Cours de mathématiques de terminale S

Nicolas FRANCOIS
nicolas.francois@free.fr

13 novembre 2009

Table des matières

Première partie

Arithmétique

L'*arithmétique* (du grec $\alpha\rho\iota\theta\mu o\varsigma$ qui signifie "nombre") est l'étude des nombres entiers. Consacrer une grande partie de l'année à un sujet *a priori* aussi restreint peut sembler étrange, mais ce thème est bien plus vaste qu'on ne l'imagine.

L'histoire de l'arithmétique remonte à plus de deux millénaires, et les plus grands mathématiciens s'y sont attelés : Pythagore (grec, -580 - -497), Euclide (grec, -325, -265), Al-Khawarizmi (perse, 783 - 850), Fermat (français, 1600 - 1665), Euler (suisse, 1707 - 1783), Lagrange (franco-italien, 1736 - 1813), Gauss (allemand, 1777 - 1855), Hilbert (allemand, 1862 - 1943), Weil (français, 1906 - 1998), Wiles (britannique, 1953 -).

En dehors de l'étude purement mathématique des nombres entiers, l'arithmétique est utilisée de nos jours en cryptologie (la science du codage et du décodage des codes secrets), dans l'étude des codes correcteurs, les nombres premiers sont utilisés dans les systèmes de protection des informations (secret bancaire...), et dans bien d'autres domaines comme la physique théorique.

C'est aussi une excellente école de raisonnement, et l'une des premières branches des mathématiques dans laquelle vous allez pouvoir exercer vos réels talents de mathématiciens.

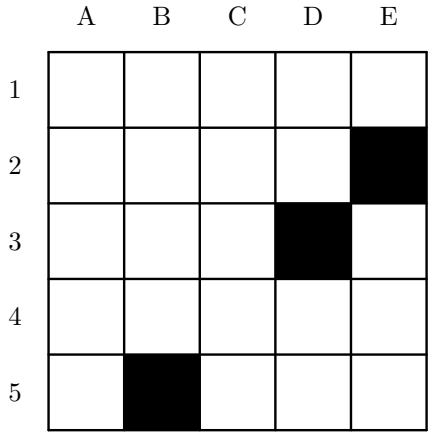
So, let's have fun with numbers !

CHAPITRE I

Divisibilité dans $\mathbb{N}$ et $\mathbb{Z}$

I Un exemple d'introduction

Remplir la grille de nombres croisés ci-dessous sachant que tous les nombres y figurant sont des entiers naturels non nuls.



Horizontalement

1. Carré parfait dont le produit des chiffres est 756.
2. Le nombre formé par ses deux premiers chiffres est le même que celui formé par ses deux derniers chiffres.
3. Multiple de 139.
   Reste de la division euclidienne de 2001 par 9.
4. Permutation de 23444.
5. Carré parfait.
   Le produit de ses chiffres est 392.

Verticalement

A. La somme de ses chiffres est 35.

B. Entier divisible par 11.

C. Nombre palindrome.

D. Nombre premier.
   Cube parfait.

E. Entier naturel admettant un seul diviseur positif.
   Le produit de ses chiffres est 72 et seul son dernier chiffre est pair.

II Préliminaires

On rappelle que $\mathbb{N}$ et $\mathbb{Z}$ représentent respectivement l'ensemble des entiers naturels et l'ensemble des entiers relatifs. Dans l'ensemble de ce cours d'arithmétique, on sortira rarement de ces deux ensembles, même si on fera parfois quelques incursions dans le domaine des rationnels (qui ne sont jamais que des quotients d'entiers !).

Sur ces deux ensembles sont définies deux opérations : l'addition et la multiplication. $\mathbb{N}$ et $\mathbb{Z}$ sont *stables* par ces opérations, au sens ou, par exemple, le produit de deux entiers naturels est encore un entier naturel[1].

L'ensemble $\mathbb{N}$ vérifie deux propriétés remarquables :

- Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
- Toute partie non vide *et majorée* de $\mathbb{N}$ admet un plus grand élément.

Nous utiliserons souvent ces deux propriétés. Notons que si la deuxième est encore valable dans $\mathbb{Z}$, la première ne l'est pas (que faut-il ajouter comme hypothèse pour $\mathbb{Z}$?).

III Divisibilité dans $\mathbb{Z}$

A Définition

Définitions 1 : *Soient a et b deux entiers relatifs.*

On dit que b est un multiple *de a si il existe un entier relatif k tel que $b = ka$. On dit aussi que a est un* diviseur *de b, ou bien que a divise b, ou que b est* divisible *par a. "a divise b" se note $a|b$.*

Exemple : De $4 \times 9 = 36$, on déduit que 4 et 9 sont deux diviseurs de 36, ou bien que 36 est un multiple de 4 et de 9.

L'ensemble des multiples de 3 est l'ensemble $\{3 \times k,\ k \in \mathbb{Z}\}$ que l'on notera $3\mathbb{Z}$. Plus généralement, les multiples d'un entier a sont les ka, avec $k \in \mathbb{Z}$, leur ensemble se note $a\mathbb{Z}$.

Pouvez-vous trouver tous les diviseurs de 36 (attention à ne pas oublier les négatifs !) ?

Montrer que la somme de trois entiers consécutifs est un multiple de 3.

Montrer que pour tout $n \in \mathbb{N}$, l'entier $n\,(n+1)\,(2n+1)$ est divisible par 6

a) par récurrence,

b) par un raisonnement direct.

B Propriétés

Voici d'abord énoncées en vrac quelques propriétés élémentaires :

- 0 est multiple de tout entier (ou bien tout entier divise 0). En particulier, même si cela peut paraître contradictoire avec tout ce qu'on vous a appris avant, 0 est bien un diviseur de 0 !
- 1 et -1 sont diviseurs de tout entier.
- Les seuls diviseurs de 1 sont 1 et -1.
- Pour tout entier relatif a, a et $-a$ ont les mêmes diviseurs.

Les démonstrations de ces propriétés utilisent simplement la définition de la divisibilité. Par exemple, si b divise a, il existe un entier k tel que $a = bk$, ce qu'on peut encore écrire $-a = b.(-k)$, ce qui prouve que b est aussi un diviseur de $-a$.

Voici maintenant des propriétés moins évidentes :

[1] Noter que ce n'est pas le cas de la différence de deux entiers naturels, ou du quotient de deux rationnels

Théorème 1
Soient a, b et c trois entiers relatifs.

a) $a|b \iff (\forall c \in \mathbb{Z})\ a|bc$.

b) $(a|b \text{ et } b \neq 0) \Longrightarrow (|a| \leqslant |b|)$.

c) $(a|b \text{ et } b|a) \iff a = \pm b$.

d) $(a|b \text{ et } b|c) \Longrightarrow a|c$ (*transitivité* de la relation de divisibilité).

e) $(a|b \text{ et } a|c) \Longrightarrow \big((\forall\,(u,v) \in \mathbb{Z}^2)\ a|ub+vc\big)$. En particulier $(a|b \text{ et } a|c) \Longrightarrow (a|b+c \text{ et } a|b-c)$.

Preuve *a) Si $a|bc$ pour tout $c \in \mathbb{Z}$, alors en particulier $a|b$ (pour $c = 1$.*
Réciproquement, si $a|b$, il existe $k \in \mathbb{Z}$ tel que $b = ak$, donc $bc = a\,(kc)$ et a divise bien bc.

b) Si $a|b$, alors il existe $k \in \mathbb{Z}^*$ tel que $b = ak$, donc on a $|b| = |a|\,|k| \geqslant |a|$.

c) Cela résulte de la propriété ci-dessus : $a|b$ entraîne $|a| \leqslant |b|$, et $b|a$ entraîne $|b| \leqslant |a|$. Ainsi $|a| = |b|$, donc $a = \pm b$ (traiter les cas particuliers $a = 0$ et $b = 0$ à part).

d) $a|b$ donc $b = ka$, $b|c$ donc $c = k'b$, d'où $c = kk'a$ et $a|c$.

e) À faire à titre d'exercice.

Exercices :

- Montrer que les diviseurs d'un entier non nul sont en nombre fini.
- Montrer la propriété : $(a|b) \iff ((\forall c \in \mathbb{Z})\ ac|bc)$.
- Montrer que si a, b, c et d sont quatre entiers tels que $ad - bc = 1$, alors la fraction $\dfrac{a+c}{b+d}$ est irréductible. La réciproque est-elle vraie ?
- Exercices 3, 6 et 8 p.20.
- Exercice 43 p.22.
- Exercice 61 p.23, 66 p.24 et 84 p.25.
- En DM : exercice 115 p.27.
- En DM encore : montrer que la somme des cubes de trois entiers consécutifs est divisible par 3.
- En DM toujours : résoudre les équations suivantes dans $\mathbb{Z}$:

  a) $6x + y - 3xy + 22 = 0$ b) $(x - 27)\,(y + 12) = xy$.

CHAPITRE II

Division euclidienne dans $\mathbb{N}$ et $\mathbb{Z}$, congruences

I Une propriété de $\mathbb{N}$

Lemme 1
Pour tout entier naturel a et tout entier naturel *non nul* b, il existe un entier n tel que $nb > a$.

Preuve *Comme b est non nul, $b \geqslant 1$, donc $(a+1)\,b \geqslant a+1 > a$. L'entier $a+1$ convient donc.*

Cette propriété de $\mathbb{N}$, peut utile par elle même, intervient dans un certain nombre de démonstrations.

Attention au fait que le nombre $a+1$ donné dans la démonstration n'est ni le seul (il y a une infinité d'entiers n vérifiant la propriété), ni forcément le premier qui convient.

II Division euclidienne dans $\mathbb{N}$

Vous avez appris il y a bien longtemps à faire une division sans virgule, entre entiers, avec reste. Cette division s'appelle *divisions euclidiennes*, nous allons fournir dans ce paragraphe les démonstrations montrant que cette division marche toujours.

Théorème 2
Soient a et b deux entiers naturels, b étant **non nul**. Il existe un unique couple (q, r) d'entiers naturels tel que $a = bq + r$ et $0 \leqslant r < b$.

Preuve *Comme dans beaucoup de théorèmes d'existence et d'unicité, les preuves se font séparément. Il est souvent intéressant de commencer par l'unicité.*

Unicité *: supposons que*[1] *les deux couples (q, r) et (q', r') conviennent. On a donc*

$$a = bq + r,\ 0 \leqslant r < b \quad et \quad a = bq' + r',\ 0 \leqslant r' < b$$

On en déduit que $bq + r = bq' + r'$, soit encore $b\,(q - q') = r' - r$. Ainsi b est un diviseur de $r' - r$.

Or de $0 \leqslant r < b$ et $0 \leqslant r' < b$, on tire $-b < r' - r < b$, donc $|r' - r| < b$. Et on a vu dans le cours précédent que $a|b$ et $b \neq 0$ entraîne $|a| \leqslant |b|$.

La seule solution possible est donc $r' - r = 0$, soit $r' = r$. On a donc $bq = bq'$, soit puisque $b \neq 0$, $q = q'$. Les couples (q, r) et (q', r') sont donc identiques.

Existence *: considérons l'ensemble M des multiples de b strictement supérieurs à a. D'après la propriété préliminaire, on sait que M est non vide.*

M est donc une partie non vide de $\mathbb{N}$, on sait qu'elle admet un plus petit élément, qui est un multiple de b, que nous pouvons donc noter $(q+1)\,b$.

[1] Notons que l'on ne fait pas ici une démonstration par l'absurde. On considère deux couple, et on montre qu'ils sont nécessairement identiques.

On a donc par hypothèse : $bq \leqslant a < b(q+1)$, et q est nécessairement un entier naturel puisque $0 = 0b \leqslant a$.

Posons $r = a - bq$. r, différence de deux entiers, est un entier. De plus, de l'inégalité précédente, on tire en retranchant partout bq :

$$0 \leqslant r = a - bq < b(q+1) - bq = b$$

Le couple (q, r) ainsi construit convient.

Remarquons que les deux démonstrations utilisent des outils assez différents.

Définition 1 : *Effectuer la division euclidienne de a par b, c'est trouver le couple (q, r) tel que $a = bq + r$ et $0 \leqslant r < b$.*

a est le dividende*, b le* diviseur*, q le* quotient *et r le* reste*.*

Exemples :

- Effectuons la division euclidienne de 37 par 5. Écrivons pour cela les multiples de 5 jusqu'à dépasser 37. On constate que $40 = 5 \times 8$ convient.

  On a donc : $5 \times 7 = 35 \leqslant 37 < 40 = 5 \times 8$. On termine en calculant la différence $37 - 35$:

  $$37 = 35 + 2 = 5 \times 7 + 2$$

  Le quotient cherché est donc 7, le reste 2.

- Le reste de la division euclidienne d'un entier par 10 est simplement son chiffre des unités. En effet[2], cela découle de

  $$\overline{a_p a_{p-1} \dots a_1 a_0} = \overline{a_p a_{p-1} \dots a_1 0} + a_0 = 10\overline{a_p a_{p-1} \dots a_1} + a_0$$

- Pour tout entier naturel n, on a :

  $$n^2 + 2n + 2 = (n+1)^2 + 1$$

  On peut en déduire que le reste de la division euclidienne de $n^2 + n + 2$ par $n + 1$ est 1. Essayez avec quelques valeurs de n.

  Oui, mais au fait, on a aussi

  $$n^2 + 2n + 2 = n(n+1) + n + 2$$

  alors pourquoi le reste ne serait pas $n + 2$? Parce qu'il manque quelque chose pour qu'une telle écriture soit la division euclidienne de $n^2 + 2n + 2$ par $n + 1$!

Une remarque qui a d'importantes conséquences :

Propriété 1

Le reste de la division euclidienne de a par b ne peut prendre que les $|b|$ valeurs entières comprises entre 0 et $b - 1$. ★

Ainsi, par exemple :

- toute entier s'écrit $2k$ ou $2k + 1$, le reste de sa division euclidienne ne pouvant être que 0 ou 1.
- Tout entier naturel n s'écrit $n = 5k + r$, avec $0 \leqslant r \leqslant 4$.

  On en déduit (activité 1 p.6) que $5k + 3$ ne peut être le carré d'un entier pour aucune valeur de k.

[2] Dans la relation ci-dessus, $\overline{a_p a_{p-1} \dots a_1 a_0}$ désigne l'entier naturel donc l'écriture décimale comporte dans l'ordre les chiffres $a_p, a_{p-1}, \dots, a_0$, avec $0 \leqslant a_i \leqslant 9$ pour tout i. On a donc :

$$\overline{a_p a_{p-1} \dots a_1 a_0} = a_p \times 10^p + a_{p-1} \times 10^{p-1} + \dots + a_1 \times 10^1 + a_0 \times 10^0$$

En effet, $(5k+r)^2 = 25k^2+10kr+r^2 = 5\left(5k^2+2kr\right)+r^2$. Si $r=0$, 1 ou 2, ceci est directement l'écriture de la division euclidienne de $(5k+r)^2$ par 5, le reste pouvant être 0, 1 ou 4. Si $r=3$, on écrit :

$$(5k+3)^2 = 5\left(5k^2+6k\right)+9 = 5\left(5k^2+6k+1\right)+4$$

et le reste est encore 4, et si $r=4$,

$$(5k+4)^2 = 5\left(5k^2+8k\right)+16 = 5\left(5k^2+6k+3\right)+1$$

et le reste est encore 1. Le reste de la division euclidienne du carré d'un entier par 5 ne peut donc être que 0, 1 ou 4, donc aucun carré n'est de la forme $5k+3$.

Exercices :

- Soient a et b deux entiers naturels, $b \neq 0$. Montrer que si le quotient de la division euclidienne de a par b n'est pas nul, a est supérieur au double du reste.
- Exercices 12, 13 et 18 p.20.
- Exercice 44 p.22.
- Exercices 46, 52, 54 et 58 p.23.

III Extension à $\mathbb{Z}$

On étend facilement la définition de la division euclidienne au cas où a et b sont entiers relatifs, il suffit pour cela d'adapter la condition sur le reste :

Théorème 3
Soient a et b deux entiers relatifs, b étant non nul. Il existe un unique couple d'entiers (q,r) tel que $a = bq+r$, avec $0 \leqslant r < |r|$.

Preuve *Laissée en exercice.*

On constate que la seule chose à ajouter à la définition précédente est la valeur absolue autour de b dans la condition portant sur r.

Exemple : On a vu plus haut que $37 = 5\times 7+2$. On déduit de cela que :

$$37 = (-5)\times(-7)+2, \quad -37 = 5\times(-7)-2 = 5\times(-8)+3 \quad \text{et} \quad -37 = (-5)\times(-7)+2$$

ce qui permet de lire les divisions euclidiennes de 37 par -5, de -37 par 5 et de -37 par -5. Remarquons que dans le deuxième cas, il faut manipuler un peu l'écriture pour respecter les conditions portant sur r.

Exercices :

- Exercice 11 p.20.
- DM : Exercice 116 p.27.

Votre calculette sait normalement faire des divisions euclidiennes. Consultez votre manuel. Les calculatrices sophistiquées possèdent deux fonctions "mod" et "quo" pour le reste et le quotient, pour les autres, vous devrez écrire un programme. Il s'en trouve des tas sur Internet !

IV Une application : les systèmes de numération de position

Notre système de numération (i.e. d'écriture des nombres) est un système de *position*. Cela signifie que la position d'un chiffre dans le nombre possède une signification liée à la base dans laquelle nous comptons, et cette signification est multipliée par cette base lorsqu'on passe d'un chiffre au suivant.

Ça n'est pas clair ? Le TD n°3 p.16 permet d'explorer les subtilités de notre système, et de quelques autres. Pour rencontrer un autre système de numération tout aussi épatant, s'adresser aux Shaddocks et leur système en base 4 : « Ga Bu Zo Meu » !

CHAPITRE III

Congruences dans $\mathbb{Z}$

I Congruences modulo m

Dans toute cette section, m désigne un entier naturel non nul.

Propriété 2
Deux entiers relatifs a et a' ont même reste dans leur division euclidienne par m si et seulement si m divise leur différence $a - a'$.

Preuve *: Écrivons les deux divisions euclidiennes : $a = mq + r$ et $a' = mq' + r'$, avec $0 \leqslant r < m$ et $0 \leqslant r' < m$. La différence s'écrit donc $a - a' = m(q - q') + r - r'$.*

m divisant $m(q - q')$, $m|a$ équivaut à $m|r - r'$. Or on sait que $|r - r'| < m$. $m|r - r'$ équivaut[1] *donc encore à $r - r' = 0$, soit $r = r'$.*

Définition 2 : *On dit que les entiers relatifs a et a' sont* congrus modulo m *s'ils vérifient l'une des deux conditions équivalentes précédentes. On note alors $a \equiv a' \,(\mathrm{mod}\, m)$, ou parfois plus simplement $a \equiv a' \,(m)$.*

Autrement dit, $a \equiv a' \,(\mathrm{mod}\, m) \iff m|a - a'$. m s'appelle le module *de la congruence.*

Exemples :
- $1 \equiv 6 \,(\mathrm{mod}\, 5)$ car $1 = 0 \times 5 + 1$ et $6 = 1 \times 5 + 1$, ou bien plus simplement $5|6 - 1$.
- $27 \equiv -3 \,(\mathrm{mod}\, 5)$ car $5|27 - (-3)$.

Remarques :
- Si r est le reste de la division euclidienne de a par m, alors $a \equiv r \,(\mathrm{mod}\, m)$. Plus précisément, $a \equiv b \,(\mathrm{mod}\, m)$ et $0 \leqslant b < m$ équivaut au fait que b est le reste de la division euclidienne de a par m.
- $a \equiv b \,(\mathrm{mod}\, m) \iff (\exists\, k \in \mathbb{Z})\ a = km + b$. On retrouve une notion similaire à celle de congruence des angles modulo 2π.
- $m|a$ équivaut à $a \equiv 0 \,(\mathrm{mod}\, m)$. En particulier, pour tout entier n non nul, $n \equiv 0 \,(\mathrm{mod}\, n)$.

Propriété 3
La relation de congruence est une *relation d'équivalence*, ce qui signifie qu'elle est :

symétrique : si $a \equiv b \,(\mathrm{mod}\, m)$, alors $b \equiv a \,(\mathrm{mod}\, m)$;

réflexive : $a \equiv a \,(\mathrm{mod}\, m)$;

transitive : si $a \equiv b \,(\mathrm{mod}\, m)$ et $b \equiv c \,(\mathrm{mod}\, m)$, alors $a \equiv c \,(\mathrm{mod}\, m)$.

[1] On peut plus simplement procéder par conditions nécessaire et suffisante.

Preuve *(à faire en exercice)*

symétrie *:* $a \equiv b \,(\mathrm{mod}\, m)$ *équivaut à* $m|b-a$*, donc* $m|a-b$*, i.e.* $b \equiv a \,(\mathrm{mod}\, m)$ *;*

réflexivité *:* $a \equiv a \,(\mathrm{mod}\, m)$ *signifie simplement* $m|a-a$ *;*

transitivité *: de* $a \equiv b \,(\mathrm{mod}\, m)$ *et* $b \equiv c \,(\mathrm{mod}\, m)$*, on tire* $m|b-a$ *et* $m|c-b$*, donc* $m|c-a = (c-b)+(b-a)$*. alors* $a \equiv c \,(\mathrm{mod}\, m)$*.*

Exercices :

- Reprendre les démonstrations ci-dessus en utilisant la définition : $a \equiv b \,(\mathrm{mod}\, m)$ si et seulement si a et b ont même reste dans la division euclidienne par m.
- Exercices 21, 22, 23 p.21.

II Règles de calcul avec les congruences

Théorème 4 (Compatibilité de la relation de congruence avec les opérations courantes)
Soient a, a', b et b' quatre entiers relatifs, m un entier naturel non nul et p un entier naturel. On suppose que $a \equiv b \,(\mathrm{mod}\, m)$ et $a' \equiv b' \,(\mathrm{mod}\, m)$. Alors :

addition : $a + a' \equiv b + b' \,(\mathrm{mod}\, m)$,

soustraction : $a - a' \equiv b - b' \,(\mathrm{mod}\, m)$,

multiplication : $a \times a' \equiv b \times b' \,(\mathrm{mod}\, m)$,

puissances : $a^p \equiv b^p \,(\mathrm{mod}\, m)$.

Preuve *: nous n'allons pas tout détailler, les démonstrations non données seont à faire en exercice.*

addition *:* $m|b-a$ *et* $m|b'-a'$ *entraîne* $m|\,(b-a)+(b'-a') = (b+b')-(a+a')$*.*

soustraction *: même démonstration.*

multiplication *: on utilise ici* $bb'-aa' = b'\,(b-a)+a\,(b'-a')$*.*

puissances *: raisonnons par récurrence sur* p*.*

La proposition $\mathscr{P}\,(p)$: $a^p \equiv b^p \,(\mathrm{mod}\, m)$ *est évidemment vraie pour* $p = 0$ *et* $p = 1$*.*

Supposons qu'elle soit vraie pour un certain exposant $p \in \mathbb{N}$ *:* $a^p \equiv b^p \,(\mathrm{mod}\, m)$*. Utilisons la compatibilité avec la multiplication :*

$$a^p \equiv b^p \,(\mathrm{mod}\, m) \;\text{ et }\; a \equiv b \,(\mathrm{mod}\, m) \;\text{ entraîne }\; a^p \times a \equiv b^p \times b \,(\mathrm{mod}\, m)$$

soit $a^{p+1} \equiv b^{p+1} \,(\mathrm{mod}\, m)$*, ce qui est bien* $\mathscr{P}\,(p+1)$*. La propriété* $\mathscr{P}$ *est donc héréditaire.*

On dit que la relation de congruence est *compatible* avec les opérations d'addition, de soustraction, de multiplication et de puissance (ou d'exponentiation). Cela autorise en particulier les règles de simplification suivantes :

Théorème 5
Si $a \equiv a' \,(\mathrm{mod}\, m)$, alors pour tout $x \in \mathbb{Z}$,

$$a + x \equiv a' + x \,(\mathrm{mod}\, m)\,, \quad a - x \equiv a' - x \,(\mathrm{mod}\, m) \quad \text{et} \quad ax \equiv a'x \,(\mathrm{mod}\, m) \qquad \bigstar$$

Remarquons que cela nous autorise à *simplifier* une relation de congruence de la forme $a+x \equiv b+x$ (il suffit d'ajouter $-x$ de chaque coté), mais pas une relation de la forme $ax \equiv bx$. On retiendra que *la relation de congruence n'est pas compatible avec la division, ni d'ailleurs avec la racine carrée.*

En effet, par exemple, $12 \equiv 24 \,(\mathrm{mod}\, 6)$, mais $3 \not\equiv 4 \,(\mathrm{mod}\, 6)$ (division par 3). De même, $4 \equiv 16 \,(\mathrm{mod}\, 12)$, mais $2 \not\equiv 4 \,(\mathrm{mod}\, 12)$ (racine carrée)[2].

Exercice : L'exercice 79 p.24 explore les liens entre la relation de congruence et la division.

Exemple : On s'intéresse au chiffre des unités de $7^{7^{7^7}}$ (mâtin, quel bestiau !). On remarque que le chiffre des unités de n est son reste dans la division euclidienne par 10. Cherchons les restes modulo 10 des puissances de 7 :

p	0	1	2	3	4
$7^p \,(\mathrm{mod}\, 10)$	1	7	9	3	1

Ainsi, $7^4 \equiv 1 \,(\mathrm{mod}\, 10)$. Si $n \equiv r \,(\mathrm{mod}\, 4)$, on a donc $7^n \equiv 7^r \,(\mathrm{mod}\, 10)$. En effet, de $n = 4k+r$, on tire :

$$7^n = 7^{4k+r} = 7^{4k}.7^r = \left(7^4\right)^k.7^r \equiv 1^k.7^r \,(\mathrm{mod}\, 10)$$

Reste à trouver le reste de la division euclidienne de 7^7 par 4 :

p	0	1	2
$7^p \,(\mathrm{mod}\, 4)$	1	3	1

Ainsi de la même façon, si $n \equiv r \,(\mathrm{mod}\, 2)$, alors $7^n \equiv 7^r \,(\mathrm{mod}\, 4)$. Ici, on remarque que 7^7 est certainement impair, donc $7^{7^7} \equiv 7^1 \equiv 3 \,(\mathrm{mod}\, 4)$.

On en déduit finalement que le chiffre des unités de $7^{7^{7^7}}$ est un ... 3 !!!

Exercices :

- TD 1, 2 et 4 p.15-19.
- Exercices 26, 29, 33, 34, 38 p.21.
- Exercice 45 p.22.
- Exercices 84, 85, 95 p.25.
- DM : 107 et 109 p.26.

[2]Par contre, de $21 \equiv 33 \,(\mathrm{mod}\, 4)$, on peut bien tirer $7 \equiv 11 \,(\mathrm{mod}\, 4)$. Bizarre, non ? À votre avis, qu'est-ce qui est différent dans cet exemple ?

Deuxième partie

Géométrie plane

CHAPITRE IV

Généralités sur les transformations du plan

Dans tout ce chapitre, $\mathscr{P}$ désigne le plan. Comme nous allons mesurer des angles et des longueurs, nous avons besoin, si nécessaire, d'un repère orthonormé. On dit alors qu'on travaille dans le *plan euclidien*.

I Généralités

- Lorsqu'une construction asocie à chaque point du plan un unique point, on dit qu'on définit une *application* du plan dans lui-même.

  Exemple : la projection orthogonale sur une droite Δ (M' est l'image de M si et seulement si $M' \in \Delta$ et $(MM') \perp \Delta$).

- Deux applications f et g sont égales si et seulement si pour tout point $M \in \mathscr{P}$, $f(M) = g(M)$.

- Une application est dite *bijective* si tout point de $\mathscr{P}$ est l'image d'un point et d'un seul, autrement dit si tout point de $\mathscr{P}$ admet un *unique antécédent*. On dit alors que f est une *transformation* du plan.

  Ainsi, une *transformation du plan* est une *application bijective du plan dans lui-même*.

  Exemple : la translation de vecteur $\vec{u}$ est une transformation du plan. En effet, dire que M' est l'image de M par $t_{\vec{u}}$ revient à dire que $\overrightarrow{MM'} = \vec{u}$, ce qui identifie de façon unique l'antécédent M de M'.

- Si f est une transformation du plan, à tout point N du plan, on peut associer l'unique point M tel que $f(M) = N$. On définit ainsi une application du plan dans lui-même, que nous noterons pour l'instant g.

  Ainsi : $f(M) = N \iff g(N) = M$.

  Théorème 6

  g est une transformation.

  Preuve *Il s'agit de montrer que tout point N du plan admet un unique antécédent par g.*

  Soit N un point de $\mathscr{P}$. Posons $M = f(P)$. Par définition, $g(M) = N$, donc M est un antécédent de N par g. Montrons que c'est le seul.

  Soit M' un autre antécédent de N par g. On a donc $g(M) = g(M') = N$, et donc par définition $M = f(N) = M'$, donc $M = M'$.

  La transformation g s'appelle la *transformation réciproque* de f, elle est notée f^{-1}.

II Les transformations du plan étudiées en seconde et première

Récapitulons l'ensemble des transformations du plan étudiées les années précédentes. Ces transformations conservent un certain nombre de propriétés parmi les suivantes :

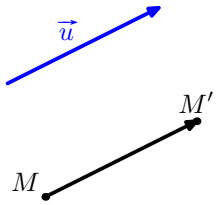
- l'alignement (A, B, C alignés entraîne $f(A)$, $f(B)$ et $f(C)$ alignés),
- le parallélisme ($d \parallel d'$ entraîne $f(d) \parallel f(d')$),
- l'orthogonalité ($d \perp d'$ entraîne $f(d) \perp f(d')$),
- les angles géométriques ($\widehat{f(A)\,f(B)\,f(C)} = \widehat{ABC}$),
- les angles orientés ($\left(\overrightarrow{f(A)\,f(B)}, \overrightarrow{f(A)\,f(C)}\right) = \left(\overrightarrow{AB}, \overrightarrow{AC}\right) \pmod{\pi}$),
- les distances ($f(A)\,f(B) = AB$).

Signalons qu'une transformation qui conserve les distances est appelée une *isométrie* (du grec *isos*, égal, et *metron*, mesure).

1 Les translations

Définition 3 : *La translation de vecteur $\vec{u}$ est notée $t_{\vec{u}}$, et est définie par :*

$$M' = t_{\vec{u}}(M) \iff \overrightarrow{MM'} = \vec{u}$$

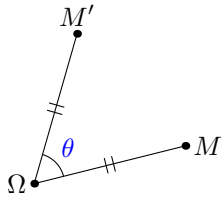


Elle conserve toutes les propriétés énumérées plus haut.

2 Les rotations

Définition 4 : *La rotation de centre Ω et d'angle θ est notée $r_{\Omega,\theta}$, et est définie par :*

$$M' = r_{\Omega,\theta}(M) \iff \begin{cases} \Omega M' = \Omega M \\ \left(\overrightarrow{\Omega M}, \overrightarrow{\Omega M'}\right) = \theta \end{cases}$$

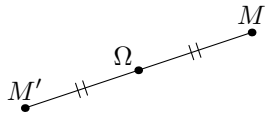


Elle conserve toutes les propriétés énumérées plus haut.

3 Les symétries centrales

Définition 5 : *La symétrie centrale de centre Ω est notée s_Ω, et est définie par :*

$$M' = s_\Omega(M) \iff \overrightarrow{\Omega M'} = \overrightarrow{M\Omega}$$

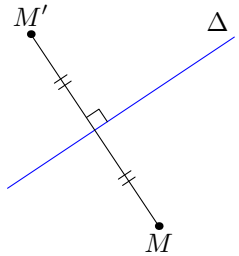


Remarquons qu'une symétrie centrale de centre Ω n'est rien d'autre qu'une rotation de centre Ω et d'angle π.
Il est donc normal que comme les rotations, elle conserve toutes les propriétés énumérées plus haut.

4 Les symétries axiales

Définition 6 : *La symétrie axiale d'axe Δ est notée s_Δ, et est définie par :*

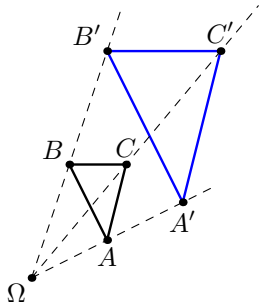
$$M' = s_\Delta(M) \iff \Delta \text{ est médiatrice de } [MM']$$



Elle conserve toutes les propriétés énumérées plus haut, **sauf l'orientation des angles** qu'elle retourne :

$$\left(\overrightarrow{s_\Delta(A)\,s_\Delta(B)}, \overrightarrow{s_\Delta(A)\,s_\Delta(C)}\right) = \boxed{-}\left(\overrightarrow{AB}, \overrightarrow{AC}\right) \pmod{\pi}$$

5 Les homothéties



Définition 7 : *L'homothétie de centre Ω et de rapport k est notée $h_{\Omega,k}$, et est définie par :*

$$M' = h_{\Omega,k}(M) \iff \overrightarrow{\Omega M'} = k\,\overrightarrow{\Omega M}$$

Elle conserve toutes les propriétés énumérées plus haut, **sauf les distances** : une homothétie de rapport k multiplie les distances par $|k|$:

$$h_{\Omega,k}(A)\,h_{\Omega,k}(B) = \boxed{|k|}\,AB$$

Exercices :

- Montrer que l'image par l'une quelconque de ces transformations d'une droite (respectivement une demi-droite, un segment, un cercle) est encore une droite (respectivement une demi-droite, un segment, un cercle).
- Exercices 1 et 6 p.114.

III Composition de transformations

Définition 8 : *Soit f et g deux transformations du plan. On peut définir une nouvelle application de $\mathscr{P}$ dans lui-même de la manière suivante : à tout point $M \in \mathscr{P}$, on associe le point N défini par $N = g(f(M))$.*

Cette application est notée $g \circ f$, et appelée composée de f par g.

Théorème 7

La composée de deux transformations du plan est une transformation du plan.

Preuve *Il s'agit de montrer que $g \circ f$ est bijective.*

Soit N un point de $\mathscr{P}$. Dire que $N = g \circ f(M)$ revient à dire que $f(M) = g^{-1}(N)$, soit $M = f^{-1}\left(g^{-1}(N)\right)$, d'où l'existence et l'unicité de M.

Ainsi $g \circ f$ est bijective, et on vient de montrer que sa bijection réciproque est

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

Une transformation joue un rôle tout à fait particulier par rapport à cette opération de composition : c'est l'*identité* :

$$\mathrm{I} : \mathscr{P} \mapsto \mathscr{P},\ M \mapsto M$$

En effet, pour toute transformation f, $_Id \circ f = f_circ\mathrm{I} = f$.

Théorème 8

Si f et g conserve une même propriété (alignements, distances...), alors il en est de même de $g \circ f$.

Preuve *La démonstration de ce théorème est évidente.*

Note culturelle

Muni de cette *opération* entre transformations, l'ensemble des transformations du plan a une structure de *groupe* (c'est même de l'étude de ces ensembles qui a lancé la théorie des groupes). Plus précisément :

- l'opération $\circ$ est *interne*, ce que l'on vient de montrer : la composée de deux transformations est encore une transformation ;
- l'opération $\circ$ est *associative* : $f \circ (g \circ h) = (f \circ g) \circ h$;
- il possède un *élément neutre* : la transformation **identité** $\mathrm{I} : M \mapsto M$;
- tout transformation f admet une réciproque g, vérifiant $f \circ g = g \circ f = \mathrm{I}$.

C'est l'étude de l'ensemble de ces transformations, ainsi que celle de ses sous-ensembles qui ont les mêmes propriétés, qui a initié, avec l'étude des équations algébriques, la *théorie des groupes* au cours des XIX$^{\text{ème}}$ et XX$^{\text{ème}}$ siècles.

Exercices :
Montrer que les ensembles suivants, muni de la composition des transformations, sont encore des groupes :

- l'ensemble $\{\mathrm{I}, s_\Delta\}$,
- l'ensemble $\mathscr{T}$ des translations,
- l'ensemble des rotations de centre Ω fixé,
- l'ensemble des homothéties de centre Ω fixé,
- l'ensemble $\mathscr{H}$ formé des homothéties et des translations,
- l'ensemble des isométries du plan,
- l'ensemble des transformations laissant globalement fixe un triangle équilatéral, un carré...

Notons que cette notion de groupe est hors programme, ni la notion, ni le vocabulaire ne sont à connaître.

CHAPITRE V

Isométries planes

I Définitions

Définition 9 : *Une* isométrie plane f *est une transformation du plan qui conserve les distances :*

$$(A' = f(A) \text{ et } B' = f(B)) \Longrightarrow A'B' = AB$$

Par exemple, une translation, une rotation, une symétrie axiale sont des isométries. Par contre, la plupart des homothéties ne *sont pas* en général des isométries.

Exercice : Quelles sont les homothéties qui sont des isométries ?

Propriétés 1

- La composée de deux isométries est encore une isométrie.
- La réciproque d'une isométrie est une isométrie.

Preuve • *En effet, si f et g sont deux isométries, notons $h = g \circ f$. On sait déjà que h est une transformation du plan.*

Soient A et B deux points, $A' = f(A)$, $A'' = g(A')$, $B' = f(B)$ et $B'' = g(B')$. On a :

$$h(A)\,h(B) = A''B'' = g(A')\,g(B') = A'B' = f(A)\,f(B) = AB$$

donc h conserve bien les distances.

• *Soit f une isométrie. On sait déjà que f^{-1} est une transformation.*

Soit A et B deux points du plan, $A' = f^{-1}(A)$ et $B' = f^{-1}(B)$. On a $A = f(A')$ et $B = f(B')$, donc $AB = A'B'$, ce qui montre que f^{-1} conserve les distances.

II Composées de deux réflexions

Les réflexions (i.e. les symétries axiales) jouent un rôle central dans l'étude des isométries. Nous allons présenter ici deux résultats fondamentaux concernant leurs composées.

Théorème 9

Soit d_1 et d_2 deux droites *parallèles*. La composée des symétries s_{d_1} et s_{d_2} est une *translation* dont le vecteur est un vecteur orthogonal à la direction commune des deux droites.

Plus précisément, si A_1 est un point de d_1 et A_2 son projeté orthogonal sur d_2, alors $s_{d_2} \circ s_{d_1} = t_{2\overrightarrow{A_1A_2}}$.

Réciproquement, toute translation peut s'écrire, d'une infinité de façons différentes, comme la composée de deux réflexions d'axes parallèles. ★

Théorème 10

Soit d_1 et d_2 deux droites *sécantes*. La composée des symétries s_{d_1} et s_{d_2} est une *rotation* dont le centre est le point d'intersection Ω des deux droites.

Plus précisément, si A_1 est un point de d_1 et A_2 un point de d_2, tous deux distincts de Ω, alors $s_{d_2} \circ s_{d_1} = r_{\Omega,2\left(\overrightarrow{OA_1},\overrightarrow{OA_2}\right)}$.

Réciproquement, toute rotation peut s'écrire, et ce d'une infinité de façons, comme la composée de deux réflexions d'axes passant par son centre. ★

La démonstration de ces deux théorèmes et de leurs réciproques fait l'objet du TD n°1 p.135, et de l'exercice 13 p.140. Ces démonstrations sont données en annexe de ce cours.

Exercices :

- Montrer que la composée de deux rotations de même centre est une rotation.
- Montrer que la composée de deux rotations de centres distincts est une rotation ou une translation.
- Exercices 4, 5 et 10 p.139.

III Classification des isométries

Nous avons vu que les symétries (axiales ou centrales), rotations et translations sont des isométries. Y en a-t-il d'autres ? Cette section va répondre en partie à cette question.

A Point invariant

Définition 10 : *On dit qu'un point A est* invariant *par la transformation f, ou bien que f laisse A invariant, si $f(A) = A$. On dit aussi parfois que A est un* point fixe *de f.*

Exercice : Quels sont les points fixes d'une translation ? D'une symétrie ? D'une homothétie ? D'une translation ?

Remarques :

- Si f est une isométrie laissant A invariant, alors pour tout point M tel que $M' = f(M) \neq M$, A appartient à la médiatrice de $[MM']$.

  Preuve *En effet, de $A = f(A)$ et $M' = f(M)$, on tire, par conservation des distances, $AM' = AM$, donc A appartient à la médiatrice de $[MM']$.*

- Si f est une isométrie laissant invariants les points distincts A et B, alors f laisse fixes *tous* les points de la droite (AB).

  Preuve *En effet, si M est un point distinct de A et B admettant pour image M' par f, alors $AM' = AM$ et $BM' = BM$, de sorte que M' appartient au cercle de centre A et de rayon AM, et au cercle de centre B et de rayon BM.*

  Or si $M \in (AB)$, ces deux cercles sont tangents en M, et ne se rencontrent donc qu'en un seul point. Ainsi M' ne peut être qu'en M.

B Classification des isométries selon le nombre de points invariants

Commençons par caractériser l'identité :

Théorème 11
Si f est une isométrie laissant fixes trois points *non alignés*, alors f est l'identité.

Preuve *Supposons que le point M soit tel que $M' = f(M) \neq M$. A, B et C doivent alors appartenir à la médiatrice de $[MM']$, ce qui n'est pas possible puisqu'ils ne sont par hypothèse pas alignés.*

Ainsi, l'hypothèse $M' \neq M$ ne tient pas, et pour tout M, $f(M) = M$. f est donc bien l'identité.

Caractérisons maintenant les symétries axiales :

Théorème 12
Si f est une isométrie laissant fixes deux points, alors f est l'identité ou la symétrie d'axe (AB).

Preuve *On sait déjà que tout point de la droite (AB) est invariant.*

Si il existe $M \notin (AB)$ tel que $f(M) = M$, alors f admet trois points invariants non alignés, on sait alors que $f = \mathrm{I}$.

Le seul autre cas possible est que $f(M) \neq M$ pour tout $M \notin (AB)$. On sait alors que (AB) est la médiatrice de $[MM']$. f est donc la symétrie d'axe (AB).

Traitons le cas des rotations :

Théorème 13
Si f est une isométrie admettant un unique point invariant. Alors f est une rotation.

Preuve *Notons Ω l'unique point fixe. Soit B un point distinct de Ω, d'image $B' = f(B)$.*

D'après la remarque précédente, la médiatrice Δ de $[BB']$ passe par Ω. Notons s la symétrie d'axe Δ, et $g = s \circ f$.

On a $g(\Omega) = s(f(\Omega)) = s(\Omega) = \Omega$ car $\Omega \in \Delta$, et $g(B) = s(f(B)) = s(B') = B$. Donc g admet deux points invariants. On a vu que g est soit l'identité, soit la symétrie axiale d'axe $\Delta' = (\Omega B)$.

De $g = s \circ f$, on tire $s \circ g = s \circ s \circ f = f$. On ne peut pas avoir $g = \mathrm{I}$, sinon f serait égale à s, et admettrait plus d'un point invariant.

Donc g est la symétrie axiale s' d'axe Δ', et f est la composée $s \circ s'$. Les axes de ces deux symétries étant sécants, f est une rotation de centre Ω.

Existe-t-il des isométries n'admettant aucun point fixe ? La réponse est oui, et ce sont des transformations que nous ne connaissions pas encore.

Théorème 14
Si f est une isométrie n'admettant aucun point invariant, alors f est uen translation, ou la composée de trois réflexions.

Preuve *Soit A un point, d'image A'. Notons Δ la médiatrice de $[AA']$, s la symétrie d'axe Δ et $g = s \circ f$.*

$g(A) = s(f(A)) = s(A') = A$, donc g laisse fixe le point A. D'après ce qui précède, g est l'identité, une réflexion d'axe Δ' ou une rotation.

Le premier cas est impossible : si g était l'identité, de $s \circ f = g$, on tirerait $f = s \circ s \circ f = s \circ g = s$, et f devrait laisser invariante la droite Δ.

De même, si g était une réflexion dont l'axe Δ' rencontrait Δ, alors f serait une rotation, ce qui est exclus.

g est donc soit une réflexion d'axe Δ' parallèle à Δ, et f est une translation, soit une rotation, donc la composée de deux réflexions, et f est la composée de trois réflexions.

Une autre façon de décrire une composée de trois réflexions est la suivante : si $f = s_1 \circ s_2 \circ s_3$, notons $r = s_2 \circ s_3$. r est une rotation, donc on peut l'écrire $s_2' \circ s_3'$, et on peut choisir l'axe de s_2' parallèle à celui de s_1.

Ainsi, $f = s_1 \circ s_2' \circ s_3'$, et comme $s_1 \circ s_2'$ est une translation, on arrive à la conclusion suivante :

f est la composée d'une translation et d'une réflexion.

Résumons les résultats de cette section sous la forme d'un *théorème de structure* :

Théorème 15

- Une isométrie plane peut se décomposer (de plusieurs façons) comme le produit d'au plus trois réflexions.
- La seule isométrie qui laisse invariants trois points non alignés est l'identité.
- Une isométrie laissant invariant au moins un point est une réflexion ou une rotation. ★

IV Propriétés des isométries

A Isométrie et produit scalaire

Théorème 16

Une isométrie conserve le produit scalaire. Autrement dit, si A, B et C sont trois points d'images respectives A', B' et C' par l'isométrie f, alors

$$\overrightarrow{A'B'}.\overrightarrow{A'C'} = \overrightarrow{AB}.\overrightarrow{AC}$$

Preuve *Calculons de deux façons différentes $B'C'^2$: d'une part*

$$B'C'^2 = \overrightarrow{B'C'}^2 = \left(\overrightarrow{A'C'} - \overrightarrow{A'B'}\right)^2 = A'C'^2 - 2\overrightarrow{A'B'}.\overrightarrow{A'C'} + A'B'^2$$

d'autre part

$$B'C'^2 = BC^2 = \left(\overrightarrow{AC} - \overrightarrow{AB}\right)^2 = AC^2 - 2\overrightarrow{AB}.\overrightarrow{AC} + AB^2$$

Comme on a de plus $A'B' = AB$ et $A'C' = AC$, on en déduit en soustrayant ces deux égalités :

$$2\left(\overrightarrow{AB}.\overrightarrow{AC} - \overrightarrow{A'B'}.\overrightarrow{A'C'}\right) = 0$$

d'où le résultat.

Voici une conséquence essentielle de ce résultat :

Théorème 17

Soit f une isométrie, et $\left(O; \overrightarrow{OI}, \overrightarrow{OJ}\right)$ un repère orthonormé du plan. Notons $O' = f(O)$, $I' = f(I)$ et $J' = f(J)$. Alors :

- le repère $\left(O'; \overrightarrow{O'I'}, \overrightarrow{O'J'}\right)$ est orthonormé ;
- si le point M a pour coordonnées $(x; y)$ dans le repère $\left(O; \overrightarrow{OI}, \overrightarrow{OJ}\right)$, alors son image $M' = f(M)$ a les mêmes coordonnées $(x; y)$ *dans le repère transformé* $\left(O'; \overrightarrow{O'I'}, \overrightarrow{O'J'}\right)$.

Preuve

- *On a d'une part $\overrightarrow{O'I'}.\overrightarrow{O'J'} = \overrightarrow{OI}.\overrightarrow{OJ} = 0$, d'autre part $O'I' = OI = OJ = O'J'$, donc le repère $\left(O'; \overrightarrow{O'I'}, \overrightarrow{O'J'}\right)$ est orthogonal et normé.*
- *Dire que M a pour coordonnées $(x; y)$ revient à dire que $\overrightarrow{OM} = x\overrightarrow{OI} + y\overrightarrow{OJ}$.*
  Ainsi $x = \overrightarrow{OM}.\overrightarrow{OI} = \overrightarrow{O'M'}.\overrightarrow{O'I'}$, ce qui revient à dire que l'abscisse de M' dans le nouveau repère $\left(O'; \overrightarrow{O'I'}, \overrightarrow{O'J'}\right)$ est encore x. On procède de même avec l'ordonnée de M.

B Isométrie et barycentres

Théorème 18

Les isométries conserve les barycentres. Autrement dit, si G est le barycentre de la famille massique $((A_1, \alpha_1), \ldots, (A_n, \alpha_n))$, si $G' = f(G)$ et $A'_i = f(A_i)$ pour $1 \leqslant i \leqslant n$, alors G' est le barycentre de la famille massique $((A'_1, \alpha_1), \ldots, (A'_n, \alpha_n))$.

Preuve *Laissée en exercice. Utiliser le résultat précédent.*

C Image d'une droite, d'un segment, d'un cercle par une isométrie

Théorème 19

- L'image d'une droite par une isométrie est une droite.
- L'image de segment $[AB]$ par une isométrie f est le segment $[A'B']$, où $A' = f(A)$ et $B' = f(B)$
- L'image d'un cercle de centre Ω par une isométrie f est un cercle de même rayon, et de centre $\Omega' = f(\Omega)$..

Preuve *Toutes ces preuves sont laissées en exercice.*

D Conservation du parallélisme, des angles...

Théorème 20

Une isométrie conserve les égalités vectorielles : A, B, C et D sont quatre points d'images respectives A', B', C' et D', et si $\overrightarrow{AB} = \overrightarrow{CD}$, alors $\overrightarrow{A'B'} = \overrightarrow{C'D'}$.

Preuve *Cela vient du fait que les coordonnées de $\overrightarrow{A'B'}$ (resp. de $\overrightarrow{C'D'}$ dans le repère image sont les mêmes que celles de $\overrightarrow{AB}$ (resp. $\overrightarrow{CD}$) dans le repère initial.*

On déduit de ce premier théorème que l'image d'un parallélogramme par une isométrie est un parallélogramme.

V Déplacements

CHAPITRE VI

Généralités sur les similitudes planes

I Les similitudes planes

Nous allons introduire, dans cette section, une nouvelle transformation du plan plus générale que celles déjà connues : la similitude plane. En effet, toutes les transformations que nous connaissons vont apparaître comme des cas particuliers de cette nouvelle transformation.

A Définition

Définition 11 : *Un* similitude *(plane) est une transformation du plan qui conserve les rapports de distances. Autrement dit, si M, N, P, Q sont quatre points ($M \neq N$ et $P \neq Q$), d'images respectives M', N', P', Q', alors :*

$$\frac{M'N'}{P'Q'} = \frac{MN}{PQ}$$

Remarquons que la définition précédente est valide : si $P \neq Q$, alors $P' \neq Q'$ (car une similitude est en particulier une transformation), donc les deux numérateurs des fractions ci-dessus sont non nuls.

Théorème 21

σ est une similitude si et seulement si il existe un réel $k > 0$ tel que σ multiplie toutes les distances par un réel $k > 0$ fixé, appelé *rapport de la similitude.*

Preuve *Soit σ une similitude., M et N deux points distincts, d'images respectives M' et N'. Notons k le rapport $\dfrac{M'N'}{MN}$, qui est non nuls car M' et N' sont nécessairement distincts.*

Si P et Q sont deux autres points, d'images P' et Q', alors $\dfrac{P'Q'}{M'N'} = \dfrac{PQ}{MN}$, donc

$$P'Q' = PQ\frac{M'N'}{MN} = kPQ$$

La donnée des images de deux points distincts fixe donc la valeur du rapport de l'homothétie.

Réciproquement, si σ est une transformation du plan multipliant toutes les distances par un même réel $k > 0$, alors si M, N, P, Q sont quatre points ($M \neq N$ et $P \neq Q$), d'images respectives M', N', P' et Q', on a : $M'N' = k\,MN$ et $P'Q' = k\,PQ$, donc

$$\frac{M'N'}{MN} = k = \frac{P'Q'}{PQ}$$

d'où $\dfrac{P'Q'}{M'N'} = \dfrac{PQ}{MN}$, i.e. σ conserve les rapports de distances et est bien une similitude.

Le problème qui se pose est le suivant : existe-t-il de telles transformations ? La réponse est clairement oui : toute translation, rotation, symétrie ou homothétie est un cas particulier de similitude. Pour les trois premières, le rapport de la similitude est 1 (c'est le cas de toutes les isométries), pour les dernières, le rapport de la similitude est $|k|$, k étant le rapport de l'homothétie.

Une autre question que l'on peut légitimement se poser : est-ce qu'une définition aussi générale a un quelconque intérêt, c'est-à-dire est-ce qu'on peut trouver des propriétés intéressantes communes à toutes ces transformations ? Encore une fois, comme on va le découvrir dans la suite de ce cours, la réponse est oui. Un certain nombre des propriétés intéressantes des transformations déjà connues se retrouvent dans ces transformations plus générales : conservation de l'alignement, du parallélisme...

Exercices :
Exercices 11, 12 et 13 p.115.

B Premières propriétés

Théorème 22
Si σ et σ' sont deux similitudes de rapports respectifs k et k', alors

- $\sigma \circ \sigma'$ est une similitude de rapport kk',
- σ^{-1} est une similitude de rapport $\dfrac{1}{k}$.

Preuve • *σ et σ' sont deux transformations du plan, donc leur composée en est aussi une. Il suffit donc de montrer que $\sigma \circ \sigma'$ multiplie les distances par kk' pour prouver que c'est une similitude.*

Soit M et M deux points distincts du plan, $M' = \sigma'(M)$, $N' = \sigma'(N)$, $M'' = \sigma(M')$ et $N'' = \sigma(N')$.

On a : $M'N' = k'\,MN$ et $M''N'' = k\,M'N'$, donc $M''N'' = (kk')\,MN$.

Comme $M'' = \sigma \circ \sigma'(M)$ et $N'' = \sigma \circ \sigma'(N)$, on a bien prouvé que $\sigma \circ \sigma'$ est une similitude de rapport kk'.

• *Soit σ une similitude de rapport k, on sait déjà que σ^{-1} est une transformation du plan, reste à montrer que c'est une similitude.*

Soit M et N deux points, M' et N' leurs images par σ^{-1} : $M' = \sigma^{-1}(M)$ et $N' = \sigma^{-1}(N)$, donc $M = \sigma(M')$ et $N = \sigma(N')$.

On a donc : $MN = k\,M'N'$, d'où $M'N' = \dfrac{1}{k}MN$, d'où le résultat.

Note culturelle

La manière mathématique d'énoncer ceci est bien entendu de dire que l'ensemble des similitudes planes est un groupe pour la loi $\circ$.

Commençons à étudier l'image de figures du plan par une similitude. On a vu ce que donnait l'image d'un couple de point, voyons ce que donne l'image d'un triangle[1]

Théorème 23
L'image d'un triangle ABC par une similitude σ est un triangle $A'B'C'$ semblable à ABC.

Preuve *On a $A' = \sigma(A)$, $B' = \sigma(B)$ et $C' = \sigma(C)$, donc si k est le rapport de la similitude σ :*

$$\frac{A'B'}{AB} = \frac{A'C'}{AC} = \frac{B'C'}{BC} = k$$

Ainsi les longueurs des cotés des deux triangles sont proportionnelles, et $A'B'C'$ est semblable à ABC.

[1] considéré pour l'instant comme le triplet de ses sommets, on ne s'intéresse pas encore à ce qu'il advient des cotés du triangle.

Cette démonstration utilise le fait que des triangles qui ont des cotés de longueurs proportionnelles sont semblables. Ceci a été démontré en seconde[2], il suffit par un déplacement de se ramener à une configuration de Thalès.

Une conséquence directe de ce théorème : pour démontrer que deux triangles sont semblables, il suffit de trouver une similitude transformant l'un en l'autre.

Voici une conséquence fondamentale de cette propriété :

Corollaire 1

Une similitude conserve les angles géométriques. ★

En fait, la démonstration précédente n'a permis de montrer que le résultat plus faible suivant : si $\widehat{ABC} \in]0, \pi[$, alors $\widehat{A'B'C'} = \widehat{ABC}$. En particulier, on n'a pas démontré que l'image d'un angle plat est un angle plat. Nous allons l'admettre pour l'instant, ceci sera démontré sans difficulté particulière plus tard à l'aide des complexes :

Théorème 24

- Une similitude conserve l'alignement des points.
- L'image d'une droite par une similitude est une droite.
- L'image d'une demi-droite (resp. d'un segment) par une similitude est une demi-droite (resp. un segment).
- L'image d'un cercle de rayon ρ par une similitude de rapport k est un cercle de rayon $\rho' = k\rho$. ★

Exercices :

- Cherchez une méthode géométrique pour démontrer qu'une similitude transforme trois points alignés en trois points alignés.
- Comment démontrer à l'aide des propriétés déjà rencontrées le fait que l'image d'un segment par une similitude est encore un segment ?
- Exercice 28 p.116.
- Exercice 50 p.118.

C Caractérisation d'une similitude par ses images

Une translation est caractérisée par la donnée de l'image d'un unique point ($M' = t_{\vec{u}}(M) \iff \vec{u} = \overrightarrow{MM'}$). Il en est de même pour une symétrie, qu'elle soit centrale ou axiale. Pour caractériser une rotation ou une homothétie, il suffit de se donner l'image de deux points distincts. On peut le vérifier à titre d'exercice en expliquant comment trouver le centre et l'angle ou le rapport.

Une question se pose alors : de combien d'images de points doit-on disposer pour caractériser une similitude ? Les théorèmes suivants répondent à cette question. Définissons d'abord un concept qui sera essentiel dans l'identification des transformations du plan.

Définition 12 : *Soit f une transformation du plan. On dit que A est un* point fixe *de f si $f(A) = A$.*

Autrement dit un point fixe de f est un point qui est... fixe sous l'action de f.

Donnons maintenant un moyen de caractériser l'identité parmi les similitudes.

Théorème 25

Si σ est une similitude admettant trois points fixes non alignés, alors σ est l'identité.

Preuve *Soit A, B et C les trois points fixes non alignés de σ. On a donc : $\sigma(A) = A$, $\sigma(B) = B$ et $\sigma(C) = C$.*

[2]Ce cours de seconde sur les triangles semblables a d'ailleurs pour unique justification le chapitre consacré aux similitudes en spécialité de TS !

Le rapport de la similitude est : $\dfrac{\sigma(A)\,\sigma(B)}{AB} = \dfrac{AB}{AB} = 1$. *$\sigma$ est donc une isométrie.*

Soit M un point quelconque. Supposons que $M' = \sigma(M) \neq M$. Du fait que σ conserve les distances, on doit avoir

$$AM' = AM,\ BM' = BM \text{ et } CM' = CM$$

donc A, B et C doivent appartenir à la médiatrice de $[MM']$. En particulier, A, B et C sont alignés, ce qui est en contradiction avec les hypothèses.

L'hypothèse $M' \neq M$ ne tient donc pas, et on a bien démontré que pour tout point $M \in \mathscr{P}$, $\sigma(M) = M$. σ est donc bien l'identité.

On a maintenant un critère pour identifier deux similitudes :

Corollaire 2

Soit σ et σ' deux similitudes, A, B et C trois points non alignés du plan.

Si $\sigma(A) = \sigma'(A)$, $\sigma(B) = \sigma'(B)$ et $\sigma(C) = \sigma'(C)$, alors $\sigma = \sigma'$.

Preuve *Considérons la similitude composée $(\sigma')^{-1} \circ \sigma$. Elle vérifie :*

$$(\sigma')^{-1} \circ \sigma(A) = (\sigma')^{-1} \circ \sigma'(A) = A, \text{ et de même } (\sigma')^{-1} \circ \sigma(B) = B \text{ et } (\sigma')^{-1} \circ \sigma(C) = C$$

Elle admet donc trois points fixes non alignés, et ne peut être que l'identité : $(\sigma')^{-1} \circ \sigma = \mathrm{I}$. En composant cette relation à gauche par σ', on obtient alors $\sigma = \sigma'$.

Ainsi, la connaissance des images de trois points non alignés suffit à déterminer de façon unique une similitude. On peut se demander si, comme pour es autres transformations, les images de deux points ne suffiraient pas. Voici un résultat qui va nous convaincre que la réponse est non :

Théorème 26

Si σ est une similitude admettant A et B comme points fixes, alors σ est soit l'identité, soit la symétrie axiale d'axe (AB).

Preuve *Soit C un point n'appartenant pas à la droite (AB), $C' = \sigma(C)$.*

- *Si $C' = C$, alors σ admet trois points fixes non alignés, et σ est l'identité.*
- *Si $C' \neq C$, alors $AC' = AC$ et $BC' = BC$, donc A et B appartiennent à la médiatrice de $[CC']$, i.e. cette médiatrice est (AB).*

  Notons s la symétrie d'axe (AB). La composée $s \circ \sigma$ vérifie :

  $$s \circ \sigma(A) = s(A) = A,\ s \circ \sigma(B) = s(B) = B \text{ et } s \circ \sigma(C) = s(C') = C$$

  $s \circ \sigma$ admet donc trois points fixes non alignés, elle est donc égale à l'identité. On a donc, en composant par s :

  $$s = s \circ \mathrm{I} = s \circ s \circ \sigma = \mathrm{I} \circ \sigma = \sigma$$

  Donc σ est la symétrie d'axe (AB).

Troisième partie

Surfaces

ANNEXE A

Index