mais inférieurs à p) et soit P le polynôme $\sum_{i=0}^{n-1} s_i X^i$.

1. En considérant les polynômes de Lagrange
$$L_i(X) = \prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} \frac{X - j}{i - j}$$
   montrer que la connaissance des $P(i)$ pour $1 \leqslant i \leqslant n$ permet de retrouver s_0.
2. On suppose connus les $P(i)$ pour $1 \leqslant i \neq i_0 \leqslant n$. Sachant que $P(X)$ est de la forme $\sum_{i=0}^{n-1} s_i X^i$, que sait-on sur s_0 ?
3. On suppose désormais connue la congruence modulo p des $P(i)$ pour $i \neq i_0$. Montrer alors que l'on ne sait rien sur s_0.
4. Le code pour déclencher une frappe nucléaire est un nombre inférieur à p que seul le président connaît. Au cas où celui-ci serait dans l'impossibilité d'agir, il est prévu que son état major constitué de n membres puissent déclencher la frappe sans que toutefois $n - 1$ parmi eux n'y parviennent. Proposer une solution mathématique à ce problème en s'inspirant des questions précédentes.
5. Généraliser la question précédente au cas où l'on voudrait que k d'entre eux le puissent sans que $k - 1$ n'y parviennent.

Problème 5.3. *Signe du discriminant*

Soit Q un polynôme unitaire de degré d à coefficients réels.

On rappelle que le discriminant D de Q est égal à $\prod_{i<j}(\alpha_i - \alpha_j)^2$, les α_i étant les racines (réelles ou complexes) de Q.

1. On définit le signe s de D comme $+1$ si $D > 0$ et -1 si $D < 0$; (on suppose $D \neq 0$). Montrer que
$$s = (-1)^{\frac{d-r}{2}}$$
où r est le nombre de racines réelles de Q comptées avec multiplicités (on regoupera dans l'expression de D chaque terme non réel avec son conjugué).
2. En déduire que
$$r \equiv d + s + 3 \bmod (4).$$
3. On pose $d = 3$ et $Q = x^3 + px + q$, $p, q \in \mathbf{R}$. En déduire le nombre de racines réelles de Q suivant le signe de D.
4. Calculer le discriminant D du polynôme Q en fonction de p et q (en évaluant le résultant $R(Q, Q')$).
5. Calculer la suite de Sturm de Q (on supposera $p \neq 0$ et $q \neq 0$). Retrouver les résultats de la question 3. ci-dessus.

Problème 5.4. *Polynômes de Tchebichev*

1. Justifier l'égalité $Re[(\cos x + i \sin x)^n] = \cos nx$ et en déduire l'existence d'un polynôme T_n de degré n tel que $T_n(\cos x) = \cos nx$.
2. On considère sur $\mathbf{R}[X]$ le produit scalaire
$$\begin{aligned} < .|. >: \mathbf{R}[X]^2 &\to \mathbf{R} \\ (f, g) &\mapsto \int_{-1}^{1} f(x)g(x)\frac{dx}{\sqrt{1-x^2}} \end{aligned}$$
Montrer que $(T_k)_{0 \leqslant k \leqslant n}$ est une base orthogonale de $(\mathbf{R}_n[X], < .|. >)$.
3. (a) Montrer que $T_n(X)$ admet n-racines réelles distinctes x_i que l'on explicitera. On note γ_n le coefficient dominant de $T_n(X)$.
(b) En utilisant le problème (5.1), montrer que pour tout $Q \in \mathbf{R}[X]$, il existe un unique $L_{n,Q} \in \mathbf{R}_n[X]$ tel que $L_{n,Q}(x_i) = Q(x_i)$ pour tout $1 \leqslant i \leqslant n$.
(c) On note φ la forme linéaire définie par $\varphi(P) = \int_{-1}^{1} P(x)\frac{dx}{\sqrt{1-x^2}}$. Soit alors Q un polynôme de degré $2n-1$. Montrer qu'il existe $S \in \mathbf{R}[X]$ de degré $n-1$ tel que $Q - L_{n,Q} = T_n S$. En déduire qu'il existe des $\lambda_i > 0$ tels que pour tout $Q \in \mathbf{R}_{2n-1}[X]$ on ait l'égalité :
$$\int_{-1}^{1} Q(x)\frac{dx}{\sqrt{1-x^2}} = \sum_{i=1}^{n} \lambda_i Q(x_i).$$
En quoi ce résultat est-il surprenant ?
(d) Que se passe-t-il pour $Q(X) = T_n^2$?

4. Soient $y_1, \cdots, y_n$ et $\nu_1, \cdots, \nu_n$ des réels tels que pour tout $Q \in \mathbf{R}_{2n-1}[X]$, on ait $\int_{-1}^{1} Q(x)\frac{dx}{\sqrt{1-x^2}} = \sum_{i=1}^{n} \nu_i Q(y_i)$. Montrer que les y_i sont forcément distincts puis que les ν_i sont uniquement déterminés par les y_i. En considérant $Q = T_n, XT_n, \cdots, X^{n-1}T_n$ conclure que l'ensemble des y_i est égal à l'ensemble des x_i et commenter.

Problème 5.5. *Polynômes cyclotomiques*

On note U_n le groupe multiplicatif des racines n-ièmes de l'unité ($U_n \subset \mathbf{C}$). On rappelle que $U_n \simeq (\mathbf{Z}/n\mathbf{Z}, +)$ (proposition 6.1) ; on note U_n' l'ensemble des générateurs de ce groupe, et un élément de U_n' est dit racine *primitive* de l'unité.

1. Soit $\Phi_n(X) = \prod_{\xi \in U_n'}(X - \xi)$; $\Phi_n(X)$ est par définition le n-ième polynôme cyclotomique et U_n' désigne l'ensemble des racines primitives n-ièmes de l'unité. Montrer que
$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$
et en déduire que $n = \sum_{d|n} \phi(d)$.
2. Calculer Φ_n pour $n = 1, 2, 3, 4, 6, 8$.
3. Montrer que $\Phi_n \in \mathbf{Z}[X]$.
4. On écrit $X^n - 1 = \Phi_n(X)P(X)$. Montrer qu'il existe un nombre premier p et un entier x tels que $p|\Phi_n(x)$ et $p \not| P(x)$. En déduire que $x^n = 0 \mod p$ mais que $x^d \neq 0 \mod p$ pour tout diviseur strict d de n. Conclure que p est du type $kn + 1$ puis qu'il existe une infinité de nombres premiers congrus à 1 modulo n.

Chapitre 6

Théorie des corps

Ce chapitre est une introduction classique à la théorie des corps, avec une section relativement étoffée traitant des corps finis.
De plus une démonstration peu habituelle (mais bien dans l'esprit de cet ouvrage) de la loi de réciprocité quadratique est proposée dans la section 6.6^* (donc hors programme pour la licence) ; une autre preuve de ce même résultat est proposée en exercice.

6.1 CARACTÉRISTIQUE

Si K est un corps commutatif, on note 0 l'élément neutre pour l'addition et 1 l'élément neutre pour la mutiplication. On a un morphisme d'anneaux canonique ϕ :

$$\mathbf{Z} \longrightarrow K$$

tel que $\phi(1) = 1$. Deux cas peuvent se présenter :

1. Le noyau de ϕ est l'idéal (0), *i.e.* ϕ est injective. On identifie alors $\mathbf{Z}$ et son image dans K. Le corps K contenant $\mathbf{Z}$ contient aussi son corps des fractions $\mathbf{Q}$. On dit dans ce cas que K est de *caractéristique 0*.
2. Le noyau de ϕ est un idéal non nul de $\mathbf{Z}$, donc de la forme $n\mathbf{Z}$ avec $n > 0$; le morphisme ϕ se factorise en un morphisme injectif $\tilde{\phi}$:

   $$\mathbf{Z}/n\mathbf{Z} \longrightarrow K.$$

   L'anneau $\mathbf{Z}/n\mathbf{Z}$ s'identifie alors à un sous-anneau du corps K, ce qui implique qu'il est intègre, et donc que n est un nombre premier p ($\mathbf{Z}/p\mathbf{Z}$ est alors un corps à p éléments, *cf.* 1.39). On dit dans ce cas que K est de *caractéristique* p.

6.2 GROUPE MULTIPLICATIF

Proposition 6.1. *Soit K un corps. Alors tout sous-groupe fini G du groupe $(K^*, \times)$ est cyclique. Si $n = |G|$ il est donc isomorphe au groupe $(\mathbf{Z}/n\mathbf{Z}, +)$ (l'isomorphisme transforme la multiplication en addition).*

Démonstration. Le groupe G étant un groupe abélien, c'est aussi un $\mathbf{Z}$-module (on garde ici la notation multiplicative pour la loi de groupe sur G, pour ne pas confondre avec l'addition de K ; la structure de $\mathbf{Z}$-module est donc définie, pour $n \in \mathbf{Z}$ et $g \in G$, par $n.g = g^n$).
Soit $b\mathbf{Z} \subset \mathbf{Z}$ l'idéal annulateur de G. On peut supposer $b > 0$. Il y a donc au moins $|G|$ solutions dans K à l'équation $X^b - 1 = 0$. D'autre part cette équation a au plus b solutions dans le corps K puisqu'elle est de degré b. On a donc $|G| \leqslant b$.
D'après le théorème 2.33 de structure des modules de type fini, appliqué au groupe G (module de type fini sur $\mathbf{Z}$), il existe des nombres entiers $a_1, \ldots, a_s$ tels que $1 < a_1 \leqslant a_2 \cdots \leqslant a_s$ (en fait $a_1|a_2| \ldots |a_s$) et tels que :

$$(G, \times) \simeq (\mathbf{Z}/a_1\mathbf{Z} \times \cdots \times \mathbf{Z}/a_s\mathbf{Z}, +).$$

On alors $b = a_s$ ((a_s) est l'annulateur de G) et $|G| = a_1 a_2 \ldots a_s$. Comme $|G| \leqslant a_s$, on a $s = 1$ et $(G, \times) \simeq (\mathbf{Z}/a_1\mathbf{Z}, +)$ est cyclique. ■

Exemple 6.2. Prenons $K = \mathbf{C}$. Alors si $G \subset \mathbf{C}^*$ est d'ordre n, G est constitué de l'ensemble des racines n-ièmes de l'unité qui est donc un groupe cyclique. Un générateur de ce groupe est appelé *racine primitive* n-ième de l'unité conformément à la définition 6.24 plus loin.

6.3 EXTENSIONS

Définition 6.3. *Si K et L sont deux corps tels que $K \subset L$, on dit que L est une* extension *de K. Le corps L est alors un espace vectoriel sur K dont la dimension, notée $[L : K]$, s'appelle l'ordre de l'extension.*

Si L et L' sont deux extensions d'un même corps K, un K-morphisme $\phi : L \to L'$ est un morphisme de corps ϕ tel que $\phi_{|K}$ est l'identité.

> ***Remarque 6.4.*** Un morphisme de corps $\phi : K \to L$ est par définition un morphisme des anneaux sous-jacents. Il vérifie donc $\phi(0) = 0$, $\phi(1) = 1$ et est toujours injectif puisque $\ker \phi$ est un idéal de K qui ne contient pas 1, donc réduit à $\{0\}$. Un morphisme de corps $\phi : K \to L$ définit donc une extension de K (avec l'abus de langage consistant à identifier K et $\phi(K)$).

Proposition 6.5. *Si $K \subset L \subset H$ sont des extensions de corps, on a :*

$$[H : K] = [H : L][L : K].$$

Démonstration. On suppose les dimensions finies, sinon la proposition est triviale. Soient $(e_1, \ldots, e_n)$ une base de L sur K, et $(f_1, \ldots, f_p)$ une base de H sur L. Nous allons montrer que les $(e_i f_j)$ $(1 \leqslant i \leqslant n, 1 \leqslant j \leqslant p)$ forment une base de H sur K, ce qui montrera la proposition.

Ces éléments sont des générateurs, car si $x \in H$, on peut écrire $x = \sum_{j=1}^{p} \lambda_j f_j$ avec $\lambda_j \in L$. Chaque λ_j peut à son tour se développer sur la base (e_i) : $\lambda_j = \sum_{i=1}^{n} \lambda_{ij} e_i$, avec $\lambda_{ij} \in K$. On obtient alors :

$$x = \sum \lambda_{ij} e_i f_j.$$

On montre de même que les $e_i f_j$ forment une famille libre ; si on a une relation linéaire :

$$\sum \lambda_{ij} e_i f_j = 0,$$

on peut l'écrire

$$\sum_{j=1}^{p} f_j \Big(\sum_{i=1}^{n} \lambda_{ij} e_i\Big) = 0$$

ce qui implique $\sum_{i=1}^{n} \lambda_{ij} e_i = 0$ pour tout j puisque les f_j sont indépendants, et donc $\lambda_{ij} = 0$ puisque les e_i sont indépendants. ■

Définition 6.6. *Soit $K \subset L$ une extension.*

1. *Soit $A = (\alpha_1, \ldots, \alpha_p)$ une partie de L. L'extension de K* engendrée par A *est le plus petit sous-corps de L contenant A ; on la note $K(\alpha_1, \ldots, \alpha_p)$. Si A est réduite à un seul élément α, on dit que l'extension $K(\alpha)$ est* monogène.
2. *Soit $\alpha \in L$, et $\phi : K[X] \to L$ le morphisme d'anneaux défini par $\phi(\lambda) = \lambda$ si $\lambda \in K$ et $\phi(X) = \alpha$.*
   - *On note $K[\alpha]$ l'image de ϕ. C'est le sous-anneau de L engendré par K et α (ensemble des « polynômes en α »).*
   - *Si ϕ est injective, on dit que α est* transcendant *(sur K) ;*
   - *sinon on dit que α est* algébrique *sur K. Le générateur unitaire de* $\ker \phi$ *est alors appelé le* polynôme minimal *de α (sur K). On le note $q_\alpha(X)$.*

Remarques 6.7.

1. Si α est transcendant, on a $K[\alpha] \simeq K[X]$ et donc $K(\alpha) \simeq K(X)$. L'anneau $K[\alpha]$ n'est alors pas un corps.
2. Si α est algébrique, le morphisme ϕ se factorise en $\overline{\phi} \circ \pi$ où $\overline{\phi}$: $K[X]/(q_\alpha) \to K[\alpha]$ est un isomorphisme. Le diagramme suivant est donc commutatif :

$$\begin{array}{ccc} K[X] & \xrightarrow{\quad\phi\quad} & K[\alpha] \\ & {\scriptstyle\pi}\searrow \quad \nearrow{\scriptstyle\overline{\phi}} & \\ & \dfrac{K[X]}{(q_\alpha)} & \end{array} \qquad (1)$$

   et l'anneau $K[\alpha]$ est un corps (*cf.* plus bas).

Rappelons maintenant quelques propriétés des quotients de l'anneau des polynômes $K[X]$ sur un corps K.

Soient $P \in K[X],\ P = a_0 + a_1X + \cdots + X^d$ un polynôme unitaire, π la surjection canonique :

$$K[X] \longrightarrow \frac{K[X]}{(P)}.$$

Posons $x = \pi(X)$ et $\frac{K[X]}{(P)} = K[x]$.

Proposition 6.8.

1. *L'anneau $K[x]$ est un espace vectoriel sur K de dimension d, dont une base est $1, x, \ldots, x^{d-1}$;*
2. *l'anneau $K[x]$ est un corps si et seulement si le polynôme P est irréductible sur K.*

Démonstration. Si $d > 0$, l'application π restreinte à K (identifié aux polynômes de degré 0) est injective puisque $\ker \pi \cap K = (P) \cap K = (0)$. On identifie alors en général K et son image $\pi(K)$ dans $K[x]$, ce qui définit la structure de K-espace vectoriel de $K[x]$. La suite est évidente, laissée en exercice au lecteur (pour *2.*, la démonstration est la même que dans le cas de $\mathbf{Z}$: *cf.* le corollaire 1.39). ■

Exemples 6.9.

1. Si $K = \mathbf{Q}$, $P = 1 + X + \cdots + X^{p-1}$, p étant un nombre premier, $\mathbf{Q}[x] = \frac{\mathbf{Q}[X]}{(P)}$ est une extension de $\mathbf{Q}$ de degré p.

   En effet, le polynôme P est irréductible (corollaire 5.11) et donc $\mathbf{Q}[x] = \frac{\mathbf{Q}[X]}{(P)}$ est un corps.

2. Toujours avec $K = \mathbf{Q}$, posons $P = X^2 - a$ avec $\sqrt{a} \notin \mathbf{Q}$. Alors $\frac{\mathbf{Q}[X]}{(P)}$ est une extension de degré 2 de $\mathbf{Q}$. On dit que c'est une extension quadratique.

Proposition 6.10. *Soient $K \subset L$ une extension, $\alpha \in L$. Les conditions suivantes sont équivalentes :*

1. *α est algébrique sur K ;*
2. *$K[\alpha] = K(\alpha)$;*
3. *$dim_K K[\alpha] < +\infty$.*

De plus, si $q_\alpha(X)$ est le polynôme minimal de α, il est irréductible et son degré q est égal à $[K[\alpha] : K]$. On dit que q est le degré de α (sur K).

Démonstration. *1. $\Rightarrow$ 2.* Si α est algébrique sur K, on a une injection

$$\overline{\phi} :\ \frac{K[X]}{(q_\alpha)} \longrightarrow L$$

et donc q_α est irréductible puisque l'anneau $\frac{K[X]}{(q_\alpha)}$ est intègre car inclus dans un corps

(on l'identifie avec son image par $\overline{\phi}$, *cf.* (1)). L'anneau $\frac{K[X]}{(q_\alpha)}$, isomorphe à $K[\alpha]$, est donc alors un corps (proposition 6.8), ce qui signifie que $K[\alpha] = K(\alpha)$.

2. $\Rightarrow$ *3.* L'anneau $\frac{K[X]}{(q_\alpha)}$ est un espace vectoriel de dimension q sur K si q est le degré de q_α et il s'identifie à son image $K[\alpha]$ par le morphisme $\overline{\phi}$.

3. $\Rightarrow$ *1.* Si $\dim_K K[\alpha] < +\infty$, le morphisme ϕ a un noyau non trivial (sinon on aurait $K[\alpha] \simeq K[X]$ qui est de dimension infinie), et donc α est algébrique par définition. ■

On dit que l'extension $K \subset L$ est *algébrique* si tout $\alpha \in L$ est algébrique sur K.

Théorème 6.11. *Soit $K \subset L$ une extension. Alors l'ensemble M des éléments de L algébriques sur K est un sous-corps de L. En particulier, la somme et le produit de deux éléments algébriques sont algébriques.*

Démonstration. Soient α et α' deux éléments de L algébriques sur K. Il faut montrer que $\alpha+\alpha'$, $\alpha\alpha'$ et $1/\alpha$ (pour $\alpha \neq 0$) sont algébriques. Comme α est algébrique sur K, la proposition 6.10 montre que $L_1 = K[\alpha]$ est un corps et que $[L_1 : K] < +\infty$. Tout élément de L_1 est donc algébrique sur K (proposition 6.10), ce qui est en particulier le cas de $1/\alpha$. L'élément α' étant algébrique sur K, il l'est *a fortiori* sur L_1. L'anneau $L_2 = L_1[\alpha']$ est donc aussi un corps, et l'on a $[L_2 : K] < +\infty$ (proposition 6.5). Mais on a évidemment $\alpha + \alpha'$ et $\alpha\alpha' \in L_2$. Une nouvelle application de la proposition 6.10 montre alors qu'ils sont algébriques sur K. ■

6.4 CORPS DE RUPTURE

Définition 6.12. *Soient K un corps, $P \in K[X]$ un polynôme irréductible non constant. Un corps L extension de K est appelé* corps de rupture *de P sur K si $L = K(\alpha)$ (extension monogène) avec $P(\alpha) = 0$.*

Proposition 6.13. *Soit $P \in K[X]$ un polynôme irréductible non constant. Il existe un corps de rupture de P sur K unique à K-isomorphisme près (définition 6.3).*

Démonstration. a) *Existence*. Posons $L = K[X]/(P)$. Comme P est irréductible, L est un corps (proposition 6.8), et donc une extension de K. Si l'on note x l'image de X dans L par l'application canonique $\pi : K[X] \to K[X]/(P)$, on a bien $L = K(x)$ et $P(x) = 0$ puisque $P(x)$ est l'image de P par π, nulle par définition.

b) *Unicité*. Si on a un corps de rupture $L' = K(\alpha)$, le morphisme canonique $\phi : K[X] \to L'$ qui envoie X sur α se factorise en un K-isomorphisme $K[X]/(q_\alpha) \simeq L'$ par (1). On a $\phi(P) = P(\alpha) = 0$ par définition, et donc $P \in \ker\phi = (q_\alpha)$. Le polynôme q_α divise donc P et n'est pas constant puisque $q_\alpha(\alpha) = 0$. Comme P est irréductible, on a $(P) = (q_\alpha)$ et donc

$$L' \simeq \frac{K[X]}{(q_\alpha)} \simeq \frac{K[X]}{(P)} = L.$$ ■

Remarque 6.14. Si L est un corps de rupture de P sur K, le polynôme P a par définition une racine α dans L. Cependant il n'est en général pas complètement factorisé dans L. Par exemple, prenons $K = \mathbf{Q}$, $P(X) = X^3 - 2$, $L = \mathbf{Q}(\sqrt[3]{2}) \subset \mathbf{R}$ et soit j une racine cubique de l'unité non réelle. Alors les deux racines non réelles $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ de P ne sont pas dans L (le lecteur vérifiera que

$$X^3 - 2 = (X - \sqrt[3]{2})\big(X^2 + X\sqrt[3]{2} + (\sqrt[3]{2})^2\big),$$

le second facteur étant irréductible sur L).

Définition 6.15. *Soit $P \in K[X]$ un polynôme de degré $d > 0$. Un corps L extension de K est appelé* corps de décomposition *de P sur K si :*

1. *Le polynôme P est scindé sur L (i.e. P a toutes ses racines dans L) ;*
2. *les racines de P engendrent L sur K (et donc L est minimal parmi les corps contenant les racines de P).*

Remarquons que dans la définition précédente, on ne fait aucune hypothèse d'irréductibilité sur le polynôme P, contrairement à ce qui se passe pour la définition du corps de rupture.

Exemples 6.16.

1. Dans la remarque 6.14, le corps $L = \mathbf{Q}(\sqrt[3]{2})$ est un corps de rupture de $P = X^3 - 2$, mais pas un corps de décomposition.
2. Si au contraire on considère un nombre premier p et le polynôme irréductible $P = 1 + X + \cdots + X^{p-1}$ (corollaire 5.11), son corps de rupture $L = \frac{\mathbf{Q}[X]}{(P)}$ est aussi un corps de décomposition. En effet, L contient par hypothèse une racine ξ de P ; les $p - 1$ racines de P sont les racines p-ièmes de l'unité différentes de 1 ; ces $p - 1$ racines sont $\xi, \xi^2, \ldots, \xi^{p-1}$ (vérification immédiate laissée au lecteur) qui sont bien dans L puisque L est un corps. Toutes les racines $\neq 1$ sont primitives puisque p est premier.

Proposition 6.17. *Pour tout polynôme $P \in K[X]$, il existe un corps de décomposition noté $D_K(P)$ unique à un K-isomorphisme près.*

Démonstration. a) *Existence*. Immédiate par récurrence sur d : si $d = 1$ ou si P est scindé sur K, on a $D_K(P) = K$. Sinon, soient $Q(X)$ un facteur irréductible de P de degré $\geqslant 2$, K' un corps de rupture de Q, x_1 une racine de Q (donc de P) dans K'. On peut donc écrire $P(X) = (X - x_1)P_1(X)$ dans $K'[X]$, avec $\deg(P_1) = d - 1$. Soit L un corps de décomposition de P_1 sur K' (obtenu par hypothèse de récurrence). Le corps L est alors aussi un corps de décomposition de P sur K (car si $x_2, \ldots, x_d$) sont les racines de P_1 dans L (éventuellement multiples), on a $L = K'(x_2, \ldots, x_d)$ et donc $L = K(x_1, \ldots, x_d)$, puisque $K' = K(x_1)$).

b) *Unicité*. La démonstration, sans difficulté mais un peu technique, se fait par récurrence sur $[L : K]$, et sera admise ici. Nous n'utiliserons pas ce résultat (on pourra se reporter à [**2**] pour une démonstration). ■

Définition 6.18. *Un corps K est dit* algébriquement clos *s'il vérifie une des propriétés équivalentes suivantes :*
1. *Tout polynôme $P \in K[X]$ de degré $\geqslant 1$ admet une racine dans K ;*
2. *tout $P \in K[X]$ est produit de polynômes de degré 1 ;*
3. *si une extension $K \subset L$ est algébrique, on a $K = L$.*

La démonstration de l'équivalence des trois propriétés ci-dessus est immédiate et laissée au lecteur. Le corps $\mathbf{C}$ est algébriquement clos (théorème de d'Alembert-Gauss), mais il y en a d'autres, par exemple le sous-corps de $\mathbf{C}$ formé des éléments algébriques sur $\mathbf{Q}$.

6.5 CORPS FINIS

Rappelons que si K est un corps fini, le morphisme $\phi : \mathbf{Z} \to K$ défini par $\phi(n) = n.1$ a un noyau de la forme $p\mathbf{Z}$, où p est un nombre premier non nul appelé la caractéristique de K. On note $\mathbf{F_p}$ le corps $\mathbf{Z}/p\mathbf{Z}$ (1.39) et $|K|$ le cardinal de K.

Lemme 6.19. *Soit K un corps fini de caractéristique p. Alors K contient un sous-corps isomorphe à $\mathbf{F_p}$ (que l'on identifie à $\mathbf{F_p}$), et son cardinal est de la forme p^n, avec n entier $\geqslant 1$.*

Démonstration. On a déjà vu que l'image de ϕ était isomorphe à $\mathbf{F_p}$. Identifions $\operatorname{Im}\phi$ et $\mathbf{F_p}$. Le corps K est un espace vectoriel sur $\mathbf{F_p}$ de dimension finie n. Son cardinal $|K|$ est donc bien p^n. ■

Lemme 6.20. *Soit K un corps de caractéristique $p > 0$. Notons F l'application $K \to K$ définie par $F(x) = x^p$ (F s'appelle le* morphisme de Frobénius*). Alors*
1. *F est un morphisme de corps (donc injectif).*
2. *Si K est fini, c'est un automorphisme (i.e. il est bijectif).*
3. *Pour $x \in K$, $F(x) = x$ si et seulement si $x \in \mathbf{F_p}$.*

Démonstration. On a évidemment $F(xy) = F(x)F(y)$ et $F(1) = 1$, ce qui implique que $F(x^{-1}) = (F(x))^{-1}$ pour $x \neq 0$. Pour l'addition, écrivons la formule du binôme :

$$(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \cdots + \binom{p}{i}x^{p-i}y^i + \cdots + y^p.$$

Il est bien connu (et facile à vérifier) que p divise $\binom{p}{i}$ $(1 \leqslant i \leqslant p-1)$. En caractéristique p, la formule du binôme devient donc : $(x+y)^p = x^p + y^p$, ce qui montre *1.* F étant un morphisme de corps, il est injectif et donc bijectif si le cardinal de K est fini. Enfin on a $x^{p-1} = 1$ pour tout $x \in \mathbf{F_p}$ non nul (car $\mathbf{F_p}^*$ est de cardinal $p-1$) et donc $x^p = x$ pour $x \in \mathbf{F_p}$. Les éléments de $\mathbf{F_p}$ sont les seuls vérifiant cette équation, puisque l'équation $X^p - X = 0$ a au plus p racines dans le corps K. ■

Le théorème suivant montre pour tout $n > 0$ l'existence d'un corps de cardinal $q = p^n$. L'unicité (à isomorphisme près) d'un tel corps sera montrée plus loin (proposition 6.30).

Théorème 6.21. *(Existence du corps $\mathbf{F_q}$)*
Soient p un nombre premier, $n \in \mathbf{N}^*$. On pose $q = p^n$. On considère le polynôme $X^q - X$ comme à coefficients dans $\mathbf{F_p}$. Alors le corps de décomposition du polynôme $X^q - X$ sur $\mathbf{F_p}$ est un corps à q éléments noté $\mathbf{F_q}$.

Démonstration. Soit K le corps de décomposition de $X^q - X$ sur le corps $\mathbf{F_p}$. L'ensemble $A \subset K$ des racines de $X^q - X$ est un corps car si $x \in A$ et $y \in A$, on a $x^q = x$ et $y^q = y$, d'où $(xy)^q = xy$ et $(x + y)^q = x + y$ car q étant égal à p^n, l'application $x \mapsto x^q$ de K dans K est le morphisme de Frobenius itéré n fois. On a donc $xy \in A$ et $x + y \in A$. De plus si $x \in A$, $x \neq 0$, on a évidemment $1/x \in A$, et A contient $\mathbf{F_p}$ (lemme 6.37). On a donc $A = K$ puisque par définition K est engendré sur $\mathbf{F_p}$ par les racines de $X^q - X$. D'autre part si l'on pose $P = X^q - X$, on a $P' = qX^{q-1} - 1 = -1$ puisque la caractéristique p de K divise q. Cela entraîne que les racines de P sont simples (puisque pour toute racine α de P dans K on a $P'(\alpha) = -1 \neq 0$), et donc que $A = K$ est un corps à q éléments (puisque le polynôme $X^q - X$ a alors exactement q racines dans K). En particulier, si $q = p$, on a $K = \mathbf{F_p}$. ■

Remarques 6.22.

1. Il résulte du théorème ci-dessus que l'on a $X^q - X = \prod_{a \in \mathbf{F_q}} (X - a)$ dans $\mathbf{F_q}[X]$, ou encore en enlevant la racine 0, $X^{q-1} - 1 = \prod_{a \in \mathbf{F_q}^*} (X - a)$.
2. Si $q = p$, on a la factorisation $X^p - X = X(X - 1) \dots (X - (p - 1))$ dans $\mathbf{F_p}[X]$, si l'on note k l'élément $k.1$ de $\mathbf{F_p} = \mathbf{Z}/p\mathbf{Z}$.
3. Posons $P = X^q - X$, P étant considéré comme un élément de $\mathbf{F_p}[X]$. Alors la factorisation de P dans $\mathbf{F_p}[X]$ (en produit de polynômes irréductibles sur $\mathbf{F_p}$) est le produit des polynômes minimaux (distincts) des éléments de $\mathbf{F_q}$. En effet, si $a \in \mathbf{F_q}$, son polynôme minimal q_a (sur le corps $\mathbf{F_p}$) est irréductible et est un diviseur de P (puisque $P(a) = 0$). Réciproquement tout facteur irréductible Q de P est le polynôme minimal d'une quelconque de ses racines.
4. On suppose toujours $q = p^n$. Si Q est un facteur irréductible de $P = X^q - X$ (sur le corps $\mathbf{F_p}$), son degré d divise n.
   En effet, soit α une racine de Q dans $\mathbf{F_q}$. Le corps $\mathbf{F_p}(\alpha)$ est alors un sous-corps de $\mathbf{F_q}$, et $[\mathbf{F_p}(\alpha) : \mathbf{F_p}] = d$ (proposition 6.10). La formule
   $$n = [\mathbf{F_q} : \mathbf{F_p}] = [\mathbf{F_q} : \mathbf{F_p}(\alpha)]\ [\mathbf{F_p}(\alpha) : \mathbf{F_p}]$$
   montre l'assertion.
5. En fait nous allons montrer ci-dessous (corollaire 6.34) que tout polynôme unitaire irréductible de $\mathbf{F_p}[X]$ dont le degré divise n apparaît une fois et une seule dans la factorisation de P.

Étudions maintenant le groupe $(\mathbf{F_q}^*, \times)$. En appliquant la proposition 6.1, on a :

Proposition 6.23. *Soit $q = p^n$, p étant un nombre premier. Alors*
$$(\mathbf{F_q}^*, \times) \simeq (\mathbf{Z}/(q-1)\mathbf{Z}, +).$$

Définition 6.24. *Un élément $a \in \mathbf{F_q}$ qui engendre le groupe cyclique $\mathbf{F_q}^*$ est dit* primitif.

Remarques 6.25.

1. Il y a $\varphi(q-1)$ éléments primitifs dans $\mathbf{F_q}^*$, φ étant la fonction d'Euler (définition 1.40).
2. Si $a \in \mathbf{F_q}^*$ est primitif, les éléments primitifs sont les a^i avec $1 \leqslant i < q-1$ et $i \wedge (q-1) = 1$ (*cf.* la proposition 1.38).

Proposition 6.26. *Soient p un nombre premier, n un entier > 0, $q = p^n$, $a \in \mathbf{F_q}$ un élément primitif, q_a son polynôme minimal sur le corps $\mathbf{F_p}$. Alors q_a est de degré n et est un diviseur irréductible du polynôme $X^q - X$. En particulier l'élément a engendre l'extension $\mathbf{F_q}$ de $\mathbf{F_p}$ (donc $\mathbf{F_q}$ est à la fois le corps de décomposition du polynôme $X^q - X$ et le corps de rupture du polynôme q_a sur le corps $\mathbf{F_p}$).*

Démonstration. Comme a est primitif, il engendre l'extension $\mathbf{F_q}$ de $\mathbf{F_p}$ puisqu'alors tout élément non nul de $\mathbf{F_q}$ est une puissance de a. On a donc $\frac{\mathbf{F_p}(X)}{(q_a(X))} \simeq \mathbf{F_q}$, ce qui implique que q_a est irréductible et de degré $n = [\mathbf{F_q} : \mathbf{F_p}]$ (proposition 6.8). De plus il divise $P = X^q - X$ puisque P annule a. ■

Remarque 6.27. Avec les notations ci-dessus, comme q_a est un diviseur de $X^q - X$, il a toutes ses racines dans $\mathbf{F_q}$ qui chacune engendre l'extension $\mathbf{F_q}$ de $\mathbf{F_p}$.

Corollaire 6.28. *Soit p un nombre premier. Alors pour tout entier n il existe un polynôme $P \in \mathbf{F_p}[X]$ de degré n irréductible.*

Démonstration. Il suffit de prendre pour P le polynôme minimal d'un élément primitif de l'extension $\mathbf{F_q}$ de $\mathbf{F_p}$ pour $q = p^n$ (le corps $\mathbf{F_q}$ existe par le théorème 6.21). ■

Exemple 6.29. Soit $q = 16 = 2^4$. Le lecteur pourra vérifier à titre d'exercice que la décomposition de $X^{16} - X$ en facteurs irréductibles sur $\mathbf{F_2}$ s'écrit :

$$X(X+1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1).$$

Si l'on note a une racine du polynôme $X^4 + X + 1$, on a $\mathbf{F_{16}} = \mathbf{F_2}(a)$. L'élément a est de plus primitif, car d'ordre (multiplicatif) 15 dans $\mathbf{F_{16}}^*$ (l'ordre de a divise 15 ; comme on a la relation $a^4 + a + 1 = 0$, il est immédiat de voir que a ne peut être d'ordre 1, 3 ou 5).

En revanche l'élément a^3 est d'ordre 5 dans $\mathbf{F_{16}}^*$; il n'est donc pas primitif. Cependant son polynôme minimal est $X^4+X^3+X^2+X+1$ aussi de degré 4, et l'on a $\mathbf{F_{16}} = \mathbf{F_2}(a^3)$.

Le lecteur vérifiera que les éléments primitifs sont les racines des polynômes X^4+X+1 et X^4+X^3+1.

Montrons maintenant l'unicité (à isomorphisme près) du corps fini à $q=p^n$ éléments.

Proposition 6.30. *« Unicité du corps $\mathbf{F_q}$ ».*
Soit L un corps fini à $q=p^n$ éléments. Alors il est isomorphe au corps $\mathbf{F_q}$ (par un $\mathbf{F_p}$-isomorphisme).

Démonstration. Comme $|L|=q=p^n$, le corps L est de caractéristique p. Il contient donc le corps $\mathbf{F_p}$.
Soit $a \in \mathbf{F_q}$ un élément primitif, $q_a \in \mathbf{F_p}[X]$ son polynôme minimal. Le polynôme q_a est de degré n, et

$$\mathbf{F_q} = \{\lambda_0 + \lambda_1 a + \cdots + \lambda_{n-1}a^{n-1},\ \lambda_i \in \mathbf{F_p}\},$$

puisque $\mathbf{F_q} \simeq \frac{\mathbf{F_p}[X]}{(q_a(X))}$.
Comme $|L|=q$, les éléments de L vérifient aussi l'équation $X^q-X=0$ (proposition 1.18) et L s'identifie aussi à l'ensemble des solutions de l'équation $X^q-X=0$. Comme q_a est un diviseur irréductible (sur $\mathbf{F_p}$) de X^q-X, il existe $b \in L$ tel que q_a soit le polynôme minimal de b (b est une racine dans L du polynôme q_a). Considérons l'application $f : \mathbf{F_q} \longrightarrow L$:

$$\lambda_0 + \lambda_1 a + \cdots + \lambda_{n-1}a^{n-1} \mapsto \lambda_0 + \lambda_1 b + \cdots + \lambda_{n-1}b^{n-1}.$$

Il est immédiat de vérifier que f est un isomorphisme (en fait un $\mathbf{F_p}$-isomorphisme) de corps. ■

Étudions maintenant les sous-corps de $\mathbf{F_q}$.

Proposition 6.31. *Posons $q=p^n$ avec p premier.*

1. *Pour tout entier d tel que $d|n$, il y a un unique corps K de cardinal p^d tel que :*

$$\mathbf{F_p} \subset K \subset \mathbf{F_q}.$$

   Ce corps K est l'ensemble des $x \in \mathbf{F_q}$ tels que $x^{p^d}=x$ et est isomorphe à $\mathbf{F_q}'$ avec $q'=p^d$.

2. *Réciproquement, tout corps K tel que $\mathbf{F_p} \subset K \subset \mathbf{F_q}$ est de cardinal p^d avec $d|n$.*

Démonstration. Soit d un entier tel que $d|n$. Montrons l'existence de K. Soit K l'ensemble des racines (dans $\mathbf{F_q}$) du polynôme $X^{p^d}-X$: il a déjà été démontré que K était un corps (démonstration du théorème 6.21).

Lemme 6.32. *Soit k un entier tels que $k-1$ soit un diviseur de $q-1$. Alors le polynôme $X^k - X$ a exactement k racines dans $\mathbf{F_q}$.*

Démonstration. Le nombre de racines d'un polynôme de degré k dans un corps est $\leqslant k$. D'autre part $(\mathbf{F_q}^*, \times) \simeq (\mathbf{Z}/(q-1)\mathbf{Z}, +)$. La proposition 1.35 implique qu'il y a dans $\mathbf{F_q}^*$ exactement $k-1$ éléments d'ordre divisant $k-1$. Ces $k-1$ éléments plus $\{0\}$ sont racines du polynôme $X(X^{k-1}-1) = X^k - X$. ■

Lemme 6.33. *Soient d et n deux entiers tels que $d|n$, p un entier > 1. Alors $(p^d-1)|(p^n-1)$.*

Démonstration. Il suffit de considérer l'identité polynomiale :

$$X^n - 1 = (X^d - 1)(X^{(n-d)} + X^{(n-2d)} + \cdots + X^d + 1)$$

et de faire $X = p$. ■

Le lemme 6.32 appliqué avec $k = p^d$ implique que $|K| = p^d$. Le corps K étant de cardinal $q' = p^d$, il est isomorphe à $\mathbf{F_{q'}}$ (théorème 6.21). Pour l'unicité, soit K_1 un sous-corps de $\mathbf{F_q}$ de cardinal p^d. Le corps K_1 est alors isomorphe aussi à $\mathbf{F_{q'}}$ ce qui montre l'unicité (*i.e.* $K = K_1$), car tout élément de $\mathbf{F_{q'}}$ vérifiant l'équation $X^{q'} - X = 0$, il en est de même pour les éléments de K_1.

Réciproquement, si K est un corps tel que :

$$\mathbf{F_p} \subset K \subset \mathbf{F_q}$$

c'est une extension de degré d de $\mathbf{F_p}$, $\mathbf{F_q}$ est une extension de degré b de K, on a donc $n = bd$ avec card(K) $= p^d$. ■

Corollaire 6.34. *Soient p un nombre premier, $q = p^n$, $\{Q_i\}$, $i \in I$, l'ensemble des polynômes unitaires irréductibles de $\mathbf{F_p}[X]$ dont le degré divise n. On a alors :*

$$X^q - X = \prod_{i \in I} Q_i$$

En particulier, les $(X - \alpha_j)_{\alpha_j \in \mathbf{F_p}}$ sont parmi les Q_i.

Démonstration. On a déjà montré (remarque 6.22) que si Q est un facteur irréductible de $P = X^q - X$, son degré divise n.

Réciproquement, soit Q un polynôme irréductible unitaire de $\mathbf{F_p}[X]$ dont le degré d divise n. Le corps $K_1 = \frac{\mathbf{F_p}[X]}{(Q)}$ est de cardinal $q' = p^d$ donc isomorphe au corps $K \simeq \mathbf{F_{q'}}$ tel que :

$$\mathbf{F_p} \subset K \subset \mathbf{F_q}$$

(proposition 6.31). L'élément $x \in K_1$ (image de X) a pour polynôme minimal le polynôme Q. Son image $\alpha \in K$ par le $\mathbf{F_p}$-isomorphisme $K_1 \simeq K$ a le même polynôme minimal qui divise donc P (puisque α est annulé par P). Ce facteur n'apparaît qu'une fois dans la décomposition de P puisque toutes les racines de P sont simples. ■

Corollaire 6.35. *Soit $P \in \mathbf{F_p}[\mathrm{X}]$ un polynôme de degré n. Les conditions suivantes sont alors équivalentes :*

1. *P est réductible sur le corps $\mathbf{F_p}$;*
2. *P a une racine dans un corps $\mathbf{F_{p^d}}$ avec $d \leqslant n/2$.*

6.6 *COMPLÉMENTS

6.6.1. Automorphismes de $\mathbf{F_q}$

Rappelons que si K est un corps, un automorphisme ϕ de K est un morphisme non nul (donc bijectif) $K \to K$.

Plus généralement, si $K \subset L$ est une extension de corps, un K-automorphisme de L est un automorphisme ϕ de L tel que $\phi|_K = \mathrm{Id}$ (*cf.* la définition 6.3). L'ensemble des automorphismes de K (resp. des K-automorphismes de L) est un groupe (pour la composition). Il résulte du lemme 6.37 que si K est un corps fini de caractéristique p, alors pour $s \in \mathbf{N}$, l'application $F^s : K \to K$ définie par $F^s(x) = x^{p^s}$ (« Frobenius itéré s fois ») est un automorphisme de K. Nous allons montrer que tout automorphisme est de cette forme. On peut supposer que $K = \mathbf{F_q}$, avec $q = p^n$ (proposition 6.30).

Proposition 6.36. *Soient p un nombre premier, n un entier > 0, $q = p^n$, ϕ un automorphisme du corps $\mathbf{F_q}$. Il existe alors un entier $s \leqslant n$ tel que $\phi(x) = x^{p^s}$ pour tout $x \in \mathbf{F_q}$.*

Démonstration. Montrons deux résultats préliminaires.

Lemme 6.37. *Soit $P \in \mathbf{F_q}[X]$ un polynôme. Alors les conditions suivantes sont équivalentes :*

1. *$P \in \mathbf{F_p}[X]$;*
2. *$(P(X))^p = P(X^p)$.*

Démonstration. Posons $P(X) = a_d X^d + \cdots + a_1 X + a_0$. On a alors $(P(X))^p = a_d^p (X^p)^d + \cdots + a_1^p X^p + a_0^p$. Ce polynôme est égal à $P(X^p)$ si et seulement si $a_i^p = a_i$ pour tout i, *i.e.* si et seulement si $a_i \in \mathbf{F_p}$ pour tout i (en effet, les p racines dans $\mathbf{F_q}$ du polynôme $X^p - X$ sont les éléments de $\mathbf{F_p}$). ■

Lemme 6.38. *Soit $\alpha \in \mathbf{F_q}$, $q_\alpha(X) \in \mathbf{F_p}[X]$ le polynôme minimal de α sur $\mathbf{F_p}$. Soit r le plus petit entier $\geqslant 0$ tel que $\alpha^{p^r} = \alpha$. On a alors*

$$q_\alpha(X) = (X - \alpha)(X - \alpha^p) \ldots (X - \alpha^{p^{r-1}}).$$

En particulier, $q_\alpha(X)$ est de degré r, et donc $r | n$ (proposition 6.31).

Démonstration. Remarquons d'abord que pour $0 \leqslant i < j < r$, on a $\alpha^{p^i} \neq \alpha^{p^j}$. En effet, dans le cas contraire on aurait :

$$\alpha^{p^{i+r-j}} = (\alpha^{p^i})^{p^{r-j}} = (\alpha^{p^j})^{p^{r-j}} = \alpha^{p^r} = \alpha$$

contrairement à la propriété de minimalité de r (car $i + r - j < r$).
Posons $P(X) = (X - \alpha)(X - \alpha^p)\dots(X - \alpha^{p^{r-1}})$. Le polynôme P est de degré r, vérifie $P(\alpha) = 0$, mais est *a priori* à coefficients dans $\mathbf{F_q}$. Montrons que $P(X) \in \mathbf{F_p}[X]$. On a :

$$P(X)^p = (X^p - \alpha^p)(X^p - \alpha^{p^2})\dots(X^p - \alpha^{p^r}) = P(X^p)$$

(puisque $\alpha^{p^r} = \alpha$), d'où $P \in \mathbf{F_p}[X]$ par le lemme 6.37. Le polynôme $q_\alpha(X)$ divise donc $P(X)$ dans $\mathbf{F_p}[X]$. Mais $q_\alpha(X)$ étant invariant par le morphisme de Frobenius F (puisque $q_\alpha(X) \in \mathbf{F_p}[X]$), l'ensemble de ses racines aussi. Les α^{p^i} étant distincts, on en déduit que $\deg(q_\alpha) \geqslant r$, et donc que $q_\alpha(X) = P(X)$. ■

Montrons maintenant la proposition 6.36. Soit ϕ un automorphisme de $\mathbf{F_q}$. On a $\phi(1) = 1$, d'où $\phi(n.1) = n.1$ pour tout entier n. On en déduit que $\phi|_{\mathbf{F_p}}$ est l'identité. Prenons pour α un élément de $\mathbf{F_q}$ primitif sur $\mathbf{F_p}$ (définition 6.24). Comme le polynôme $q_\alpha(X) \in \mathbf{F_p}[X]$ est invariant par ϕ, on a que $\phi(\alpha)$ est aussi racine de $q_\alpha(X)$, donc $\phi(\alpha) = \alpha^{p^s}$ pour un entier s tel que $0 \leqslant s < n$ (lemme 6.38). Mais l'ensemble des $x \in \mathbf{F_q}$ qui vérifient $\phi(x) = x^{p^s}$ est un sous-corps K de $\mathbf{F_q}$ qui contient $\mathbf{F_p}$ et l'élément α. On a donc $K = \mathbf{F_q}$ puisque $\mathbf{F_q} = \mathbf{F_p}(\alpha)$. ■

Corollaire 6.39.

1. *Tout automorphisme de $\mathbf{F_q}$ induit l'identité sur $\mathbf{F_p}$;*
2. *le groupe des automorphisme de $\mathbf{F_q}$ est cyclique, engendré par l'automorphisme de Frobenius $x \mapsto x^p$;*
3. *plus généralement, soient r un entier $\geqslant 1$, $q_1 = p^r$, $q = q_1^n$; on a donc $\mathbf{F_{q_1}} \subset \mathbf{F_q}$. Alors le groupe des $\mathbf{F_{q_1}}$-automorphismes de $\mathbf{F_q}$ est cyclique, engendré par l'automorphisme $x \mapsto x^{q_1}$.*

Démonstration.
1. et *2.* découlent immédiatement de la proposition 6.36. Montrons *3.*

L'automorphisme $x \mapsto x^{q_1}$ laisse fixes les éléments de $\mathbf{F_{q_1}}$ puisque ceux-ci vérifient l'équation $X^{q_1} - X = 0$ (proposition 6.36).

Réciproquement, soit ϕ un $\mathbf{F_{q_1}}$-automorphisme de $\mathbf{F_q}$; ϕ est de la forme $x \mapsto x^{p^s}$ par *2.* Remarquons d'abord que si $\alpha \in \mathbf{F_{q_1}}$ est un élément primitif, l'entier r est le plus petit entier k tel que $\alpha^{p^k} = \alpha$ puisque le polynôme minimal de α est de degré r. On en déduit tout entier s qui vérifie $\alpha^{p^s} = \alpha$ est un multiple de r (car si $s = ar + b$, on a $\alpha^{p^s} = \alpha^{p^b}$). ■

Ce résultat permet d'illustrer la « théorie de Galois » dans le cas particulier des corps finis.

Proposition 6.40. *Soit $q = p^r$, $G \simeq (\mathbf{Z}/n\mathbf{Z}, +)$ le groupe des automorphismes de $\mathbf{F_{q^n}}$ sur $\mathbf{F_q}$. Il y a une bijection Φ entre les corps K tels que $\mathbf{F_q} \subset K \subset \mathbf{F_{q^n}}$ et les sous-groupes de $H \subset G$. À un sous-corps K correspond le sous-groupe $H \subset G$ des automorphismes de $\mathbf{F_{q^n}}$ qui laissent fixes les éléments de K. Le groupe des automorphismes de K sur le corps $\mathbf{F_q}$ est alors isomorphe au quotient G/H.*

Démonstration. Soit K un corps tel que $\mathbf{F_q} \subset K \subset \mathbf{F_{q^n}}$. Le corps K est de cardinal q^d avec $d|n$ (c'est d'ailleurs l'unique sous-corps de $\mathbf{F_{q^n}}$ de cardinal q^d (proposition 6.36).

On lui fait correspondre le sous-groupe $H \subset G$ des K-automorphismes de $\mathbf{F_{q^n}}$. Comme $K \simeq \mathbf{F_{q^d}}$, ce groupe est cyclique d'ordre n/d (corollaire 6.39, 3.) : c'est l'unique sous-groupe de $G \simeq (\mathbf{Z}/n\mathbf{Z}, +)$ d'ordre n/d. Cela montre que Φ est une bijection.

Montrons maintenant la fin de la proposition. Le groupe L des $\mathbf{F_q}$-automorphismes de K est isomorphe à $\mathbf{Z}/d\mathbf{Z}$; on a une application $\psi : G \to L$ qui à un automorphisme de $\mathbf{F_{q^n}}$ fait correspondre sa restriction à K. Pour achever de montrer la proposition, il suffit de montrer le lemme suivant :

Lemme 6.41. *Soit $H \subset G$ le sous-groupe des automorphismes qui laissent fixes les éléments de K. L'application ψ est un morphisme de groupes surjectif de noyau H.*

L'application ψ est évidemment un morphisme de groupes, dont le noyau est H par définition (le noyau est l'ensemble des $\mathbf{F_q}$-automorphismes de $\mathbf{F_{q^n}}$ qui induisent l'identité sur K). Le morphisme ψ s'interprète comme un morphisme de groupes : $\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/d\mathbf{Z}$ qui envoie la classe de 1 (mod n) sur la classe de 1 (mod d), puisqu'il envoie l'identité sur l'identité. Le morphisme ψ est donc surjectif, et son noyau est isomorphe à $\mathbf{Z}/s\mathbf{Z}$ avec $s = n/d$ (proposition 1.36). ■

6.6.2. *Carrés de $\mathbf{F_q}$

Pour $q = p^n$ fixé (p nombre premier), posons :

$$(\mathbf{F_q})^2 = \{x \in \mathbf{F_q} |\ \exists\ y \in \mathbf{F_q}, y^2 = x\}, \quad {\mathbf{F_q}}^{*2} = {\mathbf{F_q}}^* \cap (\mathbf{F_q})^2.$$

Proposition 6.42.

- *Si $p = 2$, on a $(\mathbf{F_q})^2 = \mathbf{F_q}$. ;*
- *si $p > 2$, on a $|(\mathbf{F_q})^2| = \frac{q+1}{2}$, $\quad |{\mathbf{F_q}}^{*2}| = \frac{q-1}{2}$.*

Démonstration. Si $p = 2$, l'application $x \mapsto x^2$ de $\mathbf{F_q}$ dans lui-même est le morphisme de Frobenius, donc un isomorphisme (il est donc en particulier surjectif ; *cf.* le lemme 6.37).

Si $p > 2$, on a $1 \neq -1$ et l'élévation au carré donne un morphisme surjectif :

$$ {\mathbf{F_q}}^* \to {\mathbf{F_q}}^{*2}$$

dont le noyau est le sous-groupe $(-1, 1)$ de $({\mathbf{F_q}}^*, \times)$. Cela montre que $|{\mathbf{F_q}}^{*2}| = \frac{q-1}{2}$, et donc $|(\mathbf{F_q})^2| = \frac{q+1}{2}$ puisqu'il faut ajouter l'élément 0. ■

Proposition 6.43. *« Critère d'Euler »*

$$x \in {\mathbf{F_q}}^{*2} \iff x^{\frac{q-1}{2}} = 1.$$

Démonstration. Notons

$$X = \{x \in \mathbf{F_q} \,|\, x^{\frac{q-1}{2}} = 1\}.$$

On a évidemment ${\mathbf{F_q}}^{*2} \subset X$ (car si $x = y^2$ avec $y \in {\mathbf{F_q}}^*$, $y^{q-1} = 1$, d'où $x^{\frac{q-1}{2}} = 1$), et $|X| \leqslant \frac{q-1}{2}$ puisqu'il est constitué des racines d'un polynôme de degré $\frac{q-1}{2}$. On a donc $X = {\mathbf{F_q}}^{*2}$. ■

Signalons deux corollaires classiques en théorie des nombres.

Corollaire 6.44. *Soient $p > 2$ un nombre premier, n un entier, $q = p^n$. Alors*

$$-1 \in (\mathbf{F_q})^2 \iff q \equiv 1 \bmod 4$$

Démonstration.

$$-1 \in {\mathbf{F_q}}^{*2} \Leftrightarrow (-1)^{\frac{q-1}{2}} = 1 \Leftrightarrow \frac{q-1}{2} \equiv 0 \bmod 2 \Leftrightarrow q \equiv 1 \bmod 4.$$ ■

Corollaire 6.45. *Il existe une infinité de nombres premiers de la forme $4m + 1$.*

Démonstration. Soient n un entier arbitraire et p un facteur premier de $(n!)^2 + 1$. Alors on a $p > n$ (sinon p diviserait $n!$) et la classe de $(n!)^2 + 1$ est nulle dans $\mathbf{F_p}$. Donc -1 est un carré dans $\mathbf{F_p}$ (puisque $-1 = \overline{(n!)^2}$) ce qui entraîne que p est de la forme $4m + 1$ d'après le corollaire 6.44. Comme $p > n$ et que n est arbitraire, on en déduit l'assertion. ■

6.6.3. *La loi de réciprocité quadratique

Définition 6.46. *Un entier $a \in \mathbf{Z}$ est dit un résidu quadratique modulo n si l'image $\overline{a} \in \mathbf{Z}/n\mathbf{Z}$ est un carré.*

Ainsi pour connaître, par exemple, les résidus quadratique modulo 6, il suffit de faire la table des carrés dans $\mathbf{Z}/6\mathbf{Z}$:

x	0	1	2	3	4	5
x^2	0	1	4	3	4	1

de sorte que a est un résidu quadratique modulo 6 si et seulement si $a \equiv 0, 1, 3, 4 \bmod 6$.

Rappelons que dans le corps $\mathbf{F_q}$, -1 est un carré si et seulement si $q \equiv 1 \bmod 4$ (corollaire 6.44) ; donc si p est un nombre premier, -1 est résidu quadratique modulo p si et seulement si $p \equiv 1 \bmod 4$.

Définition 6.47.
– ***Symbole de Legendre*** *: pour p premier et a non divisible par p, on définit $\left(\frac{a}{p}\right) \in \{\pm 1\}$ comme étant égal à 1 si a est un résidu quadratique modulo p et -1 sinon.*
– ***Symbole de Jacobi*** *: pour p premier et a divisible par p, on prolonge le symbole de Legendre en posant $\left(\frac{a}{p}\right) = 0$. Si $b = \prod_i p_i$ où les p_i sont des nombres premiers, on pose :*

$$\left(\frac{a}{b}\right) = \prod_i \left(\frac{a}{p_i}\right)$$

(le produit est défini avec la multiplication dans $\mathbf{Z}$*).*

Lemme 6.48. *Le symbole de Legendre est multiplicatif, i.e. :*

$$\left(\frac{ac}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{c}{p}\right)$$

de sorte que le symbole de Jacobi est bi-multiplicatif (i.e. par rapport aux variables a et b).

Démonstration. La multiplicativité du symbole de Legendre découle directement du critère d'Euler (proposition (6.43). En effet si x est non nul dans $\mathbf{Z}/p\mathbf{Z}$, x est un carré si et seulement si $x^{(p-1)/2} = 1$ alors que dans le cas contraire on a $x^{(p-1)/2} = -1$. Ainsi si x et y sont des résidus quadratiques non nuls modulo p, on a $(xy)^{(p-1)/2} = x^{(p-1)/2}y^{(p-1)/2} \equiv 1 \bmod 2$ et xy est un résidu quadratique modulo p. Si x est un résidu quadratique modulo p alors que y n'en n'est pas un, l'égalité précédente donne que xy n'est pas un résidu quadratique modulo p. Enfin si x et y ne sont pas des résidus quadratiques modulo p, l'égalité précédente donne $(xy)^{(p-1)/2} \equiv 1 \bmod p$ et xy est un résidu quadratique modulo p, d'où la multiplicativité du symbole de Legendre et la bi-multiplicativité du symbole de Jacobi. ■

Lemme 6.49. *Le symbole de Jacobi $\left(\frac{a}{b}\right)$ est nul si et seulement si a et b ne sont pas premiers entre eux. Par ailleurs si $a \wedge b = 1$ et si a est un résidu quadratique modulo b alors $\left(\frac{a}{b}\right) = 1$.*

Démonstration. Supposons qu'il existe p premier divisant $a \wedge b$; on en déduit alors que $a \equiv 0 \bmod p$ et donc $\left(\frac{a}{p}\right) = 0$, soit $\left(\frac{a}{b}\right) = 0$. Réciproquement si $\left(\frac{a}{b}\right) = 0$, on en déduit qu'il existe p divisant b tel que $\left(\frac{a}{p}\right) = 0$ soit $a \equiv 0 \bmod p$ et donc p divise $a \wedge b$.
En outre s'il existe c tel que $a \equiv c^2 \bmod b$, on en déduit que $a \equiv c^2 \bmod p$ pour tout p divisant b et donc $\left(\frac{a}{b}\right) = 1$. ■

Remarquons que la réciproque de la dernière assertion est fausse : soit $b = p^2$ et a qui n'est pas un carré modulo p. On a par définition $\left(\frac{a}{b}\right) = 1$ alors que a n'est pas un carré modulo b car sinon il en serait un modulo p.

Proposition 6.50. *« **Lemme de Gauss** » (encore un !). Pour p premier impair et $n \in \mathbf{Z}$, on appelle résidu minimal de n modulo p l'unique entier $n' \in]-p/2, p/2[$ tel que $n \equiv n' \mod p$. Soit $m \in \mathbf{N}$ non multiple de p ; on note $\mu_p(m)$ (ou simplement μ s'il n'y a pas de confusion possible) le nombre d'entiers parmi $\{m, 2m, \cdots, \frac{(p-1)}{2}m\}$ dont le résidu minimal est strictement négatif. On a alors $\left(\frac{m}{p}\right) = (-1)^{\mu}$.*

Démonstration. Posons $\lambda = \frac{p-1}{2} - \mu$ et soit $r_1, \cdots, r_\lambda$ (resp. $-s_1, \cdots, -s_\mu$) les résidus minimaux positifs ou nuls (resp. strictement négatifs) de $\{m, 2m, \cdots, \frac{p-1}{2}m\}$. Notons tout d'abord que les r_i (resp. s_i) sont distincts deux à deux. Supposons par exemple qu'il existe un couple (i, j) tel que $r_i = s_j$, soit donc $am \equiv r_i \equiv s_j \equiv -bm \mod p$ avec $1 \leqslant a, b \leqslant (p-1)/2$. On obtient alors $am + bm \equiv 0$ et comme m est premier avec p, $a + b$ est divisible par p ce qui est impossible, d'où la contradiction. On a ainsi :

$$\{r_1, \cdots, r_\lambda, s_1, \cdots, s_\mu\} = \{1, 2, \cdots, (p-1)/2\};$$

on obtient en particulier :

$$m.2m \ldots \frac{p-1}{2}m \equiv (-1)^{\mu} r_1 \cdots r_\lambda s_1 \cdots s_\mu = (-1)^{\mu}\Big(\frac{p-1}{2}\Big)! \mod p$$

Comme p ne divise pas $(\frac{p-1}{2})!$, il vient $m^{\frac{p-1}{2}} \equiv (-1)^{\mu} \mod p$, d'où le résultat. ■

Corollaire 6.51. ***(Le cas de 2)** : pour p premier impair, on a $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ et donc 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \mod 8$.*

Démonstration. Il s'agit de calculer μ pour $m = 2$; on est donc ramené à compter les entiers l tels que $p/2 < 2l < p$. On vérifie aisément que si $p \equiv 1 \mod 4$ (resp. $p \equiv 3 \mod 4$) alors $\mu = \lambda = \frac{p-1}{4}$ (resp. $\lambda = \frac{p-3}{4}$ et $\mu = \frac{p+1}{4}$). On vérifie alors que $\frac{p^2-1}{4}$ a la même parité que μ, d'où le résultat. ■

Théorème 6.52. ***(Loi de réciprocité quadratique)**. Pour p et q premiers impairs on a :*

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right)$$

Énoncée la première fois par Euler en 1783, la première preuve est due à Gauss en 1798, qui en donnera 7 en tout. Aujourd'hui on en dénombre plus de 163 ! Nous proposons une preuve assez récente via le « symbole de Zolotarev ».

Notons d'abord que l'ensemble des bijections de $\mathbf{Z}/n\mathbf{Z}$ dans lui-même s'identifie au groupe S_n (*cf.* la remarque 4.11 : il suffit de choisir une bijection de l'ensemble $\{\mathbf{Z}/n\mathbf{Z}\}$ sur $\{1, 2, \ldots, n\}$, par exemple la bijection $\{\overline{1}, \ldots, \overline{n}\} \mapsto \{1, 2, \ldots, n\}$; si alors $m \wedge n = 1$, la multiplication par m dans $\mathbf{Z}/n\mathbf{Z}$ est une bijection et correspond donc à un élément de S_n.

Définition 6.53. *Pour m premier avec n on définit le symbole de Zolotarev $e_n(m)$ comme la signature de la permutation correspondant à la multiplication par m dans $\mathbf{Z}/n\mathbf{Z}$.*

Proposition 6.54. *Pour n et m des nombres premiers impairs distincts, le symbole de Zolotarev est égal au symbole de Legendre.*

Démonstration. Le résultat découle directement du lemme suivant :

Lemme 6.55. *Le symbole de Zolotarev est multiplicatif en la variable m, i.e. $e_n(mm') = e_n(m)e_n(m')$. En outre pour n premier impair $e_n(m) \equiv m^{(n-1)/2} \mod n$.*

Démonstration. La multiplicativité du symbole de Zolotarev en la variable m provient du fait que la composition de la multiplication par m avec la multiplication par m' correspond à la multiplication par mm' et que la signature d'une composée est le produit des signatures.

Soit r l'ordre de m dans le groupe $((\mathbf{Z}/n\mathbf{Z})^*, \times)$ qui est cyclique puisque n est premier ; ce groupe se décompose alors sous l'action de la multiplication par m en $(n-1)/r$ orbites chacune de longueur r et sur ces orbites la multiplication par m induit un cycle de longueur r. On en déduit alors que le symbole de Zolotarev est $(-1)^{(r-1)(n-1)/r}$. Ainsi si r est pair on a :

$$m^{(n-1)/2} = (m^{r/2})^{(n-1)/r} \equiv (-1)^{(n-1)/r} \mod n$$

car n étant premier, $m^{r/2} \equiv -1 \mod n$; si r est impair, $n-1$ étant pair est divisible par $2r$ et donc $m^{(n-1)/2} = (m^r)^{(n-1)/2r} \equiv 1 \mod n$ d'où le résultat. ■

Lemme 6.56. *On fixe n et m des nombres premiers impairs distincts. On considère alors σ (resp. τ) la permutation de $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ définie par $(i,j) \mapsto (mi+j, j)$ (resp. $(i, nj+i)$). On a alors $\varepsilon(\sigma) = \left(\frac{m}{n}\right)$ et $\varepsilon(\tau) = \left(\frac{n}{m}\right)$.*

Démonstration. La multiplication par m dans $\mathbf{Z}/n\mathbf{Z}$ étant injective, il est immédiat de voir que σ (resp. τ) est bien une permutation de $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$. La signature de σ restreinte à $\mathbf{Z}/n\mathbf{Z} \times \{j\}$, comme composée de la multiplication par m et de la translation par j sur la première composante, est de signature $\left(\frac{m}{n}\right)$ car la translation en question est de signature $(-1)^{n-1} = 1$ (proposition 6.54). En outre j décrit m valeurs de sorte que la signature de σ est $\left(\frac{m}{n}\right)^m = \left(\frac{m}{n}\right)$. Par symétrie τ est de signature $\left(\frac{n}{m}\right)$. ■

Lemme 6.57. *Soit $\pi : \mathbf{Z}/nm\mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ l'isomorphisme du lemme chinois. On considère la permutation λ de $\mathbf{Z}/nm\mathbf{Z}$ définie par $mi+j \mapsto nj+i$. On a alors $\lambda \circ \pi^{-1} \circ \sigma = \pi^{-1} \circ \tau$ et $\varepsilon(\lambda) = (-1)^{\frac{n(n-1)}{2}\frac{m(m-1)}{2}}$.*

Démonstration. L'isomorphisme canonique $\pi : \mathbf{Z}/nm\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ vérifie $\pi(mi+j) = (mi+j, j)$ et $\pi(i+nj) = (i, i+nj)$. Ainsi en notant λ la bijection

de $\mathbf{Z}/mn\mathbf{Z}$ définie par $\lambda(mi+j) = i+nj$ et qui correspond au passage de l'ordre lexicographique à l'ordre lexicographique inverse, on obtient $\lambda \circ \pi^{-1} \circ \sigma = \pi^{-1} \circ \lambda$.
Pour le calcul de $\varepsilon(\lambda)$, il s'agit de compter le nombre d'inversions, *i.e.* le nombre de $(i,j) < (i',j')$ pour l'ordre lexicographique soit $i < i'$ ou $i = i'$ et $j < j'$, tels que $(i,j) > (i',j')$ pour l'ordre lexicographique inverse, *i.e.* $j > j'$ ou $j = j'$ et $i > i'$. On obtient alors les conditions $i < i'$ et $j > j'$ soit $C_n^2 C_m^2$ possibilités, d'où le résultat. ■

Preuve de la loi de réciprocité quadratique : on réécrit l'égalité du lemme sous la forme $\lambda \circ (\pi^{-1} \circ \sigma \circ \pi) = \pi^{-1} \circ \tau \circ \pi$, d'où en prenant les signatures : $(-1)^{(m-1)(n-1)/4} \left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$. On en déduit alors la loi de réciprocité quadratique pour le symbole de Legendre.
En outre on obtient aussi la multiplicativité pour la variable n du symbole de Zolotarev et donc son égalité avec le symbole de Jacobi. ■

Exemple 6.58. Calcul de $\left(\frac{713}{1\,009}\right)$. En appliquant la loi de réciprocité quadratique, on a :

$$(\frac{713}{1\,009}) = (\frac{1\,009}{713})(-1)^{\frac{1\,008.712}{4}} = (\frac{296}{713})(+1) = (\frac{8.37}{713}) = (\frac{8}{713})(\frac{37}{713});$$

par ailleurs on a $(\frac{8}{713}) = (\frac{2}{713}) = 1$ car $713 \equiv 1 \mod 8$. On calcule alors

$$(\frac{37}{713}) = (\frac{5}{37})(-1)^{\frac{712.36}{4}} = (\frac{5}{37})(+1) = (\frac{2}{5})(-1)^{\frac{4.36}{4}}$$

et $(\frac{2}{5}) = -1$ et finalement $(\frac{713}{1\,009}) = 1$ soit 713 est un carré modulo $1\,009$.

EXERCICES

Les solutions des exercices et problèmes sont données en fin d'ouvrage.

FACTORISATION DES POLYNÔMES

Exercice 6.1. Soient K un corps et $P \in K[X]$ un polynôme irréductible de degré d. Montrer que les conditions suivantes sont équivalentes :

(i) Le polynôme P est réductible sur K.

(ii) Le polynôme P possède une racine dans une extension L de K de degré inférieur ou égal à $\frac{d}{2}$.

Exercice 6.2. En utilisant le corollaire (6.34), déterminer tous les polynômes irréductibles de degré inférieur à 4 sur $\mathbf{F}_2$.

Exercice 6.3.

1. Soit p un nombre premier, $q_1 = p^{n_1},\ q = q_1^n$. Soient $P = X^q - X$, Q un diviseur de P de degré d irréductible sur le corps $\mathbf{F_{p^{q_1}}}$; montrer que d divise n (même démonstration que pour la remarque 6.22, 4.).
2. Déterminer tous les polynômes irréductibles de degré inférieur ou égal à 2 sur $\mathbf{F}_4$ (appliquer 1. et l'exercice 6.2).

Exercice 6.4. On considère le polynôme $Q(X) = X^9 - X + 1$ sur $\mathbf{F}_3$.

1. Montrer que le polynôme Q n'a pas de racines dans $\mathbf{F_3}, \mathbf{F_9}$.
2. Montrer que $\mathbf{F_{27}} \simeq \frac{\mathbf{F_3[X]}}{\mathbf{(X^3-X-1)}}$.
3. Montrer que toute racine $\alpha \in \mathbf{F_{27}}$ du polynôme $X^3 - X - 1$ est une racine du polynôme Q.
4. Déterminer toutes les racines de Q dans $\mathbf{F_{27}}$.
5. Factoriser le polynôme Q sur le corps $\mathbf{F_3}$.

Exercice 6.5. À quelle condition un polynôme P à coefficients dans $\mathbf{F}_p$ de degré d est-il irréductible sur $\mathbf{F}_{p^n}$? Dans le cas où P est irréductible sur $\mathbf{F}_p$, on donnera des précisions sur les degrés des facteurs irréductibles de P sur $\mathbf{F}_{p^n}$. En particulier pour $d = 5$, donner n minimal tel que tout polynôme de degré 5 à coefficients dans $\mathbf{F}_p$ soit totalement décomposé (resp. possède une racine) sur $\mathbf{F}_{p^n}$.

Exercice 6.6. Montrer que $X^4 + 1$ est irréductible sur $\mathbf{Z}$ et réductible modulo tout nombre premier p (on pourra utiliser que pour p premier impair le groupe $(\mathbf{F_{p^2}})^*$ est cyclique d'ordre $p^2 - 1$, montrer que le polynôme $X^4 + 1$ a une racine dans le corps $\mathbf{F_{p^2}}$ et appliquer l'exercice 6.1).

Exercice 6.7. Soit $P(X) = X^4 - 10X^3 + 21X^2 - 10X + 11$.

1. Décomposer P en facteurs irréductibles modulo 2,3.
2. Montrer que P est irréductible sur $\mathbf{Q}$.

CORPS FINIS

Exercice 6.8.

1. Quels sont les ordres (multiplicatifs) des éléments de $\mathbf{F_{23}^*}$?
2. Calculer 5^2 et 5^{11} modulo 23.
3. En déduire que la classe de 5 modulo 23 engendre le groupe $\mathbf{F_{23}^*}$

Exercice 6.9. Soit $P[X]$ un polynôme unitaire de degré n sur un corps K. On note $\sigma_1, \ldots, \sigma_n$ les fonctions symétriques élémentaires des racines α_i ($1 \leqslant i \leqslant n$) de P, et

$$N_k = \sum_{i=1}^{n} \alpha_i^k.$$

On rappelle que pour $1 \leqslant k \leqslant n$,

$$N_k = P_k(\sigma_1, \ldots, \sigma_k)$$

où P_k est un polynôme en k variables.

1. Calculer P_1, P_2, P_3.
2. Soit $\mathbf{F_q}$ le corps fini à q éléments avec $q = p^r$, p nombre premier. On pose

$$\psi(i) = \sum_{x \in \mathbf{F_q}} x^i$$

Montrer que

- $\psi(i) = -1 \bmod p$ si $q - 1 \mid i$
- $\psi(i) = 0$ sinon.

Exercice 6.10. Soit p un nombre premier, $q = p^n$, $\mathbf{F}_q$ le corps à q éléments. Soit $a \in \mathbf{F}_q^*$, q_a le polynôme minimal de a sur le corps $\mathbf{F}_p$.

1. Que peut-on dire du degré de q_a ?
2. Montrer que q_a est aussi le polynôme minimal de a^p.
3. On suppose que q_a est de degré n ; montrer que les racines de q_a sont alors :

$$a, a^p, a^{p^2}, \ldots, a^{p^{n-1}}.$$

Exercice 6.11. Montrer les isomorphismes suivants et donner un générateur du groupe des inversibles des corps en question :

1. $\mathbf{F_4} \simeq \mathbf{F_2}[X]/(X^2 + X + 1)$;
2. $\mathbf{F_8} \simeq \mathbf{F_2}[X]/(X^3 + X + 1)$;
3. $\mathbf{F_9} \simeq \mathbf{F_3}[X]/(X^2 + X - 1)$.

Exercice 6.12. Montrer l'existence d'une infinité de nombres premiers p tels que :

1. $p \equiv 1 \mod 8$ (on pensera à utiliser l'exercice 1.17) ;
2. $p \equiv 3 \mod 4$;
3. $p \equiv 5 \mod 6$;
4. $p \equiv 5 \mod 8$.

(La méthode est la même que pour le corollaire 6.45 : on suppose par l'absurde que l'ensemble en question est fini ; on aboutit alors à une contradiction en notant n le plus grand élément de cet ensemble et en considérant l'entier $N = 2(n!) - 1$ pour 1., $N = n! - 1$ pour 2. et $N = (2.3.5.7.11...n)^2 + 4$ pour 3. On utilisera de plus pour 3. l'exercice 1.19).

PROBLÈMES

Problème 6.1. *Irréductibilité modulo 5*

1. Le nombre 2 est-il un carré dans $\mathbf{F_5}$? Montrer que $X^2 + X + 1$ est irréductible sur $\mathbf{F_5}$.
2. Soit $P(X) \in \mathbf{F_5}[X]$ un polynôme unitaire irréductible de degré deux. Montrer que le quotient
$$\frac{\mathbf{F_5}[X]}{(P(X))}$$
est isomorphe au corps $\mathbf{F_{25}}$ et que P a deux racines dans $\mathbf{F_{25}}$.
3. On note α une racine de $X^2 + X + 1$ dans $\mathbf{F_{25}}$. Montrer que tout $\beta \in \mathbf{F_{25}}$ peut s'écrire $a\alpha + b$ avec a et b dans $\mathbf{F_5}$.
4. Soit $P = X^5 - X + 1$. Montrer que pour tout $\beta \in \mathbf{F_{25}}$, on a $P(\beta) \neq 0$. En déduire que P est irréductible sur $\mathbf{F_5}$. P est-il irréductible sur $\mathbf{Q}$?

Problème 6.2. *Un critère d'irréductibilité*

Soient p et l deux nombres premiers impairs. On suppose que p engendre $(\mathbf{Z}/l\mathbf{Z})^*$ et que $l \equiv 2 \mod 3$. On note $P(X) = X^{l+1} - X + p$. On veut montrer que P est irréductible sur $\mathbf{Z}$.

1. Montrer que P n'a pas de racine rationnelle.
2. On raisonne par l'absurde et on suppose $P = QR$ avec $Q, R \in \mathbf{Z}[X]$ unitaire et de degré au moins 2. Montrer que $\overline{P} = X(X-1)\overline{\Phi}_l$ est la décomposition en polynômes irréductibles de $\overline{P}$ sur $\mathbf{F}_p$ (avec $\Phi_l = 1 + X + \cdots + X^{l-1}$) ; en déduire alors que $\overline{Q} = \overline{\Phi}_l$ et $\overline{R} = X(X-1)$.
3. En passant modulo 2, en déduire une contradiction. Comme exemple on propose le polynôme $X^{72} - X + 47$.

Problème 6.3. *Une démonstration de la loi de réciprocité quadratique*

Soient p et q des nombres premiers impairs distincts. On considère un surcorps K de $\mathbf{Z}/p\mathbf{Z}$ contenant une racine primitive q-ième de l'unité que l'on note w, et on introduit $\tau := \sum_{x \in (\mathbf{Z}/q\mathbf{Z})^*} \left(\frac{x}{q}\right) w^x \in K$ (*cf.* la définition 6.47). On notera en particulier que la somme précédente a un sens car w^x ne dépend que de la classe de x modulo q.

1. En écrivant τ^2 sous la forme $\sum_{x,y\in(\mathbf{Z}/q\mathbf{Z})^*}\left(\frac{xy}{q}\right)w^{x+y}$ et en effectuant le changement de variable $y=xz$, montrer que $\tau^2=\left(\frac{-1}{q}\right)(q-1)+\sum_{\substack{z\in(\mathbf{Z}/q\mathbf{Z})^\times\\ z\neq -1}}-\left(\frac{z}{q}\right)$.
2. En notant que dans $(\mathbf{Z}/q\mathbf{Z})^*$, il y a autant de carrés que de non carrés ; en déduire que $\tau^2=\left(\frac{-1}{q}\right)q$.
3. En déduire que $\left(\frac{-1}{q}\right)q$ est un carré dans $\mathbf{Z}/p\mathbf{Z}$ si et seulement si $\tau^p=\tau$.
4. En utilisant le calcul de $\left(\frac{-1}{q}\right)=(-1)^{(q-1)/2}$ (*cf.* la proposition (6.43)), montrer alors la loi de réciprocité quadratique (théorème (6.52)), à savoir

$$\left(\frac{p}{q}\right)=(-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right)$$

Problème 6.4. *« Jeu du solitaire »*

Le jeu du solitaire se joue sur un plateau disposant de 33 réceptacles (cercles vides) dans lesquels il peut y avoir des billes notés avec un cercle plein. À chaque étape on peut faire passer une bille au-dessus d'une autre sur un axe vertical ou horizontal, pourvu que le réceptacle suivant soit vide, comme dans la figure 6.1 :

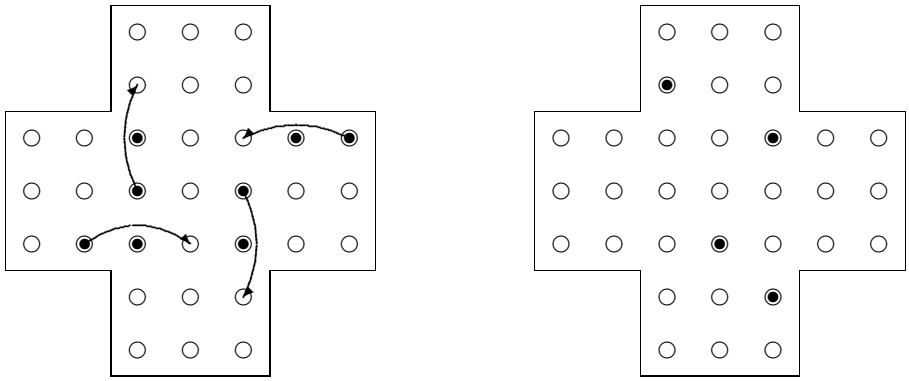


Figure 6.1

Soit alors O placé au centre du plateau et un repère (O,x,y) comme dans la figure 6.2 et pour une configuration $\mathcal{C}$ quelconque de billes sur le plateau on introduit :

$$\alpha_{\mathcal{C}}:=\sum_{(x,y)\in\mathcal{C}}j^{x+y}\in F_4\quad \beta_{\mathcal{C}}:=\sum_{(x,y)\in\mathcal{C}}j^{x-y}\in F_4$$

où j est un générateur de F_4^*.

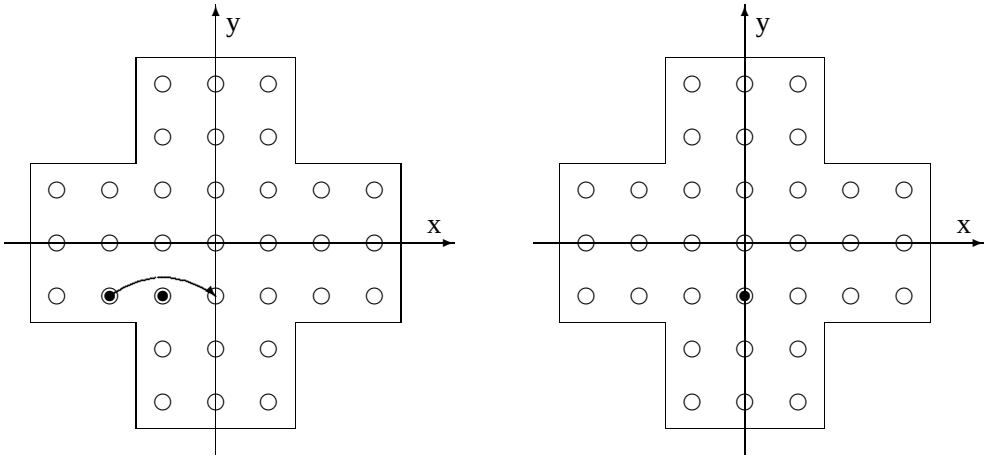


Figure 6.2

1. Montrer que (α, β) est un invariant du jeu.
2. Habituellement le jeu consiste à partir d'une configuration où l'on place des billes dans tous les réceptacles sauf un seul, disons (x_0, y_0), et à arriver à la configuration où tous les réceptacles sont vides sauf celui (x_0, y_0). Montrer qu'effectivement les deux configurations précédentes, possèdent les mêmes invariants (α, β).
3. Partant de la configuration de la figure 6.3, montrer qu'il est impossible d'arriver à une configuration où il n'y aurait qu'une seule bille sur le plateau.

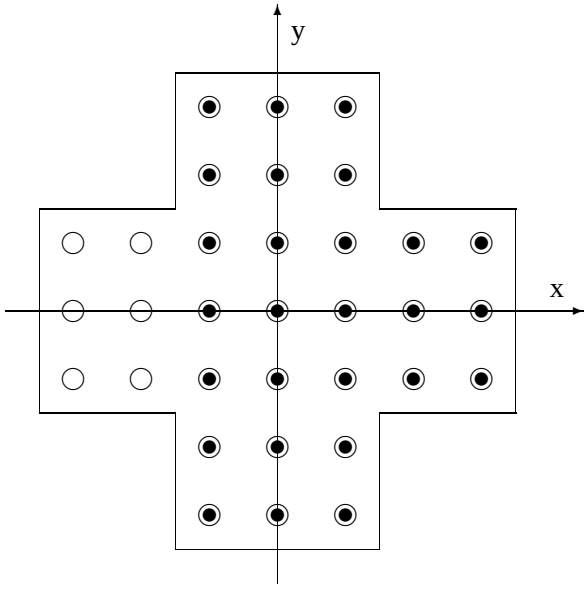


Figure 6.3

Solutions des exercices du chapitre 1

ANNEAUX

Exercice 1.1.

1. A^* est constitué des fonctions qui ne s'annulent jamais.

2. $V(G)$ est clairement un idéal de A ; il est fermé car si une suite (f_n) de fonctions converge simplement vers une fonction f et si pour un $x \in G$, $f_n(x) = 0$ pour tout n, on a aussi $f(x) = 0$.

3. Soit $a \in E$; montrons que $\mathfrak{m} = V(\{a\})$ est maximal ; soit $f \notin \mathfrak{m}$. On écrit alors $1 = \frac{f}{f(a)} + \frac{f - f(a)1}{f(a)}$ de sorte que 1 appartient à l'idéal engendré par f et $\mathfrak{m}$, ce qui entraîne que $\mathfrak{m}$ est maximal.

Réciproquement soit $\mathfrak{m}$ un idéal maximal de A ; $Z(\mathfrak{m}) = \{x \in E,\ \forall f \in \mathfrak{m},\ f(x) = 0\}$ est un fermé de E (intersection des fermés $f^{-1}(0)$ pour f parcourant $\mathfrak{m}$). Montrons que $Z(\mathfrak{m})$ est non vide ; dans le cas contraire, pour tout $x \in E$, il existerait une fonction continue $f_x \in \mathfrak{m}$ telle que $f_x(x) \neq 0$. Par continuité, il existerait un voisinage ouvert U_x de x sur lequel f_x ne s'annule pas ; les ouverts U_x recouvrent E et par compacité, on peut en extraire un recouvrement fini $U_{x_1}, \cdots, U_{x_r}$. Ainsi $f_{x_1}^2 + \cdots + f_{x_r}^2$ est un élément de $\mathfrak{m}$ qui ne s'annule pas, d'où $\mathfrak{m} = A$ ce qui n'est pas. Soit donc $x \in Z(\mathfrak{m})$; on a alors $\mathfrak{m} \subset V(\{x\})$ et par maximalité $\mathfrak{m} = V(\{x\})$, d'où le résultat.

4. On a clairement $V(G) = V(\overline{G})$, d'où $\overline{G} = \overline{H} \quad \Rightarrow \quad V(G) = V(H)$.

Réciproquement, supposons $\overline{G} \neq \overline{H}$. On peut supposer (quitte à échanger les rôles de G et H) qu'il existe un point $x \in \overline{G} \setminus \overline{H}$; d'après le théorème de Tietze-Urysohn il existe $f \in A$ tel que $f(x) = 1$ et $f_{|\overline{H}} = 0$; on a alors $f \in V(\overline{H})$ et $f \notin V(\overline{G})$.

L'ANNEAU $\mathbb{Z}$

Exercice 1.2.

On note $a_n = 2^n + 3^n$ et soit $\delta := a_n \wedge a_{n+1}$ le pgcd de a_n et a_{n+1}. On a alors $\delta = a_n \wedge (a_{n+1} - 2a_n) = a_n \wedge 3^n = (a_n - 3^n) \wedge 3^n = 2^n \wedge 3^n = 1$.

Exercice 1.3. On rappelle que les sous-groupes de $\mathbf{Z}$ sont de la forme $n\mathbf{Z}$; l'inclusion $48\mathbf{Z} \subset n\mathbf{Z}$ se traduit par n divise 48 soit $n = 1, 2, 3, 4, 6, 8, 12, 16, 18, 24, 48$ avec les inclusions :

$$\begin{array}{ccccccccc} (16) & \subset & (8) & \subset & (4) & \subset & (2) & \subset & (1) = \mathbf{Z} \\ \cup & & \cup & & \cup & & \cup & & \cup \\ (48) & \subset & (24) & \subset & (12) & \subset & (6) & \subset & (3) \end{array}$$

Exercice 1.4.

1. Tout nombre divisant ac et b est premier avec a par hypothèse et donc divise c par le lemme de Gauss. Les diviseurs communs à ac et b sont donc les mêmes que ceux communs à c et b.

2. On décompose a en facteurs premiers :

$$a = \prod_{p \in \mathcal{P}} p^{\nu_p(a)}$$

où $\mathcal{P}$ est l'ensemble des nombres premiers et où la famille $\nu_p(a)$ est nulle sauf pour un nombre fini de nombres premiers. On introduit de même les multiplicités $\nu_p(b)$ et $\nu_p(c)$. On a alors

$$(ab) \wedge c = \prod_{p \in \mathcal{P}} p^{\nu_p}$$

avec $\nu_p := \min(\nu_p(a) + \nu_p(b), \nu_p(c))$. L'hypothèse $a \wedge b = 1$ s'interprète par $\nu_p(a)\nu_p(b) = 0$, *i.e.* $\nu_p(a)$ et $\nu_p(b)$ ne sont jamais tous deux non nuls. On en déduit alors que $\nu_p = \min(\nu_p(a), \nu_p(c)) + \min(\nu_p(b), \nu_p(c))$ soit donc $(ab) \wedge c = (a \wedge b)(b \wedge c)$.

Dans le cas où l'on ne suppose plus $a \wedge b = 1$, la deuxième égalité est fausse comme le montre le cas $a = b = c = 2 : 4 \wedge 2 \neq (2 \wedge 2)(2 \wedge 2)$. En ce qui concerne la première égalité, on peut choisir $a = b = 2$ et $c = 3$ ce qui donne $6 \wedge 2 \neq 3 \wedge 2$.

Exercice 1.5.

1. D'après l'exercice précédent (1.4), on a $(a \wedge 6) = (a \wedge 2)(a \wedge 3)$ pour tout entier $a > 0$. On calcule alors $(n^2 + 2n - 2) \wedge 2 = n^2 \wedge 2 = n \wedge 2$. De même on a $n^2 + 2n - 2 \equiv 0 \mod 3$ si et seulement si $n \equiv 2 \mod 3$ (il suffit de tester $n = 0, 1, 2$ modulo 3). Ainsi le pgcd en question est égal ± 1 (resp. 2, resp. 3, resp. 6) si et seulement si $n \equiv 1 \mod 2$ et $n \not\equiv 2 \mod 3$ (resp. $n \equiv 0 \mod 2$ et $n \not\equiv 2 \mod 3$, resp. $n \equiv 1 \mod 2$ et $n \equiv 2 \mod 3$, resp. $n \equiv 0 \mod 2$ et $n \equiv 2 \mod 3$) soit $n \equiv 1, 3 \mod 5$ (resp. $n \equiv 0, 4 \mod 6$, resp. $n \equiv 5 \mod 6$, resp. $n \equiv 2 \mod 6$).

2. Le but est de faire des combinaisons pour faire descendre le degré en utilisant des égalités du genre $a \wedge b = (a-b) \wedge b$. Concrètement appelons $\delta(n)$ ce pgcd. On a $n^3+n^2+1 = (n^2+2n-1)(n-1)-(n+1)$ de sorte que $\delta(n) = (n^2+2n-1)\wedge(n+1)$. De même $n^2+2n-1 = (n+1)^2-2$ et donc $\delta(n) = (n+1) \wedge 2$ soit $\delta(n) = 2$ si $n \equiv 1 \mod 2$ et $\delta(n) = 1$ si $n \equiv 0 \mod 2$.

Exercice 1.6.

On suppose a et b positifs et on décompose a et b en facteurs premiers :

$$a = \prod_{p\in\mathcal{P}} p^{\nu_p(a)} \qquad b = \prod_{p\in\mathcal{P}} p^{\nu_p(b)}$$

où $\mathcal{P}$ est l'ensemble des nombres premiers > 0 et où les familles d'entiers $(\nu_p(a))_{p\in\mathcal{P}}$ et $(\nu_p(b))_{p\in\mathcal{P}}$ sont nulles sauf pour un ensemble fini de nombres premiers. Soit alors $u \in \mathbf{N}$ tel que $ab = u^k$. On écrit de même $u = \prod_{p\in\mathcal{P}} p^{\nu_p(u)}$ avec pour tout $p \in \mathcal{P}$

$$\nu_p(a) + \nu_p(b) = k\nu_p(u).$$

L'hypothèse a et b premiers entre eux signifie que pour tout $p \in \mathcal{P}$, $\nu_p(a)$ et $\nu_p(b)$ ne sont pas tous deux non nuls. On en déduit donc que pour tout $p \in \mathcal{P}$, $\nu_p(a)$ et $\nu_p(b)$ sont divisibles par k : $\nu_p(a) = ka_p$ et $\nu_p(b) = kb_p$ avec à nouveau a_p et b_p non tous deux non nuls. En posant $\alpha = \prod_{p\in\mathcal{P}} p^{a_p}$ et $\beta = \prod_{p\in\mathcal{P}} p^{b_p}$, on en déduit $a = \alpha^k$ et $b = \beta^k$.

Exercice 1.7.

1. On remarque tout d'abord que $650 = 2 \times 325$ et $66 = 2 \times 33$. On va appliquer l'algorithme d'Euclide à 325 et 33 puis on multipliera par deux.

$$\begin{aligned} 325 &= 33 \times 9 + 28 \\ 33 &= 28 + 5 \\ 28 &= 5 \times 5 + 3 \\ 5 &= 3 + 2 \\ 3 &= 2 + 1 \end{aligned}$$

On remonte alors les calculs :

$$\begin{aligned} 1 &= 3 - 2 \\ 1 &= 3 - (5-3) = 2 \times 3 - 5 \\ 1 &= 2 \times (28 - 5 \times 5) - 5 = 2 \times 28 - 11 \times 5 \\ 1 &= 2 \times 28 - 11 \times (33 - 28) = 13 \times 28 - 11 \times 33 \\ 1 &= 13 \times (325 - 9 \times 33) - 11 \times 33 = 13 \times 325 - 128 \times 33 \end{aligned}$$

Finalement la relation de Bézout est $2 = 13.650 - 128.66$; on rappelle que les autres sont données par :

$$2 = (13 + k \times 66)650 - (128 - k \times 650)66$$

pour $k \in \mathbf{Z}$ (*cf.* la remarque 1.11)

2. (i) L'ensemble des $n = ua + vb$ avec $(u, v) \in \mathbf{Z}^2$ est par définition le sous-groupe de $\mathbf{Z}$ engendré par a et b qui est alors égal à $(a \wedge b)\mathbf{Z}$, soit ici $\mathbf{Z}$, *i.e.* tout entier relatif $n \in \mathbf{Z}$ peut s'écrire sous la forme $ua + vb$ pourvu que u et v puissent prendre des signes quelconques.

(ii) Soit $(u, v) \in \mathbf{Z}^2$ tels que $n = ua + vn$. Par ailleurs toute autre écriture $n = u'a + v'b = ua + vb$ donne $(u - u')a = (v' - v)b$ soit, comme a et b sont premiers entre eux, $u - u' = tb$ et $v' - v = ta$ de sorte qu'il existe un unique couple (u_0, v_0) tel que $0 \leqslant u_0 < b$ (*cf.* la remarque 1.11).

(iii) En utilisant (ii), on écrit $n = ab - a - b - t$ avec $t = u_0a + v_0b < 0$ tel que $0 \leqslant u_0 < b$ et donc $v_0 < 0$, soit $n = (b-1-u_0)a+b(-v_0-1)b$ avec $b-1-u_0 \geqslant 0$ et $-v_0 - 1 \geqslant 0$.

(iv) Si $v_0 \geqslant 0$, le couple (u_0, v_0) convient. Réciproquement on écrit $m = u_0a + v_0b = ua + vb$ avec $0 \leqslant u_0 < b$ et $u, v \geqslant 0$. Il existe alors t tel que $u = u_0 + tb$ et $v = v_0 - ta$. On a ainsi $0 \leqslant u - tb < b$ et $u \geqslant 0$ de sorte que $t \geqslant 0$ et donc $v_0 = v + ta \geqslant 0$.

(v) L'égalité $m + n = ab - a - b$ donne $ab = a(u_0 + u'_0 + 1) + b(v_0 + v'_0 + 1)$: a et b étant premiers entre eux, le lemme de Gauss nous dit que b divise $u_0 + u'_0 + 1$. Or comme[1] $0 \leqslant u_0, u'_0 \leqslant b - 1$, on a $1 \leqslant u_0 + u'_0 + 1 \leqslant 2b - 1$ et le seul multiple de b dans cet intervalle est b lui-même, soit $u_0 + u'_0 + 1 = b$ et donc $v_0 + v'_0 + 1 = 0$.

Les nombres v_0 et v'_0 étant des entiers, exactement un parmi eux deux est positif ou nul, l'autre étant strictement négatif. Ainsi d'après (iv), parmi n et m exactement un peut s'écrire sous la forme $ua + vb$ avec u et v positifs ou nuls.

(vi) Posons $n = 0$ et $m = ab-a-b$ de sorte que d'après (v), parmi n et m exactement un des deux peut s'écrire sous la forme $ua+vb$ avec u et v positifs. Clairement il s'agit de $n = 0a + 0b$, d'où le résultat.*

(vii) Pour $0 \leqslant n \leqslant ab - a - b$, l'entier n' tel que $n + n' = ab - a - b$ est distinct de n. D'après (v), exactement un des deux nombres n ou n' appartient à l'ensemble considéré, d'où le résultat.

> ***Remarque :*** on peut par ailleurs retrouver (iii) en posant, pour $m > ab-a-b$, $n = ab - a - b - m < 0$ de sorte que d'après (v) exactement un parmi n et m peut s'écrire sous la forme $ua + vb$ avec u et v positifs. Clairement il ne peut pas s'agir de n car il est strictement négatif, de sorte qu'il s'agit de m.

3. Il s'agit d'appliquer la question 2.

(i) Toutes les sommes peuvent être payées en écrivant tout $n \in \mathbf{Z}$ sous la forme $ua+vb$ ce qui correspond, par exemple si $u > 0$ et $v < 0$, à donner u pièces de valeur a et le marchand nous rend v pièces de valeur b.

(ii) Il s'agit de 2.

1. On notera que pour un entier l'inégalité $u_0 < b$ est équivalente à $u_0 \leqslant b - 1$; cependant quand on désire additionner deux telles inégalités, pour ne pas perdre en précision, il vaut mieux utiliser l'inégalité stricte. Notez bien qu'ici la perte de précision aurait été préjudiciable.

(iii) On écrit $48x + 20y + 15z = 3(16x + 5z) + 20y$. D'après ce qui précède, tout nombre de la forme $60+t$ avec $t \geqslant 0$ peut s'écrire sous la forme $16x+5z$ avec $x \geqslant 0$, $y \geqslant 0$. De même tout nombre de la forme $38 + s$ avec $s \geqslant 0$, peut s'écrire sous la forme $3t + 20y$ avec $t \geqslant 0$, $y \geqslant 0$. Finalement toute somme supérieure ou égale à 218 est payable. Étudions le cas de 217 : $217 = 20y + 3u$, $217 \equiv -3 \mod 20$, on en déduit que $-3(u+1)$ doit être divisible par 20, soit $u = 20k-1$ et $220 = 20(y+3k)$ soit $11 = y + 3k$ ce qui donne $u = 19, 39, 59$ et on vérifie aisément qu'aucune de ses possibilités ne s'écrit sous la forme $16x + 5z$ avec x, z positifs.

4. Il s'agit encore d'appliquer 2. Ainsi tous les scores strictement supérieurs à $3 \times 7 - 3 - 7 = 11$ peuvent être atteints, 11 ne le pouvant pas. En ce qui concerne les scores entre 1 et 10, seuls $3, 6, 7, 9, 10$ peuvent être obtenus.

L'ANNEAU $\mathbb{Z}/N\mathbb{Z}$, CONGRUENCES

Exercice 1.8.

L'ordre (multiplicatif) de 2 dans $(\mathbf{Z}/7\mathbf{Z})^*$ est 3 comme on le constate immédiatement. Si n est pair, on a $2^n \equiv 1 \mod 3$ et donc $2^{2^n} \equiv 2 \mod 7$; si n est impair, $2^n \equiv 2 \mod 3$ et donc $2^{2^n} \equiv 4 \mod 7$. Le même raisonnement pour 4 (aussi d'ordre (multiplicatif) 3 dans $(\mathbf{Z}/7\mathbf{Z})^*$ donne $4^{2^n} \equiv 4 \mod 7$ si n est pair et $4^{2^n} \equiv 2 \mod 7$ si n est impair, d'où le résultat.

Exercice 1.9.

Lorsqu'il n'y a pas d'ambiguïté possible, on note de la même manière un nombre entier et sa classe modulo n.

On rappelle que les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ sont indexés par les diviseurs d de n ; concrètement l'application $d|n \mapsto (\frac{n}{d})$ qui à un diviseur d de n associe le sous-groupe de $\mathbf{Z}/n\mathbf{Z}$ engendré par $\frac{n}{d}$ est une bijection (proposition 1.35. Pour $n = 24$, les sous-groupes sont ceux engendrés par les classes de $1, 2, 3, 4, 6, 8, 12, 0$ avec les relations d'inclusion :

$$\begin{array}{ccccccc} (8) & \subset & (4) & \subset & (2) & \subset & (1) \\ \cup & & \cup & & \cup & & \cup \\ (0) & \subset & (12) & \subset & (6) & \subset & (3) \end{array}$$

En outre on rappelle que le groupe engendré par k dans $\mathbf{Z}/n\mathbf{Z}$ est le même que celui engendré par $k \wedge n$ (remarque 1.37). On a ainsi $(16) = (8)$ et $(18) = (6)$.

Exercice 1.10.

D'après le lemme chinois, il suffit de donner la congruence de $a = 2\,005^{2\,005}$ modulo 2 et 7. On a d'abord de manière immédiate $a \equiv 1 \mod 2$. D'autre part, on a $2\,005 \equiv 0 \mod 7$ et donc $a \equiv 0 \mod 7$. On en déduit alors que $a \equiv 7 \mod 14$, par exemple parce que $a = 7\alpha$ avec α impair.

Exercice 1.11.

Comme précédemment on cherche la congruence de $a = 10^{100}$ modulo 13 et 19. On a $10 \equiv -3 \mod 13$ et d'après le petit théorème de Fermat (proposition 1.46)) on a $(-3)^{12} \equiv 1 \mod 13$. Comme $100 \equiv 4 \mod 12$, on obtient $a \equiv (-3)^4 \mod 13$ soit $a \equiv 3 \mod 13$.

De la même façon, on a $10 \equiv -9 \mod 19$ avec $(-9)^{18} \equiv 1 \mod 19$. Comme $100 \equiv 10 \mod 18$, on obtient $a \equiv (-9)^{10} \mod 19$. Or on a $9^2 \equiv 5 \mod 19$, $9^4 \equiv 5^2 \equiv 6 \mod 19$ et $9^8 \equiv 6^2 \equiv -2 \mod 19$ et donc $9^{10} = 9^2 9^8 \equiv -10 \mod 19$.

On a alors $a \equiv -10 \mod 13$ et $a \equiv -10 \mod 19$ soit $a \equiv -10 \mod 247$. De manière générale on rappelle que pour trouver la congruence de a modulo 247 , on cherche une relation de Bézout. Pour cela on effectue l'algorithme d'Euclide, soit $19 - 13 = 6$ et $13 - 2.6 = 1$ ce qui donne $1 = 13 - 2(19 - 13) = 3 \times 13 - 2 \times 19$. On a alors $a \equiv 9 \times 3 \times 13 - 3 \times 2 \times 19 \mod 247$ soit $a \equiv 237 \mod 247 \equiv -10 \mod 247$ (*cf.* l'exemple 1.52).

Exercice 1.12. On a $1\,035\,125 \equiv 12 \mod 17$. D'après le petit théorème de Fermat on a $12^{16} \equiv 1 \mod 17$. Or $5\,642 \equiv 10 \mod 16$ de sorte que $1\,035\,125^{5\,642} \equiv 12^{10} \mod 17$. Or $12 \equiv -5 \mod 17$ et $12^2 \equiv 8 \mod 17$ soit $12^4 \equiv -4$ soit $12^8 \equiv -1$ de sorte que l'ordre de $12^{10} = 12^2 12^8 = -12^2 = -8 = 9 \mod 17$.

Exercice 1.13.

On a $1\,823 \equiv 5 \mod 18$; or $5 \in (\mathbf{Z}/18\mathbf{Z})^*$; on peut donc utiliser le petit théorème de Fermat avec $\varphi(18) = \varphi(2)\varphi(9) = 1.6 = 6$ soit $5^6 \equiv 1 \mod 18$. Or on a $242 \equiv 2 \mod 6$ soit $1\,823^{242} \equiv 5^2 \equiv 7 \mod 18$.

De même $2\,222 \equiv 2 \mod 20$ avec $2 \notin (\mathbf{Z}/20\mathbf{Z})^*$; on ne peut donc pas utiliser le petit théorème de Fermat (2^8 est pair et ne peut donc pas être congru à 1 modulo 20). On utilise l'isomorphisme du lemme chinois : on a $2\,222 \equiv 2 \mod 4$ de sorte que $2\,222^n \equiv 0 \mod 4$ dès que $n \geqslant 2$. On a aussi $2\,222 \equiv 2 \mod 5$ et $321 \equiv 1 \mod 4$ et donc d'après le petit théorème de Fermat $2\,222^{321} \equiv 2 \mod 5$ d'où $2\,222^{321} \equiv 5 \times 0 - 4 \times 2 \equiv 12 \mod 20$.

Exercice 1.14.

On a $42 = 2 \times 3 \times 7$, il suffit alors de vérifier la congruence modulo 2, 3 et 7 (corollaire 1.50). Pour 2 et 3, on a clairement $n^7 \equiv n$ et pour 7 le résultat découle du petit théorème de Fermat.

Exercice 1.15. On rappelle que 700 n'étant pas premier, 429 est inversible dans $\mathbf{Z}/700\mathbf{Z}$ si et seulement s'il est premier avec 700 et son inverse est donné par la

relation de Bézout, *i.e.* si $1 = 700a + 429b$ alors l'inverse cherché est la classe de b. Il suffit donc d'appliquer l'algorithme d'Euclide :

$$\begin{aligned} 700 &= 429 + 271 \\ 429 &= 271 + 158 \\ 271 &= 158 + 113 \\ 158 &= 113 + 45 \\ 113 &= 2 \times 45 + 23 \\ 45 &= 23 + 22 \\ 23 &= 22 + 1 \end{aligned}$$

On remonte alors les calculs et on obtient la relation de Bézout : $1 = 19 \times 700 - 31 \times 429$ de sorte que l'inverse de 429 dans $\mathbf{Z}/700\mathbf{Z}$ est $\overline{-31} = \overline{669}$.

Exercice 1.16.

(i) 3 étant premier avec 7, il est inversible dans $\mathbf{Z}/7\mathbf{Z}$; on calcule rapidement que $3 \times 5 \equiv 1 \mod 7$, *i.e.* $5 = 1/3$ dans $\mathbf{Z}/7\mathbf{Z}$ de sorte que l'équation s'écrit $x \equiv 20 \mod 7$ soit $x \equiv 6 \mod 7$;

(ii) d'après le corollaire 1.50 il suffit de vérifier l'équation modulo 3 et 7. L'équation s'écrit $0.x \equiv 0 \mod 3$ et est donc toujours vérifiée. D'autre part l'équation s'écrit $2x \equiv -2 \mod 7$; l'inverse de 2 dans $\mathbf{Z}/7\mathbf{Z}$ est -3, soit donc $x \equiv 6 \mod 7$. Le résultat final est donc $x \equiv 6 \mod 7$;

(iii) on a $676 = 2^2 \times 13^2$; par le théorème chinois (*cf.* le corollaire 1.50) on est donc ramené à résoudre $-x \equiv 0 \mod 4$ et $103x \equiv 105 \mod 169$. L'algorithme d'Euclide fournit $64 \times 103 - 39 \times 169 = 1$ soit donc $x \equiv 64 \times 105 \mod 169$ soit $x \equiv -40 \mod 169$ et donc $x \equiv -40 \mod 676$.

Exercice 1.17.

Dans le corps $\mathbf{Z}/p\mathbf{Z}$, on a $\overline{a}^2 + \overline{b}^2 = 0$. On a aussi $\overline{b} \neq 0$ par hypothèse. Posons $x = \overline{a}^2/\overline{b}^2$. On a alors $x^2 = -1$. par suite, 4 est l'ordre de x dans le groupe $(\mathbf{Z}/p\mathbf{Z})^*$. D'après le petit théorème de Fermat, on a $x^{p-1} = 1$ et donc 4 divise $p - 1$.

Exercice 1.18.

1. On commence par regarder la congruence de a^4 modulo 16. On remarque tout d'abord que si a est pair, celle-ci est nulle. Si a est impair, sa classe modulo $16 = 2^4$ appartient à $(\mathbf{Z}/16\mathbf{Z})^*$ qui est de cardinal $\varphi(2^4) = 4$ de sorte que $a^4 \equiv 1 \mod 16$. On en déduit alors que si a et b sont premiers entre eux et donc ne sont pas tous deux pairs, $a^4 + b^4 \equiv 1, 2 \mod 16$.

2. Si p divisait a, il diviserait $b^4 = n - a^4$ et donc diviserait b ce qui n'est pas car a et b sont premiers entre eux. On en déduit donc que les classes de a et b dans $\mathbf{Z}/p\mathbf{Z}$ en sont des éléments inversibles.

3. $\mathbf{Z}/p\mathbf{Z}$ étant un corps, on déduit de la relation $n = a^4 + b^4$ que $(\frac{\overline{a}}{\overline{b}})^4 = -1$ dans $\mathbf{Z}/p\mathbf{Z}$. On en déduit donc que $\frac{\overline{a}}{\overline{b}}$ est d'ordre 8 puisque $(\frac{\overline{a}}{\overline{b}})^8 = 1$ et $(\frac{\overline{a}}{\overline{b}})^4 \neq 1$.

4. Le groupe $(\mathbf{Z}/p\mathbf{Z})^*$ est d'ordre $p-1$ et contient un élément d'ordre 8 de sorte que, d'après le théorème de Lagrange, 8 divise $p-1$, soit $p \equiv 1 \mod 8$.

Exercice 1.19.

Si p est premier, le résultat découle du fait que p divise le coefficient binomial $\binom{p}{i}$, pour $0 < i < p$. En effet on a $p\binom{p-1}{i-1} = i\binom{p}{i}$ de sorte que p divise $i\binom{p}{i}$ et comme $p \wedge i = 1$, p divise $\binom{p}{i}$.

Réciproquement supposons p non premier ; soit alors q un facteur premier de $p = q^k m$ avec $q \wedge m = 1$ et $k \geqslant 1$. On a alors $\binom{p}{q} = q^{k-1}\tilde{m}$ avec $q \wedge \tilde{m} = 1$ et donc q^k ne divise pas $\binom{p}{q}$, de sorte que le coefficient de X^q de $(X-a)^p$, qui est égal à $\binom{p}{q}a^{p-q}$ est non nul modulo p.

Exercice 1.20.

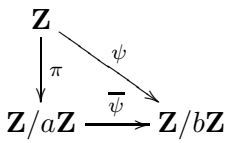
1. Il résulte du lemme chinois (corollaire 1.50) que l'on a $(\mathbf{Z}/pq\mathbf{Z})^* \simeq (\mathbf{Z}/p\mathbf{Z})^* \times (\mathbf{Z}/q\mathbf{Z})^*$ de sorte que ce dernier est de cardinal $(p-1)(q-1)$. Les éléments x égaux à leur inverse sont ceux qui vérifient $x^2 = 1$, *i.e.* ceux d'ordre divisant 2, ce qui donne 4 éléments, à savoir $(\pm 1, \pm 1)$ c'est-à-dire les classes dans $\mathbf{Z}/pq\mathbf{Z}$ de $1, -1, x_1, x_2$ avec $x_i \equiv (-1)^i \mod p$ et $x_i \equiv (-1)^{i-1} \mod q$, pour $i = 1, 2$.

2. On considère alors le produit de tous les éléments de $(\mathbf{Z}/pq\mathbf{Z})^*$ *i.e.* le produit des $pq-1$ premiers entiers auxquels il faut enlever tous les multiples de p ainsi que tous les multiples de q. Les multiples de p (resp. q) sont $p, 2p, \cdots, (q-1)p$ (resp. $q, 2q, \cdots, (p-1)q$), de sorte que le produit en question vaut $\frac{(pq-1)!}{(q-1)!p^{q-1}(p-1)!q^{p-1}}$ (modulo pq). Par ailleurs en regroupant les classes distinctes de $1, -1, x_1, x_2$ avec leur inverse ce produit est égal à $a = 1(-1)x_1x_2 = -x_1x_2$. On a donc $a \equiv 1 \mod p$ et $a \equiv 1 \mod q$ de sorte que $a \equiv 1 \mod pq$ (lemme chinois), d'où le résultat.

MORPHISMES

Exercice 1.21.

1. On a $\phi(k) = k\phi(1)$ de sorte que ϕ est déterminé par $\phi(1)$. En outre on doit avoir $\phi(a.1) = \phi(0) = 0 = a\phi(1)$ et donc l'ordre de $\phi(1)$ divise a.
Réciproquement, si l'ordre de $x \in \mathbf{Z}/b\mathbf{Z}$ divise a, le morphisme $\psi : \mathbf{Z} \to \mathbf{Z}/b\mathbf{Z}$ tel que $\psi(1) = x$ se factorise par le morphisme canonique $\pi : \mathbf{Z} \to \mathbf{Z}/a\mathbf{Z}$ (proposition 1.19) pour donner un diagramme commutatif :



On pose alors $\phi = \overline{\psi}$.

2. Si a et b sont premiers entre eux, soit $\phi : \mathbf{Z}/a\mathbf{Z} \to \mathbf{Z}/b\mathbf{Z}$ un morphisme de groupes. L'élément $\phi(1)$ est d'ordre divisant a et b, donc $\phi(1)$ est d'ordre 1 *i.e.* $\phi(1) = 0$ et donc ϕ est le morphisme nul. Pour la réciproque, on raisonne par contraposée. Supposons que a et b ne soient pas premiers entre eux et soit ψ le morphisme de $\mathbf{Z}$ dans $\mathbf{Z}/b\mathbf{Z}$ tel que $\psi(1) = b/a \wedge b \bmod b$ et donc $\psi(1) \neq 0 \bmod b$. On a alors $\psi(a) = 0$ (car $\frac{ab}{a\wedge b}$ est divisible par b) et le morphisme ψ se factorise par un morphisme non nul $\phi : \mathbf{Z}/a\mathbf{Z} \to \mathbf{Z}/b\mathbf{Z}$.

Exercice 1.22.

Dans le premier cas comme 3 et 4 sont premiers entre eux, les seuls éléments d'ordre divisant 3 dans $\mathbf{Z}/4\mathbf{Z}$ sont le seul d'ordre 1 à savoir 0 de sorte que tout morphisme $\mathbf{Z}/3\mathbf{Z} \to \mathbf{Z}/4\mathbf{Z}$ est nul.

Dans $\mathbf{Z}/15\mathbf{Z}$ les éléments d'ordre divisant 12 sont d'ordre divisant $12 \wedge 15 = 3$ et sont donc $0, 5, 10$, ce qui donne 3 morphismes distincts (dont le morphisme nul).

Exercice 1.23.

1. D'après l'exercice 1.21, la condition nécessaire et suffisante est que p divise n.

2. D'après l'exercice 1.21, il faut et il suffit que x soit d'ordre divisant p^a. Comme $p^b x = 0$ pour $a \geqslant b$, tout élément x convient, tandis que pour $a \leqslant b$, il faut et il suffit que x soit divisible par p^{b-a}.

3. Le nombre de morphismes distincts est donc, d'après ce qui précède, égal au nombre d'éléments d'ordre divisant p^a dans $\mathbf{Z}/p^b\mathbf{Z}$ qui est donc égal à p^a si $a \leqslant b$ (et à p^b si $a \geqslant b$).

Exercice 1.24.

On note $n \vee m$ le PPCM de n et m. On a évidemment $n \vee m \subset \ker \pi$. Réciproquement, soit $k \in \ker \pi$: k est alors divisible par n et m donc par $n \vee m$ (par définition du PPCM). On a donc $\ker \pi = (n \vee m)$. Soient maintenant a, b tels que $b - a$ soit divisible par $n \wedge m$. On écrit une relation de Bézout $un + vm = n \wedge m$ et on pose $k = u\frac{n}{(n\wedge m)}b + v\frac{m}{(n\wedge m)}a$. On a alors $k = un\frac{(b-a)}{n\wedge m} + a \equiv a \bmod n$; de même on a $k = vm\frac{(a-b)}{n\wedge m} + b \equiv b \bmod m$, de sorte que (a, b) est dans l'image de π. Pour la réciproque, si $(\overline{a}, \overline{b}) = \pi(k)$, on a $k = a + \lambda n = b + \mu m$ soit $(b - a) = \lambda n - \mu m$ qui est donc divisible par $n \wedge m$. En particulier lorsque n et m sont premiers entre eux, π induit un isomorphisme $\mathbf{Z}/nm\mathbf{Z} \simeq \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ et on retrouve le lemme chinois.

Si $k \equiv 3 \bmod 6$, on applique ce qui précède avec $n = 6, m = 10$. On a alors $k \equiv a \bmod 10$ avec $a - 3$ divisible par $2 = 6 \wedge 10$, soit $a = 1, 3, 5, 7, 9$.

PROBLÈMES

Problème 1.1.

1. Si q divise $a^m - 1$, on a $a^m \equiv 1 \mod q$, d'où $a^{mp^{r-1}} \equiv 1 \mod q$ et donc q divise $a^{\frac{n-1}{p}} - 1$ et n ce qui contredit l'hypothèse.

2. On a $a^{n-1} \equiv 1 \mod n$ par hypothèse, donc *a fortiori* $a^{n-1} \equiv 1 \bmod q$, soit $(a^m)^{p^r} \equiv 1 \bmod q$. On en déduit que la classe b de a^m est inversible dans $\mathbf{Z}/q\mathbf{Z}$ et que son ordre (multiplicatif) divise p^r. Ce dernier est donc de la forme p^k avec $0 \leqslant k \leqslant r$. Si on avait $k < r$, on aurait aussi $b^{p^{r-1}} = 1$ dans $\mathbf{Z}/q\mathbf{Z}$ ce qui impliquerait que q divise $a^{\frac{n-1}{p}} - 1$ ce qui n'est pas. Ainsi b est d'ordre p^r.

3. Le groupe $(\mathbf{Z}/q\mathbf{Z})^*$ qui est d'ordre $q-1$ contient un élément d'ordre p^r ce qui impose, d'après le théorème de Lagrange, que p^r divise $q-1$ soit $q \equiv 1 \mod p^r$.

4. Soit q premier divisant n. Pour p premier divisant u, on écrit u (resp. v) sous la forme $p^r m$ (resp. $p^s m'$) avec p ne divisant pas m (resp. m'). D'après ce qui précède, $q \equiv 1 \mod p^{r+s}$ et donc $q \equiv 1 \mod p^r$. La propriété étant vérifiée pour tout diviseur premier p de u, on en déduit par application du lemme chinois que $q \equiv 1 \bmod u$.

5. Les facteurs premiers de n sont tous de la forme $1 + \alpha u$. Si n n'était pas premier, il possèderait au moins deux facteurs de la forme précédente et serait donc supérieur ou égal à $(1+u)^2 > 1 + u + 2u = 1 + uv$ d'où la contradiction et donc n est premier.

Problème 1.2.

1. (i) $\Longrightarrow$ (ii) Supposons $n = p_1 . \cdots . p_s$ les p_i étant distincts deux à deux. Le lemme chinois donne alors $\mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}/p_1\mathbf{Z} \times \cdots \times \mathbf{Z}/p_s\mathbf{Z}$ et la congruence $a^n \equiv a \mod n$ est équivalente à $a^n \equiv a \mod p_i$ pour tout i (corollaire 1.50). Pour i fixé, si p_i divise a le résultat est clair, sinon la congruence est équivalente à $a^{n-1} \equiv 1 \mod p_i$ (lemme de Gauss). Le petit théorème de Fermat donne alors $a^{p_i - 1} \equiv 1 \mod p_i$ soit $a^{n-1} \equiv 1 \mod p_i$ puisque $p_i - 1$ divise $n-1$ par hypothèse.

(ii) $\Longrightarrow$ (iii) Si a et n sont premiers entre eux l'implication est évidente car a est inversible dans $\mathbf{Z}/n\mathbf{Z}$.

(iii) $\Longrightarrow$ (i) Commençons par montrer que n est sans facteur carré ; supposons par l'absurde que $n = p^r q$ avec $r > 1$, p premier et q non divisible par p. Pour a non divisible par p, on a $a^{n-1} \equiv 1 \mod p^r$ par hypothèse. On choisit alors un élément a de $(\mathbf{Z}/p^r\mathbf{Z})^*$ d'ordre p (c'est possible car $r > 1$). On en déduit que p divise $p^r q - 1$ ce qui n'est pas. Montrons ensuite la deuxième propriété ; soit p premier divisant n et soit a tel que sa classe modulo p engendre $(\mathbf{Z}/p\mathbf{Z})^*$. La congruence $a^n \equiv a \mod n$ implique $a^n \equiv a \mod p$ soit $a^{n-1} \equiv 1 \mod p$ et donc $p-1$ divise $n-1$ car $p-1$ est l'ordre de a.

2. L'implication $(i) \Rightarrow (ii)$ se prouve exactement comme dans 1., en utilisant que dans $\mathbf{Z}/p\mathbf{Z}$, $x^{p-1} = 1$ de sorte que si $p-1$ divise $(n-1)/2$ alors $x^{(n-1)/2} = 1$.

Pour la réciproque, on raisonne comme dans 1. Supposons que $n = p^r q$ avec $r \geqslant 2$ et soit a un élément de $(\mathbf{Z}/p^r\mathbf{Z})^*$ d'ordre p. L'égalité $a^{(n-1)/2} \equiv 1 \mod p^r$, implique alors que $2p$ divise $p^r q - 1$ ce qui n'est pas. Ainsi n est sans facteur carré. Soit alors p divisant n et a un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$; l'égalité $a^{(n-1)/2} \equiv 1 \mod p$ implique alors que $p-1$ divise $(n-1)/2$, d'où le résultat.

3. Si $p = 6m+1$ (resp. $p = 12m+1$, resp. $p = 18m+1$), $n \equiv 1 \mod 6m$ (resp. $n \equiv (1+6m)^2 \equiv 1 \mod 12m$, resp. $n \equiv (1+12m)(1-12m) \equiv 1 \mod 18m$).

Par ailleurs $p-1$ divise $\frac{n-1}{2}$ si et seulement si $2(p-1)$ divise $n-1$. Ainsi pour m impair, si $n-1$ est divisible par 8, étant divisible par $12m$ et $18m$ d'après ce qui précéde, on en déduit qu'il sera divisible par $8 \vee (12m) = 24m$ et par $(18m) \vee 8 = 36m$ ($a \vee b$ désigne le PPCM des nombres a et b). Or on a $n \equiv (1-2m)(4m+1)(1+2m) \equiv (1-4m^2)(1+4m) \equiv (1-4m)(1+4m) \equiv 1 \mod 8$, d'où le résultat.

Problème 1.3.

1. Pour $n > 0$, on a la factorisation :

$$X^{2n+1} + 1 = (X+1)(X^{2n} - X^{2n-1} + \cdots + 1)$$

car -1 est racine de ce polynôme. On écrit m sous la forme $2^n k$ avec k impair. Si $k > 1$, on en déduit l'égalité :

$$2^m + 1 = (2^{2^n})^k + 1 = (2^{2^n} + 1)((2^{2^n})^{k-1} - \cdots + 1).$$

On obtient alors que $2^{2^n}+1$ est un diviseur propre de m, d'où la contradiction, et donc $k = 1$ et m est une puissance de 2.

2. On trouve $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65\,537$ et l'on vérifie aisément qu'ils sont tous premiers.

3. Soit p premier divisant F_5, on a alors $2^{2^5} = -1$ dans $\mathbf{Z}/p\mathbf{Z}$ et 2 est d'ordre (multiplicatif) 2^6 dans $(\mathbf{Z}/p\mathbf{Z})^*$. D'après le petit théorème de Fermat, on a $2^{p-1} \equiv 1 \mod p$ et donc $2^6 = 64$ divise $p-1$, d'où le résultat.

4. On vérifie que 641 est premier. Dans le corps $\mathbf{Z}/641\mathbf{Z}$, on a $0 = 641 = 1 + 5.2^7$ soit $2^7 = -1/5$. Ainsi $F_5 = 2^{32} + 1 = (2^7)^4.2^4 + 1$ car $32 = 7.4 + 4$. D'où dans $\mathbf{Z}/641\mathbf{Z}$, $F_5 = (-1/5)^4.2^4 + 1 = (2^4 + 5^4)/5^4 = 0$.

5. Supposons $n = m + r$ avec $r > 0$. On a $2^{2^n} = (2^{2^m})^{2^r}$ et dans $\mathbf{Z}/F_m\mathbf{Z}$, on a alors $F_n \equiv (-1)^{2^r} + 1 \mod F_m$. Ainsi le pgcd de F_m et de F_n divise 2 ; or 2 ne divise pas F_n d'où le résultat.

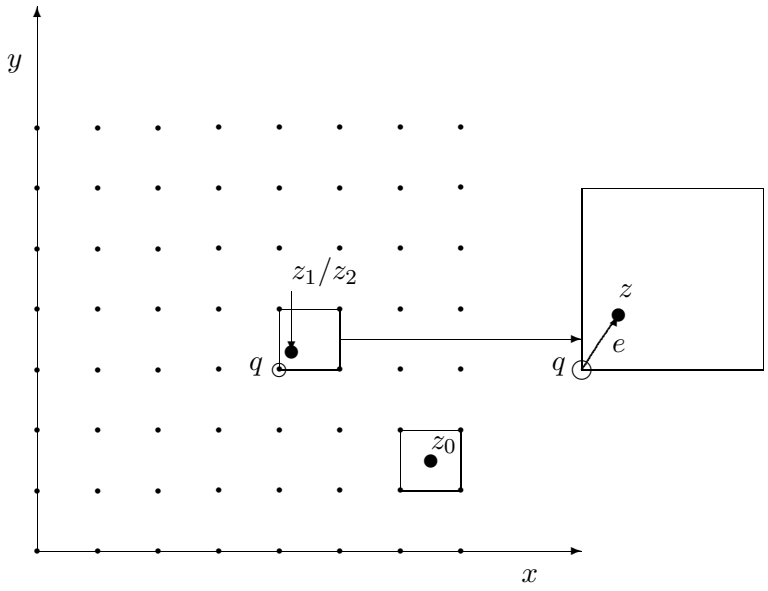
L'ensemble $\mathcal{P}$ des nombres premiers positifs contient la réunion disjointe $\coprod_n \mathfrak{F}_n$ où $\mathfrak{F}_n$ est le sous-ensemble de $\mathcal{P}$ des diviseurs premiers divisant F_n ; $\mathfrak{F}_n$ étant non vide pour tout n car $F_n > 1$, on en déduit que $\mathcal{P}$ est infini.

Problème 1.4.

1. La multiplicativité de N découle de la multiplicativité bien connue de la norme complexe (N est le carré de la norme complexe).

Si $z \in A^*$, on a $zz' = 1$ et donc $N(zz') = N(z)N(z') = 1$ soit $N(z) = 1$. En écrivant $z = a + ib$, $N(z) = 1$ donne $a^2 + b^2 = 1$ soit $(a, b) = (\pm 1, 0)$ ou $(0, \pm 1)$ soit $z = \pm 1, \pm i$. L'égalité $N((a + ib)(c + id)) = N(a + ib)N(c + id)$ donne alors l'identité remarquable de Lagrange.

2. Soit z_1 et z_2 des éléments de A ; on écrit $z = z_1/z_2 = q + e$ avec $q \in A$ et $e \in \mathbf{C}$ de module strictement plus petit que 1. On a alors $z_1 = qz_2 + r$ avec $r = z_2 e = z_1 - qz_2 \in A$ et $N(r) < N(z_2)$.



Par ailleurs on remarque qu'en général le choix de q n'est pas unique ; par exemple pour le point z_0 au centre d'un carré, les quatres sommets du carré conviennent pour q.

3. Le fait que S est stable par multiplications découle directement de l'identité de Lagrange.

4. On rappelle que p est irréductible si et seulement si $A/(p)$ est intègre ; or $A/(p) \simeq \mathbf{Z}/p\mathbf{Z}[X]/(X^2 + 1)$ qui est intègre si et seulement si $X^2 + 1$ n'a pas de racines dans $\mathbf{Z}/p\mathbf{Z}$, soit si et seulement si (-1) n'est pas un carré modulo p et donc si et seulement si $p \equiv 3 \mod 4$ (cela est démontré au chapitre 6 : corollaire 6.44).

En outre $n \in S$ si et seulement s'il existe $z \in A$ tel que $n = N(z)$ de sorte que si $p \in S$, on a $p = z\overline{z}$ avec $N(z) = p$ et donc z et $\overline{z}$ ne sont pas inversibles et donc p est réductible. Réciproquement si p est réductible, on a $p = zz'$ avec z et z' non inversibles, soit $p^2 = N(z)N(z')$ avec $N(z)$ et $N(z')$ distincts de 1 ce qui impose $N(z) = N(z') = p$ et $p \in S$.

5. Si p premier est congru à 3 modulo 4 alors p est irréductible dans A d'après (iv). De même si $N(z)$ est premier, z est irréductible car $z = xy$ implique $N(x)N(y)$ premier et donc $N(x)$ ou $N(y)$ est égal à 1, *i.e.* x ou y est inversible.

Montrons qu'aux inversibles près, ce sont les seuls ; soit z irréductible et p premier divisant $N(z)$. Si $p \equiv 3 \mod 4$, alors p est irréductible et $p|z\overline{z}$, donc $p|z$ ou $p|\overline{z}$. On remarque alors que p divise à la fois z et $\overline{z}$ (car $p = \overline{p}$) de sorte que z étant irréductible, on a $z = \epsilon p$ avec ϵ inversible.

Si $p = 2$ ou $p \equiv 1 \mod 4$, on a $p = a^2+b^2$ par (iv) de sorte que $a+ib$ est irréductible et divise p et donc divise z de sorte que $z = \epsilon(a+ib)$ avec ϵ inversible, d'où le résultat.

6. Soit $n \geqslant 2$ et supposons que pour tout $p \equiv 3 \mod 4$, $v_p(n)$ est pair. Pour montrer que $n \in S$, il suffit de montrer que pour tout p, $p^{v_p(n)} \in S$. Le résultat est clair pour $p \equiv 3 \mod 4$ car $v_p(n)$ est pair ; pour $p = 2$ et $p \equiv 1 \mod 4$, on a $p \in S$ et donc $p^{v_p(n)} \in S$.

Réciproquement, raisonnons par récurrence sur $n \geqslant 2$: le cas $n = 2$ est trivial et pour $n \geqslant 3$, $n = a^2+b^2$, si $p \equiv 3 \mod 4$ premier, divise n, alors p divise $(a+ib)(a-ib)$; or p est irréductible dans A de sorte que p divise $a + ib$ et $a - ib$, et donc p divise a et b ; ainsi $n = p^2((a/p)^2 + (b/p)^2)$ et $n/p^2 \in S$. Par hypothèse de récurrence $v_p(n/p^2)$ est pair et donc $v_p(n)$ aussi.

Problème 1.5.

1. L'application N est bien sur multiplicative, *i.e.* $N(zz') = N(z)N(z')$, à valeurs dans $\mathbf{N}$. Si z est inversible, on en déduit qu'il existe z' tel que $zz' = 1$ soit $N(z)N(z') = 1$ ce qui impose $N(z) = 1$, c-à-d. si $z = a + b\sqrt{5}$, $a^2 + 5b^2 = 1$, d'où $a = \pm 1$, $b = 0$. Réciproquement si on a $N(z) = z\overline{z} = 1$ alors $\overline{z}$ est l'inverse de z.

Soit alors z tel que $N(z)$ soit premier ; soit $z_1 z_2 = z$ avec z_1 non inversible, il s'agit alors de montrer que z_2 l'est. On a donc $N(z) = N(z_1)N(z_2)$ et donc $N(z_2) = 1$ et $z_2 \in A^*$.

2. On va montrer que si z est tel que $N(z) = 9$ alors z est irréductible de sorte que 3, $2 \pm i\sqrt{5}$ sont tous irréductibles, et l'égalité $3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ correspond à deux factorisations distinctes en produit d'irréductibles. Soit donc $z \in \mathbf{Z}[i\sqrt{5}]$ tel que $N(z) = 9$; on écrit $z = z_1 z_2$ avec $N(z_1) \neq 1$. On a donc $N(z) = 9 = N(z_1)N(z_2)$; or les factorisations de 9 dans $\mathbf{Z}$, sont 3×3 et 9×1. On remarque que $N(a + ib\sqrt{5}) = a^2 + 5b^2 = 3$ est impossible, de sorte $N(z_2) = 1$ *i.e.* z_2 inversible.

3. De la même façon, si $N(z) = 4$ ou 6, alors z est irréductible de sorte que $2\times 3 = (1+i\sqrt{5})(1-i\sqrt{5})$ est un autre contre-exemple à l'unicité de la décomposition en produit d'irréductibles. En particulier 2 est irréductible et divise $6 = ab$ et 2 ne divise ni a, ni b. Soit δ un éventuel pgcd de $2a$ et ab ; on a 2 et a qui divisent δ, de sorte que $N(\delta)$ est un multiple de 4 et de 6 et donc un multiple de 12. De la même façon comme d divise 6 et $2a$, on en déduit que $N(\delta)$ divise 36 et 24 et donc leur pgcd qui est 12. Ainsi on obtiendrait $N(\delta) = 12 = a^2 + 5b^2$ qui n'a pas de solution, d'où la contradiction.

Solutions des exercices du chapitre 2

CALCULS MATRICIELS

Exercice 2.1.

1. Posons $M = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$. C'est la matrice du morphisme d'inclusion dans la base $(2e_1, 3e_2)(= (g_1, g_2))$ de G et la base canonique de $\mathbf{Z}^2$. On détermine deux matrices L et R de $SL_2(\mathbf{Z})$ telles que LMR soit réduite. Conformément à l'algorithme décrit dans le théorème 2.17 on procède comme suit :

1.1 On multiplie à gauche M par $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ de façon à remplacer la première ligne de M par la somme de ses deux lignes. On obtient

$$M_1 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} M = \begin{pmatrix} 2 & 3 \\ 0 & 3 \end{pmatrix}.$$

1.2 On fait apparaître un zéro à la place $(1, 2)$ de M_1. Pour cela, on multiplie M_1 à droite par la transposée de la matrice $\begin{pmatrix} -1 & 1 \\ -3 & 2 \end{pmatrix}$. On obtient

$$M_2 := M_1 \begin{pmatrix} -1 & -3 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 3 & 6 \end{pmatrix}.$$

1.3 On fait apparaître un zéro à la place $(2,1)$ de M_2. On multiplie à gauche M_2 par la matrice $\begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}$, ce qui donne

$$M_3 := \begin{pmatrix} -1 & 0 \\ -3 & 1 \end{pmatrix} M_2 = \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}.$$

Les matrices

$$L = \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -3 & -2 \end{pmatrix} \quad \text{et} \quad R = \begin{pmatrix} -1 & -3 \\ 1 & 2 \end{pmatrix},$$

conviennent. On a alors que (f_1, f_2) où

$$f_1 = -2e_1 + 3e_2 \quad \text{et} \quad f_2 = -e_1 + e_2,$$

est une base adaptée de $\mathbf{Z}^2$ au sous-module G_1. Les facteurs invariants de $\mathbf{Z}^2/G_1$ sont $\mathbf{Z}$ et $6\mathbf{Z}$, ou bien $a_1 = 1$ et $a_2 = 6$. En particulier, $\mathbf{Z}^2/G_1$ est isomorphe à $\mathbf{Z}/6\mathbf{Z}$ (cette dernière assertion était d'ailleurs prévisible au départ).

2. Posons $M = \begin{pmatrix} 2 & 3 \\ 0 & 4 \end{pmatrix}$. On procède comme ci-dessus.

2.1 On fait apparaître un zéro à la place $(1,2)$ en multipliant M à droite par la transposée de $\begin{pmatrix} -1 & 1 \\ -3 & 2 \end{pmatrix}$. On trouve

$$M \begin{pmatrix} -1 & -3 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 4 & 8 \end{pmatrix}$$

2.2 On fait apparaître un zéro dans cette matrice à la place $(2,1)$ en la multipliant à gauche par $\begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix}$, et l'on obtient

$$\begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 4 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix}.$$

On en déduit que l'on a

$$\begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix} = LMR \quad \text{avec} \quad L = \begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix} R = \begin{pmatrix} -1 & -3 \\ 1 & 2 \end{pmatrix}.$$

Il en résulte que $(f_1, f_2) = (e_1 + 4e_2, e_2)$ est une base adaptée de $\mathbf{Z}^2$ à G_2. Les facteurs invariants de $\mathbf{Z}^2/G_2$ sont $\mathbf{Z}$ et $8\mathbf{Z}$ et $\mathbf{Z}^2/G_2$ est isomorphe à $\mathbf{Z}/8\mathbf{Z}$.

3. Posons $M = \begin{pmatrix} 2 & 2 \\ 2 & 6 \end{pmatrix}$. On vérifie dans ce cas que l'on a

$$\begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} = LMR \quad \text{avec} \quad L = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix},\ R = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

On en déduit que $(e_1 + e_2, e_2)$ est une base de $\mathbf{Z}^2$ adaptée à G_3. Les facteurs invariants de $\mathbf{Z}^2/G_3$ sont $2\mathbf{Z}$ et $4\mathbf{Z}$ et $\mathbf{Z}^2/G_3$ est isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

Exercice 2.2.

On suit les étapes de la preuve du théorème 2.17 : on note M la matrice des éléments e'_i en colonnes (comme dans le théorème 2.29) :

$$M = \begin{pmatrix} 2 & 1 & 3 \\ -1 & 4 & -1 \\ 1 & -1 & -1 \end{pmatrix}$$

1. On fait apparaître un zéro à la place $(2,1)$ en multipliant à gauche par la matrice $L_1 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. On a :

$$L_1 M = \begin{pmatrix} 1 & 5 & 2 \\ 0 & 9 & 1 \\ 1 & -1 & -1 \end{pmatrix}$$

2. On fait apparaître un zéro à la place $(3,1)$ en multipliant à gauche par $L_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}$. On a alors :

$$L_2 L_1 M = \begin{pmatrix} 1 & 5 & 2 \\ 0 & 9 & 1 \\ 0 & -6 & -3 \end{pmatrix}, \quad L_2 L_1 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 0 \\ -1 & -1 & 1 \end{pmatrix}$$

3. On fait apparaître un zéro à la place $(1,2)$ en multipliant à droite par la matrice $R_1 = \begin{pmatrix} 1 & -5 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, $\quad L_2 L_1 M R_1 = \begin{pmatrix} 1 & 0 & 7 \\ 0 & 9 & 10 \\ 0 & -6 & -9 \end{pmatrix}$;

4. On multiplie ensuite par $R_2 = \begin{pmatrix} 1 & 0 & -7 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ pour avoir un zéro à la place $(1,3)$:

$$L_2 L_1 M R_1 R_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 9 & 10 \\ 0 & -6 & -9 \end{pmatrix}$$

5. On mutiplie à gauche par $L_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 3 \end{pmatrix}$ pour obtenir :

$$L_3 L_2 L_1 M R_1 R_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & -7 \end{pmatrix}$$

6. Puis à droite par $R_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 1 & 3 \end{pmatrix}$ pour obtenir :

$$L_3L_2L_1MR_1R_2R_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -7 & -21 \end{pmatrix}$$

7. Et enfin à gauche par $L_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 7 & 1 \end{pmatrix}$ pour obtenir finalement :

$$L_4L_3L_2L_1MR_1R_2R_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -21 \end{pmatrix}.$$

8. On a donc

$$R = R_1R_2R_3 = \begin{pmatrix} 1 & -7 & -16 \\ 0 & 1 & 2 \\ 0 & 1 & 3 \end{pmatrix}$$

et

$$MR = \begin{pmatrix} 2 & -10 & -21 \\ -1 & 10 & 21 \\ 1 & -9 & -21 \end{pmatrix}$$

d'où la base adaptée :

$$(f_1, f_2, f_3) = \begin{pmatrix} 2 & -10 & 1 \\ -1 & 10 & -1 \\ 1 & -9 & 1 \end{pmatrix}$$

puisque l'on doit avoir $LMRe_i = a_ie_i$ et donc $MR(e_i) = a_if_i$ $(1 \leqslant i \leqslant 3)$.

Comme confirmation le lecteur pourra vérifier que $Lf_i = e_i$ $(1 \leqslant i \leqslant 3)$, la matrice L étant $L = L_4L_3L_2L_1$ (ce qui peut être une autre façon de déterminer les f_i).

On en déduit alors que $\mathbf{Z}^3/L \simeq \mathbf{Z}/21\mathbf{Z}$. On peut retrouver ce dernier résultat sans calculs, car le calcul du déterminant de la matrice de départ donne -21 qui est donc égal au produit des facteurs invariants, ce qui impose $a_1 = a_2 = 1$ et $a_3 = 21 = 3 \times 7$ et donc $\mathbf{Z}^3/L \simeq \mathbf{Z}/21\mathbf{Z}$ (on rappelle que les facteurs invariants sont définis au signe près si on est dans $\mathbf{Z}$).

Exercice 2.3.

1. (i) implique (ii) : les n_i étant premiers entre eux par hypothèse, il existe des nombres entiers u_i tels que $u_1n_1 + \cdots + u_pn_p = 1$ (car 1 appartient à l'idéal engendré par les n_i). On considère le morphisme $\phi : \mathbf{Z}^p \longmapsto \mathbf{Z}$ défini par $\phi(x_1, \ldots, x_p) = u_1x_1 + \cdots + u_px_p$. Le théorème fondamental du cours dit de la base adaptée (théorème 2.29), nous assure l'existence d'une base $(f_1, \ldots, f_p)$ de $\mathbf{Z}^p$ tel que $\ker\phi = \mathbf{Z}a_1f_1 \oplus \cdots \oplus \mathbf{Z}a_kf_k$ avec $k \leqslant p$ et $a_i|a_{i+1}$ dans $\mathbf{Z}$

(les $a_i \in \mathbf{Z}$ sont les facteurs invariants du $\mathbf{Z}$-module $\mathbf{Z}^p/\ker\phi$) ; le morphisme $\phi : \mathbf{Z}^p \longrightarrow \mathbf{Z}$ est surjectif car $1 \in \operatorname{Im}\phi$ par hypothèse (relation de Bézout entre les n_i). On a donc $\mathbf{Z}^p/\ker\phi \simeq \mathbf{Z}$. Comme le théorème de la base adaptée dit que $\mathbf{Z}^p/\ker\phi \simeq \mathbf{Z}/a_1\mathbf{Z} \times \cdots \times \mathbf{Z}/a_k\mathbf{Z}$, on en déduit $k = p-1$ et $a_1 = \cdots = a_{p-1} = 1,\ a_p = 0$.

Les vecteurs $f_1, \ldots f_p$ formant une base de $\mathbf{Z}^p$, il en est de même des vecteurs $f_1, \ldots, f_{p-1}, x$ comme on le voit tout de suite : si $\phi(f_p) = \lambda$, on a $f_p - \lambda x \in \ker\phi$ et donc ils forment un système de générateurs. Ils forment un système libre car une relation linéaire entre $f_1, \ldots f_{p-1}, x$ donnerait (après multiplication par $\lambda \neq 0$) une relation linéaire entre les f_i.

(ii) implique (iii) : Le vecteur x faisant partie d'une base de $\mathbf{Z}^p$, la matrice de passage A de cette base (avec x comme premier vecteur) dans la base canonique vérifie bien $A^t x = {}^t(1, 0, \ldots, 0)$.

(iii) implique (i) : soit $(v_1, \ldots v_p)$ la première ligne de la matrice A ; on a : $1 = v_1 n_1 + \cdots + v_p n_p$ par hypothèse, et donc les (n_i) sont premiers entre eux.

2. On a la relation $7 - 6 = 1$ de sorte que la matrice suivante est de déterminant -1 :

$$\begin{pmatrix} 10 & 6 & 7 & 11 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

(on développe le déterminant par rapport à l dernière ligne, puis à l'avant dernière). Les 4 vecteurs colonnes de la transposée de la matrice ci-dessus constituent donc une base de $\mathbf{Z}^4$.

Exercice 2.4.

Résoudre cette équation revient comme d'habitude à trouver une solution particulière, puis déterminer le noyau de la matrice en question. On fait d'une pierre deux coups en cherchant les éléments du noyau de la matrice

$$M = \begin{pmatrix} 3 & 2 & 3 & 4 & 8 \\ 1 & -2 & 1 & -1 & 3 \end{pmatrix}$$

dont la dernière coordonnées est 1.

On commence par trigonaliser la matrice M en faisant apparaître des zéros sur les lignes, donc en multipliant à droite par des matrices de $SL_2(\mathbf{R})$.

1.

$$\begin{pmatrix} 3 & 2 & 3 & 4 & 8 \\ 1 & -2 & 1 & -1 & 3 \end{pmatrix} \begin{pmatrix} 1 & -2 & 0 & 0 & 0 \\ -1 & 3 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 3 & 4 & 8 \\ 3 & -8 & 1 & -1 & 3 \end{pmatrix}$$

2.

$$\begin{pmatrix} 1 & 0 & 3 & 4 & 8 \\ 3 & -8 & 1 & -1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 & -3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 4 & 8 \\ 3 & -8 & -8 & -1 & 3 \end{pmatrix}$$

3.

$$\begin{pmatrix} 1 & 0 & 0 & 4 & 8 \\ 3 & -8 & -8 & -1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & -4 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 8 \\ 3 & -8 & -8 & -13 & 3 \end{pmatrix}$$

4.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 8 \\ 3 & -8 & -8 & -13 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & -8 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 3 & -8 & -8 & -13 & -21 \end{pmatrix}$$

5.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 3 & -8 & -8 & -13 & -21 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 3 & -8 & 0 & -13 & -21 \end{pmatrix}$$

6.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 3 & -8 & 0 & -13 & -21 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -5 & 0 & 13 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 3 & 0 & -8 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & -21 \end{pmatrix}$$

7.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & -21 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -21 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 \end{pmatrix}$$

La matrice R, produit des 7 matrices de $SL_2(\mathbf{R})$ ci-dessus, est égale à

$$R = \begin{pmatrix} 1 & 2 & -1 & 6 & 34 \\ 1 & -27 & -6 & 58 & -575 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 3 & 0 & -8 & 63 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Un élément X du noyau de M vérifie $MX = 0$, et on cherche X sous la forme $X = RY$. Le vecteur Y étant dans le noyau de MR est de la forme ${}^t\begin{pmatrix} 0 & 0 & \alpha & \beta & 1 \end{pmatrix}$ où α et β sont des paramètres réels ; la solution demandée est donc :

$$X = \alpha\, {}^t\begin{pmatrix} -1 & -6 & 1 & 0 & O \end{pmatrix} + \beta\, {}^t\begin{pmatrix} 6 & 58 & 0 & -8 & 0 \end{pmatrix} + {}^t\begin{pmatrix} 34 & -575 & 0 & 63 & 1 \end{pmatrix}$$

(somme de la solution générale de l'équation sans second membre et d'une solution particulière).

STRUCTURE DES GROUPES ABÉLIENS FINIS

Exercice 2.5.

Les groupes abéliens d'ordre $8 = 2^3$, à isomorphismes près, sont en bijection (*cf.* la proposition (2.48)) avec les suites $0 < a_1 \leqslant a_2 \leqslant \cdots \leqslant a_r$ telles que $a_1 + \cdots + a_r = 3$: à une telle suite on associe le groupe $\mathbf{Z}/2^{a_1}\mathbf{Z} \times \cdots \mathbf{Z}/2^{a_r}\mathbf{Z}$. On trouve alors : $3 = 1 + 2 = 1 + 1 + 1$ soit les groupes $\mathbf{Z}/2^3\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^2\mathbf{Z}$ et $(\mathbf{Z}/2\mathbf{Z})^3$.

Exercice 2.6.

On a $72 = 2^3 3^2$ et donc $G = G(2) \times G(3)$ pour un groupe G d'ordre 72.

D'après la remarque 2.49, il y a trois possibilités pour $G(2)$: $(\mathbf{Z}/2\mathbf{Z})^3$, $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$, $\mathbf{Z}/8\mathbf{Z}$ correspondant respectivement aux suites $(1,1,1)$, $(1,2)$ (3), et deux pour $G(3)$: $(\mathbf{Z}/3\mathbf{Z})^2$ et $\mathbf{Z}/9\mathbf{Z}$ (correspondant aux suites $(1,1)$ et (2)), ce qui donne au total 6 possibilités pour G.

Pour trouver les facteurs invariants, on fait comme dans l'exemple 2.46, ce qui donne immédiatement :

$$\begin{array}{lcl}
(\mathbf{Z}/2\mathbf{Z})^3 \times (\mathbf{Z}/3\mathbf{Z})^2 & \simeq & \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z} \\
(\mathbf{Z}/2\mathbf{Z})^3 \times \mathbf{Z}/9\mathbf{Z} & \simeq & \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/18\mathbf{Z} \\
\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times (\mathbf{Z}/3\mathbf{Z})^2 & \simeq & \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/12\mathbf{Z} \\
\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z} & \simeq & \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/36\mathbf{Z} \\
\mathbf{Z}/8\mathbf{Z} \times (\mathbf{Z}/3\mathbf{Z})^2 & \simeq & \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/24\mathbf{Z} \\
\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z} & \simeq & \mathbf{Z}/72\mathbf{Z}
\end{array}$$

Exercice 2.7.

On fait comme dans le cours (exemple 2.46).

On a ainsi :

$$\begin{array}{lcl}
M(2) & = & \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \\
M(3) & = & \mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \\
M(5) & = & \mathbf{Z}/5\mathbf{Z}.
\end{array}$$

Les facteurs invariants s'obtiennent en lisant ce tableau par colonnes (en commençant par la dernière), d'où :

$$a_1 = 2,\ a_2 = 4 \times 3,\ a_3 = 4 \times 9,\ a_4 = 4 \times 9 \times 5$$

Exercice 2.8.

On utilise la remarque 2.49.

Si G est d'ordre $2^4 3^2 5$, on a pour $G(2)$ les possibilités :

$$\mathbf{Z}/2^4\mathbf{Z}, \quad \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^3\mathbf{Z}, \quad (\mathbf{Z}/2^2\mathbf{Z})^2, \quad (\mathbf{Z}/2\mathbf{Z})^2 \times \mathbf{Z}/2^2\mathbf{Z} \quad (\mathbf{Z}/2\mathbf{Z})^4$$

pour $G(3)$:

$$\mathbf{Z}/3^2\mathbf{Z}, \quad (\mathbf{Z}/3\mathbf{Z})^2$$

et

$$G(5) = \mathbf{Z}/5\mathbf{Z}.$$

Pour chacune de ces solutions on construit $G = G(2) \times G(3) \times G(5)$ ce qui donne en tout 10 solutions.

Pour la détermination dans chaque cas des facteurs invariants, la technique est la même que dans l'exercice précédent.

PROBLÈMES

Problème 2.1.

1. Le théorème de la base adaptée (théorème 2.29) fournit une base $(f_1, \cdots, f_n)$ de $\mathbf{Z}^n$ ainsi que des entiers $1 < a_1 | \cdots | a_n \neq 0$ tels que $(a_1 f_1, \cdots, a_n f_n)$ soit une base de G. On obtient alors $\mathbf{Z}^n/G \simeq \mathbf{Z}/a_1\mathbf{Z} \times \cdots \times \mathbf{Z}/a_n\mathbf{Z}$ qui est donc fini de cardinal $a_1 \ldots a_n$ (les a_i sont tous non nuls car G est supposé de rang n).

2. D'après ce qui précède, on a $\mathrm{card}(\mathbf{Z}^n/G) = \prod_{i=1}^n a_i$ qui est donc égal à $\det M$.

3. Soit $M = \begin{pmatrix} 3 & 1 & 1 \\ 25 & 8 & 10 \\ 46 & 20 & 11 \end{pmatrix}$ de sorte que $M \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$

Il existe alors (théorème 2.17) des matrices $L, R \in GL_3(\mathbf{Z})$ telles que $M = L\,\mathrm{diag}(a_1, a_2, a_3)R$ avec $a_1|a_2|a_3$. En outre si on pose $\begin{pmatrix} h'_1 \\ h'_2 \\ h'_3 \end{pmatrix} := R \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix}$, H est aussi engendré par h'_1, h'_2, h'_3 et l'équation

$$L\,\mathrm{diag}(a_1, a_2, a_3) \begin{pmatrix} h'_1 \\ h'_2 \\ h'_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

est équivalente à :

$$\begin{cases} a_1 h'_1 = 0 \\ a_2 h'_2 = 0 \\ a_3 h'_3 = 0 \end{cases}$$

et donc $H \simeq \mathbf{Z}/a_1\mathbf{Z} \times \mathbf{Z}/a_2\mathbf{Z} \times \mathbf{Z}/a_3\mathbf{Z}$, avec $a_1.a_2.a_3 = \det M$. L'énoncé nous suggère de simplement calculer $\det M$; on vérifie aisément qu'il est égal à -19 (cf. (iv) ci-après) comme annoncé. On obtient alors $a_1 = a_2 = 1$ et $a_3 = 19$.

De manière générale si la décomposition en facteurs premiers de $\det M$ ne fait apparaître aucune multiplicité (*i.e.* $p^2 \nmid \det M$ pour tout premier p), alors tous les a_i sont égaux à 1 sauf le dernier égal à $\det M$ et le groupe quotient est alors cyclique.

4. Les étapes du calcul sont les suivantes (*cf.* le théorème 2.17) :

(i)
$$\begin{pmatrix} 3 & 1 & 1 \\ 25 & 8 & 10 \\ 46 & 20 & 11 \end{pmatrix} \begin{pmatrix} 0 & -1 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 8 & -1 & 10 \\ 20 & 14 & 11 \end{pmatrix}$$

(ii)
$$\begin{pmatrix} 1 & 0 & 1 \\ 8 & -1 & 10 \\ 20 & 14 & 11 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 8 & -1 & 2 \\ 20 & 14 & -9 \end{pmatrix}$$

(iii)
$$\begin{pmatrix} 1 & 0 & 0 \\ 8 & -1 & 2 \\ 20 & 14 & -9 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 8 & 1 & 0 \\ 20 & -14 & -19 \end{pmatrix}$$

5. Le produit des trois matrices de $SL_2(\mathbf{R})$ ci-dessus est égal à :
$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & -3 & -5 \\ 0 & 0 & -1 \end{pmatrix}.$$
On a $\begin{pmatrix} h'_1 \\ h'_2 \\ h'_3 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 1 & -3 & -5 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix}$ ce qui s'inverse facilement : $h_3 = h'_3$, $h_2 + 2h_3 = h'_1$ soit $h_2 = h'_1 - 2h'_3$ et $h_1 - 3h_2 - 5h_3 = h'_2$ soit $h_1 = 3h'_1 + h'_2 - h'_3$. Comme $\phi(h'_1) = \phi(h'_2) = 0$ et $\phi(h'_3) = 1$, on obtient $\phi(h_1) = -1$, $\phi(h_2) = -2$ et $\phi(h_3) = 1$.

Problème 2.2.

1. Considérons les deux morphismes de groupes suivants :
$$\begin{array}{ccc} (\mathbf{Z}/n\mathbf{Z})^* & \longrightarrow & \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) \\ a & \longmapsto & k \mapsto ak \end{array}$$
$$\begin{array}{ccc} \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) & \longrightarrow & (\mathbf{Z}/n\mathbf{Z})^* \\ \phi & \longmapsto & \phi(1) \end{array}$$
On vérifie aisément qu'ils sont inverses l'un de l'autre : ce sont donc des isomorphismes.

> ***Remarque :*** Un morphisme d'un groupe cyclique vers un groupe est caractérisé par la donnée de l'image d'un générateur.

2. Le corollaire 1.53 du lemme chinois, généralisé au cas de r facteurs, donne l'isomorphisme :
$$(\mathbf{Z}/n\mathbf{Z})^* \simeq \prod_{i=1}^{r} (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^* \tag{2}$$
d'où le résultat.

3. (i) On raisonne par récurrence : pour $k = 0$, $(1+p)^{p^0} = 1 + p = 1 + p^{0+1}$ et pour $k = 1$ par la formule du binôme de Newton, on a $(1+p)^p = 1 + p^2\lambda_1$ avec $\lambda_1 = (1 + p(p-1)/2 + \cdots + p^{p-2})$, soit $\lambda_1 \equiv 1 \mod p$: c'est ici que l'on utilise l'hypothèse $p > 2$ puisque le nombre $p(p-1)/2$ n'est divisible par p que pour $p > 2$. Supposons donc le résultat vrai au rang k ; on obtient :

$$(1+p)^{p^{k+1}} = (1 + \lambda_k p^{k+1})^p = 1 + \lambda_{k+1} p^{k+2}$$

en posant $\lambda_{k+1} = \lambda_k + p^k \sum_{\alpha=2}^{p} \binom{\alpha}{p} \lambda_k^\alpha p^{(\alpha-2)(k+1)}$. Comme $k > 1$, on a $\lambda_{k+1} \equiv \lambda_k \mod p$.

Ainsi $(1+p)^{p^{\alpha-1}} \equiv 1 \mod p^\alpha$ de sorte que l'ordre de $(1+p)$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ divise $p^{\alpha-1}$ et est donc de la forme p^k pour $k \leqslant \alpha - 1$. En outre on a $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$ avec λ_k non divisible par p ; en particulier $(1+p)^{p^{\alpha-2}} \not\equiv 1 \mod p^\alpha$, de sorte que l'ordre de $1 + p$ est $p^{\alpha-1}$.

(ii) C'est la proposition 6.1 du chapitre 6.

(iii) Le morphisme ψ est clairement surjectif. Soit donc y un antécédent d'un générateur h de $(\mathbf{Z}/p\mathbf{Z})^*$; l'ordre m de y est alors un multiple de $p - 1$ (car $1 = \psi(y^m) = h^m$) : $m = (p-1)k$, de sorte que $x = y^k$ est d'ordre $p - 1$.

(iv) Le groupe $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ est abélien et donc de la forme $\mathbf{Z}/a_1\mathbf{Z} \times \cdots \times \mathbf{Z}/a_r\mathbf{Z}$ avec $1 < a_1 | \cdots | a_r \neq 0$ et $p^{\alpha-1}(p-1) = \prod_{i=1}^r a_i$. Tout élément a alors un ordre divisant a_r ce qui d'après (ii) et (iii) implique $p^{\alpha-1}$ et $p-1$ divisent a_r et donc comme $p \wedge (p-1) = 1$, a_r est divisible par leur produit, soit donc $r = 1$ et $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ est cyclique.

Posons $u = (1+p)x$ et soit m son ordre ; $1 = \psi(u^m) = \psi(u)^m = \psi(x)^m$, soit $p - 1$ divise m et donc $u^m = (1+p)^m$ soit $p^{\alpha-1}$ divise m. En outre $u^{(p-1)p^{\alpha-1}} = 1$ et donc u est un générateur de $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$. On construit alors un isomorphisme $\mathbf{Z}/p^{\alpha-1}(p-1)\mathbf{Z} \longmapsto (\mathbf{Z}/p^\alpha\mathbf{Z})^*$ en envoyant 1 sur u.

(v) On a $g^{p-1} = 1 + p\lambda$ avec $\lambda \not\equiv 0 \mod p$; notons d l'ordre de g qui est un multiple de $p - 1$ et un diviseur de $\phi(p^\alpha) = p^{\alpha-1}(p-1)$ soit $d = (p-1)p^e$ avec $0 \leqslant e < \alpha$ car p est premier avec $p-1$. Par une récurrence comme dans (i), on obtient $(1 + p\lambda)^{p^e} = 1 + \mu p^{e+1}$ avec p ne divisant pas μ de sorte que $g^d = 1 \mod p$ si et seulement si $e = \alpha - 1$ et donc g est un générateur.

Supposons maintenant $g^{p-1} \equiv 1 \mod p^2$. On remarque que $\psi(g+p) = \psi(g)$ est générateur, il suffit donc de montrer que $(g+p)^{p-1} \neq 1 \mod p^2$. Or on a

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \equiv 1 - pg^{p-2} \mod p^2$$

et g^{p-2} est inversible dans $\mathbf{Z}/p^2\mathbf{Z}$ (d'inverse g) de sorte que $pg^{p-2} \not\equiv 0 \mod p^2$, d'où le résultat.

4. (i) On a de manière directe $(\mathbf{Z}/2\mathbf{Z})^* = \{1\}$ et $(\mathbf{Z}/4\mathbf{Z})^* = \{1, -1\} \simeq \mathbf{Z}/2\mathbf{Z}$.

(ii) On raisonne à nouveau par récurrence, les cas $k = 0$ et $k = 1$ étant directs. Supposons donc que $5^{2^k} = 1 + \lambda_k 2^{k+2}$ avec λ_k impair. On a alors $5^{2^{k+1}} = (1 + \lambda_k 2^{k+2})^2 = 1 + 2^{k+3}(\lambda_k + 2^{k+1}\lambda_k^2)$ d'où le résultat en posant $\lambda_{k+1} = \lambda_k + \lambda_k^2 2^{k+1} \equiv \lambda_k \mod 2$. Comme précédemment, on en déduit que 5 est d'ordre $2^{\alpha-2}$ dans $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$.

(iii) Le groupe $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ en tant que groupe abélien fini est de la forme $\mathbf{Z}/2^{\alpha_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/2^{\alpha_r}\mathbf{Z}$ avec $0 < \alpha_1 \leqslant \cdots \leqslant \alpha_r$ et $\sum_{i=1}^r \alpha_i = \alpha - 1$. Comme dans les questions précédentes, tout élément est alors d'ordre divisant 2^{α_r} ce qui, d'après (ii), impose $\alpha_r \geqslant \alpha - 2$. Restent alors deux possibilités pour les α_i à savoir $r = 2$ et $(\alpha_1, \alpha_2) = (1, \alpha - 2)$ ou bien $r = 1$ et $\alpha_1 = \alpha - 1$. Dans le premier cas on compte 3 éléments d'ordre 2 alors que dans le second on en compte qu'un. Reste donc à déterminer le nombre d'éléments d'ordre 2 de $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$. Or on a vu que $5^{2^{\alpha-3}}$ et -1 étaient d'ordre 2 ; montrons qu'ils ne sont pas égaux. Considérons le morphisme canonique $\phi : (\mathbf{Z}/2^\alpha\mathbf{Z})^* \longmapsto (\mathbf{Z}/4\mathbf{Z})^*$; on a $\phi(-1) = -1$ et $\phi(5^{2^{\alpha-3}}) = 1^{2^{\alpha-3}} = 1$. Comme $1 \neq -1$ dès que $\alpha \geqslant 2$, cela entraîne que $5^{2^{\alpha-3}} \neq -1$ dans $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$. On en déduit donc que $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ est isomorphe à $(\mathbf{Z}/2^{\alpha-2}\mathbf{Z}) \times \mathbf{Z}/2\mathbf{Z}$.

Construisons explicitement un tel isomorphisme $\overline{f} : \mathbf{Z}/2^{\alpha-2}\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \longmapsto (\mathbf{Z}/2^\alpha\mathbf{Z})^*$. On définit tout d'abord $f : \mathbf{Z}^2 \longmapsto (\mathbf{Z}/2^\alpha\mathbf{Z})^*$ en posant $f((1,0)) = 5$ et $f((0,1)) = -1$. L'application f passe alors au quotient pour définir une application $\overline{f}$. Pour montrer que $\overline{f}$ est un isomorphisme, en vertu de l'égalité des cardinaux, il suffit de montrer qu'elle est injective ou qu'elle est surjective. Pour l'injectivité soit $(\overline{i}, \overline{k}) \in \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{\alpha-2}\mathbf{Z}$ tel que $(-1)^i 5^k = 1$ soit $(-1)^i = 5^k$. Or d'après la remarque ci-dessus -1 n'appartient pas au groupe engendré par 5 de sorte que $i \equiv 0 \mod 2$ et $5^k \equiv 1 \mod 2^\alpha$ soit $k \equiv 0 \mod 2^{\alpha-2}$ et donc $(\overline{i}, \overline{k}) = (0, 0)$.

> ***Remarque :*** Pour prouver la surjectivité directement, il suffit de remarquer que l'image de $\overline{f}$ contient le groupe engendré par 5 strictement car il contient -1 ce qui n'est pas le cas du groupe engendré par 5. On en déduit alors que le cardinal de cette image est divisible strictement par $2^{\alpha-2}$, car il contient strictement un groupe de cardinal $2^{\alpha-2}$, et divise $2^{\alpha-1}$ de sorte que ce dernier est égal à $2^{\alpha-1}$ et donc $\overline{f}$ est surjective.

5. Pour $n = 2^\alpha \prod_{p \in \mathcal{P}} p^{\alpha_p}$ où $\mathcal{P}$ désigne l'ensemble des premiers impairs, le théorème chinois donne

$$(\mathbf{Z}/n\mathbf{Z})^* \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{\alpha-2}\mathbf{Z} \times \prod \mathbf{Z}/p^{\alpha_p - 1}(p-1)\mathbf{Z}.$$

Pour que ce dernier soit cyclique il faut et il suffit que les nombres $2, 2^{\alpha-2}, p_i, p_i - 1$ pour p_i premier impair divisant n, soient premiers entre eux deux à deux. On en déduit alors $n = 2, p^{\alpha_p}, 2p^{\alpha_p}$.

Solutions des exercices du chapitre 3

POLYNÔME MINIMAL

Exercice 3.1.

1. Il suffit de vérifier que si $x \in E_i$, alors $u(x) \in E_i$, soit $P_i(u)(u(x)) = 0$. Mais $P_i(u)(u(x)) = u(P_i(u)(x)) = 0$, car u commute avec $P_i(u)$.

2. P_1 et P_2 étant premiers entre eux, on écrit une relation de Bézout $UP_1 + VP_2 = 1$ où U, V sont des polynômes de $\mathbf{R}[X]$. Ainsi pour tout vecteur x de V, on a $x = x_1 + x_2$ avec $x_1 = (UP_1)(u)(x)$ et $x_2 = (VP_2)(u)(x)$. En outre on a $P_2(u)(x_1) = (Uq_U)(u)(x) = 0$ car $q_u(u)$ est l'endomorphisme nul et $q_u = P_1P_2$ par hypothèse ; on a donc $x_1 \in E_2$. De la même façon on a $P_1(u)(x_2) = 0$ de sorte que $E_u = E_1 + E_2$. Par ailleurs si x est un élément de $E_1 \cap E_2$, on a $x_1 = x_2 = 0$ et donc $x = 0$, d'où le résultat.

3. Le polynôme minimal q_1 de $u_{|E_1}$ divise P_1 tandis que celui q_2 de $u_{|E_2}$ divise P_2. En outre d'après (b), q_1q_2 est un polynôme annulateur de u et donc q_1q_2 est divisible par le polynôme minimal $q_u = P_1P_2$. Cela entraîne immédiatement que $q_1 = P_1$ et $q_2 = P_2$ puisque tous ces polynômes sont unitaires.

INVARIANTS DE SIMILITUDE

Exercice 3.2.

1. Sur $\mathbf{C}$ tout endomorphisme possède une valeur propre et donc un vecteur propre v tel que $\mathbf{C}v$ soit un sous-espace stable non réduit au vecteur nul de sorte que par hypothèse il est égal à l'espace tout entier qui est donc de dimension 1.

Sur $\mathbf{R}$, l'énoncé est faux : il suffit de considérer dans $\mathbf{R}^2$ une matrice de rotation d'angle $\theta < \pi$.

2. On décompose χ_u, qui par convention est unitaire, en produits de facteurs irréductibles $Q_1^{\nu_1} \cdots Q_r^{\nu_r}$ et on remarque que R_i se définit comme le produit des Q_j tels que $\nu_j = i$.

3. En tant que $\mathbf{C}[X]$-module, V est par hypothèse de la forme

$$(\mathbf{C}[X]/(X-\alpha_1))^{\nu_1} \times \cdots \times (\mathbf{C}[X]/(X-\alpha_r))^{\nu_r},$$

où les α_i sont les valeurs propres de u et ν_i leur multiplicité dans le polynôme caractéristique. Avec les notations de (b), on a $R_i = \prod_{j|\nu_j=i}(X-\alpha_j)$. Les invariants de similitude sont de la forme $P_1|P_2|\cdots|P_l$ où chacun des P_j est de la forme $\prod_{i\in I_j}(X-\alpha_i)$, I_j étant un certain sous-ensemble de $\{1,\cdots,r\}$ tel que $I_j \subset I_{j+1}$. L'hypothèse implique en effet que le polynôme minimal $q_u(X) = P_l(X)$ n'a pas de facteur multiple. Ainsi les éléments de I_1 sont répétés l fois, ceux de I_2 le sont $(l-1)$ fois et de manière générale ceux de I_j le sont $(l+1-j)$ fois. On en déduit donc que $l = \max_i\{\nu_i\}$ puis que I_j est l'ensemble des i tels que $\nu_i \geqslant l+1-j$ de sorte que les invariants de similitude sont $R_l, R_lR_{l-1},\ R_lR_{l-1}R_{l-2}, \cdots, R_l\cdots R_1$.

Exercice 3.3.

On remarque tout d'abord que u possède une unique valeur propre car dans le cas contraire, pour λ_1 et λ_2 des valeurs propres distinctes, $W = \ker(u-\lambda_1 Id)$ et $W' = \ker(u-\lambda_2 Id)$ auraient une intersection réduite au vecteur nul. Soit alors λ l'unique valeur propre de u (sur $\mathbf{C}$, un endomorphisme possède toujours au moins une valeur propre). On remarque alors que $\ker(u-\lambda Id)$ est de dimension 1, car sinon pour x_1 et x_2 des vecteurs propres non colinéaires, $W = \mathbf{C}x_1$ et $W' = \mathbf{C}x_2$ auraient une intersection réduite au vecteur nul. On en déduit donc que u admet un unique invariant de similitude égal à son polynôme minimal et à son polynôme caractéristique, soit $(X-\lambda)^n$.

Exercice 3.4.

Considérons un endomorphisme u de E. Soient q_1, q_2, q_3 les trois invariants de similitude de u tels que q_1 divise q_2 et q_2 divise q_3. Le polynôme q_3 est le polynôme minimal de u et $\chi := q_1q_2q_3$ est le polynôme caractéristique de u. Si le degré de q_3 vaut 1, on a les égalités $q_1 = q_2 = q_3$. Si q_3 est de degré 2, on a $q_1 = 1$, q_2 est de degré 1 et l'on a $\chi = q_2q_3$. Si le degré de q_3 vaut 3, on a $q_1 = q_2 = 1$ et $q_3 = \chi$. Deux endomorphismes de E ayant le même polynôme minimal et le même polynôme caractéristique, ont donc les mêmes invariants de similitude, ils sont donc semblables. L'implication réciproque est évidente.

Exercice 3.5.

1. On note I la matrice identité d'ordre n. Le polynôme caractéristique de M est $(X-\lambda)^n$, donc λ est l'unique valeur propre de M. Par ailleurs, la matrice $M-\lambda I$ est de rang $n-1$. En effet, $M-\lambda I$ n'est pas inversible, et l'on peut en extraire une

matrice carrée d'ordre $n-1$ inversible. La dimension du noyau de $M-\lambda I$ vaut donc 1, qui n'est autre que la dimension du sous-espace propre associé à λ.

2. On a $M=\lambda I+N$, où N est nilpotente. Notons $(e_1,\cdots,e_n)$ la base canonique de K^n. Pour tout k tel que $0\leqslant k\leqslant n-1$, on a $N^k(e_n)=e_{n-k}$. Il en résulte que la famille $\big(e_n,N(e_n),N^2(e_n),\cdots,N^{n-1}(e_n)\big)$ est une base de K^n, ce qui montre que le $K[X]$-module associé à N est cyclique. Le polynôme minimal de N est donc égal à son polynôme caractéristique *i.e.* à X^n. Il en résulte que le polynôme minimal de M est $(X-\lambda)^n$. En particulier, si u est l'endomorphisme représenté par M dans la base canonique de K^n, le $K[X]$-module associé à u est cyclique isomorphe à $K[X]/(X-\lambda)^n$.

Exercice 3.6.

1. Considérons un élément $\lambda\in\mathbf{C}$. Il existe une base de E dans laquelle la matrice de u est la matrice compagnon M du polynôme minimal (ou caractéristique) de u. On peut extraire de $M-\lambda I$ une matrice d'ordre $n-1$ inversible. Par suite, le rang de $u-\lambda I$ est $n-1$ ou n, suivant que λ est une valeur propre de u ou non. La dimension du noyau de $u-\lambda I$ est donc au plus 1.

2. Soit $E=E_1\bigoplus\cdots\bigoplus E_r$ une décomposition de E en somme directe de sous-modules cycliques, pour laquelle E_i est $\mathbf{C}[X]$-isomorphe à $\mathbf{C}[X]/(P_i)$ (avec $P_i\in\mathbf{C}[X]$ unitaire de degré $\geqslant 1$) et P_i divise P_{i+1} (théorème 2.33). Les invariants de similitude non constants de u sont les polynômes P_i. Il y en a donc r (dont certains peuvent être éventuellement égaux). Les sous-espaces E_i sont stables par u. Soit λ une valeur propre de u. On a

$$\ker\big(u-\lambda I\big)=\bigoplus_{i=1}^{r}\ker\big(u|_{E_i}-\lambda I|_{E_i}\big). \tag{1}$$

En effet, soit y un élément de $\ker\big(u-\lambda I\big)$. Pour tout $i=1,\cdots,r$, il existe $x_i\in E_i$ tel que $y=x_1+\cdots+x_r$. Par ailleurs, on a les égalités

$$u(y)=\sum_{i=1}^{r}u(x_i)=\sum_{i=1}^{r}\lambda x_i.$$

Puisque $u(x_i)$ et λx_i sont dans E_i, on en déduit que $u(x_i)=\lambda x_i$ (par l'unicité de la décomposition d'une somme directe). Par suite, x_i appartient à $\ker\big(u|_{E_i}-\lambda I|_{E_i}\big)$, ce qui prouve l'égalité (1). (On notera que $\ker\big(u|_{E_i}-\lambda I|_{E_i}\big)=\ker\big(u-\lambda I\big)\cap E_i$). D'après la question 1, la dimension de $\ker\big(u|_{E_i}-\lambda I|_{E_i}\big)$ est 0 ou 1. On en déduit que la dimension de $\ker\big(u-\lambda I\big)$ est au plus r. Le maximum des dimensions des sous-espaces propres associés à u est donc $\leqslant r$. Considérons alors une racine α de P_1, qui existe car P_1 n'est pas constant. Puisque P_1 divise les P_i, le polynôme minimal de $u|_{E_i}$ étant P_i, α est donc valeur propre de $u|_{E_i}$ et la dimension de $\ker\big(u|_{E_i}-\alpha I|_{E_i}\big)$ vaut 1. L'égalité (1) entraîne alors que $\ker\big(u-\alpha I\big)$ est de dimension r.

Exercice 3.7.

Soit α_i une valeur propre de u. Le sous-espace caractéristique correspondant est $E(X-\alpha_i) = \oplus_j E_{ij}$ avec $E_{ij} \simeq \frac{\mathbf{C}[X]}{(X-\alpha_i)^{\beta_{ij}}}$ (définition 3.24). Or le sous-espace propre de chaque E_{ij} est de dimension 1 (engendré par la classe de $(X-\alpha_i)^{\beta_{ij}}$). La dimension n_i de l'espace propre correspondant à la valeur propre α_i est donc le nombre de facteurs Eij (i fixé). D'autre part, le nombre d'invariants de similitude est clairement égal à $\sup(n_i)$ (*cf.* l'exemple 2.46).

Exercice 3.8.

Le polynôme $(X-\alpha)^{r_\alpha}$ annule le A-module E_u (avec $E = \mathbf{C}^n$), le polynôme caractéristique est égal à $(X-\alpha)^n$ et les deux endomorphismes correspondants à ces deux polynômes ont même noyau par hypothèse.

En revanche, le polynôme $(X-\alpha)^{r_\alpha - 1}$ n'annule pas E_u par hypothèse ; il est donc clair que $q_u = (X-\alpha)^{r_\alpha}$.

Exercice 3.9.

1. Le A-module V est clairement isomorphe à $(A/(X-a))^3 \times (A/(X-b))^2 \times A/(X-c)$; on calcule alors les invariants de similitude via le théorème chinois comme dans les exercices du chapitre 2, ce qui donne : $(X-a)$, $(X-a)(X-b)$ et $(X-a)(X-b)(X-c)$. La matrice étant diagonalisable, les sous-espaces propres sont les sous-espaces caractéristiques, et le polynôme minimal est $(X-a)(X-b)(X-c)$.

2. On a de même

$$V \simeq (A/(X-1))^3 \times (A/(X-1)^2)^2 \times (A/(X-1)^3)^2 \times \\ (A/(X-2))^2 \times A/(X-2)^3 \times (A/(X-3))^2 \times A/(X-3)^2$$

les invariants de similitude donnés comme d'habitude par application du théorème chinois sont alors

$$(X-1), \quad (X-1), \quad (X-1), \quad (X-1)^2, \quad (X-1)^2(X-2)(X-3), \\ (X-1)^3(X-2)(X-3), \qquad (X-1)^3(X-2)^3(X-3)^3.$$

Le polynôme minimal est le dernier invariant de similitude, soit $(X-1)^3(X-2)^3(X-3)^3$.

Les dimensions des sous-espaces caractéristiques sont 11 pour la valeur propre 1, 8 pour la valeur propre 2 et 5 pour la valeur propre 3.

3. La matrice étant sous forme triangulaire, on voit que les valeurs propres sont 0,1 et a_n.

Le sous-espace propre associé à la valeur propre 0 (resp. 1) est de dimension supérieure ou égale à 1 (resp. $n-2$). Si $a_n \neq 0, 1$ alors la somme des dimensions des sous-espaces propres associés aux valeurs propres $0, 1, a_n$ est n de sorte que la matrice est diagonalisable et donc

$$V \simeq A/(X) \times A/(X-a_n) \times (A/(X-1))^{n-2}$$

et les invariants de similitude sont

$$a_1(X) = (X-1), \quad a_2(X) = X-1, \quad \cdots \quad a_{n-2}(X) = (X-1)X(X-a_n).$$

Si $a_n = a_1 = 0$, on est dans la même situation, car le noyau de la matrice est alors de dimension 2 parce que son rang est de manière évidente $n-2$; les invariants de similitude sont alors :

$$P_1(X) = \cdots = P_{n-4}(X) = X-1, P_{n-3} = P_{n-2} = X(X-1).$$

Dans le cas où $a_n = 0$ et a_1 non nul, on a alors

$$V \simeq A/(X^2) \times (A/(X-1))^{n-2}$$

soit

$$P_1(X) = \cdots = P_{n-3}(X) = (X-1), \quad P_{n-2} = X^2(X-1).$$

Exercice 3.10.

D'après l'exercice 3.7, le nombre d'invariants de similitude est égal à la dimension maximale des sous-espaces propres soit donc ici 4 invariants de similitude P_1, P_2, P_3, P_4. Le polynôme minimal s'écrit sous la forme $P_4(X) = X^4(X-1)^3$ d'après l'exercice 3.8 appliqué successivement aux valeurs propres 0 et 1).
La seconde question de ce même exercice fournit immédiatement :

$$P_1(X) = X(X-1), \quad P_2(X) = X^2(X-1),$$
$$P_3(X) = X^3(X-1),$$
$$P_4(X) = X^4(X-1)^3.$$

Exercice 3.11.

On note n la dimension de l'espace vectoriel sur lequel agit u (n est la somme des degrés des invariants de similitude).

On reprend les notations de l'exercice 3.9 : pour $n > 1$, on note $J_n \in \mathcal{M}_n(\mathbf{C})$ la matrice nilpotente dont tous les coefficients sont nuls, sauf ceux de la première surdiagonale $j_{i,i+1}$ pour $1 \leqslant i < n$ qui sont égaux à 1.

(a) Ici $n = 1$ et l'endomorphisme en question est l'identité.

(b) On a $n = 2$ et deux valeurs propres distinctes ; u est donc diagonalisable et sa matrice dans une base de diagonalisation est la matrice diagonale $\mathrm{diag}(0, 1)$.

(c) $n = 3$ et 0 est la seule valeur propre et la matrice de Jordan associée est $\mathrm{diag}(0, J_2)$.

(d) $n = 3$ et $0, 1$ sont les valeurs propres de u. L'endomorphisme est diagonalisable puisque le polynôme minimal est à racines simples.

(e) $n = 24$, les valeurs propres étant $0, 1, 2$; la forme de Jordan est la matrice diagonale par blocs

$$\mathrm{diag}(J_2, J_2, J_3, J_4, I_1, I_1, I_2, I_3, 2I_2, 2I_4 + J_4).$$

PROBLÈMES

Problème 3.1.

1. On remarque que la multiplicité de λ_i dans P' est égale à $n_i - 1$ de sorte que λ_i est une racine à l'ordre 1 de $\frac{\chi_A(X)}{\chi_A(X) \wedge \chi'_A(X)}$ et qu'en outre ce sont ces seules racines d'où le résultat. On notera en particulier que la connaissance des λ_i n'est pas nécessaire pour calculer P qui peut se calculer via l'algorithme d'Euclide.

2. – L'idée est d'utiliser la relation formelle $(1-x)(1+x+x^2+\cdots+x^k) = 1-x^{k+1}$ avec $x = U^{-1}N$ et k tel que $N^{k+1} = 0$ soit $(1-U^{-1}N)(1+U^{-1}N+\cdots+(U^{-1}N)^k) = I_n$ car $(U^{-1}N)^{k+1} = U^{-k-1}N^{k+1}$ car U et N commutent entre eux ; soit en multipliant à gauche par U et à droite par U^{-1},

$$(U - N)(U^{-1} + U^{-2}N + \cdots + U^{-k-1}N^k) = I_n.$$

– Les valeurs propres de A ne sont pas des racines de P' car $P \wedge P' = 1$. On considère alors une relation de Bézout $UP' + VP = 1$ pour P et P' qui en l'appliquant à A, donne $U(A)P'(A) = 1 - N$ avec $N = V(A)P(A)$. Or d'aprés le théorème de Cayley-Hamilton, on a $P^r(A) = 0$ pour $r \geqslant \max_i(n_i)$ de sorte que N est nilpotente et donc par application de ce qui précède $P'(A)$ est une matrice inversible dont l'inverse commute avec A (car c'est un polynôme en A).

3. Il s'agit de la méthode de Newton appliquée aux matrices, le but étant de construire une racine de P, *i.e.* de trouver la partie diagonalisable de A dans sa décomposition de Dunford. Remarquons que pour $n = 0$, $P'(A_0)$ est inversible d'après la question précédente.

(i) Il suffit par exemple de le vérifier sur les monômes X^m, soit $(X+Y)^m = X^m + mYX^{m-1} + Y^2 \sum_{k=2}^{m} (k\lambda m)\, Y^{k-2}X^{m-k}$.

(ii) Il est clair d'après (a) que pour tout $0 \leqslant k \leqslant n$, A_k est un polynôme en A. On raisonne par récurrence sur n. Pour $n = 0$, on a $P(A_0) = P(A)$. Supposons donc le résultat acquis jusqu'au rang k. D'après (i), on écrit $P(A_{k+1}) = P(A_k + Y) = P(A_k) + YP'(A_k) + Y^2\tilde{Q}(A_k, Y)$ avec Y tel que $P(A_k) + YP'(A_k) = 0$. D'après (a) $Y = P(A_k)Q(A_k)$ et donc $P(A_{k+1})$ est de la forme $P(A)^{2^{k+1}}B_{k+1}$ pour une matrice B_{k+1} qui en tant que polynôme en A_k commute avec A.

(iii) La formule de Taylor donne $P'(A_{n+1}) - P'(A_n) = (A_{n+1} - A_n)Q(A_n)$ où $Q \in K[X]$. Or $A_{n+1} - A_n$ est de la forme $P(A_n)\tilde{Q}(A_n)$ et est donc nilpotent et commute avec A_n qui est un polynôme en A. On en déduit alors que $P'(A_{n+1})$ est inversible d'après (a).

4. On rappelle que $P^r(A) = 0$ pour $r = \max_i\{n_i\}$ de sorte que la sous-suite $(A_k)_{k \geqslant n}$ est constante dès que $2^n \geqslant r$. La limite D est un polynôme en A tel que $P(D) = 0$ de sorte que D est diagonalisable car elle possède un polynôme annulateur scindé à racines simples (dans $\mathbf{C}$). Par ailleurs, pour n tel que $2^n \geqslant r$, on a $A - D = A_0 - A_n = \sum_{i=0}^{n-1}(A_i - A_{i+1})$ avec $A_i - A_{i+1}$ nilpotente et qui est un polynôme en A. Ainsi les $A_i - A_{i+1}$ commutent en eux de sorte que leur somme est nilpotente d'où le résultat.

Solutions des exercices du chapitre 4

GROUPES

Exercice 4.1.

1. Soient x, y deux éléments quelconques de G, il s'agit alors de monter que $xy = yx$ ce qui revient à prouver aussi que $xyx^{-1}y^{-1} = 1$. Or x (resp. y) étant d'ordre 2, on a $xx = 1 = x^{-1}x$ soit $x = x^{-1}$ (resp. $y = y^{-1}$). L'égalité cherchée s'écrit alors $xyxy = 1$ ce qui revient à montrer que xy est d'ordre 2 ce qui est vrai par hypothèse.

2. Supposons, par récurrence, que si le cardinal de G est inférieur à r alors il est de la forme 2^n. La récurrence est clairement vérifiée pour $r = 1$ et $r = 2$, supposons-la vraie jusqu'au rang r et traitons le cas de $r + 1$. Soit alors $g_1 \neq 1$ un élément de G qui engendre, par hypothèse, un sous-groupe d'ordre 2 qui est distingué car $gg_1g^{-1} = g_1$. On considère alors le groupe quotient $G/(g_1)$ qui est de cardinal $\frac{r}{2}$ et dont tous les éléments sont d'ordre 2 ; en effet $\overline{gg} = \overline{gg} = \overline{1}$. Par récurrence on a donc $\frac{r}{2}$ qui est de la forme 2^n, d'où le résultat.

3. Soit $h \in H$ et soit $g \in G$, il s'agit de montrer que $ghg^{-1} \in H$. Or H étant d'indice 2, il existe $g_0 \notin H$ tel que G soit la réunion disjointe de H et de g_0H. Il suffit alors de montrer que $g_0hg_0^{-1}$ ne s'écrit pas g_0h'. On raisonne par l'absurde ce qui donne $hg_0^{-1} = h'$ et donc $g_0 = h(h')^{-1}$ soit $g_0 \in H$ ce qui n'est pas.

Exercice 4.2.

Il existe un élément a de G tel que la classe aC engendre G/C. Soient x et y deux éléments de G. Il existe des entiers p et q tels que $xC = (aC)^p$ et $yC = (aC)^q$. Il existe donc des éléments α et β de C tels que l'on ait les égalités $x = a^p\alpha$ et $y = a^q\beta$. On obtient les égalités $xy = a^p\alpha a^q\beta = a^{p+q}\alpha\beta = yx$, et le fait que G est abélien.

Exercice 4.3.

On considère la surjection canonique $s : G \to G/H$. Soit N un sous-groupe de G d'ordre n. Alors, l'ordre de $s(N)$ divise l'ordre n de N. Par ailleurs, $s(N)$ étant un sous-groupe de G/H, son ordre divise l'indice de H dans G. On déduit de là (et de l'hypothèse), que $s(N)$ est nul, autrement dit que N est contenu dans H. Puisque N et H ont le même ordre, on a donc $N = H$. D'où le résultat.

Exercice 4.4.

1. Supposons que HK soit un sous-groupe de G. Soit hk un élément de HK. Cet élément possède un inverse uv dans HK. On a donc $hk = (uv)^{-1} = v^{-1}u^{-1}$ qui est donc dans KH. Cela montre que HK est contenu dans KH. Par ailleurs soit kh un élément de KH. L'inverse de kh qui est $h^{-1}k^{-1}$ appartient à HK. Puisque HK est un sous-groupe de G, kh est donc aussi dans HK. D'où l'inclusion $KH \subseteq HK$, et l'égalité $HK = KH$.

Inversement supposons $HK = KH$. D'abord $e \in HK$ et si x est dans HK, il est clair que x^{-1} aussi. Considérons par ailleurs, deux éléments $u = ab$ et $v = cd$ dans HK. On a $bc = fg$, où $f \in H$ et $g \in K$. D'où $uv = (af)(gd) \in HK$. Cela prouve que HK est un sous-groupe de G.

2. Soit hk un élément de HK. On a $hk = k(k^{-1}hk)$, ce qui prouve que $hk \in KH$ (car H est distingué dans G) : d'où $HK \subseteq KH$. Inversement, soit $kh \in KH$. L'élément $khk^{-1} = h'$ est dans H. D'où $kh = h'k \in HK$ et l'on a $KH \subseteq HK$. D'où le résultat.

3. D'abord l'ensemble quotient HK/H est un groupe car H est distingué dans G (donc aussi dans HK) et φ est un homomorphisme de groupes (car $kk'H = (kH)(k'H)$). Par ailleurs φ est surjective : en effet, soit $a = hkH$ un élément de HK/H : on a $a = k'h'H$ où $k' \in K$ et $h' \in H$ (car on a $HK = KH$). D'où $a = k'H$ et l'on a $\varphi(k') = a$. Enfin étant donné un élément k de K, on a $kH = H$ si et seulement si k est dans H. Le théorème de factorisation des homomorphismes de groupes entraîne alors notre assertion.

4. Par définition l'application ψ est surjective. Elle est injective car $H \cap K$ est réduit à l'élément neutre de G. Tout revient à vérifier que ψ est un homomorphisme de groupes. Considérons pour cela deux éléments (h, k) et (h', k') de $H \times K$. On a les égalités suivantes : $\psi\big((h, k)(h', k')\big) = \psi\big((hh', kk')\big) = (hh')(kk')$. Par ailleurs, tout élément de H commute avec tout élément de K : en effet, si $h \in H$ et $k \in K$, l'élément $hkh^{-1}k^{-1}$ appartient à $H \cap K$ car H et K sont par hypothèse distingué dans G ; d'où $hkh^{-1}k^{-1} = e$ et le fait que $hk = kh$. On a donc $\psi\big((h, k)(h', k')\big) = (hk)(h'k')$ *i.e.* $\psi\big((h, k)(h', k')\big) = \psi\big((h, k)\big)\psi\big((h', k')\big)$.

5. Soit I la matrice identité de $SL_2(\mathbf{Z})$. On vérifie que $M^2 \neq I$ et les égalités $M^4 = I$, et $N^3 = I$. Donc l'ordre de M est 4 et celui de N est 3. Par ailleurs, pour tout entier $n \geqslant 0$, on a les égalités

$$(MN)^{2n} = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad (MN)^{2n+1} = \begin{pmatrix} -1 & -1-2n \\ 0 & -1 \end{pmatrix}.$$

Il en résulte que MN n'est pas d'ordre fini (MN est donc d'ordre infini).

6. Supposons que HK soit un sous-groupe de $SL_2(\mathbf{Z})$; c'est alors un groupe fini (car par exemple l'application $H \times K \to HK$ définie par $(h,k) \mapsto hk$ est surjective). Mais cela conduit à une contradiction car MN appartient à HK et MN est d'ordre infini. D'où l'assertion.

Exercice 4.5.

1. On rappelle que dans un groupe fini G, l'ordre de tout élément est un diviseur du cardinal de G. Ainsi, si dans un groupe de cardinal 10 il n'y a aucun élément d'ordre 5, il n'y aurait aucun élément g d'ordre 10 car sinon g^2 serait d'ordre 5, de sorte que tout élément $g \neq 1$ serait d'ordre 2 ce qui contredit l'exercice précédent 4.1 car 10 n'est pas une puissance de 2.

2. Soit alors g un élément d'ordre 5 ; le sous-groupe H qu'il engendre est d'indice 2 et est donc distingué d'après le point (c) de l'exercice 4.1. Soit alors $x \notin H$. Dans le groupe quotient G/H, on a $(\overline{x})^2 = 1$ de sorte que x^2 appartient à H. Si on avait $x^2 \neq 1$, x^2 serait alors d'ordre 5 et x serait d'ordre 10 et G serait cyclique donc abélien.

3. Supposons pour commencer que G est non commutatif. Soit $x \notin H$ de sorte que tout élément de G s'écrit de manière unique sous la forme $g^k x^i$ avec $0 \leqslant k < 5$ et $i = 0, 1$. On considère alors l'application $f : G \longmapsto D_5$ qui envoie $g^k x^i$ sur $r^k \circ s^i$ où r est la rotation d'angle $2\pi/5$ et s la réflexion d'axe (Ox). Montrons que f est un morphisme de groupe, *i.e.* $f(g^k x^i g^{k'} x^{i'}) = r^k s^i r^{k'} s^{i'}$. Pour $i = 0$ ou $k' = 0$, le résultat découle de la définition. Dans le cas $i = i' = 1$, comme $(g^{k'} x)^2 = 1$ (resp. $(r^{k'} s)^2 = 1$), on a $g^k x g^{k'} x = g^{k-k'}$ (resp. $r^k s r^{k'} s = r^{k-k'}$), d'où le résultat. Si $i' = 0$ on écrit $g^k x g^{k'}$ (resp. $r^k s r^{k'}$) sous la forme $g^k x g^{k'} xx$ (resp. $r^k s r^{k'} ss$) et on applique le calcul précédent.

On obtient ainsi un morphisme $G \longmapsto D_5$ qui est clairement injectif par définition, et qui réalise donc, vu l'égalité des cardinaux de G et D_5, un isomorphisme.

Si G est commutatif, on reprend le raisonnement de (b). Si $x^2 \neq 1$, x est d'ordre 10 et G est cyclique. Si $x^2 = 1$, x est alors d'ordre 2. Considérons alors $y = xg$ et soit n tel que $y^n = x^n g^n = 1$ soit $x^{-n} = x^n = g^n$. Si n était impair, on aurait $x \in H$ ce qui ne se peut pas car H ne contient pas d'éléments d'ordre 2. Ainsi n est pair et $g^n = 1$ soit 5 divise n et donc 10 divise n, de sorte que y est d'ordre 10, d'où le résultat.

Exercice 4.6.

Soit $Z(G)$ le centre de G ; c'est un groupe (abélien) d'ordre p^r avec $1 \leqslant r \leqslant k$ (Proposition 4.30). Le groupe $Z(G)$ étant distingué, le groupe quotient G/Z est un groupe d'ordre p^{k-r} auquel on peut appliquer l'hypothèse de récurrence. Donc si $i \geqslant r$, le groupe $G/Z(G)$ possède un sous-groupe d'ordre p^{i-r} (par hypothèse de récurrence). Si $\pi : G \to G/Z(G)$ désigne l'application canonique, $\pi^{-1}(x)$ est de

cardinal r (ordre de $Z(G)$) pour tout $x \in G/Z(G)$, et donc $\pi^{-1}(H)$ est un sous-groupe de G de cardinal $p^{i-r} \times p^r = p^i$.

Si $i \leqslant r$, il suffit de montrer que $Z(G)$ possède un sous-groupe d'ordre p^i, ce qui est clair puisqu'il est commutatif.

GROUPE SYMÉTRIQUE

Exercice 4.7.

L'ensemble des 5-cycles est en bijection avec les 5-uplets (a, b, c, d, e) d'éléments distincts modulo permutation circulaire, *i.e.* :

$$(a, b, c, d, e) \sim (b, c, d, e, a) \sim (c, d, e, a, b) \sim (d, e, a, b, c) \sim (e, a, b, c, d)$$

de sorte que chaque classe est constituée de 5 éléments. On obtient alors $\binom{5}{5}\frac{5!}{5}$ tels cycles, où $\binom{5}{5}$ est le coefficient binomial.

Pour les 4-cycles le même raisonnement donne $\binom{4}{5}3!$ et de manière générale le nombre de r-cycles dans $\mathcal{S}_n$ est $\binom{r}{n}(r-1)!$.

Exercice 4.8.

1. Soit c un p-cycle et soit $\overline{c}$ son image dans $\mathcal{S}_p/H$ qui n'est qu'un ensemble et n'est pas muni de structure de groupe car H n'est pas distingué. L'ensemble $\mathcal{S}_p/H$ étant de cardinal strictement inférieur à p, on en déduit qu'il existe $0 \leqslant i < j < p$ tel que $\overline{c^i} = \overline{c^j}$ de sorte qu'il existe $h \in H$ tel que $c^j = c^i h$ soit $c^{j-i} \in H$. Or p étant premier, il existe u et v tel que $u(j-i) + vp = 1$ de sorte que $c^{(j-i)u} = c \in H$ (car $c^p = Id$ puisque c est un p-cycle.

2. On calcule $(1\ 3\ 2\ 4 \cdots p)^{-1} \circ (1\ 2\ 3 \cdots\ p) = (1\ 3\ 2)$ de sorte que pour un 3-cycle quelconque $(a\ b\ c)$ on a $(a\ b\ c) = (a\ b\ c\ i_1 \cdots i_{p-3})^{-1} \circ (a\ c\ b\ i_1 \cdots i_{p-3})$ où $\{i_1, \cdots, i_{p-3}\} = \{1, \cdots, n\} \backslash \{a, b, c\}$.

3. Le groupe $\mathcal{A}_p$ étant engendré par les 3-cycles (exercice 4.8) qui d'après la question précédente appartiennent à H, on en déduit que $\mathcal{A}_p \subset H \subset \mathcal{S}_p$ de sorte que $\frac{p!}{2}$ divise le cardinal de H qui est lui-même un diviseur de $p!$. Comme H est un sous-groupe strict de $\mathcal{S}_p$, on en déduit alors que H est de cardinal $\frac{p!}{2}$ et donc que $\mathcal{A}_p = H$.

4. On applique ce qui précède au cas $p = 5$. Si H était un sous-groupe de $\mathcal{S}_5$ de cardinal 30 (resp. 40), il serait d'indice 4 (resp. 3) de sorte qu'il devrait contenir $\mathcal{A}_5$ ce qui ne se peut pas.

Exercice 4.9.

On trouve $\sigma = (1, 10, 4, 11, 6)(2, 7, 3, 9, 8, 5)$. L'ordre de σ est donc le ppcm de 5 et 6, soit 30 ; sa signature est -1.

Exercice 4.10.

1. On part du fait que $\mathcal{S}_n$ est engendré par les transpositions $(i\ j)$. La technique est alors de montrer que toutes ces transpositions appartiennent au sous-groupe engendré par les éléments que l'on considère.

(i) On a $(i\ j) = (1\ i) \circ (1\ j) \circ (1\ i)$; de plus pour $2 \leqslant i_0 \leqslant n$, i_0 est laissé fixe par toutes les transpositions $(1\ i)$ pour $i \neq i_0$ de sorte que $\mathcal{S}_n$ ne peut pas être engendré par un sous-ensemble strict de celui considéré.

(ii) Pour $1 \leqslant i < j-1 \leqslant n-1$, on a $(i\ j) = (j-1\ j) \circ (i\ j-1) \circ (j-1\ j)$, le résultat découle alors d'une récurrence simple sur $j - i$; soit $1 \leqslant i_0 < n$, l'intervalle $\{1, \cdots, i_0\}$ est laissé globalement stable par tous les éléments $(i, i+1)$ pour $i \neq i_0$, de sorte que $\mathcal{S}_n$ ne peut pas être engendré par un sous-ensemble strict de celui considéré.

(iii) On a $(i, i+1) = c_n^{i-1} \circ \tau \circ c_n^{-i+1}$; le résultat découle alors de (ii).

2. Le résultat est clair pour $n = 3$. Pour $n \geqslant 4$, si $a \neq b$ et $b \neq c$ alors $(a\ b) \circ (b\ c) = (a\ b\ c)$; ainsi si a, b, c, d sont deux à deux distincts, $(a\ b) \circ (c\ d) = (a\ b\ c) \circ (b\ c\ d)$, d'où le résultat.

3. Soit $T = \tau_1, \ldots, \tau_k$ un ensemble de k transpostions. Considérons le graphe Γ avec n sommets $P_1, \ldots, P_n$, une arête joignant P_i à P_j si et seulement si la transposition (i, j) est dans T. Le fait que T engendre S_n implique que Γ est connexe : il possède donc au moins $n-1$ arêtes, soit $k \geqslant n-1$.

Exercice 4.11.

On a $\sigma = (1\ 2\ 3) \circ (2\ 4) \circ (1\ 3)$ qui est bien une décomposition en cycles mais pas à supports disjoints ; on vérifie sans peine que $\sigma = (3\ 2\ 4)$. De même $(1\ 2\ \cdots\ n-1) \circ (1\ n) = (1\ n\ 2\ \cdots\ n-1)$.

Exercice 4.12.

Si $\sigma = c_1 \circ \cdots \circ c_r$ est la décomposition en cycles à supports disjoints de σ, chaque cycle est d'ordre sa longueur et ces cycles commutent car leurs supports sont disjoints, de sorte que l'ordre de σ est le ppcm des longueurs des cycles c_i pour $1 \leqslant i \leqslant r$. En particulier dans $\mathcal{S}_5$, on trouve que l'ordre maximal d'un élément est 6.

Exercice 4.13.

Soit $x \in \{1, \cdots, n\}$; déterminons le cycle de la décomposition de $\sigma = c^k$ auquel il appartient (on appelle ce cycle l'orbite de x sous c^k) :

$$(c^k)^i(x) = x \iff n | ki \iff \frac{n}{(n \wedge k)} | i$$

de sorte que l'orbite de x sous c^k est toujours de longueur $n/(n \wedge k)$. La décomposition en cycles à supports disjoints de c^k est donc constitué de $(n \wedge k)$ cycles de longueur $n/(n \wedge k)$.

OPÉRATION D'UN GROUPE SUR UN ENSEMBLE

Exercice 4.14.

1. On rappelle (théorème 4.31) que pour $n \geqslant 5$, $\mathcal{A}_n$ est simple et que les sous-groupes distingués de $\mathcal{S}_n$ sont $\{1\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$. On considère l'action par translations à gauche de $\mathcal{S}_n$ sur $\mathcal{S}_n/H$, ce qui donne un morphisme $\phi : \mathcal{S}_n \longmapsto \mathcal{S}(\mathcal{S}_n/H)$; $\mathcal{S}(\mathcal{S}_n/H)$ désigne le groupe des permutations de l'ensemble $\mathcal{S}_n/H$. Si $\sigma \in \ker\phi$, on a en particulier $\sigma H = H$, soit $\sigma \in H$, de sorte que $\ker\phi \subset H$; H étant d'indice n dans $\mathcal{S}_n$, $\ker\phi$ ne peut qu'être le sous-groupe trivial puisqu'il est distingué. Le sous-groupe $\phi(H)$ est ainsi un sous-groupe de cardinal $(n-1)!$ laissant stable l'élément $\overline{Id}$ (la classe de H), de sorte que $\phi(H)$ est inclus dans un sous-groupe de $\mathcal{S}(\mathcal{S}_n/H)$ qui est isomorphe à $\mathcal{S}_{n-1}$; par cardinalité on en déduit $H \simeq \mathcal{S}_{n-1}$.

2. On considère de même l'action par translation à gauche de $\mathcal{S}_n$ sur $\mathcal{S}_n/H$ ce qui donne un morphisme de groupe $\mathcal{S}_n \longmapsto \mathcal{S}_k$ qui pour des raisons évidentes de cardinalité ($k < n$) ne peut être injectif ; or le noyau étant un sous-groupe distingué contenu dans H car stabilisant la classe de l'identité, on en déduit $\mathcal{A}_n \subset H$ et donc comme $k > 1$, $H = \mathcal{A}_n$.

Exercice 4.15.

Le groupe H agit sur l'ensemble G/H des classes à gauche de G modulo H par translation à gauche : $(h, xH) \mapsto hxH$.

Soient n le nombre des H-orbites distinctes de G/H, et $(\Omega_k)_{1\leqslant k\leqslant n}$ ces orbites. On a

$$|G/H| = p = \sum_{1\leqslant k\leqslant n} |\Omega_k|. \quad (1)$$

Par ailleurs, pour tout k compris entre 1 et n, le cardinal de Ω_k est égal à 1 ou p : en effet, le cardinal de Ω_k divise $|H|$, $|H|$ divise $|G|$ et p est le plus petit diviseur premier de l'ordre de G. Toutes les orbites sont en fait de cardinal 1. En effet, dans le cas contraire, il n'y aurait d'après (1) qu'une seule orbite de cardinal p, ce qui n'est pas, car l'orbite de H est réduite à $\{H\}$. Il en résulte que le stabilisateur de tout élément de G/H est H tout entier. Considérons alors un élément a de G. Pour tout élément h de H on a donc $haH = aH$; ainsi $a^{-1}Ha$ est contenu dans H, et donc H est distingué dans G.

Exercice 4.16.

1. L'équation aux classes s'écrit :

$$n = a_1 + 3a_2 + 7a_3 + 21a_4 \quad (3)$$

où a_1 (resp. a_2, resp. a_3, resp. a_4) désigne le nombre de classes de cardinal 1 (resp. 3, resp. 7, resp. 21). Pour $n = 19$, a_4 est forcément nul et si par ailleurs on impose a_1 nul, l'équation (3) s'écrit $3a_2 + 7a_3 = 19$ ce qui impose $a_3 = 1$ et $a_2 = 4$, soit 5 orbites dont une de cardinal 7 et 4 de cardinal 3.

2. Pour $n = 11$, a_4 est aussi nul. Par ailleurs l'équation $3a_2 + 7a_3 = 11$ n'a pas de solutions entières de sorte que a_1 ne peut pas être nul, *i.e.* il existe au moins un point fixe.

3. Il suffit de montrer que tout entier $n \geqslant 12$ peut s'écrire $3a + 7b$ avec $a, b \geqslant 0$. Or c'est vrai pour 12, 13 et 14 et donc pour tout entier plus grand en rajoutant un multiple de 3.

EXEMPLES LIÉS À LA GÉOMÉTRIE

Exercice 4.17.

$(i) \Rightarrow (ii)$. Supposons que f soit une symétrie par rapport à un sous-espace vectoriel F de E. Notons $F^\perp$ l'orthogonal de F. On a $E = F \bigoplus F^\perp$. Par définition, la restriction de f à F est l'identité et la restriction de f à $F^\perp$ est moins l'identité. Par suite, on a $f \circ f = \mathrm{Id}_E$ (où Id_E est l'identité de E).

$(ii) \Rightarrow (iii)$. Supposons $f \circ f = \mathrm{Id}_E$. Le polynôme minimal de f divise alors $X^2 - 1 \in \mathbf{R}[X]$. Ses racines étant réelles et simples, f est donc diagonalisable.

$(iii) \Rightarrow (i)$. Supposons f diagonalisable. Il s'agit de démontrer que f est une symétrie de E. Puisque f est une isométrie, ses seules valeurs propres possibles sont -1 et 1. D'après l'hypothèse faite, E est somme directe des sous-espaces propres de f. On a ainsi

$$E = \ker(f - \mathrm{Id}_E) \bigoplus \ker(f + \mathrm{Id}_E).$$

Par ailleurs, les sous-espaces vectoriels $\ker(f - \mathrm{Id}_E)$ et $\ker(f + \mathrm{Id}_E)$ sont orthogonaux. En effet, si x et y sont des éléments respectivement de $\ker(f - \mathrm{Id}_E)$ et $\ker(f + \mathrm{Id}_E)$, on a les égalités

$$(x|y) = \big(f(x)|f(y)\big) = (x| - y) = -(x|y),$$

d'où $(x|y) = 0$. Il en résulte que $\ker(f - \mathrm{Id}_E)$ est contenu dans $\ker(f + \mathrm{Id}_E)^\perp$. Puisqu'ils ont tous les deux pour dimension la codimension de $\ker(f + \mathrm{Id}_E)$, on a donc l'égalité $\ker(f - \mathrm{Id}_E) = \ker(f + \mathrm{Id}_E)^\perp$. Par suite, f est la symétrie par rapport à $\ker(f - \mathrm{Id}_E)$.

Exercice 4.18.

Considérons une symétrie f par rapport à un plan H transformant a en b. On a $f(a) = b$, $f(b) = a$, d'où $f(a - b) = b - a$, de sorte que $a - b$ appartient à la droite $H^\perp$ (l'orthogonal de H). Puisque a et b sont distincts, on a donc $H^\perp = \mathbf{R}(a - b)$. Il en résulte que l'on a nécessairement $H = \mathbf{R}(a - b)^\perp$. Inversement, soit S la symétrie de E par rapport à $\mathbf{R}(a - b)^\perp$. Il s'agit de vérifier que l'on a $S(a) = b$. Les normes de a et b étant les mêmes, on a les égalités

$$(a + b|a - b) = ||a||^2 - ||b||^2 = 0.$$

On en déduit que $a + b$ appartient à $\mathbf{R}(a - b)^\perp$, d'où $S(a + b) = a + b$. On a par ailleurs $S(a - b) = b - a$. L'égalité

$$a = \frac{1}{2}\big((a + b) + (a - b)\big),$$

entraîne alors le résultat.

Exercice 4.19.

Notons (e_1, e_2, e_3) la base canonique de $\mathbf{R}^3$ et Id l'identité de $\mathbf{R}^3$. L'espace $\mathbf{R}^3$ est muni de sa structure euclidienne pour laquelle (e_1, e_2, e_3) est une base orthonormée.

1. On vérifie que ${}^tMM$ est la matrice identité, ce qui prouve que u est une isométrie. Le déterminant de u étant égal à 1, u est donc une isométrie directe.

2. On vérifie que le noyau de $u - \mathrm{Id}$ est la droite engendrée par le vecteur $e_2 + e_3$. Le plan H orthogonal à cette droite a pour équation $y+z = 0$ et une base est (e_1, e_2-e_3). Il en résulte que le système

$$B = \Big(\frac{e_2 + e_3}{\sqrt{2}}, e_1, \frac{e_2 - e_3}{\sqrt{2}}\Big),$$

est une base orthonormée de $\mathbf{R}^3$. L'endomorphisme u fixe la droite engendrée par $e_2 + e_3$, en particulier H est stable par u. La restriction de u à H est une isométrie de H. Puisque le déterminant de u vaut 1, on en déduit que la restriction de u à H est une isométrie directe de H. La matrice de u dans B est donc de la forme

$$M' := \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix},$$

où $\theta \in \mathbf{R}$. La trace de M étant nulle, on a $2\cos\theta + 1 = 0$ *i.e.* $\cos\theta = -1/2$. Déterminons $\sin\theta$. Soit P la matrice de passage de la base canonique à la base B. Les bases (e_1, e_2, e_3) et B étant orthonormées, P est une matrice orthogonale, autrement dit, on a ${}^tP = P^{-1}$. On a donc l'égalité $M' = {}^tPMP$. On obtient ainsi

$$M' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix},$$

d'où $\sin\theta = \sqrt{3}/2$.

TROIS POLYÈDRES RÉGULIERS ET LEURS GROUPES

Exercice 4.20. *Le tétraèdre régulier*

1. L'isobarycentre O du tétraèdre est invariant par tout élément de $\mathcal{I}_T$ de sorte que l'application $vect : g \in \mathcal{I}_T \mapsto \vec{g} \in O(3)$ définie par $\vec{g}(\vec{v}) = Og(\vec{M})$ où M est tel que $\vec{OM} = \vec{v}$ est un morphisme de groupes injectif.

2. Une application affine est déterminée par les images de 4 points non coplanaires. Tout élément de $\mathcal{I}_T$ permute les 4 sommets, de sorte que l'on a une injection $i : \mathcal{I}_T \longmapsto \mathcal{S}_4$.

3. Il suffit de vérifier que la transposition (12) est dans l'image de i ; en effet toute transposition est alors dans l'image et comme les transpositions engendrent $\mathcal{S}_4$, i sera alors un isomorphisme. La transposition (12) est l'image par i de la réflexion par

rapport au plan médiateur du segment $[1, 2]$. Le sous-groupe $\mathcal{D}_T$ étant d'indice 2, il en est de même de son image soit $\mathcal{D}_T \simeq \mathcal{A}_4$.

Exercice 4.21. *Le cube*

1. Comme dans l'exercice précédent, on a une injection $i : \mathcal{I}_C \hookrightarrow \mathcal{S}_8$. L'indice $[\mathcal{I}_C : \mathcal{D}_T]$ est égal à 2 ou 1 selon que $\mathcal{I}_C$ contient ou non une isométrie négative ; clairement la réflexion par rapport à un plan qui coupe le cube en deux selon le milieu de 4 arêtes parallèles appartient à $\mathcal{I}_C \backslash \mathcal{D}_C$ de sorte que $[\mathcal{I}_C : \mathcal{D}_C] = 2$.

2. On remarque que les grandes diagonales sont les plus grandes distances entre deux éléments du cubes et sont donc conservées par toute isométrie. On obtient ainsi un morphisme $f : \mathcal{I}_C \longmapsto \mathcal{S}_4$. Soit alors $g \in \ker f$. On vérifie aisément que $g = \pm Id$. Pour montrer la surjectivité, il suffit comme précédemment de montrer que la transposition (12) est obtenue. Notons $abcd$ les sommets de la face du dessus du cube et $a'b'c'd'$ les points de la face du dessous de sorte que les grandes diagonales soient aa', bb', cc' et dd'. La réflexion par rapport au plan contenant aa' et la direction orthogonale à la face du dessus a pour image la transposition qui échange bb' et dd' et laisse fixe aa' et cc'. On obtient ainsi que f induit un isomorphisme de $\mathcal{D}_C$ sur $\mathcal{S}_4$.

Exercice 4.22. *L'octaèdre*

On remarque que le dual du dual d'un point (resp. d'un plan) est le même point (resp. plan). Ainsi le dual du cube est l'octaédre. En outre toute isométrie préserve le produit scalaire, de sorte qu'une isométrie conservant une figure, conserve aussi la figure duale. On en déduit alors que le groupe de l'octaèdre est celui du cube.

Remarque : Le tétraèdre est autodual.

PROBLÈMES

Problème 4.1.

1. Un élément x de G est dans $\ker \phi$, si et seulement si, pour tout $g \in G$, $xg \in gH$ ou de manière équivalente, $x \in gHg^{-1}$, d'où le résultat.

2. On fait agir H sur $E = G/H$ par translation à gauche ; l'équation aux classes s'écrit $p = \sum_{x \in \mathcal{O}} |x|$, où $\mathcal{O}$ désigne l'ensemble des orbites. On sépare cette somme en deux en différenciant les orbites de cardinal 1 : $p = k + \sum_{x \in \mathcal{O}^1} [G : G_x]$, où $\mathcal{O}^1$ est l'ensemble des orbites de cardinal supérieur strictement à 1, et G_x est le stabilisateur d'un élément quelconque de l'orbite x ; G_x est un sous-groupe de G et d'après le théorème de Lagrange, $[G : G_x]$ est un diviseur de $|G|$ et est donc supérieur ou égal à p. Or on a $k \geqslant 1$ car H est stable sous l'action de H ; ainsi $\mathcal{O}^1$ est vide, soit toutes les orbites sont de cardinal 1, *i.e.* $H = H_1$ et donc H est distingué dans G.

3. *Cf.* l'exercice 4.1.

4. Le raisonnement est strictement identique à celui de l'exercice 4.5, 1.

5. Même preuve que dans l'exercice 4.5, 2.

6. *Cf.* l'exercice 4.5, 3.

Problème 4.2. (*« Jeu de taquin »*)

1. On remarque qu'une opération élémentaire correspond, dans $\mathcal{S}_{16}$, à une transposition et fait passer la case vide, numérotée 16, d'une case marquée (resp. non marquée) à une case non marquée (resp. marquée), de sorte qu'au bout de n opérations élémentaires la signature de la permutation obtenue est $(-1)^n$ et la case 16 se trouve sur une case non marquée pour n impair et marquée pour n pair.

Ainsi si la case vide se retrouve en position initiale, la signature de la permutation obtenue est forcément égale à 1 de sorte qu'il est impossible d'obtenir la transposition $(14\ 15)$ et de gagner la fortune promise.

2. (i) On obtient le 3-cycle $(11\ 15\ 12)$.

(ii) Pour obtenir les autres 3-cycles de l'énoncé, il suffit de faire glisser la case vide dans la bonne position et d'opérer les manipulations de l'énoncé pour obtenir le nouveau 3-cycle, puis de ramener la case vide dans sa position initiale. On illustre se principe dans le cas de $(9\ 13\ 10)$.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

1	2	3	4
5	6	7	8
9	10	11	12
13		14	15

1	2	3	4
5	6	7	8
10	13	11	12
9		14	15

1	2	3	4
5	6	7	8
10	13	11	12
9	14	15	

(iii) On rappelle que $\mathcal{A}_{15}$ est engendré par les 3-cycles. Le principe est alors d'écrire tout 3-cycle $(i\ j\ k)$ comme un produit de 3-cycles $(1\ 2\ s)$. L'idée est de considérer des conjugués ; par exemple pour i, j, k distincts et distincts de 1 et 2, on a : $(1\ 2\ i)(1\ 2\ j)(1\ 2\ i)^{-1} = (2\ i\ j)$ et $(1\ 2\ k)(2\ i\ j)(1\ 2\ k)^{-1} = (k\ i\ j)$ d'où le résultat.

(iv) D'après (iii), $\mathcal{A}_5$ est engendré par les 3-cycles $(2\ 1\ i)$ pour $3 \leqslant i \leqslant 15$. Par ailleurs, pour un mouvement autorisé on peut revenir en arrière et l'on peut enchaîner deux mouvements autorisés ; le sous-ensemble cherché est ainsi évidemment un sous-groupe de $\mathcal{A}_5$. Il suffit donc de montrer que l'on peut obtenir tous les $(2\ 1\ i)$. À nouveau, on considère des conjugaisons des éléments dont on dispose. Ainsi en conjugant $(2\ 1\ 6)$ avec $(5\ 9\ 6)$, $(5\ 9\ 6)^{-1}$, $(6\ 10\ 7)$, $(6\ 11\ 7)$, $(6\ 7\ 3)$ et $(6\ 7\ 3)^{-1}$, on obtient respectivement $(2\ 1\ 5)$, $(2\ 1\ 9)$, $(2\ 1\ 10)$, $(2\ 1\ 11)$, $(2\ 1\ 7)$ et $(2\ 1\ 3)$. En conjuguant $(2\ 1\ 3)$ (resp. $(2\ 1\ 11)$, resp. $(2\ 1\ 10)$) avec $(3\ 8\ 4)$ et $(3\ 8\ 4)^{-1}$ (resp. $(11\ 15\ 12)$, resp. $(10\ 14\ 11)$, $(9\ 13\ 10)$ et $(9\ 13\ 10)^{-1}$), on obtient $(2\ 1\ 8)$ et $(2\ 1\ 4)$ (resp. $(2\ 1\ 15)$, resp. $(2\ 1\ 14)$, $(2\ 1\ 9)$ et $(2\ 1\ 13)$), d'où le résultat.

3. La condition de parité du point (i) est le seul impératif. En effet, il suffit de décider d'un chemin pour faire passer la case vide de la position initiale (celle de (i)) à la position cherchée, ce qui induit une bijection de l'ensemble des configurations avec la case vide en position initiale avec l'ensemble des configurations avec la case vide à la position considérée, d'où le résultat.

Ainsi, si on remonte le jeu au hasard, on a une chance sur deux de tomber juste.

Solutions des exercices du chapitre 5

POLYNÔMES

Exercice 5.1.

On a $a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_0 q^n = 0$ de sorte que p (resp. q) divise $a_0 q^n$ (resp. $a_n p^n$), et comme $(p \wedge q) = 1$, p (resp. q) divise a_0 (resp. a_n) par le lemme de Gauss.

Ainsi les solutions rationnelles de $P(X) = 3X^3 + 4X^2 + 2X - 4$ sont à chercher avec $p = 1, 2, 4$ et $q = 1, 3$; on vérifie alors que $2/3$ est solution et $P(X) = 3(X - 2/3)(X^2 + 2X + 2)$. Le polynôme $X^2 + 2X + 2$ est irréductible sur $\mathbf{R}$, donc sur $\mathbf{Q}$, et possède deux racines complexes.

Exercice 5.2.

On raisonne par récurrence sur le degré de P ; le résultat est évident pour P de degré 1. Supposons le résultat vrai pour tout polynôme de degré inférieur ou égal à n et soit P de degré $n+1$. On note $\Delta = (P \wedge P')$ de degré supérieur ou égal à 1 par hypothèse car $\Delta(x) = 0$. Ainsi Δ divise P et donc P n'est pas irréductible ($\deg \Delta < \deg P$). Soit donc $P = QR$ dans $\mathbf{Q}[X]$ avec Q et R de degré inférieur à n.

Pour un polynôme P et x une racine, notons $\nu_P(x)$ la multiplicité de la racine x. On a par hypothèse $\nu_P(x) = \nu_Q(x) + \nu_R(x) > (n+1)/2$ et donc soit $\nu_Q(x) > (\deg Q)/2$, soit $\nu_R(x) > (\deg R)/2$ et par hypothèse de récurrence $x \in \mathbf{Q}$.

Exercice 5.3.

On écrit $P = P'Q$ avec Q de degré 1, soit $Q(X) = a(X-\alpha)$ et $P(X) = aP'(X)(X-\alpha)$. En dérivant k fois cette égalité, on obtient $P^{(k)}(X) = aP^{(k+1)}(X)(X-\alpha)+kaP^{(k)}(X)$ et pour $k < \deg P$ on a $ak \neq 1$ car sinon $P^{(k+1)}$ serait le polynôme nul, ce qui n'est pas. En évaluant en α, l'expression précédente on obtient $P^{(k)}(\alpha) = 0$ pour $k < \deg P$. La formule de Taylor pour le polynôme P donne alors :

$$P(X) = P(\alpha) + P'(\alpha)(X-\alpha) + \cdots + P^{(\deg P-1)}(\alpha)\frac{(X-\alpha)^{\deg P-1}}{(\deg P-1)!} +$$

$$P^{(\deg P)}(\alpha)\frac{(X-\alpha)^{\deg P}}{(\deg P)!} = \frac{P^{(\deg P)}(\alpha)}{(\deg P)!}(X-\alpha)^{\deg P}.$$

Réciproquement on vérifie immédiatement qu'un polynôme de la forme aX^n est divisible par son polynôme dérivé.

Exercice 5.4.

En regardant les coefficients dominants et en notant que, dans $\mathbf{R}$, l'égalité $a^2+b^2 = 0$ est équivalente à $a = b = 0$, on obtient que $\deg P$ est pair. On raisonne alors par récurrence sur le degré $2n$ de P. Pour $n = 1$, on a $aX^2+bX+c = a(X+\frac{b}{2a})^2+(c-\frac{b^2}{4a})$. Par ailleurs comme la limite en $+\infty$ de P est positive, on en déduit $a > 0$ et comme $P(0) \geqslant 0$ on obtient aussi $c - \frac{b^2}{4a} \geqslant 0$ qui est donc de la forme δ^2 de sorte que aX^2+bX+c est bien de la forme Q^2+R^2 avec $Q(X) = \sqrt{a}(X-\frac{b}{2a})$ et $R(X) = \delta$.

Supposons donc le résultat acquis jusqu'au rang $n-1$ et traitons le cas de $\deg P = 2n$. On considère la factorisation de $P = \prod_i (X-\lambda_i)^{n_i}\prod_j D_j(X)^{m_j}$ où D_j est un polynôme irréductible de degré 2 sur $\mathbf{R}$. S'il existe j tel que m_j est non nul, le polynôme $\frac{P(X)}{D_j(X)}$ est alors de degré inférieur à $2(n-1)$ et vérifie la condition de l'énoncé de sorte qu'il existe Q_1 et R_1 tel que $\frac{P}{D_j} = Q_1^2+R_1^2$. D'après le cas $n = 1$, il existe aussi Q_2 et R_2 tels que $D_j = Q_2^2+R_2^2$. On considère alors l'identité remarquable de Lagrange (*cf.* le problème (1.4))

$$(a^2+b^2)(c^2+d^2) = (ab-cd)^2+(ad+bc)^2$$

de sorte que $P = Q^2+R^2$ avec $Q = Q_1Q_2-R_1R_2$ et $R = Q_1R_2+R_1Q_2$.

De la même façon s'il existe i tel que $n_i \geqslant 2$ est pair, on remarque que $Q(X) := \frac{P(X)}{(X-\lambda_i)^2}$ vérifie les hypothèses ; on a en effet $P(x) = Q(x)(x-\lambda_i)^2$ de sorte que pour tout $x \neq \lambda_i$, on a $Q(x) \geqslant 0$. En outre Q étant un polynôme, est continu de sorte que $Q(\lambda_i) \geqslant 0$. On conclut alors comme précédemment, en appliquant l'hypothèse de récurrence et l'identité de Lagrange.

Le dernier cas à étudier est celui où $P(X)$ est scindé à racines simples. On remarque alors qu'au passage d'une racine α, P change de signe car $P(X)$ est équivalent, au voisinage de α à $P'(\alpha)(X-\alpha)$. Un tel P ne vérifie pas l'hypothèse de l'énoncé.

Exercice 5.5.

On utilise la formule de Taylor $P(X) = P(a)+(X-a)P'(a)+\cdots+\frac{(X-a)^n}{n!}P^{(n)}(a)$ qui est une égalité car P est un polynôme de degré n. On en déduit donc que $P(x) > 0$ pour tout $x > a$.

Exercice 5.6.

Si x est une racine multiple de P, on a alors $P(x) = P'(x) = 0$ soit $1 + x + \cdots + \frac{x^n}{n!} = 1 + x + \cdots + \frac{x^{n-1}}{(n-1)!} = 0$ soit $x^n = 0$ et donc $x = 0$ qui ne convient pas.

Exercice 5.7.

On a $P'(X) = 6X(X^4 - 5X^3 + 10X^2 - 10X + 4)$ et X étant premier avec $P(X)$, on calcule alors le PGCD δ de $P(X)$ avec $X^4 - 5X^3 + 10X^2 - 10X + 4$ selon l'algorithme d'Euclide :

$$\begin{aligned}\delta &= \big((P(X) - (X^2 + X)(X^4 - 5X^3 + 10X^2 - 10X + 4)\big)\wedge \\ &\qquad\qquad \big(X^4 - 5X^3 + 10X^2 - 10X + 4)\big) \\ &= (X^2 - 2X + 2) \wedge (X^4 - 5X^3 + 10X^2 - 10X + 4) \\ &= (X^2 - 2X + 2)\wedge \\ &\qquad (X^4 - 5X^3 + 10X^2 - 10X + 4 - (X^2 - 3X)(X^2 - 2X + 2)) \\ &= X^2 - 2X + 2\end{aligned}$$

Comme $X^2 - 2X + 2$ divise à la fois $P(X)$ et $P'(X)$, on en déduit que $(X^2 - 2X + 2)^2$ divise P. On effectue alors la division et on obtient finalement $P(X) = (X^2 - 2X + 2)^2(X^2 - 2X - 1)$.

Exercice 5.8.

On a $X^2 - 2\cos\theta X + 1 = (X - e^{i\theta})(X - e^{-i\theta})$ et on évalue le polynôme en question en $e^{i\theta}$ et $e^{-i\theta}$: $e^{in\theta}\sin\theta - e^{i\theta}\sin(n\theta) + \sin(n-1)\theta = a + ib$ avec $a = \sin\theta\cos(n\theta)-\cos\theta\sin(n\theta)+\sin(n-1)\theta = 0$ et $b = \sin(n\theta)\sin\theta-\sin\theta\sin(n\theta) = 0$. Ainsi $(X-e^{i\theta})$ et $(X-e^{-i\theta})$ divisent $X^n\sin\theta-X\sin(n\theta)+\sin(n-1)\theta$ et donc aussi le ppcm de $(X - e^{i\theta})$ et $(X - e^{-i\theta})$ qui est égal au produit $(X - e^{i\theta})(X - e^{-i\theta})$ car le pgcd $((X - e^{i\theta}), (X - e^{-i\theta})) = 1$.

On calcule facilement par récurrence $X^n\sin\theta - X\sin(n\theta) + \sin(n-1)\theta = (X^2-2\cos\theta X+1)(X^{n-2}\sin(n\theta)+X^{n-3}\sin(2\theta)+\cdots+X^{n-k}\sin(k-1)\theta)+\Delta_k$ avec $\Delta_k = \sin(k\theta)X^{n-k+1} - \sin(k-1)\theta X^{n-k} - X\sin(n\theta) + \sin(n-1)\theta$.

Exercice 5.9.

Au lieu de prendre la base $(1, X, X^2)$ de $\mathbf{C}_2[X]$, on choisit la base $(1, X - a, (X-a)(X-b))$ et on évalue en a et b. On écrit ainsi $P(X) = Q(X)(X-a)(X-b) + \alpha + \beta(X - a)$. En évaluant en a on trouve $\alpha = P(a)$ puis en évaluant en b on obtient finalement $P(X) = Q(X)(X - a)(X - b) + P(a) + \frac{P(b)-P(a)}{b-a}(X - a)$.

RACINES DES POLYNÔMES À COEFFICIENTS COMPLEXES

Exercice 5.10. Posons $M = \sup_{0\leqslant i\leqslant d-1}\left(d\frac{|a_i|}{|a_d|}\right)^{1/d-i}$. Soit $z \in \mathbf{C}$ tel que $|z| > M$ alors, pour $0 \leqslant i < d$, on a $|a_i| < \frac{|a_d|}{d}|z|^{d-i}$ et donc $|a_{d-1}z^{d-1} + \cdots + a_0| < |a_d z^d|$ soit $P(z) \neq 0$.

Exercice 5.11.

1. Soit $z \in \mathbf{C}$ une racine de P' et supposons $P(z) \neq 0$; on écrit $\frac{P'(z)}{P(z)} = \sum_{i=1}^n \frac{1}{z-z_i} = 0$ soit en « multipliant par la quantité conjuguée » : $\sum_{i=1}^n \frac{\overline{z-z_i}}{|z-z_i|^2} = 0$ d'où $\sum_{i=1}^n \frac{z-z_i}{|z-z_i|^2} = 0$. On a donc $z = \frac{\sum_{i=1}^n \frac{z_i}{|z-z_i|^2}}{\sum_{i=1}^n \frac{1}{|z-z_i|^2}}$ et z est un barycentre à coefficients strictement positifs des z_i et appartient donc à l'enveloppe convexe des z_i.

2. On pose $Q(z) = (P(z) - \omega_1)^{n_1}(P(z) - \omega_2)^{n_2}$ et donc

$$Q'(z) = (n_1+n_2)P'(z)(P(z)-\omega_1)^{n_1-1}(P(z)-\omega_2)^{n_2-1}[P(z)-(\frac{n_1\omega_2+n_2\omega_1}{n_1+n_2})]$$

Soit alors $E = \{\omega \in \mathbf{C} \,/\, \{z \,/\, P(z) = \omega\} \subset K\}$; ainsi pour tous $\omega_1, \omega_2 \in E$ et tous $n_1, n_2 \in \mathbf{N}^*$, on a $\{z \,/\, P(z) = \frac{n_1\omega_2+n_2\omega_1}{n_1+n_2}\} \subset \{z \,/\, Q'(z) = 0\}$. Or $\{z \,/\, Q'(z) = 0\}$ est inclus dans l'enveloppe convexe des zéros de $P(z) - \omega_1$ et $P(z) - \omega_2$ et donc contenu dans K car K est convexe. On conclut alors par un petit argument de topologie en utilisant le fait que $\mathbf{Q}$ est dense dans $\mathbf{R}$.

RACINES DES POLYNÔMES À COEFFICIENTS RÉELS

Exercice 5.12.

Soit $P(X) = a_n X^n + \cdots + a_0$ avec $a_n \neq 0$ et $a_0 \neq 0$. Supposons que P ne s'annule pas sur $\mathbf{R}^+$ de sorte que $a_0 = P(0)$ est du même signe que a_n car la limite de P en $+\infty$ est $a_n(+\infty)$. On en déduit alors que V_P, qui est égal au nombre de changements de signe entre a_0 et a_n est pair, d'où le lemme de Descartes dans ce cas. Supposons le résultat acquis pour tout polynôme possédant strictement moins de n racines réelles positives. Soit alors $\alpha > 0$ une racine de P et considérons $P(X) = (X - \alpha)Q(X)$ avec $Q(X) = b_{n-1}X^{n-1} + \cdots + b_0$ de sorte que

$$\left\{\begin{array}{l} a_n = b_{n_1} \\ a_{n-1} = b_{n-2} - \alpha b_{n-1} \\ \vdots \\ a_i = b_{i-1} - \alpha b_i \\ \vdots \\ a_1 = b_0 - \alpha b_1 \\ a_0 = -\alpha b_0 \end{array}\right.$$

On remarque tout d'abord que les égalités $a_n = b_{n-1}$ et $a_0 = -\alpha b_0$ avec $\alpha > 0$, impliquent que $V(P) \equiv V(Q) + 1 \mod 2$. Il ne reste alors plus qu'à montrer que $V(P) \geqslant V(Q)$. On remarque d'abord que a_0 et b_0 sont de signes contraires. Considérons un changement de signes dans la suite des b_i : $b_{i-1}, 0, \ldots, O, b_j, \ldots..$ avec $j \geqslant i$ et b_j de signe contraire à celui de b_{i-1}. On voit alors que a_i est du signe de b_{i-1}, ce qui implique que $V(P) \geqslant V(Q)$, d'où le résultat.

Exercice 5.13.

Si x est une racine d'un $P^{(i)}$ pour $i > 0$ avec $P(x) \neq 0$, alors $V(x^+) - V(x^-)$ est un nombre négatif pair ; en effet soit $[i, i + r] \subset [1, d - 1]$ un segment tel que $P^{(j)}(x) = 0$ pour $i \leqslant j \leqslant i + r$ et $P^{(i-1)}(x)P^{(i+r+1)} \neq 0$, on remarque que $i + r < d$ car $P^{(d)}$ est une constante non nulle, on a alors $P^{(i+k)}(x + h) = h^{r+1-k}P^{(i+r+1)}(x) + o(h^2)$ de sorte le nombre de changements de signes de la sous-suite $(P^{(i)}(x^-), \cdots, P^{(i+r+1)}(x^-))$ est maximal tandis que celui de $(P^{(i)}(x^+), \cdots, P^{(i+r+1)}(x^+))$ est minimal, de sorte que la différence du nombre de changements de signes de la sous-suite $(P^{(i-1)}, \cdots, P^{(i+r+1)})$ est négatif ou nul. On conclut alors aisément que $V(x^+) - V(x^-)$ est négatif ou nul ; ce nombre est de plus pair car les signes des deux extrémités $P, P^{(d)}$ est le même en x^- et x^+ et que le signe de $P^{(d)}(x)$ est égal au signe de $P(x)$ multiplié par $(-1)^{V(x)}$.

Si x est une racine de P d'ordre r, le même raisonnement permet de conclure que $V(x^-) - V(x^+)$ est égal à $k + 2l$ pour un certain entier l.

On en déduit alors facilement l'énoncé de l'exercice. Le lemme de Descartes correspond alors au calcul de $V(0) - V(+\infty)$.

Exercice 5.14.

On pose $G(x) = e^{-\alpha_0 x}F(x)$; les zéros de G sont les mêmes que ceux de F ; on raisonne alors par récurrence sur la somme m des degrés des P_i, le premier cas, $m = 0$ étant une application directe du lemme de Rolle, comme dans la démonstration du lemme de Descartes ; par hypothèse de récurrence $G^{(d_0)}$ a alors au plus $\sum_{i=1}^{n} d_i + (n - 1)$ zéros réels de sorte que d'après le théorème de Rolle G a au plus $\sum_{i=0}^{n} d_i + n$ zéros réels.

Exercice 5.15.

D'après le lemme de Descartes, le nombre de racines réelles positives est inférieur à $V(P) = V(-13\times6, -14\times6, -7\times13, 1) = 1$ tout en y étant congru modulo 2, ce qui donne donc exactement 1 racine positive. En ce qui concerne les racines réelles négatives, on considère le polynôme $P(-X) = X^{14} - 7\times13X^2 + 14\times6X - 13\times6$ de sorte que le nombre de racines négatives est inférieur à $V(P(-X)) = V(-13 \times 6, 14 \times 6, -7 \times 13, 1) = 3$ tout en y étant congru modulo 2 ce qui donne une ou trois racines réelles négatives.

Afin de déterminer le nombre de racines négatives, on applique la règle de Sturm : on a $P'(X) = 14(X^{13} - 13X - 6)$ de sorte que modulo P', on a $X^{13} \equiv 13X + 6$ soit

$P(X) \equiv X(13X+6)-7\times 13X^2-14\times 6X-13\times 6 \equiv -13\times 6(X^2+X+1) \mod P'$. On pose $P_1 = 13.6(X^2+X+1)$ de sorte que $X^3 \equiv 1 \mod P_1$ et donc $X^{13} \equiv X \mod P_1$ de sorte que $P' \equiv -14(X-13X+6) \equiv -14\times 6(2X+1) \mod P_1$. On pose $P_2 = 14\times 6(2X+1)$ de sorte que $P_1 \equiv 13\times 6((-1/2)^2+(-1/2)+1) \equiv 13\times 6\times 3/4 \mod P_2$. La règle de Sturm donne alors que le nombre de racines réelles négatives de P est égale à $V(P,P',-\infty) - V(P,P',0) = V(1,-14\times 13.6,-12\times 3/4) - V(-13\times 6,-6\times 14,13\times 6,12\times 3/4) = 4-1 = 3$. On retrouve par ailleurs que le nombre de racines réelles positives est égale à

$$V(P,P',0) - V(P,P',+\infty) = V(-13\times 6,-6\times 14,13\times 6,12\times 3/4) \\ -V(1,14,13\times 6,12\times 3/4) = 1-0 = 1$$

RÉSULTANT, DISCRIMINANT

Exercice 5.16.

L'équation algébrique est donnée par le résultant des polynômes à coefficient dans $\mathbf{Q}[x,y]$, $t^2+t+1-x$ et $t^2-1)-y(t^2+1)$, soit :

$$\begin{vmatrix} 1 & 1 & 1-x & 0 \\ 0 & 1 & 1 & 1-x \\ 1-y & 0 & -1-y & 0 \\ 0 & 1-y & 0 & -1-y \end{vmatrix}$$

c'est-à-dire $y^2x^2 - 2yx^2 + (y+x)^2 - 2x + 3 = 0$.

Exercice 5.17.

L'ensemble cherché est le lieu où le discriminant du polynôme caractéristique est non nul ; cela définit donc un ouvert dans l'ensemble des matrices identifié à $\mathbf{R}^{n^2}$.

Exercice 5.18.

1. Il s'agit de calculer le déterminant suivant :

$$\begin{vmatrix} q & p & 0 & 1 & 0 \\ 0 & q & p & 0 & 1 \\ p & 0 & 3 & 0 & 0 \\ 0 & p & 0 & 3 & 0 \\ 0 & 0 & p & 0 & 3 \end{vmatrix}$$

On peut par exemple faire les manipulations suivantes sur les lignes : $L_5 \leftarrow L_5 - 3L_2$ et $L_4 \leftarrow L_4 - 3L_1$ ce qui donne le déterminant suivant :

$$\begin{vmatrix} q & p & 0 & 1 & 0 \\ 0 & q & p & 0 & 1 \\ p & 0 & 3 & 0 & 0 \\ -3q & -2p & 0 & 0 & 0 \\ 0 & -3q & -2p & 0 & 0 \end{vmatrix}$$

qui vaut $4p^3 + 27q^2$.

2. On suppose pour commencer $p \neq 0$. En notant que $X^2 \equiv -p/3 \mod (3X^2+p)$, on obtient $X^3+pX+q \equiv \frac{2pX}{3}+q \mod (3X^2+p)$ soit $P_1(X) = -(\frac{2pX}{3}+q)$. Ensuite on a $3X^2+p \equiv 3(\frac{-3q}{2p})^2+p \equiv \frac{27q^2+4p^3}{4p^2} \mod P_1$. Ainsi P et P' sont premiers entre eux si et seulement si $27q^2+4p^3 \neq 0$ de sorte que $P(X) = X^3+pX+q$ et P' ont une racine commune si et seulement si $27q^2+4p^3 = 0$. On en déduit que le discriminant est égal à $27q^2+4p^3$.

Pour $p = 0$, on a $X^3+q \equiv q \mod (3X^2)$ de sorte que $P(X) = X^3+q$ et P' ont une racine commune si et seulement si $q = 0$, soit si et seulement si $27q^2 = 0$, d'où le résultat.

Exercice 5.19.

On considère donc $P_X(Y)$ et $Q_X(Y)$ comme des polynômes à coefficients dans $\mathbf{C}[X]$. Le résultant est alors donné par le déterminant

$$\begin{vmatrix} 1 & -X & X^2-1 & 0 \\ 0 & 1 & -X & X^2-1 \\ 1 & -1 & 2X^2-2 & 0 \\ 0 & 1 & -1 & 2X^2-2 \end{vmatrix}$$

Un calcul aisé nous donne alors $3X(X^2-1)(X-1)$.

Les points d'intersection cherchés ont pour abscisse $0, 1$ et -1 ce qui donne, en calculant Y, les points $(0,-1)$, $(1,0)$, $(1,1)$ et $(-1,0)$, soit 4 points réels (on rappelle que le théorème de Bézout donne 4 points dans le plan projectif *a priori* non réels).

Exercice 5.20.

1. Le résultant est donné par le déterminant

$$\begin{vmatrix} 1 & b & X^2+c \\ 1 & X^2+g & 0 \\ 0 & 1 & X^2+g \end{vmatrix}$$

soit $X^4+(2g-b+1)X^2+(g^2-bg+c)$: c'est évidemment ce que l'on trouve en éliminant Y dans les deux équations. On pose dans la suite $\alpha = 2g-b+1$ et $\beta = g^2-bg+c$.

2. Si on veut 4 points de même abscisse, *i.e.* $P(X) = X^4+\alpha X^2+\beta = (X-x_0)^4$, il faut $x_0 = 0$ ce qui revient à imposer $\alpha = \beta = 0$.

3. Pour avoir 4 racines réelles il faut et il suffit que l'équation $Z^2+\alpha Z+\beta = 0$ ait deux racines réelles positives, soit $\delta = \alpha^2-4\beta \geqslant 0$, $\beta \geqslant 0$ et $\alpha \leqslant 0$ (la somme des racines et le produit doivent être positifs).

En utilisant la règle de Sturm (*cf.* le théorème (5.18), on effectue les divisions euclidiennes suivantes :

$$X^4 + \alpha X^2 + \beta = (4X^3 + 2\alpha X)\frac{X}{4} - (-X^2\frac{\alpha}{2} - \beta)$$

$$4X^3 + 2\alpha X = (-X^2\frac{\alpha}{2} - \beta)(-X\frac{8}{\alpha}) - (-X\frac{2\delta}{\alpha})$$

$$-X^2\frac{\alpha}{2} - \beta = (-X\frac{2\delta}{\alpha})X\frac{\alpha^2}{4\delta} - \beta$$

de sorte que $V(P, P', -\infty) = V(1, -4, -\alpha/2, 2\delta\alpha, \beta)$ et $V(P, P', +\infty) = V(1, 4, -\alpha/2, -2\delta/\alpha, \beta)$. Si on veut 4 racines réelles il faut $V(P, P', -\infty) - V(P, P', +\infty) = 4$ soit $V(P, P', -\infty) = 4$ et $V(P, P', +\infty) = 0$ soit $\alpha \leqslant 0$, $\delta \geqslant 0$ et $\beta \geqslant 0$.

Exercice 5.21.

1. Le système d'équations $A(X) = B(Y - X) = 0$ possède comme solutions les couples $(x_a, x_b + x_a)$ où x_a (resp. x_b) décrit les solutions de $A(X) = 0$ (resp. $B(X) = 0$). On considère alors les polynômes $A(X)$ et $B(Y - X)$ comme des polynômes à valeurs dans $K[Y]$ et on introduit leur résultant qui est un polynôme en Y dont les zéros sont d'après ce qui précède, exactement les sommes des zéros de A avec ceux de B.

2. Appliquons ce qui précède à $A(X) = X^2 - 2$ et $B(X) = X^3 - 7$. Le résultant en question est donné par le déterminant

$$\begin{vmatrix} 1 & 0 & -2 & 0 & 0 \\ 0 & 1 & 0 & -2 & 0 \\ 0 & 0 & 1 & 0 & -2 \\ -1 & 3Y & -3Y^2 & Y^3 - 7 & 0 \\ 0 & -1 & 3Y & -3Y^2 & Y^3 - 7 \end{vmatrix}$$

soit après calcul $Y^6 - 6Y^4 - 14Y^3 + 12Y^2 - 84Y + 41$.

FONCTIONS SYMÉTRIQUES DES RACINES

Exercice 5.22.

1. L'inégalité proposée découle directement de la concavité du logarithme : pour n nombres réels positifs) (a_i) $1 \leqslant i \leqslant n$, on a $\frac{\ln a_1 + \cdots + \ln a_n}{n} \leqslant \ln \frac{a_1 + \cdots + a_n}{n}$, d'où le résultat en prenant les exponentielles des deux membres.

2. Quitte à factoriser par une puissance de X, on suppose $P(0) \neq 0$ et on écrit $P(X) = X^n - \sigma_1 X^{n-1} + \cdots + (-1)^n \sigma_n$ avec $\sigma_n \neq 0$. On applique alors (a) ce qui donne $(\sigma_n^2)^{1/n} \leqslant \frac{\sigma_1^2 - 2\sigma_2}{n} \leqslant 3/n$, d'où $n \leqslant 3$. Une inspection cas par cas donne $X \pm 1$, $X^2 \pm X - 1$, $X^3 + X^2 - X - 1$ et $X^3 - X^2 - X + 1$.

Exercice 5.23.

On a $\alpha+\beta+\gamma+\delta=2=2(\alpha+\beta)$, $\alpha\beta\gamma\delta=1=-(\alpha\beta)^2$ de sorte que α,β (resp. γ,δ) sont les racines de X^2-X+i (resp. X^2-X-i). En outre on a $(\beta+\alpha)(\gamma+\delta)+(\alpha\beta+\gamma+\delta)=-a=1$ et $\alpha\beta(\gamma+\delta)+\gamma\delta(\alpha+\beta)=b=0$. Finalement $(\alpha,\beta,\gamma,\delta)$ sont les racines de $X^4-2X^3-X^2-1$ qui se factorise sous la forme $(X^2-X+i)(X^2-X-i)$; on les calcule alors par la formule du binôme.

Exercice 5.24.

Une CNS pour que ABC soit rectangle isocèle en A est $b-a=\pm i(c-a)$, soit $(b-a)^2+(c-a)^2=0$, i.e. $b^2+c^2+2a^2=2a(b+c)$. En outre on a $a+b+c=0$, $abc=-q$ et $ab+ac+bc=p$. Le but est alors d'éliminer dans la CNS a,b,c et de les remplacer par p et q ; on a $a^2+b^2+c^2=(a+b+c)^2-2p=-2p$ de sorte que la CNS s'écrit $-2p+a^2=-2a^2$ soit $3a^2=2p$. Or on a $a^3=-pa+q\neq 0$ de sorte que la CNS s'écrit $-3pa+3q=2pa$, soit $a=\frac{3q}{5p}$. Ainsi l'équation $3a^2=2p$ devient $27q^2-50p^3=0$.

Exercice 5.25.

Les relations de Newton donnent

$$\left\{\begin{array}{l} 2=s_1^2-2s_2\\ 2=s_1^3-3s_2s_1+3s_3\\ 2=s_1^4-4s_2s_1^2+4s_3s_1+2s_2^2\end{array}\right.$$

ce qui donne

$$\left\{\begin{array}{l} s_2=s_1^2/2-1\\ 3s_3=2-s_1^3+3s_1(s_1^2/2-1)\\ s_1(s_1^3/6-2s_1+8/3)=0\end{array}\right.$$

Les racines de $X^3-12X+16$ étant 2 et -4, on obtient alors $s_1=0,2,-4$ et donc $s_2=-1,1,7$ et $s_3=2,0,-6$. Les triplets (x,y,z) sont alors les racines des polynômes X^3-X-2, $\quad X^3-2X^2+X$, $\quad X^3+4X^2+7X+6$.

PROBLÈMES

Problème 5.1.

1. Soit $l_i(X)=\prod_{0\leqslant j\neq i\leqslant n}\frac{(X-a_j)}{a_i-a_j}$ et soit $P(X)=\sum_{i=0}^n b_il_i(X)$ qui est donc de degré inférieur ou égal à n. On a alors $P(a_i)=b_i$ pour tout $i=0,\cdots,n$.

Montrons alors l'unicité d'une telle solution dans $\mathbf{C}_n[X]$. Si P et Q sont des polynômes de degré $\leqslant n$ prenant la valeur b_i au point a_i ($0\leqslant i\leqslant n$, le polynôme $P-Q$ est de degré $\leqslant n$ et a $n+1$ racines, il est donc identiquement nul.

2. (i) La réponse est évidemment négative comme on peut le constater dans le cas $Q(X)=X$ et $P(X)=X^2$.

(ii) On note n_i (resp. m_i) la multiplicité de α_i (resp. β_i) dans P (resp. dans $P-1$). On a alors $\sum_{i=1}^{r} n_i = \sum_{i=1}^{s} m_i$. Par ailleurs si $n_i \geqslant 2$ (resp. $m_i \geqslant 2$), alors α_i (resp. β_i) est une racine de P' de multiplicité $n_i - 1$ (resp. $m_i - 1$). Par ailleurs comme les α_i sont distincts de β_j, on en déduit alors l'inégalité

$$\sum_{i=1}^{s}(m_i - 1) + \sum_{i=1}^{r}(n_i - 1) \leqslant \deg P - 1$$

soit $2\deg P - r - s \leqslant \deg P - 1$ et donc $r + s \geqslant \deg P + 1$.

(iii) On considère le polynôme $R = P - Q$ de sorte que les α_i et les β_i sont des racines de R. D'après la question précédente, on a ainsi $r + s > \deg R$ racines ce qui impose que R soit le polynôme nul.

Problème 5.2.

1. Le polynôme $\sum_{i=0}^{n-1} P(i)L_i(X) - P(X)$ est dans $\mathbf{Q}_{n-1}[X]$ et appartient à l'intersection des noyaux $\ker f_i$ où f_i est la forme linéaire $P \in \mathbf{Q}_n[X] \mapsto P(i) \in \mathbf{Q}$. Or la famille des $(f_i)_{0\leqslant i\leqslant n-1}$ est libre ; en effet étant donnée une relation $\sum_i \lambda_i f_i = 0$, en la testant sur L_i, on obtient $\lambda_i = 0$. Ainsi l'espace vectoriel $\bigcap_{i=0}^{n-1} \ker f_i$ est de dimension nulle de sorte que $P(X) = \sum_{i=0}^{n-1} P(i)L_i(X)$.

2. Comme précédemment soit $R \in \mathbf{Q}_{n-1}[X]$ tel que $R(i) = P(i)$ pour tout $0 \leqslant i \neq i_0 \leqslant n-1$. Ainsi $P - R$ appartient à $\bigcap_{\substack{0\leqslant i\leqslant n-1 \\ i\neq i_0}} \ker f_i$ qui est de dimension 1 engendré par $\prod_{0\leqslant i\neq i_0\leqslant n-1}(X - i)$ de sorte qu'il existe $\lambda \in \mathbf{Q}$ tel que $R(X) = P(X) + \lambda \prod_{i\neq i_0}(X - i)$; or R est à coefficients dans $\mathbf{Z}$ de sorte que $\lambda \in \mathbf{Z}$. Ainsi pour le coefficient constant de R on obtient $s_0 + (-1)^{n-1}\lambda\frac{n!}{i_0}$ où $\lambda \in \mathbf{Z}$ est non déterminé ; on connaît alors s_0 à un multiple de $\frac{n!}{i_0}$ près. Si $p < \frac{n!}{i_0}$, alors s_0 est connu.

3. On travaille cette fois-ci dans $\mathbf{Z}/p\mathbf{Z}[X]$ et comme dans *2.*, le coefficient constant d'un R tel que $R(i) = P(i)$ pour tout $i \neq i_0$ est de la forme $s_0 + \lambda\frac{n!}{i_0}$ où $\lambda \in \mathbf{Z}/p\mathbf{Z}$ est indéterminé. Or $\frac{n!}{i_0}$ est inversible dans $\mathbf{Z}/p\mathbf{Z}$, de sorte que lorsque λ décrit $\mathbf{Z}p\mathbf{Z}$, $s_0 + \lambda\frac{n!}{i_0}$ aussi.

4. Le code est s_0. On tire au sort les s_i, et on transmet $P(i)$ modulo p à la personne numérotée i. D'après (2), les n personnes réunies peuvent reconstituer s_0 alors que d'après *3.*, $n-1$ quelconques ne le peuvent pas.

5. De la même façon soit $P(X) = \sum_{i=0}^{k-1} s_i X^i$ et on transmet $P(i)$ à la personne i pour $1 \leqslant i \leqslant n$. Comme précédemment, k personnes quelconques peuvent reconstituer P et donc s_0 alors que $k-1$ quelconques ne le peuvent pas

> ***Remarque :*** Si une personne mal intentionnée i_0 transmet une mauvaise valeur distincte de $P(i_0)$ alors que toutes les autres transmettent leur $P(i)$, la personne i_0 sera la seule à connaître le code s_0. Bien sûr, s'il y en a deux qui trichent, personne ne sait rien.

Problème 5.3.

1. On a $D(Q) = \prod_{i<j}(\alpha_i - \alpha_j)^2$, les α_i étant les racines (réelles ou non) de Q. Si $\alpha_i \neq \alpha_j$, le terme $(\alpha_i - \alpha_j)^2$ (si α_i et α_j son réelles) ou $(\alpha_i - \alpha_j)^2\overline{\alpha_i} - \overline{\alpha_j})^2$ (si au moins l'une des deux n'est pas réelle) est positif. Les seuls termes négatifs du produit sont donc ceux de la forme $\alpha_i - \overline{\alpha_i}$ pour α_i non réel, d'où la formule demandée.

2. Il suffit d'envisager séparément les cas $s = 1$ et $s = -1$.

3. Si $d = 3$, on a $r \equiv s + 2 \bmod 4$. Donc si $s = +1$, il il y 3 racines réelles, et si $s = -1$ il n'y en a qu'une seule.

4. La suite de Sturm est : $R_0 = Q = X^3 + pX + q$, $R_1 = Q' = 3X^2 + p$, $R_2 = -\frac{2pX}{3} - q$, $R_3 = -p - \frac{27q^2}{4p^2} = \frac{1}{4p^2}(-4p^3 - 27q^2) = \frac{1}{4p^2}D(Q)$. Si on note V la variation de cette suite, on a pour $D(Q) > 0$ la suite de signes $(- + - +)$ en $-\infty$ (car p est alors nécessairement < 0) et $(+ + + +)$ en $+\infty$, d'où $V(_\infty) = 3$ et $V(+\infty) = 0$; dans ce cas là, le polynôme Q a donc 3 racines réelles. Si au contraire $D(Q) < 0$ (et donc $4p^3 + 27q^2 > 0$), on trouve $(- + \pm -)$ en $-\infty$ (le signe $\pm$ étant le signe de p) et $(+ + \pm -)$ en $+\infty$ d'où $V(-\infty) = 2$ et $V(+\infty) = 1$ quel que soit le signe de p, et il y a dans ce cas une racine réelle.

Problème 5.4.

1. L'égalité correspond à dire que la partie réelle de $e^{inx} = (e^{ix})^n = (\cos(x) + i\sin(x))^n$ est égale à $\cos(nx)$.

2. La règle de Riemann justifie la convergence en ± 1. Pour le calcul de $< T_i|T_j >$ on effectue le changement de variable $x = \cos t$ de sorte que $\frac{dx}{\sqrt{1-x^2}} = dt$ ce qui donne $< T_i|T_j >= \int_0^\pi \cos(it)\cos(jt)dt$. Par ailleurs on a $2\cos(it)\cos(jt) = \cos(i+j)t + \cos(i-j)t$ et pour $k \neq 0$, $\int_0^\pi \cos ktdt = 0$ d'où le résultat. On remarquera que la base n'est pas orthogonale car on calcule aisément $||T_0||^2 = \pi$ et $||T_i||^2 = \pi/2$ pour $i \neq 0$.

3. (a) On remarque que pour t tel que $\cos nt = 0$, $\cos(t)$ est racine de $T_n(X)$. Ainsi pour $t_i = \pi/2n + i\pi/n$ pour $0 \leqslant i < n$, $\cos(t_i)$ est racine de $T_n(X)$. Par ailleurs les angles t_i sont distincts deux à deux et appartiennent à l'intervalle dans $[0, \pi]$ sur lequel $\cos$ réalise une bijection avec $[-1, 1]$, de sorte que les $\cos(t_i)$ sont n-racines réelles distinctes de $T_n(X)$ qui étant de degré n, n'en possède pas d'autres :

$$T_n(X) = \gamma_n \prod_{i=0}^{n-1}(X - \cos(\frac{\pi}{2n} + i\frac{\pi}{n})).$$

Remarque : On peut aussi raisonner de manière générale.
Soit $T_n(X) = \prod_i (X - \lambda_i)^{n_i} \prod_j D_j(X)$, la factorisation de T_n, où les D_i sont des polynômes de degré 2 irréductibles sur $\mathbf{R}$. On considère alors le polynôme

$$S(X) = \prod_{i \equiv 1 \mod 2} (X - \lambda_i).$$

Si T_n n'est pas scindé à racines simples, $S(X)$ est alors de degré strictement inférieur à n de sorte que $< T_n|S >= 0$ alors que ce dernier est l'intégrale sur $[-1,1]$ d'une fonction positive non nulle, d'où la contradiction.

(b) Il s'agit du polynôme d'interpolation de Lagrange : $L_{n,Q} = \sum_i Q(x_i)l_i$ où $l_i = \prod_{1\leqslant j\neq i\leqslant n} \frac{(X-x_j)}{(x_i-x_j)}$.

(c) $Q - L_{n,Q}$ s'annule aux points x_i et est donc divisible par $\prod_{i=1}^n (X-x_i) = T_n/\gamma_n$, d'où l'existence de S. On écrit alors $Q(X) = \sum_i Q(x_i)l_i(X) + S(X)T_n(X)$. On a alors $\varphi(Q) = \sum_i Q(x_i)\lambda_i + < S|T_n >$ avec $\lambda_i = \varphi(l_i)$ et $< S|T_n >= 0$ car T_n est orthogonal à $\mathbf{R}_{n-1}[X]$ et donc à S.

On applique ce qui précède à $l_i(X)^2$ qui est de degré $2n-2$, de sorte que $\varphi(l_i^2) = \lambda_i$ qui est donc strictement positif.

Commentaire du résultat : soient n points y_i quelconques et soient δ_{y_i} la forme linéaire définie par $P \mapsto P(y_i)$. On dispose alors de $n+1$ formes linéaires $\varphi, \delta_{y_1}, \cdots, \delta_{y_n}$. Celles-ci sont alors liées quand on les considère comme des formes linéaires sur $\mathbf{R}_{n-1}[X]$ car cet espace est de dimension n. Sur $\mathbf{R}_{2n-1}[X]$, qui est de dimension $2n$, il est *a priori* étonnant qu'elles soient liées. Nous verrons à la question suivante que cela ne se produit que pour les points x_i définis ci-dessus et que l'on appelle les points de Gauss.

(d) On a $\varphi(T_n^2) > 0$ alors que la somme $\sum_{i=1}^n \lambda_i T_n(x_i)^2$ est nulle. Ainsi l'égalité précédente n'est pas valable sur $\mathbf{R}_{2n}[X]$. Le résultat est par ailleurs valable quels que soit les points x_i, *i.e.* avec n points d'interpolation, une égalité comme dans la question précédente ne peut pas être vraie sur $\mathbf{R}_{2n}[X]$.

4. Les y_i sont forcément distincts sinon cela contredirait (d). En regardant les égalités données sur $1, X, \cdots, X^{n-1}$, on obtient une matrice de Vandermonde A telle que $A(\nu_i) = (\varphi(X^i))$ de sorte que les ν_i sont uniquement déterminés et comme précédemment strictement positifs. En appliquant à nouveau pour $T_n, XT_n, \cdots, X^{n-1}T_n$, on obtient $A(\nu_i T_n(y_i)) = 0$. La matrice A étant inversible, on en déduit alors que pour tout i, $\nu_i T_n(y_i) = 0$. Or les ν_i sont non nuls, sinon comme précédemment on aurait strictement moins de n points d'interpolation ce qui contredirait (d). On en déduit donc que pour tout i, $T_n(y_i) = 0$ et donc que les y_i sont les racines de T_n.

Problème 5.5.

1. On rappelle que $\Phi_n(X)$ est le produit des $X-\xi$ où ξ décrit l'ensemble des racines primitives n-ièmes de l'unité soit $\Phi_n(X) = \prod_{\substack{k\wedge n=1\\ 1\leqslant n\leqslant n}} (X - e^{2ik\pi/n})$ qui est donc un polynôme de degré $\phi(d)$. Pour ξ une racine n-ième de l'unité le groupe qu'il engendre est un sous-groupe cyclique d'ordre d divisant n des racines n-ièmes de l'unité, de sorte que $X^n - 1 = \prod_{d|n} \Phi_d(X)$. En regardant les degrés, on obtient $n \sum_{d|n} \phi(d)$.

2. On a $\Phi_1(X) = X-1$, $\Phi_2(X) = X+1$, $\Phi_3(X) = X^2+X+1$, $\Phi_4(X) = X^2+1$ et $\Phi_8(X) = X^4+1$.

3. On calcule Φ_n par récurrence en utilisant l'égalité $\Phi_n(X) = \frac{X^n-1}{\prod_{\substack{d|n \\ d\neq n}} \Phi_d(X)}$ et donc $\Phi_n(X) \in \mathbf{Q}[X]$. En outre par récurrence, les $\Phi_d(X)$ sont des polynômes de $\mathbf{Z}[X]$ unitaires, de sorte que l'égalité précédente nous donne que $\Phi_n(X)$ est aussi à coefficients dans $\mathbf{Z}$ et unitaire.

4. Comme Φ_n et P sont premiers entre eux et unitaires, on en déduit qu'il existe $A, B \in \mathbf{Z}[X]$ tels que $A\Phi_n + BP = 1$. En écrivant $2 \leqslant \Phi_n(k!) = (k!)^{\phi(n)} + \cdots + a_1(k!) + 1$, pour k assez grand, on en déduit que l'ensemble des diviseurs premiers de $\{\Phi_n(x) \ / \ x \in \mathbf{Z}\}$ est infini. Soit donc p divisant $\Phi_n(x)$ alors $p \geqslant k$ divise $x^n - 1$ et ne divise pas $P(x)$ soit p ne divise pas $x^d - 1$ pour $n \neq d$ divisant n. Ainsi l'ordre de x dans $\mathbf{Z}/p\mathbf{Z}$ est exactement n qui divise donc $p - 1$, soit $p \equiv 1 \mod n$.

Solutions des exercices du chapitre 6

FACTORISATION DES POLYNÔMES

Exercice 6.1.

(i) $\Rightarrow$ (ii) : parmi les facteurs irréductibles de P, il y en a au moins un de degré inférieur ou égal à $\frac{d}{2}$, soit Q. On considère alors $L = K[X]/(Q(X))$; comme Q est irréductible, L est un sur-corps de K de degré $r = \deg Q \leqslant \frac{d}{2}$ de sorte qu'en notant x l'image dans $\mathbf{F_{q^r}}$ de la classe de X dans L, on a $Q(x) = 0$ et donc $P(x) = 0$.

(ii) $\Rightarrow$ (i) : soit $x \in L$ une racine de P. On rappelle que le polynôme minimal q_x de x sur K est, par définition, le générateur de l'idéal principal des polynômes $Q \in K[X]$ tels que $Q(x) = 0$. Par ailleurs $K/(q_x(X))$ est un sous-corps de L tel que $[K[X]/(q_x(X)) : K] = \deg q_x$ soit un diviseur de $[L : K]$. Ainsi $P(X)$ est divisible par $q(X)$ qui constitue ainsi un diviseur irréductible de degré inférieur ou égal à $\frac{\deg P}{2}$.

Exercice 6.2.

Les polynômes irréductibles de degré 1 sont X et $X-1$; ceux de degré 2 sont tels que $X^4-X = X(X-1)P$ (corollaire 6.34), ce qui donne X^2+X+1. Pour ceux de degré 3, on a $X^8 - X = X(X-1)P_1P_2$ et on trouve $X^3 + X + 1$ et $X^3 + X^2 + 1$. Enfin pour ceux de degré 4, on a $X^{16} - X = (X^4 - X)Q_1Q_2Q_3$ et on trouve $X^4 + X + 1$, $X^4 + X^3 + X^2 + X + 1$ et $X^4 + X^3 + 1$. Ces polynômes sont irréductibles sur $\mathbf{F_2}$ car un élément j de $\mathbf{F_4}$ qui n'est pas dans $\mathbf{F_2}$ vérifie $j^3 = 1$ de sorte qu'il ne peut être racine des polynômes en question.

Exercice 6.3.

Pour la première question, il suffit de recopier la démonstration de la remarque 6.22.

Pour la seconde, on a $X^{16} - X = (X^4 - X)Q_1Q_2Q_3$ (exercice 6.2), avec $Q_1 = X^4 + X + 1,\ Q_2 = X^4 + X^3 + X^2 + X + 1, Q_3 = X^4 + X^3 + 1$.

Notons $0, 1, j, j^2$ les éléments de $\mathbf{F_4}$ avec $1 + j + j^2 = 0$. Les polynômes de degré 1 sont $X, X-1, X-j, X-j^2$ de produit X^4-X. En ce qui concerne le degré 2, on voit en appliquant la question 1. que X^4+X+1, $X^4+X^3+X^2+X+1$ et X^4+X^3+1 doivent s'écrire chacun comme le produit de deux polynômes irréductibles de degré deux sur $\mathbf{F_4}$. On trouve alors $X^4 + X + 1 = (X^2 + X + j)(X^2 + X + j^2)$, $X^4 + X^3 + 1 = (X^2 + jX + j)(X^2 + j^2X + j^2)$ et $X^4 + X^3 + X^2 + X + 1 = (X^2 + jX + 1)(X^2 + j^2X + 1)$.

Exercice 6.4.

1. On note $(1, -1, 0)$ les éléments du corps $\mathbf{F_3}$. On vérifie rapidement que $Q(0)$, $Q(1)$ et $Q(-1)$ ne sont pas nuls de sorte que Q n'a pas de racine dans $\mathbf{F}_3$. On cherche alors ses racines dans $\mathbf{F}_9$. Pour $a \in \mathbf{F}_9$, on a $a^9 = a$ de sorte que $a^9 - a + 1 = 1$ et donc Q n'a pas de racine dans $\mathbf{F}_9$.

2. Afin de calculer dans $\mathbf{F}_{27}$, on commence par le décrire concrètement : on vérifie aisément que $X^3 - X - 1$ n'a pas de racines dans $\mathbf{F}_3$ et est donc irréductible sur $\mathbf{F}_3$ ce qui implique $\mathbf{F}_{27} \simeq \mathbf{F}_3[X]/(X^3 - X - 1)$.

3. Soit alors $\alpha \in \mathbf{F}_{27}$ tel que $\alpha^3 = \alpha + 1$. On a alors $\alpha^9 = \alpha^3 + 1 = \alpha + 2 = \alpha - 1$ et donc finalement α est une racine de Q dans $\mathbf{F}_{27}$ de sorte que Q est divisible par X^3-X-1, polynôme minimal de α sur $\mathbf{F_3}$. Cela donne $X^9-X+1 = (X^3-X-1)$ $(X^6 + X^4 + X^3 + X^2 - X - 1)$.

4. Cherchons de manière générale toutes les racines de Q dans $\mathbf{F}_{27}$; d'après (b), un élément quelconque de $\mathbf{F}_{27}$ s'écrit sous la forme $x = a\alpha^2 + b\alpha + c$ avec $a, b, c \in \mathbf{F}_3$. On a alors $x^9 = a\alpha^{18} + b\alpha^9 + c$ avec $\alpha^9 = \alpha - 1$ et donc $\alpha^{18} = \alpha^2 + \alpha + 1$ de sorte que $x^9-x+1 = a\alpha+a-b+1$ ce qui impose $a = 0$ et $b = 1$ soit $x = \alpha, \alpha+1, \alpha-1$.

5. On en déduit alors que $X^6 + X^4 + X^3 + X^2 - X - 1$ n'a pas de racines dans $\mathbf{F}_{27}$; cela implique qu'il est irréductible sur $\mathbf{F_3}$, car sinon il aurait un facteur irréductible de degré 1, 2 ou 3 et donc une racine dans $\mathbf{F_3}$, $\mathbf{F_9}$ ou $\mathbf{F_{27}}$.

Exercice 6.5.

Si P est réductible sur $\mathbf{F_p}$, il l'est sur toute extension $\mathbf{F_{p^n}}$. Supposons donc P irréductible sur $\mathbf{F_p}$ de sorte que P a d racines dans $\mathbf{F_{p^d}}$ et aucune n'appartient à un sous-corps strict (remarque 6.27). On regarde alors P comme un polynôme dans $\mathbf{F_{p^n}}[X]$ dont on se demande s'il est encore irréductible. Il faut regarder s'il possède ou non des racines dans $\mathbf{F_{p^{nr}}}$ pour $r \leqslant d/2$ (exercice 6.1) et donc si $\mathbf{F_{p^d}} \subset \mathbf{F_{p^{nr}}}$; cela signifie que d divise nr ce qui est possible si et seulement si d et n ne sont pas premiers entre eux. En outre en notant $\delta = d \wedge n$, les facteurs irréductibles sont alors de degré r un multiple de d/δ.

La décomposition en facteurs irréductibles d'un polynôme de degré 5 donne en prenant les degrés les décompositions suivantes de $5 : 5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1$. Si on veut être sûr d'avoir toutes les racines (resp. au moins une racine) il faut donc se placer dans $\mathbf{F}_{\mathbf{P}^{60}}$ (resp. $\mathbf{F}_{\mathbf{P}^{10}}$) avec $60 = 5.4.3$ (resp. $10 = 5.2$).

Exercice 6.6.

Le polynôme $P = X^4 + 1$ est irréductible sur $\mathbf{Q}$ (donc sur $\mathbf{Z}$) car sa décomposition en facteurs irréductibles unitaires sur $\mathbf{R}$ n'est pas à coefficients dans $\mathbf{Q}$ ($X^4 + 1 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$).

Modulo 2, on a $X^4 + 1 = (X + 1)^4$ et pour $p \neq 2$, le groupe $\mathbf{F}_{p^2}^*$ est cyclique d'ordre $p^2 - 1$ qui est divisible par 8. Soit alors $x \in \mathbf{F}_{p^2}^*$ d'ordre 8, on a $x^8 = (x^4)^2 = 1$ et $x^4 \neq 1$ soit $x^4 = -1$ de sorte que P a une racine dans $\mathbf{F}_{p^2}$ et donc P est réductible modulo p (exercice 6.1). On a ainsi un exemple d'un polynôme irréductible sur $\mathbf{Z}$ et réductible modulo tout nombre premier p.

Exercice 6.7.

1. – Modulo 2, on a $\overline{P} = X^4 + X^2 + 1$ que l'on factorise facilement en $(X^2 + X + 1)^2$.

– Modulo 3, on a $\overline{P} = X^4 - X^3 - X - 1$ qui n'a pas de racine dans $\mathbf{F}_3$. On regarde alors dans $\mathbf{F}_9$, qui en remarquant que $X^2 + 1$ n'a pas de racines dans $\mathbf{F}_3$, est alors isomorphe à $\mathbf{F}_3[X]/(X^2 + 1)$. Notons i l'image de X dans $\mathbf{F}_9$ par l'isomorphisme $\mathbf{F}_3[X](X^2 + 1) \longrightarrow \mathbf{F}_9$. On a alors $i^4 = 1$ et $i^3 = -i$ de sorte que $\overline{P}(i) = 0$. On en déduit alors que $\overline{P}$ est divisible par $X^2 + 1$ et on calcule le quotient $X^2 - X - 1$ qui, ne possédant pas de racine sur $\mathbf{F}_3$, est irréductible sur $\mathbf{F}_3$, d'où la factorisation $\overline{P} = (X^2 + 1)(X^2 - X - 1)$.

2. Il suffit de montrer que P est irréductible sur $\mathbf{Z}$. Sur $\mathbf{Z}$, P n'a pas de racine car sinon il en aurait modulo 2 ce qui n'est pas. Si P était réductible, on aurait alors $P(X) = (X^2 + aX + b)(X^2 + cX + d)$ et donc

$$\begin{cases} a + c = -10 \\ b + d + ac = 21 \\ ad + bc = -10 \\ bd = 11 \end{cases}$$

Ainsi on obtient soit $\{b, d\} = \{1, 11\}$ et donc $ac = 9$ et $\{a, c\} = \{-1, -9\}$ car $a+c = -10$, et $ad+bc \neq -10$; soit $\{b, d\} = \{-1, -11\}$ et $ac = 33$ et $a+c \neq -10$. Ainsi P est irréductible sur $\mathbf{Z}$.

CORPS FINIS

Exercice 6.8.

1. Le groupe multiplicatif $\mathbf{F}_{23}^*$ est cyclique, (proposition 6.1), et donc isomorphe à $(\mathbf{Z}/22\mathbf{Z}, +)$, de sorte que l'ordre d'un élément distinct de 1 est 2, 11 ou 22.

2. On a $5^2 \equiv 2 \mod 23$ de sorte que 5 n'est pas d'ordre 2. Pour calculer 5^{11}, on propose d'écrire 11 en base 2, *i.e.* $11 = 2^3 + 2^1 + 2^0$ et de calculer 5^{2^i} pour $i \leqslant 3$ de sorte que $5^{11} = 5^{2^3}5^{2^1}5^{2^0}$, ce qui donne : $5^{2^4} = (5^2)^2 \equiv 2^2 \mod 23$ et $5^{2^3} \equiv 4^2 \mod 23$. On obtient alors $5^{11} \equiv 16.2.5 \mod 23$ soit $5^{11} \equiv -1 \mod 23$.

3. On déduit de (b) que 5 est d'ordre 22 et engendre donc $\mathbf{F}_{23}^*$.

Exercice 6.9.

1. – De manière évidente $P_1(X_1, \cdots, X_s) = X_1$.

– De l'égalité $\sum_{i=1}^s \alpha_i^2 = (\sum_{i=1}^s \alpha_i)^2 - 2\sum_{1\leqslant i<j\leqslant s} \alpha_i\alpha_j$, on déduit que $P_2(X_1, X_2) = X_1^2 - 2X_2$.

– On calcule de même $\sum_{i=1}^s \alpha_i^3 = (\sum_{i=1}^s \alpha_i)^3 - 3\sum_{1\leqslant i\neq j\leqslant s} \alpha_i^2\alpha_j)$ ce qui donne $P_3(X_1, X_2, X_3) = X_1^3 - 3(X_1X_2 - 3X_3)$.

2. On rappelle que les $x \in \mathbf{F}_q$ sont les racines du polynôme $X^q - X$ de sorte que $\sigma_1 = \cdots = \sigma_{q-2} = \sigma_q = 0$ et $(-1)^{q-1}\sigma_{q-1} = -1$ dans $\mathbf{F}_p$. Pour i divisible par $q-1$, on a $x^i = 1$ pour tout $x \in \mathbf{F}_q^*$ puisque $x^{q-1} = 1$, d'où $\psi(i) = 0 + (q-1).1 = -1$ dans $\mathbf{F}_q$. De manière générale, le même argument montre que $\psi(i) = \psi(r)$ où r est le reste de la division euclidienne de i par $q-1$. Par ailleurs, pour $1 \leqslant r \leqslant q$, $\psi(r)$ est un polynôme en les σ_k pour $1 \leqslant k \leqslant i$ de sorte que $\psi(i) = 0$ si i n'est pas congru à 0 modulo $q-1$.

Exercice 6.10.

1. Le sous-anneau de $\mathbf{F}_{p^n}$ engendré par a est un sous-corps isomorphe à $\mathbf{F}[X]/(q_a(X))$ qui est isomorphe à $\mathbf{F}_{p^{\deg q_a}}$ de sorte que $\deg q_a$ divise n.

2. L'application de Frobenius $Fr : x \mapsto x^p$ est un automorphisme du corps $\mathbf{F}_{p^n}$ qui laisse stable le sous-corps $\mathbf{F}_p$. On applique alors le Fr à l'égalité $q_a(a) = 0$ ce qui donne $q_a(a^p) = 0$, car q_a étant à coefficients dans $\mathbf{F}_p$ est invariant par Fr. On en déduit alors que a^p est une racine de q_a ; ce dernier étant irréductible, c'est le polynôme minimal de a^p.

3. Le lemme 6.38 implique immédiatement que n est le plus petit entier s tel que $a^{p^s} = a$. On en déduit donc que pour tout $0 \leqslant i \neq j \leqslant n-1$, $a^{p^i} \neq a^{p^j}$ de sorte que les q_a admet les n racines : $a, a^p, \cdots, a^{p^{n-1}}$. Or q_a étant de degré n, ce sont exactement toutes ses racines.

Exercice 6.11.

1. On vérifie rapidement que $X^2 + X + 1$ n'a pas de racines dans $\mathbf{F}_2$; étant de degré 2 il est alors irréductible de sorte que $\mathbf{F}_2[X]/(X^2 + X + 1)$ est un corps, une extension de degré 2 de $\mathbf{F}_2$ et donc isomorphe à $\mathbf{F}_4$.

2. De même, on vérifie que $X^3 + X + 1$ n'a pas de racines dans $\mathbf{F}_2$; étant de degré 3 il est alors irréductible sur $\mathbf{F}_2$ de sorte que $\mathbf{F}_2[X]/(X^3 + X + 1)$ est un corps de

cardinal 8 et donc isomorphe à $\mathbf{F}_8$. Comme $\mathbf{F}_8^* \simeq \mathbf{Z}/7\mathbf{Z}$ tout élément autre que 1 est un générateur du groupe des inversibles, par exemple x (x désigne la classe de X dans $\mathbf{F}_2[X]/(X^3+X+1)$).

3. À nouveau X^2+X-1 n'a pas de racines dans $\mathbf{F}_3$, il y est donc irréductible et $\mathbf{F}_9 \simeq \mathbf{F}_3[X]/(X^2+X-1)$. En outre $\mathbf{F}_9^* \simeq \mathbf{Z}/8\mathbf{Z}$ de sorte qu'il y a $\varphi(8)=4$ générateurs. On a $X^4=(X-1)^2=X^2-2X+1=-3X+2=-1$ et X est un générateur de $\mathbf{F}_9^*$.

Exercice 6.12.

Le schéma de démonstration est le même que celui du cours : on raisonne par l'absurde en supposant la finitude de l'ensemble considéré et on construit un entier N qui permette d'aboutir à une contradiction. On note n le plus grand élément de l'ensemble supposé fini. Toute la difficulté revient donc à construire N en fonction de n et de l'ensemble considéré :

1. $N=(n!)^2+1$; d'après l'exercice 1.17, si p premier divise N alors $p \equiv 1 \mod 4$ et donc par hypothèse $p \leqslant n$ ce qui implique que p divise $n!$ et donc $p|N-(n!)^2=1$ d'où $p=1$ et N premier. Or visiblement, on a $N>n$ d'où la contradiction.

2. $N=2(n!)-1$; soit p premier divisant N alors $p \equiv 1 \mod 4$ car p étant impair car N l'est, on aurait $p \leqslant n$ d'après la définition de n et donc p divise $n!$ ainsi que $N-2(n!)=1$. En remarquant judicieusement que dans $\mathbf{Z}/4\mathbf{Z}$ on a $1.1=1$, on en déduit que $N \equiv 1 \mod 4$, ce qui n'est pas.

3. $N=n!-1$; soit p premier divisant N ; visiblement $p>5$ de sorte que $p \equiv 1 \mod 6$ ou $p \equiv 5 \mod 6$. Comme précédemment $p \equiv 5 \mod 6$ est exclu ; en remarquant à nouveau que $1.1=1$ dans $\mathbf{Z}/6\mathbf{Z}$, on en déduit que $N \equiv 1$ ce qui n'est pas.

4. $N=3^2 5^2 7^2 11^2 \cdots n^2+2^2$; N est visiblement impair. Soit alors p premier divisant N, p ne divise pas 4, de sorte que d'après l'exercice (1.17), $p \equiv 1 \mod 4$, soit $p \equiv 1$ ou $5 \mod 8$. À nouveau $p \equiv 5 \mod 8$ est exclu car sinon p diviserait $4=N-3^2\cdots n^2$. On en déduit donc $N \equiv 1 \mod 8$. Or si p est premier impair on a $p \equiv 1,3,5,7 \mod 8$ et on vérifie aisément que p^2 est alors congru à 1 modulo 8 et donc $N \equiv 5 \mod 8$, d'où la contradiction.

PROBLÈMES

Problème 6.1.

1. On écrit la table des carrés de $\mathbf{F}_5$, soit

x	0	1	2	-2	-1
x^2	0	1	-1	-1	1

et on remarque que 2 n'est pas un carré dans $\mathbf{F}_5$.

On vérifie rapidement que pour $P(x) := X^2 + X + 1$, $P(0)$, $P(\pm 1)$ et $P(\pm 2)$ ne sont pas nuls de sorte que P n'a pas de racine dans $\mathbf{F}_5$; étant de degré 2 il y est donc irréductible.

2. Le corps $\mathbf{F}_5[X]/(P(X))$ est de cardinal 25 et donc isomorphe à $\mathbf{F}_{25}$ qui est un corps de décomposition de $X^{25} - X$.

Par ailleurs la classe x de X dans $\mathbf{F}_5[X]/(P(X))$ vérifie $P(x) = 0$ de sorte que x est une racine de P qui étant de degré 2, y est alors totalement décomposé. On en déduit alors que P admet deux racines dans $\mathbf{F}_{25}$.

3. Un isomorphisme $f : \mathbf{F}_5[X]/(X^2 + X + 1) \simeq \mathbf{F}_{25}$ étant fixé, l'image $\alpha \in \mathbf{F}_{25}$ de X par f vérifie alors $\alpha^2 + \alpha + 1 = 0$ et est donc une racine de $X^2 + X + 1$. Le sous-espace vectoriel sur $\mathbf{F}_5$ de $\mathbf{F}_{25}$ engendré par 1 et α est de dimension 2 car $\alpha \notin \mathbf{F}_5$ et est donc égal à $\mathbf{F}_{25}$ de sorte que tout élément $\beta \in \mathbf{F}_{25}$ s'écrit sous la forme $a\alpha + b$ avec $a, b \in \mathbf{F}_5$.

4. On vérifie rapidement que P n'a pas de racine dans $\mathbf{F}_5$. Soit alors $\beta = a\alpha + b \in \mathbf{F}_{25}$; on a $\beta^5 = a^5\alpha^5 + b^5 = a\alpha^5 + b$. Or on a $\alpha^2 = -\alpha - 1$ soit $\alpha^4 = \alpha^2 + 2\alpha + 1 = \alpha$ et donc $\alpha^5 = \alpha^2 = -\alpha - 1$. Ainsi $\beta^5 - \beta + 1 = \alpha(-a - a) + (b - b - a + 1) \neq 0$ car $\alpha \notin \mathbf{F}_5$ et donc P n'a pas de racine dans $\mathbf{F}_{25}$ de sorte qu'il est irréductible sur $\mathbf{F}_5$.

Par ailleurs P en tant que polynôme de $\mathbf{Z}[X]$ unitaire est irréductible. En effet une factorisation $P = QR$ dans $\mathbf{Z}[X]$ induit par réduction modulo 5 une factorisation $\overline{P} = \overline{Q} \cdot \overline{R}$ dans $\mathbf{F}_5[X]$. Comme P est unitaire, Q et R le sont aussi, de sorte que $\deg Q = \deg \overline{Q}$ et $\deg R = \deg \overline{R}$; $\overline{P}$ étant irréductible, on en déduit que $\overline{Q}$ ou $\overline{R}$ est un polynôme constant donc, étant unitaire, égal à $\overline{1}$ et donc Q ou R est le polynôme constant égal à 1. Ainsi P est irréductible sur $\mathbf{Z}$ et donc irréductible sur $\mathbf{Q}$ d'après le lemme de Gauss (proposition (5.7)).

Problème 6.2.

1. Si $x = a/b \in \mathbf{Q}$ avec $(a, b) = 1$, est une racine de P alors comme P est unitaire on a b divise 1 et donc $x \in \mathbf{Z}$. En outre modulo 2, $x^{l+1} - x + 1 \equiv 1 \mod 2$ de sorte que P n'a pas de racine modulo 2 et donc n'a pas de racine dans $\mathbf{Z}$.

2. Modulo p, on a $\overline{P} = X(X-1)\overline{\Phi}_l$ (où $\Phi_l = 1 + X + \cdots + X^{l-1}$; il suffit donc de prouver que $\overline{\Phi}_l$ est irréductible. Considérons pour $1 \leqslant n < (l+1)/2$, $x \in \mathbf{F}_{p^n}$ une racine de $\overline{\Phi}_l$. On a $x \neq 1$ car $\overline{\Phi}_l(1) = \overline{l} \neq 0$ et $x^{l+1} = x$ avec l premier implique que l est l'ordre M de x dans $\mathbf{F}_{p^n}^*$ et donc l divise $p^n - 1$ d'où $p^n \equiv 1 \mod l$. Or comme p engendre $(\mathbf{Z}/l\mathbf{Z})^*$, on en déduit que n est un multiple de $l - 1$ ce qui contredit le fait que $n < (l+1)/2$.

3. Modulo 2, $\overline{P}$ admet donc un diviseur de degré 2 qui est donc irréductible car $\overline{P}$ n'a pas de racine. Or sur $\mathbf{F}_2$, il y a un unique polynôme irréductible de degré 2, à savoir $X^2 + X + 1$. Ainsi sur $\mathbf{F}_4$, on doit avoir $P(j) = 0$ où j est un générateur de $\mathbf{F}_4^*$, soit $j^{l+1} = j + 1 = j^2$ et donc $l + 1 \equiv 2 \mod 3$ ce qui n'est pas.

Problème 6.3.

1. On pose donc $y = xz$ de sorte que $\left(\frac{xy}{q}\right) = \left(\frac{x}{q}\right)^2 \left(\frac{z}{q}\right) = \left(\frac{z}{q}\right)$. On obtient alors

$$\tau^2 = \sum_{z\in(\mathbf{Z}/q\mathbf{Z})^\times} \left(\frac{z}{q}\right) \sum_{x\in(\mathbf{Z}/q\mathbf{Z})^\times} w^{x(1+z)}$$

En outre on a $\sum_{x=1}^{q-1} w^x = 0$ de sorte que si $z \neq -1$, $\sum_{x\in(\mathbf{Z}/q\mathbf{Z})^\times} w^{x(1+z)} = -1$ ce qui permet d'écrire

$$\tau^2 = \left(\frac{-1}{q}\right)(q-1) + \sum_{\substack{z\in(\mathbf{Z}/q\mathbf{Z})^* \\ z\neq -1}} -\left(\frac{z}{q}\right)$$

2. Comme il y a autant de carrés que de non carrés dans $(\mathbf{Z}/q\mathbf{Z})^*$, on en déduit que $\sum_{x\in(\mathbf{Z}/q\mathbf{Z})^*} \left(\frac{x}{q}\right) = 0$ d'où le résultat.

3. Ainsi $\left(\frac{-1}{q}\right) q$ est un carré dans $\mathbf{Z}/p\mathbf{Z}$ si et seulement si τ appartient à $\mathbf{Z}/p\mathbf{Z}$, soit si et seulement si $\tau^p = \tau$. En effet on rappelle que $\mathbf{Z}/p\mathbf{Z} \subset K$ est l'ensemble des racines de l'équation $X^p - X$.

4. On calcule alors

$$\begin{aligned}\tau^p &= \textstyle\sum_{x\in(\mathbf{Z}/q\mathbf{Z})^\times} \left(\frac{x}{q}\right) w^{px} \\ &= \left(\frac{p}{q}\right)^{-1} \textstyle\sum_{y\in(\mathbf{Z}/q\mathbf{Z})^\times} \left(\frac{y}{q}\right) w^y = \left(\frac{p}{q}\right)\tau\end{aligned}$$

Ainsi $\left(\frac{-1}{q}\right) q$ est un carré si et seulement si $\left(\frac{p}{q}\right) = 1$ *i.e.* p est un résidu quadratique modulo p. On a alors

$$\begin{aligned}\left(\frac{p}{q}\right) &= \left(\frac{\left(\frac{-1}{q}\right) q}{p}\right) = \left(\frac{(-1)^{(q-1)/2}}{p}\right)\left(\frac{q}{p}\right) \\ &= \left(\frac{-1}{q}\right)^{(q-1)/2} \left(\frac{q}{p}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{2}}\end{aligned}$$

Problème 6.4. (*« Jeu du solitaire »*).

1. Prenons par exemple le mouvement élémentaire de la figure 6.2. Dans le plateau de gauche on a $\alpha = j^{x_0+y_0}(1+j)$ (resp. $\beta = j^{x_0-y_0}(1+j)$) alors que dans le plateau de droite on a $\alpha = j^{x_0+y_0}.j^2$ (resp. $\beta = j^{x_0-y_0}j^2$), avec $(x_0, y_0) = (-2, -1)$. Le résultat découle alors de l'égalité $1 + j = j^2$ dans $\mathbf{F}_4$ (on rappelle que dans $\mathbf{F}_4$, on a $1 = -1$). Les autres mouvements élémentaires se traitent de manière strictement identique.

2. Commençons par calculer (α, β) pour la configuration où tous les réceptacles contiennent une bille. La configuration étant invariante par la réflexion d'axe (Oy), on a $\alpha = \beta$, calculons donc α. Pour cela on propose de sommer sur les droites $x + y$

constantes, de sorte que ne contribuent que les droites où il y a un nombre impair de billes, ce qui donne $\alpha = j^0 + j^2 + j^{-2} = 0$, comme on le voit sur la figure 6.4.

Notons alors avec un indice tot (resp. $\mathcal{C}_0$, resp. 0) ce qui fait référence à la configuration où tous les réceptacles sont remplis (resp. tous sauf en (x_0, y_0), resp aucun sauf en (x_0, y_0)). On a ainsi $(\alpha_{tot}, \beta_{tot}) = (\alpha_{\mathcal{C}_0}, \beta_{\mathcal{C}_0}) + (\alpha_0, \beta_0) = (0, 0)$ de sorte que $(\alpha_{\mathcal{C}_0}, \beta_{\mathcal{C}_0}) = (\alpha_0, \beta_0)$.

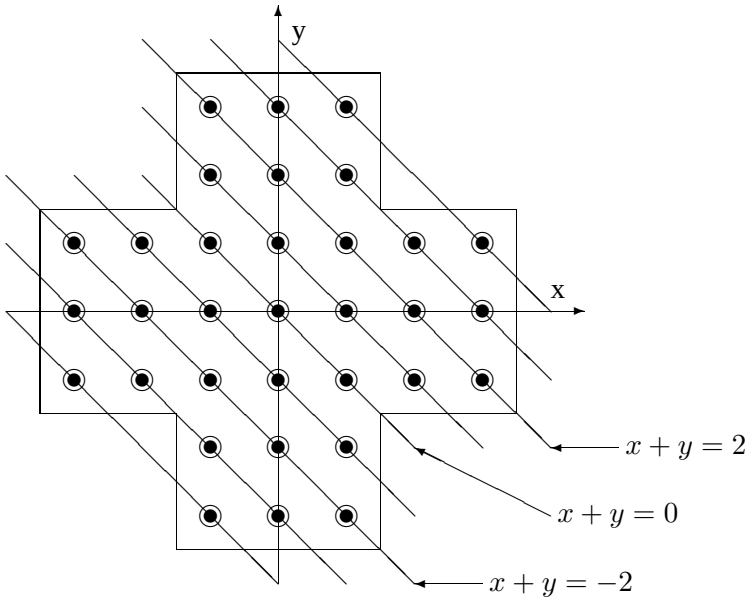


Figure 6.4

3. On calcule comme précédemment les invariants (α, β) ce qui donne $(0, 0)$ qui ne peut pas être de la forme $(j^{x_0+y_0}, j^{x_0-y_0})$.