



Cours de spécialité mathématiques en T^{ale}S

Vincent PANTALONI

VERSION DU 16 SEPTEMBRE 2009

Table des matières

I	Arithmétique	1
I	Divisibilité et congruences dans \mathbb{Z}	3
1	Divisibilité dans \mathbb{Z}	3
1.1	Vocabulaire	3
1.2	Propriétés	3
2	Division euclidienne	5
2.1	Division euclidienne	5
2.2	Disjonction de cas	7
3	PGCD, algorithme d'EUCLIDE	7
3.1	PGCD	7
3.2	Algorithme d'EUCLIDE	8
3.3	Propriétés du PGCD	9
3.4	Nombres premiers entre eux	9
4	Congruences dans \mathbb{Z}	10
4.1	Définition	10
4.2	Propriétés immédiates	10
4.3	Compatibilité avec les opérations	11
4.4	Réduction modulo n	11
II	Nombres premiers	13
0.5	Définition	13
0.6	PGCD, PPCM et décomposition	13
III	Théorèmes de BÉZOUT et de GAUSS	17
1	Théorème de BÉZOUT	17
2	Théorème de GAUSS	19
3	Application : Équation diophantienne $ax + by = c$	19
II	Similitudes	21
IV	Similitudes	23
1	Définition géométrique	23
1.1	Similitudes du plan	23
1.2	Conservation des angles géométriques	23
2	Similitudes directes	24
2.1	Écriture complexe	24
2.2	Décomposition, éléments caractéristiques	24
2.3	Propriétés des similitudes directes	26
3	Étude générale des similitudes	28
3.1	Similitudes et points fixes	28
3.2	Caractérisation des similitudes non directes	28

Première partie

rithmétique

Chapitre I

Divisibilité et congruences dans \mathbb{Z}

Dans ce chapitre, entier signifie entier relatif, *i.e.* appartenant à \mathbb{Z} .

1 Divisibilité dans \mathbb{Z}

1.1 Vocabulaire

Définition 1. Soit a et b deux entiers relatifs ($a \in \mathbb{Z}$, $b \in \mathbb{Z}$). On dit que a divise b , et on note $a|b$ si il existe un entier relatif c tel que :

$$b = ac$$

Exemples:

- ① $3|6$ car $6 = 3 \times 2$
- ② $13|(-52)$ car $-52 = 13 \times 4$
- ③ n est pair signifie que $2|n$.
- ④ $\forall n \in \mathbb{Z}, 2|n(n+1)$ En effet :
 - Si n est pair, $n = 2p$ pour $p \in \mathbb{Z}$ et donc $n(n+1) = 2 \times p(n+1)$
 - Si n est impair, alors $n = 2p+1$ pour $p \in \mathbb{Z}$ (admis pour le moment) et donc $n(n+1) = n(2p+2) = 2 \times n(p+1)$ □

Remarque. Attention au zéro!

- ① Tout entier divise zéro. $\forall n \in \mathbb{Z}, n|0$ en effet : $0 = n \times 0$
- ② En particulier zéro divise zéro.
- ③ Zéro ne divise aucun entier non nul n en effet : $\forall c \in \mathbb{Z}, 0 \times c = 0 \neq n$

Remarque. Autres formulations. $a|b$ signifie que :

- ① b est un multiple de a .
- ② a est un diviseur de b .
- ③ Le reste dans la division euclidienne (que l'on définira plus tard dans \mathbb{Z}) de b par a est nul.
- ④ (pour $a \neq 0$) $\frac{b}{a}$ comme élément de \mathbb{Q} est un entier relatif.

⚠ Attention à l'ordre! $a|b$ signifie que $b/a = \frac{b}{a} \in \mathbb{Z}$

1.2 Propriétés

a, b, c désignent des entiers relatifs.

Propriété 1 (Réflexivité). $\forall n \in \mathbb{Z}, n|n$

Démonstration. $n = n \times 1$ □

Propriété 2 (Transitivité).

$$\begin{cases} a|b \\ b|c \end{cases} \implies a|c$$

Démonstration. On traduit les hypothèses : il existe p et q entiers tels que :

$$\begin{cases} b = ap \\ c = bq \end{cases} \implies c = (ap) \times q = a \times pq$$

□

Propriété 3. Tout entier n admet au moins quatre diviseurs (non nécessairement distincts) 1, -1 , n et $-n$.

Démonstration. Soit $n \in \mathbb{Z}$. $n = n \times 1 = 1 \times n$ et $n = -n \times (-1) = -1 \times (-n)$

□

Propriété 4. Les diviseurs d'un entier non nul n sont en nombre fini, et dans l'intervalle $[-|n|; |n|]$.

Démonstration. Soit $n \in \mathbb{Z}^*$ et soit $b, c \in \mathbb{Z}$ tel que $n = bc$. Alors $|bc| = |n|$ donc $|b| \times |c| = |n|$. Or $|c| \geq 1 \implies |b| \times |c| \geq |b|$ soit $|b| \leq |n|$. Ainsi tout diviseur b de n est compris entre $-|n|$ et $|n|$. □

Exemples: Chercher des diviseurs.

① Les diviseurs de 1 sont -1 et 1.

② Les diviseurs de 6 sont à chercher dans l'ensemble : $\{-6, -5, -4, -3, -2, -1, 1, 2, 3, 4, 5, 6\}$. Dans cet ensemble, seuls $-5, -4, 4$ et 5 ne divisent pas six. En effet : $2 \times 4 > 6$ et $2 \times 5 > 6$

Propriété 5. Pour tout entier k :

$$a|b \implies (ka)|(kb)$$

Démonstration. Il existe un entier p tel que $b = ap$, donc $kb = (ka)p$.

□

Théorème 1 (Combinaison linéaire). Si a divise b et c , alors a divise toute combinaison linéaire de b et c . i.e. $\forall k \in \mathbb{Z}, k' \in \mathbb{Z}$:

$$\begin{cases} a|b \\ a|c \end{cases} \implies a|(kb + k'c)$$

Démonstration. il existe p et q entiers tels que :

$$\begin{cases} b = ap \\ c = aq \end{cases} \implies kb + k'c = kap + k'aq \implies kb + k'c = a(kp + k'q)$$

□

Exemple: $n \in \mathbb{N}$. Prouvons que si a ($a \in \mathbb{Z}$) divise $3n + 2$ et $n - 3$ alors a divise 11. $a|(1 \times (3n + 2) - 3(n - 3))$ donc $a|11$.

Propriété 6 (Corollaire). Si a divise b et c , alors a divise $(b + c)$ et $(b - c)$.

Démonstration. On prend $k = k' = 1$ ou $k = -k' = 1$.

□

La réciproque est fautive : $2|(3 + 1)$ mais 2 ne divise ni 3 ni 1. Cependant si a divise toute combinaison linéaire de b et c , alors $a|b$ et $a|c$. Il suffit de prendre $k = 1$ et $k' = 0$ puis $k = 0$ et $k' = 1$. On a aussi la propriété utile :



Propriété 7. Si a divise b alors on a l'équivalence :

$$a|(b + c) \iff a|c$$

Démonstration. Soit a qui divise b .

(\implies) Si a divise aussi $b + c$, par le corollaire, a divise $b + c - b = c$.

(\impliedby) Si a divise aussi c , on conclut par le corollaire : $a|(b + c)$

□

Remarque. On a aussi que $d|a \iff d|(-a)$ avec $k = 1$ et $k' = 0$ dans la prop. 1.

Exemple: Déterminer les entiers naturels n tels que $n - 2$ divise $n + 12$.

$n + 12 = (n - 2) + 14$ donc :

$$(n-2)|(n+12) \iff (n-2)|((n-2)+14) \iff (n-2)|14 \iff (n-2) \in \{-14; -7; -2; -1; 1; 2; 7; 14\}$$

Ainsi les entiers naturels solution sont : 0, 1, 3, 4, 9, 16.

Exemple: ★ On appelle nombre impair, un nombre qui n'est pas pair, *i.e.* qui n'est pas divisible par 2. Prouver que les nombres impairs sont exactement les entiers de la forme $2p + 1$ où $p \in \mathbb{Z}$.

Démonstration. Il y a deux choses à prouver.

- ① Tout nombre de la forme $2p + 1$ où $p \in \mathbb{Z}$ est impair. _____
En effet, $2|2p$ mais 2 ne divise pas 1, donc $2p + 1$ n'est pas divisible par 2, donc est impair.
- ② Tout nombre impair s'écrit sous la forme $2p + 1$ où $p \in \mathbb{Z}$. _____
Par l'absurde. Supposons qu'il existe un nombre impair positif m tel que $m - 1$ n'est pas pair. On note encore m le plus petit entier vérifiant cette propriété. On va prouver qu'en fait $(m - 1)$ la vérifie aussi.
 $2|(-2)$ donc : $2|m \iff 2|(m - 2)$ par la prop 7. Or 2 ne divise pas m , donc :
 m impair $\implies m - 2$ impair. Mais alors $m - 1$ est encore un nombre impair à qui si on retranche un, donne un nombre impair $(m - 2)$. Ceci contredit que m est le plus petit impair vérifiant cette propriété. Ainsi pour tout impair positif q , $q - 1$ est pair donc $q - 1 = 2p \implies q = 2p + 1$. De même avec les négatifs.

□

Propriété 8 (Combinaison linéaire, généralisation). Si a divise n entiers $(a_i)_{1 \leq i \leq n}$ (où $n \in \mathbb{N}$) alors a divise toute combinaison linéaire des a_i . *i.e.*

$$\forall (k_i)_{1 \leq i \leq n} \in \mathbb{Z}^n, \quad a \mid \left(\sum_{i=1}^n k_i a_i \right)$$

Démonstration. Par récurrence sur n à partir du théorème 1. □

Exemple: 3 divise tout nombre qui s'écrit en base 10 avec uniquement les chiffres 0, 3, 6, 9. En effet un tel nombre est une combinaison linéaire de 0, 3, 6 et 9, or 3 divise 0, 3, 6 et 9. Par exemple, $60393 = 6 \times 10^4 + 0 \times 10^3 + 3 \times 10^2 + 9 \times 10^1 + 3 \times 10^0 = 6 \times 10^4 + 3 \times (10^2 + 1) + 9 \times 10$. C'est le cas où $a = 3$ et par exemple $a_1 = 6$ et $k_1 = 10^4$, $a_2 = 3$ et $k_2 = 101$, $a_3 = 9$ et $k_3 = 10$

Exercice n° 1

Prouver que la somme de trois entiers consécutifs est divisible par 3.

Exercices

Pages 29–31 n° de 1 à 23

n° 4, 6, 7, 8, 11, 12, 17, 18, 19, 20, 21.

2 Division euclidienne

2.1 Division euclidienne

Théorème 2. Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q; r)$ d'entiers relatifs tels que :

$$a = bq + r \text{ et } 0 \leq r < b$$

Définition 2. Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Effectuer la division euclidienne de a par b , c'est trouver l'unique couple $(q; r)$ d'entiers relatifs tels que $a = bq + r$ et $0 \leq r < b$.

- a s'appelle le dividende.
- b s'appelle le diviseur.
- q s'appelle le quotient.
- r s'appelle le reste.

Démonstration. On doit prouver l'existence et l'unicité du couple $(q; r)$.

Existence On note bq le plus grand multiple de b qui est inférieur ou égal à a . Le multiple suivant est $b(q+1)$. On a donc :

$$bq \leq a < b(q+1) \implies 0 \leq a - bq < b$$

On pose alors : $r = a - bq$ et on a bien l'égalité voulue.


Unicité On suppose qu'il existe deux couples d'entiers $(q; r)$ et $(q'; r')$ vérifiant la conclusion du théorème. En soustrayant les deux égalités on obtient :

$$\begin{cases} a = bq + r \\ a = bq' + r' \end{cases} \implies 0 = b(q - q') + r - r' \implies r' - r = b(q - q')$$

Ainsi $r' - r$ est un multiple de b . Par ailleurs :

$$\begin{cases} 0 \leq r < b \\ 0 \leq r' < b \end{cases} \implies \begin{cases} 0 \geq -r > -b \\ 0 \leq r' < b \end{cases} \implies -b < -r \leq r' - r < b - r \leq b \implies -b < r' - r < b$$

Donc $r' - r$ est un multiple de b strictement compris entre $-b$ et b . C'est donc ... zéro ! Ainsi $r = r'$ et par suite $q = q' = \frac{a-r}{b}$. \square

Remarque. Pour trouver q et r , on pose la division comme au primaire. Si on veut utiliser la calculatrice, on a en fait que $q = E\left(\frac{a}{b}\right)$. Puis $r = a - bq$. 

Il ne faut pas oublier la condition d'encadrement du reste.

Exemples:

- ① $47 = 5 \times 8 + 7$ traduit la division euclidienne de quoi par quoi ? Donner dividende, diviseur, quotient et reste. Effectuer à la main à partir de cette égalité la division de 47 par 5. Puis la division de -47 par 8 ($-47 = -5 \times 8 - 7 = -5 \times 8 - 7 + 8 - 8 = -6 \times 8 + 1$).
- ② $127 = 16 \times 7 + 15$. Idem. Effectuer la division de 127 par 7 ($18 \times 7 + 1$) Puis la division de -127 par 16 ($-127 = -7 \times 16 - 15 = -7 \times 16 - 15 + 16 - 16 = -8 \times 16 + 1$).

Exercice n° 2

Calculer à la main $\sin\left(2007 \times \frac{\pi}{2}\right)$.

$\sin(n\frac{\pi}{2})$ est 4 périodique, or $2007 = 4 \times 501 + 3$. Donc :

$$\sin\left(2007 \times \frac{\pi}{2}\right) = \sin\left(501 \times 2\pi + 3 \times \frac{\pi}{2}\right) = \sin\left(\frac{3\pi}{2}\right) = -1$$

Exercice n° 3

Soit $n \in \mathbb{N}$. Quel est le reste de la division euclidienne de $(n+2)^2$ par $n+3$?

$$(n+2)^2 = n^2 + 4n + 4 = n(n+3) + n + 4 = (n+1)(n+3) + 1 \quad \text{et} \quad 0 \leq 1 < n+3$$

Le reste est donc 1.

Exercice n° 4

Soit $n \in \mathbb{N}$. Quel est le reste de la division euclidienne de $(n+5)^2$ par $n+3$? Pour quelle(s) valeur(s) de n , $(n+5)^2$ est-il un multiple de $n+3$?

$$(n+5)^2 = n^2 + 10n + 25 = n(n+3) + 7n + 25 \quad \text{mais} \quad 7n + 25 > n+3$$

$$(n+5)^2 = n(n+3) + 7(n+3) + 4 = (n+7)(n+3) + 4$$

Le reste est donc 4 si $4 < n+3$ i.e. lorsque $n \geq 2$. Sinon :

$$(n+5)^2 = (n+8)(n+3) + 4 - n - 3$$

Pour $n=0$ et $n=1$ le reste est donc $1-n$ i.e. resp. 1 et 0. Ainsi c'est uniquement lorsque $n=1$ que $(n+5)^2$ est un multiple de $n+3$. On vérifie : $36 = 9 \times 4$.

2.2 Disjonction de cas

D'après le théorème 2 tout nombre entier a a une écriture comme multiple de b ($b \in \mathbb{N}^*$) plus un reste qui est parmi une des b valeurs : $0, 1, \dots, b-1$.

Exemples:

- ① Tout entier s'écrit (de manière unique) sous la forme $2p$ ou $2p+1$ avec $p \in \mathbb{Z}$.
- ② Tout entier s'écrit (de manière unique) sous la forme $3p$ ou $3p+1$ ou $3p+2$ avec $p \in \mathbb{Z}$.

Ceci permet de résoudre des problèmes par disjonctions de cas, en fonction des différents restes possibles.

Exercice n° 5

Prouver que parmi trois entiers consécutifs il y a un multiple de trois et un seul.

Trois entiers consécutifs sont de la forme $n, n+1, n+2$ où $n \in \mathbb{Z}$.

1^{er} cas Soit $n = 3k$, $k \in \mathbb{Z}$, et alors $n+1$ et $n+2$ ne sont pas multiples de 3, mais n l'est.

2^e cas Soit $n = 3k+1$, $k \in \mathbb{Z}$, et alors n et $n+1 = 3k+2$ ne sont pas multiples de 3 mais $n+2 = 3(k+1)$ l'est.

3^e cas Soit $n = 3k+2$, $k \in \mathbb{Z}$, et alors n et $n+2 = 3(k+1) + 1$ ne sont pas multiples de 3 mais $n+1 = 3(k+1)$ l'est. □

Exercices

page 31–32 n° 24–44.

3 PGCD, algorithme d'EUCLIDE

Prérequis sur les ensembles :

- ① Toute partie non vide de \mathbb{N} admet un plus petit élément.
- ② Toute partie non vide et finie de \mathbb{Z} admet un plus grand élément.
- ③ Pour tous ensembles A et B , on a : $A \cap B \subset A$.
- ④ Dire que deux ensembles A et B sont égaux (ont les mêmes éléments) revient à dire que $A \subset B$ et $B \subset A$.

3.1 PGCD

Soit a et b dans \mathbb{Z}^* . On note \mathcal{D}_a (resp. \mathcal{D}_b) l'ensemble des diviseurs de a (resp. de b). Ces ensembles sont finis par la propriété 4. L'intersection $\mathcal{D}_a \cap \mathcal{D}_b$ est l'ensemble des diviseurs communs à a et à b . Cette intersection est donc un ensemble fini, et non vide puisqu'elle contient au moins 1 et -1 . Ainsi elle admet un plus grand élément qui est le plus grand diviseur qui soit commun à a et b . C'est le PGCD de a et b .

Définition 3. Soit a et b dans \mathbb{Z}^* . Le plus grand entier qui divise a et b est appelé « plus grand commun diviseur de a et b » on le note $\text{PGCD}(a; b)$

Remarque. Cette notion peut s'étendre à plus que deux entiers.

Propriété 9. $b|a \iff \text{PGCD}(a; b) = |b|$

Démonstration. On démontre chaque sens séparément.

(\implies) Supposons $b|a$. Cela implique que $|b|$ divise a et b et comme $|b|$ est le plus grand diviseur de b , c'est *a fortiori* le plus grand diviseur de a et b . Donc $\text{PGCD}(a; b) = |b|$.

(\impliedby) Supposons $\text{PGCD}(a; b) = |b|$. Alors $|b|$ est un diviseur de a et b , donc $b|a$. □

Une méthode pour déterminer le PGCD de deux entiers est l'algorithme d'EUCLIDE.

3.2 Algorithme d'EUCLIDE

Lemme 1 (d'Euclide). Soit a, b, q, r dans \mathbb{Z} tels que $a = bq + r$. Alors : $\text{PGCD}(a; b) = \text{PGCD}(b; r)$

Démonstration. On prouve que $\mathcal{D}_a \cap \mathcal{D}_b = \mathcal{D}_b \cap \mathcal{D}_r$. Soit $d \in \mathbb{Z}$ tel que $d|b$ i.e. $d \in \mathcal{D}_b$. Par la propriété 1 on a :

$$d|a \implies d|(a - bq) \implies d|r \quad \text{i.e.} \quad \mathcal{D}_a \cap \mathcal{D}_b \subset \mathcal{D}_b \cap \mathcal{D}_r$$

$$d|r \implies d|(bq + r) \implies d|a \quad \text{i.e.} \quad \mathcal{D}_b \cap \mathcal{D}_r \subset \mathcal{D}_a \cap \mathcal{D}_b$$

Ainsi on a l'équivalence $\boxed{d|a \iff d|r}$ i.e. $\mathcal{D}_a \cap \mathcal{D}_b = \mathcal{D}_b \cap \mathcal{D}_r$. Donc ces ensembles ont le même plus grand élément, d'où le résultat. \square

Propriété 10 (Algorithme d'Euclide). Pour calculer le PGCD de deux entiers a et b dans \mathbb{N}^* avec $a > b$ on procède par divisions euclidiennes successives, jusqu'à obtenir un reste nul. Le dernier reste non nul est $\text{PGCD}(a; b)$.

Démonstration. Dans le tableau schématisant I.1 schématisant les différentes opérations, on a noté r_0, r_1, \dots, r_n les restes successifs qui forment une suite strictement décroissante d'entiers naturels :

$$b > r_0 > r_1 > r_2 > \dots > r_n$$

Une telle suite finit nécessairement par atteindre zéro. On note $r_{n+1} = 0$ et il suffit donc de prouver que $r_n = \text{PGCD}(a; b)$. Par le lemme d'Euclide, on a à chaque étape :

$\text{PGCD}(a; b) = \text{PGCD}(b; r_0) = \text{PGCD}(r_0; r_1) = \dots = \text{PGCD}(r_{n-1}; r_n)$ Or la division euclidienne de r_{n-1} par r_n admet un reste nul donc $r_n | r_{n-1}$. Par la propriété 9 : $\text{PGCD}(r_{n-1}; r_n) = r_n$ \square

Division de ...	reste
a par b	r_0
b par r_0	r_1
r_0 par r_1	r_2
r_1 par r_2	r_3
\vdots	\vdots
r_{n-2} par r_{n-1}	r_n
r_{n-1} par r_n	0

TAB. I.1 – Algorithme d'EUCLIDE

Remarque. Quel est le nombre maximum d'étapes possibles dans l'algorithme d'Euclide si on cherche le PGCD de deux **chiffres** ? On peut tout essayer, ou remonter l'algorithme d'Euclide. Ce maximum est atteint, si l'on divise les deux termes successifs 8 et 5 de la suite de Fibonacci. Pour le PGCD de 8 et 5, on a 4 divisions ce qui est le maximum pour l'algorithme appliqué à deux chiffres :

Division de ...	reste
8 par 5	3
5 par 3	2
3 par 2	1
2 par 1	0

TAB. I.2 – Algorithme d'EUCLIDE pour 8 et 5

Remarque. On s'est borné au cas où a et b dans \mathbb{N}^* avec $a > b$. Cette condition n'est pas restrictive car les diviseurs d'un nombre et de son opposé sont les mêmes, donc $\text{PGCD}(a; b) = \text{PGCD}(|a|; |b|)$ pour a et ab dans \mathbb{Z} . Et par ailleurs, parmi deux entiers naturels a et b , il y en a un qui est plus grand que l'autre. On commence donc par diviser le plus grand par le plus petit.

3.3 Propriétés du PGCD

Propriété 11. Soit a, b, d dans \mathbb{Z} . Les diviseurs communs de a et b sont exactement les diviseurs de $\text{PGCD}(a; b)$ i.e. :

$$\left\{ \begin{array}{l} d|a \\ d|b \end{array} \right\} \iff d|\text{PGCD}(a; b)$$

Démonstration. On démontre chaque sens séparément. On pose $g = \text{PGCD}(a; b)$.

- (\Leftarrow) Si $d|g$, comme $g|a$ alors par transitivité, $d|a$. De même si $d|g$, comme $g|b$ alors par transitivité, $d|b$.
 (\Rightarrow) Si $d|a$ et $d|b$, alors si on suit l'algorithme d'Euclide appliqué à $|a|$ et $|b|$, on a : $|a| = |b|q + r_0 \Rightarrow r_0 = |a| - |b|q$ donc $d|r_0$. On continue ainsi, donc :

$$\left\{ \begin{array}{l} d|a \\ d|b \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} d|b \\ d|r_0 \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} d|r_0 \\ d|r_1 \end{array} \right\} \Rightarrow \dots \Rightarrow \left\{ \begin{array}{l} d|r_{n-1} \\ d|r_n \end{array} \right\}$$

Or $r_n = g$ donc $d|g$ □

Exemple: Déterminer les diviseurs communs à 3042 et 315.
 $3042 = 2 \times 3^2 \times 13^2$ et $315 = 3^2 \times 5 \times 7$ donc $g = 9$.

Propriété 12. $a \in \mathbb{N}, b \in \mathbb{N}, k \in \mathbb{N}^*$. $\text{PGCD}(ka; kb) = k \times \text{PGCD}(a; b)$

Démonstration. On opère la division euclidienne de a par b : $a = bq + r \Rightarrow ka = kb \times q + kr_0$. Or $0 \leq r_0 < b \Rightarrow 0 \leq kr_0 < kb$. Donc $ka = kb \times q + kr_0$ décrit la division euclidienne de ka par kb , il reste kr_0 . On suit alors l'algorithme d'Euclide appliqué à ka et kb et on obtient les restes $kr_0, kr_1, kr_2, \dots, kr_n$ puis zéro. Donc le PGCD de ka et kb est bien $k \times \text{PGCD}(a; b)$. □

Remarque. $a \in \mathbb{Z}, b \in \mathbb{Z}, k \in \mathbb{Z}^*$. $\text{PGCD}(ka; kb) = |k| \times \text{PGCD}(a; b)$

On utilise parfois cette propriété avec une division ayant pour but de simplifier :

Propriété 13 (Corollaire). $a \in \mathbb{N}, b \in \mathbb{N}, k \in \mathbb{N}^*$. $\text{PGCD}(\frac{a}{k}; \frac{b}{k}) = \frac{1}{k} \times \text{PGCD}(a; b)$

Exemple: $\text{PGCD}(800; 500) = 100$. Comme $\text{PGCD}(36; 24) = 12$ alors $\text{PGCD}(3; 2) = 1$

3.4 Nombres premiers entre eux

Définition 4. On dit que deux entiers sont premiers entre eux si leur PGCD est 1.

Ce qui signifie que les deux entiers n'ont que deux diviseurs communs : 1 et -1 .

Exemple: 36 et 35 sont premiers entre eux, 16 et 18 ne le sont pas car ils sont tous deux pairs.
 ⚠ Ne pas confondre avec la notion de nombre premier.

Exercice n° 6

Prouver que deux entiers consécutifs sont toujours premiers entre eux.

$d|n$ et $d|(n+1)$ implique $d|1$ donc $d \in \{-1; 1\}$ donc $\text{PGCD}(n; n+1) = 1$.

Remarque. Cette notion s'étend à un nombre quelconque d'entiers. Dire que trois entiers sont premiers entre eux signifie que le plus grand nombre divisant ces trois entiers est 1.

Exemple: Prouver que 6, 10 et 15 sont premiers entre eux mais ne sont pas deux à deux premiers entre eux. Les diviseurs positifs de 6 sont 1, 2, 3, 6 or seul 1 et 3 divise 15 mais 3 ne divise pas 10, donc le plus grand entier divisant ces trois nombres est 1. Mais $\text{PGCD}(6, 10) = 2$ et $\text{PGCD}(10, 15) = 5$ et $\text{PGCD}(6, 15) = 3$.

Parfois on a besoin de se ramener à un couple d'entiers qui sont premiers entre eux, proportionnels aux entiers de départ. C'est possible :

Propriété 14. $a \in \mathbb{Z}^*, b \in \mathbb{Z}^*$. On pose $g = \text{PGCD}(a; b)$. Alors $\frac{a}{g}$ et $\frac{b}{g}$ sont deux entiers premiers entre eux.

Démonstration. D'abord, ce sont bien des entiers, et par la propriété 13 on a :

$$\text{PGCD}\left(\frac{a}{g}; \frac{b}{g}\right) = \frac{1}{g} \times \text{PGCD}(a; b) = 1$$

□

pages 33–34 n° 60–81 **Exercices**

4 Congruences dans \mathbb{Z}

$n \in \mathbb{N}$.

4.1 Définition

Définition 5. On dit que deux entiers relatifs a et b sont « congrus modulo n » si leur différence est un multiple de n . On le note :

$$a \equiv b [n] \quad \text{ou} : \quad a \equiv b \pmod{n}$$

On a donc :

$$a \equiv b [n] \iff \exists k \in \mathbb{Z}; a = b + kn$$

Exemples:

- ① $43 \equiv 3 [10]$ car $43 - 3 = 4 \times 10$ ou $43 = 4.10 + 3$ et $3 = 0.10 + 3$
- ② $43 \equiv -7 [10]$ car $43 + 7 = 5 \times 10$
- ③ $-43 \equiv 7 [10]$ car $-43 - 7 = -5 \times 10$
- ④ « a est pair » se traduit par : $a \equiv 0 [2]$.
- ⑤ « a est impair » se traduit par : $a \equiv 1 [2]$.

Propriété 15. Deux entiers ont même reste dans la division euclidienne par n ssi leur différence est un multiple de n .

Démonstration. Straight forward. Soit a et b dans \mathbb{Z}^* . On écrit la division euclidienne de a et b par n :

$$a = nq + r \quad \text{avec } 0 \leq r < n \quad \text{et} \quad b = nq' + r' \quad \text{avec } 0 \leq r' < n$$

$$a - b = n(q - q') + (r - r'). \quad \text{Et } -n < r - r' < n. \quad \text{Donc } n|(a - b) \iff n|(r - r') \iff r - r' = 0. \quad \square$$

Remarque (importante). Par la prop. précédente, la def de a est congru à b modulo n est donc : équivalente à : a et b sont « congrus modulo n » si ils ont même reste dans la division euclidienne par n .

4.2 Propriétés immédiates

Propriété 16. Si r est le reste de la division euclidienne de a par n alors on a : $a \equiv r [n]$

Réciproque ? Vraie si $0 \leq r \leq n - 1$

Propriété 17. Si $a = b$, alors $a \equiv b [n]$.

Propriété 18. Si $a \equiv b [n]$ alors $a \equiv b + kn [n]$ pour $k \in \mathbb{Z}$. En particulier :

$$a \equiv b [n] \implies a \equiv b \pm n [n]$$

Propriété 19. (***) La relation $\equiv [n]$ est comme l'égalité une relation d'équivalence. Elle est (RST) Réflexive, symétrique et transitive.

Démonstration. Straight forward

(***)

□

4.3 Compatibilité avec les opérations

a, b, c, d dans \mathbb{Z} . La relation de congruence est compatible avec la somme, la différence, le produit et l'exponentiation (les puissances). Plus précisément :

Propriété 20. Si $a \equiv b [n]$ et $c \equiv d [n]$ alors :

- ① $a + c \equiv b + d [n]$
- ② $a - c \equiv b - d [n]$
- ③ $ac \equiv bd [n]$
- ④ $a^p \equiv b^p [n]$ pour tout $p \in \mathbb{N}$

Démonstration. On part de $a = b + kn$ et $c = d + k'n$ où $k \in \mathbb{Z}, k' \in \mathbb{Z}$

- ① $a + c = b + kn + d + k'n = b + d + n(k + k')$ donc : $a + c \equiv b + d [n]$
- ② $a - c = b + kn - d - k'n = b - d + n(k - k')$ donc : $a - c \equiv b - d [n]$
- ③ $ac = (b + kn)(d + k'n) = bd + n(kd + k'b)$ donc : $ac \equiv bd [n]$
- ④ On déduit de la précédente que : $a^2 \equiv b^2 [n]$ puis : $a^3 \equiv b^3 [n]$ puis de proche en proche (ou par récurrence immédiate) : $a^p \equiv b^p [n]$ pour tout $p \in \mathbb{N}$

□

Exemple: Quel est le reste de 4^{2007} dans la division par 5?

$4 \equiv -1 [5] \implies 4^{2007} \equiv (-1)^{2007} [5]$. Donc $4^{2007} \equiv 4 [5]$. D'où un reste de 4. Même question avec 4^{2008} donne un reste de 1.

Exemple: Prouver que la somme (resp. le produit) de deux impairs est pair (resp. impair).

$a \equiv 1 [2], b \equiv 1 [2]$. Alors :

- ① $a + b \equiv 2 [2] \implies a + b \equiv 0 [2]$ Donc $a + b$ est pair.
- ② $ab \equiv 1 [2]$ Donc ab est impair.

Exemple: Si $a = 14k - 9$ pour $k \in \mathbb{Z}$ prouver que $58a^2 - 11a + 12$ est un multiple de 7.

$a = 14k - 9 \implies a \equiv -2 [7]$ et $58a^2 - 11a + 12 \equiv 2a^2 + 3a + 5 [7]$ donc $58a^2 - 11a + 12 \equiv 2 \times 4 + 3 \times (-2) + 5 [7]$ Ainsi : $58a^2 - 11a + 12 \equiv 0 [7]$.

4.4 Réduction modulo n

On peut utiliser conjointement les différentes opérations et transformer une égalité en une congruence modulo n .

Exemple: Je dis que $23 \times 47 = 1081$ mais je ne suis pas sûr, on vérifie en réduisant modulo 2 puis modulo 3 et 5 :

$1 \times 1 \equiv 1 [2]$ OK puis : $2 \times 0 \equiv 0 [3]$ OK puis $3 \times 2 \equiv 1 [5]$ OK. Les disjonctions de cas selon le reste d'un entier dans la division par n seront plus pratiques avec des congruences modulo n . On peut utiliser un tableau :

Exemple: Prouver que l'équation

$$5x^3 + 12y^2 = 504 \quad (\text{I.1})$$

n'admet aucune solution dans \mathbb{Z}^2 . On pourra raisonner modulo 5.

Si il existe deux entiers x et y tels que $5x^3 + 12y^2 = 504$ alors on a modulo cinq : $5x^3 + 12y^2 \equiv 504 [5]$ et donc $2y^2 \equiv 4 [5]$. On va voir que c'est impossible :

$y \equiv \dots [5]$	0	1	2	3	4
$y^2 \equiv \dots [5]$	0	1	-1	-1	1
$2y^2 \equiv \dots [5]$	0	2	3	3	2

Exercice n° 7

Preuve par neuf!

Exemple: $123456789 \times 111111111 = 13717420986282579$ (changer un chiffre!) (= 13717420986282579 en fait)

Chapitre II

Nombres premiers

PPCM

0.5 Définition

On notera a et b deux entiers dans \mathbb{Z}^* .

Définition 6. Le plus petit multiple commun strictement positif de a et b est appelé noté $PPCM(a; b)$.

Propriété 21. Les multiples communs à a et b sont les multiples de $PPCM(a; b)$.

Démonstration. On prouve les deux sens. Notons $m = PPCM(a; b)$.

- ① Si k est un multiple de m , c'est un multiple de a et b .
- ② Supposons que k est un multiple de a et b . On note $k = mq + r$ la division euclidienne de k par m . On a donc $0 \leq r \leq m - 1$. Prouvons que $r = 0$. Comme a et b divisent k et m , ils divisent la combinaison linéaire $k - mq$ c'est à dire r . Ainsi r est un multiple de a et b qui est strictement inférieur à $m = PPCM(a; b)$, c'est nécessairement zéro par définition du $PPCM(a; b)$. Finalement $k = mq$, i.e. k est un multiple de m .

□

0.6 PGCD, PPCM et décomposition

On notera a et b deux entiers naturels supérieurs à 2. Et on note p_1, p_2, \dots, p_n les nombres premiers intervenant dans la décomposition en produit de facteurs premiers (notée dpfp ensuite) de a ou de b . Les dpfp de a et b sont notées :

$$a = \prod_{i=1}^n p_i^{\alpha_i} \quad \text{et} \quad b = \prod_{i=1}^n p_i^{\beta_i}$$

Certains α_i ou β_i pouvant être nuls.

Exemple: Si $a = 2^2 \times 3^2 \times 11$ et $b = 3 \times 5^3 \times 7^2$. On prendra 2, 3, 5, 7, 11 pour les p_i et donc $n = 5$. Par exemple : $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11$. Alors $a = 2^2 \times 3^2 \times 5^0 \times 7^0 \times 11$ et $b = 2^0 \times 3 \times 5^3 \times 7^2 \times 11^0$. On a donc $\alpha_3 = \alpha_4 = \beta_1 = \beta_5 = 0$.

Propriété 22 (Calcul du PGCD et du PPCM avec les dpfp). En notant $Max\{\alpha_i; \beta_i\}$ le plus grand de α_i et β_i et $Min\{\alpha_i; \beta_i\}$ le plus petit de α_i et β_i , on a alors :

$$PPCM(a; b) = \prod_{i=1}^n p_i^{Max\{\alpha_i; \beta_i\}} \quad \text{et} \quad PGCD(a; b) = \prod_{i=1}^n p_i^{Min\{\alpha_i; \beta_i\}}$$

Démonstration. Pour le PGCD. Un diviseur de a et de b a une dpfp de la forme $\prod_{i=1}^n p_i^{\gamma_i}$ où chaque γ_i est inférieur à α_i et à β_i , donc au plus petit des deux. Ainsi $\gamma_i \leq Min\{\alpha_i; \beta_i\}$. On obtient le plus grand diviseur commun à a et à b en prenant le plus grand exposant γ_i possible pour chaque i , i.e. $\gamma_i = Min\{\alpha_i; \beta_i\}$. Même raisonnement pour le PPCM. □

Exemple: On reprend l'exemple précédent : $a = 2^2 \times 3^2 \times 11$ et $b = 3 \times 5^3 \times 7^2$. Alors :

$$PPCM(a; b) = 2^2 \times 3^2 \times 5^3 \times 7^2 \times 11 \quad \text{et} \quad PGCD(a; b) = 2^0 \times 3^1 \times 5^0 \times 7^0 \times 11^0 = 3.$$

On en déduit une relation entre PGCD et PPCM :

Propriété 23. $PPCM(a; b) \times PGCD(a; b) = ab$

Démonstration. Cela vient simplement de ce que : $\alpha_i \times \beta_i = \text{Min}\{\alpha_i; \beta_i\} \times \text{Max}\{\alpha_i; \beta_i\}$ □

Comme on sait que si k est dans \mathbb{N}^* on a : $PGCD(ka; kb) = kPGCD(a; b)$, on en déduit que :

Propriété 24. Si k est dans \mathbb{N}^* , alors $PPCM(ka; kb) = kPPCM(a; b)$

Démonstration. Laissée en exercice. □

Remarques utiles :

- Le $PGCD(a, b)$ divise a donc ses multiples et donc : $PGCD(a, b) \mid PPCM(a, b)$.
- Deux nombres a et b sont premiers entre eux signifie que $PGCD(a, b) = 1$ ce qui est équivalent à $PPCM(a, b) = ab$ par la propriété 23.

Méthode. Dans les exercices où on cherche des entiers a et b dont le $PGCD$ et le $PPCM$ satisfont des relations, une bonne méthode est la suivante. Pour alléger les notations on pose :

$$m = PPCM(a, b) \quad \text{et} \quad g = PGCD(a, b)$$

On considère alors les entiers a' et b' tels $a = a'g$ et $b = b'g$. Alors on a :

- $g = PGCD(a, b) = PGCD(ga', gb') = gPGCD(a', b')$. Donc $PGCD(a', b') = 1$, i.e. a' et b' sont premiers entre eux et donc :

$$PPCM(a', b') = a'b'$$

- Alors : $m = PPCM(a, b) = PPCM(ga', gb') = gPPCM(a', b') = ga'b'$. Ainsi :

$$a'b' = \frac{m}{g}$$

Si on connaît m et g , alors on est ramené à trouver deux entiers a' et b' premiers entre eux dont on connaît le produit : $n = m/g$.

- Alors on décompose n en produit de facteurs premiers et on détermine les différentes possibilités pour a' et b' sachant qu'ils n'ont aucun facteur premier en commun puisqu'ils sont premiers entre eux.
- On détermine alors a et b en multipliant a' et b' par g . Comme $PGCD(a, b) = PGCD(b, a)$, et $PPCM(a, b) = PPCM(b, a)$ ces problèmes ont des couples de solution qui sont symétriques. On peut donc étudier les cas où $a \leq b$ et en déduire tous les couples solution en échangeant a et b .

Exercice résolu :

Déterminer les entiers naturels a et b tels que $a \leq b$, $PGCD(a, b) = 5$ et $PPCM(a, b) = 100$.

$PGCD(a, b) = 5$ donc il existe a' et b' tels que $a = 5a'$ et $b = 5b'$ avec a' et b' premiers entre eux. Alors $PPCM(a', b') = a'b'$ et :

$$PPCM(a, b) = PPCM(5a', 5b') = 5PPCM(a', b') = 5a'b'$$

On veut $PPCM(a, b) = 100$ c'est à dire $5a'b' = 100$ soit $a'b' = 20$. On décompose 20 en produit de facteurs premiers : $20 = 2^2 \times 5$. Comme a' et b' sont premiers entre eux ils n'ont aucun facteur premier en commun et les seules possibilités pour $(a'; b')$ sont $(1; 20)$ et $(4; 5)$ en tenant compte de : $a' \leq b'$. Ainsi les couples d'entiers naturels a et b tels que $a \leq b$, $PGCD(a, b) = 5$ et $PPCM(a, b) = 100$ sont parmi $(5; 100)$ et $(20; 25)$, et ces deux couples conviennent.

Exercices du livre : p62 n° 48, 49, (50), (52), 55. cf exo résolu n° 3 p51

Chapitre III

Théorèmes de BÉZOUT et de GAUSS

1 Théorème de BÉZOUT

Théorème 3 (de BÉZOUT). *Deux entiers relatifs non nuls a et b sont premiers entre eux ssi il existe des entiers relatifs u et v tels que : $\boxed{au + bv = 1}$*

Il y a deux sens à prouver. Prouver le sens facile : « Si il existe des entiers relatifs u et v tels que : $au + bv = 1$, alors a et b sont premiers entre eux. »

.....
.....
.....

Pour l'autre sens : « Si a et b sont premiers entre eux il existe des entiers relatifs u et v tels que : $au + bv = 1$ » nous prouverons un résultat plus fort : l'identité de BÉZOUT :

Propriété 25 (Identité de BÉZOUT). *Soit deux entiers relatifs a et b non nuls. Il existe des entiers relatifs u et v tels que : $au + bv = PGCD(a; b)$*

Démonstration. Pour prouver que u et v existent, on va donner une méthode pour les calculer. Cette méthode consiste à « remonter » l'algorithme d'EUCLIDE qu'on utilise pour déterminer le PGCD de a et b . Traitons un exemple.

Exemple:

1. Déterminer le PGCD de 330 et 72 par l'algorithme d'EUCLIDE.

- ① $330 = \dots \times 72 + \dots$
② $72 =$
③
④
⑤

Donc $PGCD(330; 72) =$

2. On part de la ligne ④ en exprimant le PGCD obtenu et on remonte les calculs en remplaçant un par un les restes obtenus par leur expression en fonction de la ligne du dessus, sans effectuer les multiplications. Finissez le calcul :

$$\begin{aligned} 6 &= 30 - 2 \times 12 = 30 - 2 \times (42 - 30) = 3 \times 30 - 2 \times 42 \\ &= 3 \times (\quad) - 2 \times 42 = \\ &= \\ &= \end{aligned}$$

Ainsi on trouve $u = -5$ et $v = 23$ qui vérifient : $330u + 72v = PGCD(330; 72)$ Si a et b ne sont pas positifs, on peut appliquer l'algorithme d'Euclide à leurs valeurs absolues. Par exemple pour 330 et -72 on obtient $(u; v) = (-5; -23)$ qui convient. La méthode se généralise. cf p. 74 pour une preuve. \square

Remarque. Les entiers $(u; v)$ ne sont pas uniques. Par exemple pour $a = 2$ et $b = 3$ qui sont premiers entre eux, on a :

$$(-1) \times 2 + 1 \times 3 = 1 \quad \text{et} \quad 1 \times 2 + (-1) \times 3 = 1$$

Trouver une solution particulière à l'équation d'inconnues entières x et y : $21x + 12y = 6$

2 Théorème de GAUSS

Théorème 4 (de GAUSS). a, b, c désignent trois entiers non nuls. Si $a|bc$ et que a et b sont premiers entre eux, alors $a|c$.

Démonstration. Par le théorème de Bézout il existe u et v entiers tels que $au + bv = 1$. On multiplie par c , on a donc que a divise $c - bcv$ et comme $a|bc$, on conclue par combinaison linéaires que $a|c$. cf livre p.76 \square

Remarque. La condition « a et b sont premiers entre eux » est nécessaire. Trouver un exemple où $a|bc$ mais a ne divise ni b ni c .

3 Application : Équation diophantienne $ax + by = c$

On veut résoudre des équations d'inconnues entières x et y de la forme :

$$ax + by = c \quad (\text{III.1})$$

où a, b, c sont des entiers, a et b non nuls. On pose $d = \text{PGCD}(a; b)$.

Il faut que $d|c$. Si c n'est pas un multiple de d , alors l'équation (III.1) n'a pas de solution. En effet, comme $d|a$ et $d|b$, d divise toute combinaison linéaire $(ax + by)$ de a et b . Donc nécessairement $d|c$. Si ce n'est pas le cas, alors (III.1) n'a pas de solution.

Méthode de résolution de l'équation (III.1)

- ① On suppose maintenant que $d|c$. Ainsi on peut « **simplifier** » l'équation (III.1) par d . Ainsi on se ramène à une équation équivalente de la forme $a'x + b'y = c'$ où maintenant a' et b' sont premiers entre eux. Pour éviter les primes dans la suite on va résoudre (III.1) dans le cas où a et b sont **premiers entre eux**.
- ② On trouve une solution particulière de $ax + by = 1$ à vue ou en remontant l'algorithme d'Euclide. En la multipliant par c on a une **solution particulière** $(x_0; y_0)$ de (III.1)
- ③ On cherche maintenant *toutes* les solutions. Comme pour les équations différentielles linéaires, $(x; y)$ est solution de (III.1) ssi $(x - x_0; y - y_0)$ est solution de l'**équation sans second membre** :

$$aX + bY = 0 \quad (\text{III.2})$$

En effet, comme $ax_0 + by_0 = c$, alors :

$$ax + by = c \iff ax + by = ax_0 + by_0 \iff a(x - x_0) + b(y - y_0) = 0.$$

- ④ L'équation (III.2) est équivalente à $aX = -bY$. Ainsi b divise aX , or a et b sont premiers entre eux on peut en déduire grâce au **théorème de GAUSS** que $b|X$, i.e. $X = bk$ (où $k \in \mathbb{Z}$). En remplaçant dans (III.2) et en simplifiant par b on en déduit que $Y = -ak$. Ainsi les solutions de (III.2) sont nécessairement de la forme : $(bk; -ak)$ où $k \in \mathbb{Z}$. On vérifie que ce sont bien tous des solutions.
- ⑤ Finalement les solutions de (III.1) sont de la forme $(bk + x_0; -ak + y_0)$ où k décrit \mathbb{Z} .

Applications : Utiliser cette méthode pour résoudre dans \mathbb{Z} les équations :

① $4x - 6y = 12$

② $15x + 6y = 9$

③ $7x + 23y = 5$

Deuxième partie

Similitudes

Chapitre IV

Similitudes

1 Définition géométrique

1.1 Similitudes du plan

Définition 7. On dit que f est une **transformation du plan** si

- ① tout point du plan a une unique image par f
- ② tout point du plan admet un unique antécédent par f

Par exemple, une projection orthogonale n'est pas une transformation du plan selon notre définition. Dans la suite, pour tout point M , on notera M' désignera $f(M)$. Une similitude, elle, est définie par :

Définition 8. Une **similitude** est une transformation du plan qui conserve les rapports de longueurs

C'est à dire que, avec des notations habituelles et des points distincts, $\frac{A'B'}{C'D'} = \frac{AB}{CD}$

Remarque. Si I est une isométrie, alors c'est une similitude.

Propriété 26. Si S est une transformation telle qu'il existe $k \in \mathbb{R}_*^+$ pour lequel S multiplie toutes les longueurs par k , alors S est une similitude.

Démonstration. Facile. □

Exemple: Toute homothétie est une similitude!

Propriété 27. Si S est une similitude, alors il existe $k \in \mathbb{R}_*^+$ appelé rapport de la similitude S tel que S multiplie toutes les longueurs par k . i.e. $M'N' = kMN \ \forall M, N$.

Démonstration. Soit M, N, P, Q ($M \neq N$ et $P \neq Q$) d'image par une similitude $S : M', N', P', Q'$. Alors $\frac{M'N'}{P'Q'} = \frac{MN}{PQ}$ donc, puisque $M \neq N$, et ... : $\frac{M'N'}{MN} P'Q' = \frac{P'Q'}{PQ}$. Donc ce rapport ne dépend pas des points choisis, on le note k . On a alors $M'N' = kMN$. Si $M=N$ alors $M' = N'$ et cette égalité tient encore. □

Propriété 28. Une **isométrie** est une similitude de rapport 1.

Remarque. Si le rapport k est strictement supérieur à 1, on a un effet d'agrandissement, et si $k \in]0; 1[$ on a un effet de réduction.

1.2 Conservation des angles géométriques.

On veut prouver que... or les angles sont intimement liés au produit scalaire. Souvenez vous des formules :

$$\vec{u} \cdot \vec{v} = \frac{1}{2} (||\vec{u}||^2 + ||\vec{v}||^2 - ||\vec{u} - \vec{v}||^2) \quad (\text{IV.1})$$

$$\cos(\vec{u}, \vec{v}) = \frac{\vec{u} \cdot \vec{v}}{||\vec{u}|| \times ||\vec{v}||} \quad (\text{IV.2})$$

À l'aide de (IV.1) prouver que pour tous points M, N, P d'images... par une similitude de rapport k , on a :

$$\overrightarrow{M'N'} \cdot \overrightarrow{M'P'} = \frac{1}{2}(M'N'^2 + M'P'^2 - N'P'^2) = \frac{1}{2}(k^2 MN^2 + k^2 MP^2 - k^2 NP^2) = k^2 \overrightarrow{MN} \cdot \overrightarrow{MP}$$

En déduire que :

$$\cos(\overrightarrow{M'N'}, \overrightarrow{M'P'}) = \cos(\overrightarrow{MN}, \overrightarrow{MP})$$

Que peut-on dire de deux réels θ et θ' qui ont même cosinus ? Ils sont égaux ou opposés mod 2π , donc égaux en valeur absolue mod 2π . D'où :

Propriété 29. Une similitude conserve les angles géométriques. i.e. $\widehat{M'N'P'} = \widehat{MNP}$

2 Similitudes directes

Définition 9. On appelle similitude directe une similitude qui conserve les angles orientés.

2.1 Écriture complexe

Reprenons nos trois petits points M, N et P d'affixes m, n et p et leurs images par une similitude directe respectivement primées.

Notons $Z = \frac{p-m}{n-m}$ et $Z' = \frac{p'-m'}{n'-m'}$. Comment interprétez-vous géométriquement ces deux nombres ?

- ① Les rapports de distances se conservent, donc $|Z| = MP/MN = M'P'/M'N' = |Z'|$
- ② Les angles orientés se conservent donc $\arg(Z) = \arg(Z')$
- ③ Donc $Z' = Z$!

Ainsi on a : $\frac{p'-m'}{n'-m'} = \frac{p-m}{n-m}$.

Propriété 30. Une similitude directe a nécessairement pour écriture complexe :

$$z' = az + b$$

Où a et b sont dans \mathbb{C} , $a \neq 0$.

Démonstration. En posant $p = z, p' = z', m = 0, n = 1$ on obtient le résultat. □

Réciproquement,

Propriété 31. Si une transformation du plan a une écriture complexe de la forme $z' = az + b$ ($a \in \mathbb{C}^*$) alors c'est une similitude directe, de rapport $|a|$.

Démonstration. cf p104. □

Finalement...

Théorème 5. Les similitudes directes du plan sont les transformations qui ont une écriture complexe de la forme : $z' = az + b$ ($a \in \mathbb{C}^*, b \in \mathbb{C}$)

2.2 Décomposition, éléments caractéristiques.

Soit une similitude directe S d'écriture complexe : $z' = az + b$ avec ($a \in \mathbb{C}^*, b \in \mathbb{C}$).

Rapport

Le rapport de la similitude est $|a|$. S est une isométrie ssi a est de module 1.

Centre

On recherche les points invariants de S , on résout donc :

$$z = az + b \iff z(1 - a) = b \quad (\text{IV.3})$$

On distingue alors les cas suivants :

- ① Si $a \neq 1$, alors il y a un unique point invariant Ω appelé centre de la similitude qui a pour affixe $\omega = \frac{b}{1-a}$.
- ② Si $a = 1$ alors la similitude est la translation de vecteur \vec{w} d'affixe b . ($z' = z + b$)
 - a. Si $b = 0$, cette translation est l'identité, tous les points du plan sont invariants.
 - b. Si $b \neq 0$, il n'y a aucun point invariant.

Théorème de décomposition.

On se place dans le cas où S n'est pas une translation. On a donc $a \in \mathbb{C} \setminus \{0; 1\}$ et $b \in \mathbb{C}$.

Théorème 6. *Toute similitude directe qui n'est pas une translation est la composée d'une rotation et d'une homothétie. Plus précisément, si $z' = az + b$ ($a \in \mathbb{C} \setminus \{0; 1\}$ et $b \in \mathbb{C}$) alors S est la composée de la rotation de centre Ω d'affixe $\omega = \frac{b}{1-a}$ et d'angle $\arg(a)$ et de l'homothétie de centre Ω et de rapport $|a|$.*

Démonstration. L'écriture complexe de la rotation \mathcal{R} de centre Ω d'affixe ω et d'angle θ où $\theta = \arg(a)$ est : $z' - \omega = e^{i\theta}(z - \omega)$. L'écriture complexe de l'homothétie \mathcal{H} de centre Ω et de rapport $|a|$ est : $Z' - \omega = |a|(Z - \omega)$. Schéma de composition :

$$\begin{array}{ccc} z & \xrightarrow{\mathcal{R}} & z' \quad \text{et} \quad Z \xrightarrow{\mathcal{H}} Z' \\ z & \xrightarrow{\mathcal{R}} z' \xrightarrow{\mathcal{H}} z'' \\ & \searrow \mathcal{H} \circ \mathcal{R} \nearrow & \end{array}$$

Pour déterminer l'écriture complexe de la composée $\mathcal{H} \circ \mathcal{R}$ il faut exprimer z'' en fonction de z , or :

$$z'' - \omega = |a|(z' - \omega) = |a|(z - \omega) = |a|e^{i\theta}(z - \omega) = a(z - \omega)$$

Ainsi $\mathcal{H} \circ \mathcal{R}$ a pour écriture complexe $z' - \omega = a(z - \omega)$. On vérifiera aussi que $\mathcal{H} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{H}$.

Pour prouver le théorème, il suffit de vérifier que $z' - \omega = a(z - \omega)$ est une autre écriture de $z' = az + b$. En tenant compte de $\omega = a\omega + b$. On a :

$$z' = az + b \iff z' - \omega = az + b - (a\omega + b) \iff z' - \omega = a(z - \omega)$$

□

On vient de prouver au passage que :

Propriété 32. *La similitude directe de centre d'affixe ω , d'angle θ et de rapport k (où $\omega \in \mathbb{C}$, $\theta \in \mathbb{R}$ et $k \in \mathbb{R}_+^*$) a une écriture complexe de la forme :*

$$\boxed{z' - \omega = k(z - \omega)e^{i\theta}}$$

Conclusion

Lorsque $a \neq 1$, un argument de a est appelé angle de la similitude S . Ainsi une similitude directe qui n'est pas une translation a trois éléments caractéristiques :

- ① Son centre : Ω (l'unique point invariant)
- ② Son rapport : $|a|$
- ③ Son angle : $\arg(a)$

L'ensemble des similitudes directes contient donc :

1. Les isométries suivantes :
 - a. Toutes les translations. ($a = 1$)
 - b. Toutes les rotations ($|a| = 1$)
 - c. Les symétries centrales (rotation d'angle π)
2. Toutes les homothéties ($a \in \mathbb{R}$)
3. Les composées d'homothéties et rotations de même centre

Exercice n° 8

Déterminer les éléments caractéristiques des similitudes directes dont on donne une écriture complexe.

$$\textcircled{1} \quad z' = 3iz + 2 - i$$

$$\textcircled{2} \quad z' = 2z + 1 - 2i$$

$$\textcircled{3} \quad z' = (1 - i)z$$

$$\textcircled{4} \quad z' = (\sqrt{3} - i)z + i$$

Exercice n° 9

Déterminer les images des points A et B d'affixes respectives $z_A = 1 - i$ et $z_B = 2$ par la similitude de centre $\Omega(1; 2)$, d'angle $\frac{\pi}{6}$ et de rapport 2.


2.3 Propriétés des similitudes directes

Composées

Propriété 33. La composée de deux similitudes directes \mathcal{S} et \mathcal{S}' est une similitude directe Σ . Si $\mathcal{S} \circ \mathcal{S}' = \Sigma$ et que \mathcal{S} et \mathcal{S}' ne sont pas des translations, on a que :

- ① le rapport de Σ est le produit des rapports de \mathcal{S} et de \mathcal{S}' .
- ② l'angle de Σ est la somme des angles de \mathcal{S} et de \mathcal{S}' .

Démonstration. Facile : $a(\alpha z + \beta) + b = a\alpha z + a\beta + b$ □

La composition n'est pas commutative en général. i.e. $\mathcal{S} \circ \mathcal{S}' \neq \mathcal{S}' \circ \mathcal{S}$ car $a\beta + b \neq \alpha b + \beta$ en général. ($a = 1, \alpha = -1, b = \beta = 1$ donne 2 et 0) 

Propriété 34. Toute similitude directe \mathcal{S} admet une unique inverse pour la composition qui est une similitude directe notée \mathcal{S}^{-1} . i.e. il existe une unique similitude directe \mathcal{S}^{-1} vérifiant :

$$\mathcal{S}^{-1} \circ \mathcal{S} = \mathcal{S} \circ \mathcal{S}^{-1} = Id$$

Démonstration. On note $z' = az + b$ l'écriture complexe d'une similitude directe \mathcal{S} . On reprend les calculs faits dans la preuve précédente, on distingue deux cas :

- ① Si $a \neq 0$. $\mathcal{S}^{-1} \circ \mathcal{S} = Id$ impose $a\alpha = 1$ et $a\beta + b = 0$. Donc $\alpha = \frac{1}{a}$ et $\beta = -\frac{b}{a}$. On vérifie qu'alors la similitude \mathcal{S}^{-1} d'écriture complexe $z' = \frac{1}{a}z - \frac{b}{a}$ vérifie aussi : $\mathcal{S} \circ \mathcal{S}^{-1} = Id$. En effet $a\alpha z + \alpha b + \beta = z + b\frac{1}{a} - \frac{b}{a} = z$.
- ② Si $a = 0$, \mathcal{S} est la translation de vecteur \vec{w} d'affixe b . Alors \mathcal{S}^{-1} est la translation de vecteur $-\vec{w}$. □

Propriétés géométriques

Propriété 35. Soit quatre points A, B, A' et B' avec $A \neq B$ et $A' \neq B'$. Il existe une unique similitude directe \mathcal{S} telle que $\mathcal{S}(A) = A'$ et $\mathcal{S}(B) = B'$.

Démonstration. On résout le système... □

La preuve montre que :

- ① Si $\overrightarrow{A'B'} = \overrightarrow{AB}$ alors \mathcal{S} est la translation ($a = 1$) de vecteur $\overrightarrow{AA'}$

- ② Si $\overrightarrow{A'B'} \neq \overrightarrow{AB}$ alors \mathcal{S} est une similitude de rapport $\frac{A'B'}{AB}$ et d'angle $(\overrightarrow{AB}, \overrightarrow{A'B'})$. Il suffit de regarder le module et un argument de a .

Remarque. Ne pas apprendre ces formules par cœur mais savoir mener le calcul au cas par cas.
Exo n° 31p126

Exemple: On considère les points A, B, C et D d'affixes :

$$z_A = 1 + i \quad z_B = \quad z_C = \quad z_D =$$

Déterminer les éléments caractéristiques de la similitude \mathcal{S} qui transforme A en C et B en D .

Comme conséquence :

Propriété 36. La seule similitude directe qui a deux points distincts invariants est l'identité.

Démonstration. L'identité convient, et d'après la prop précédente, c'est la seule. \square

Propriétés de conservations.

Propriété 37. Toute similitude directe conserve :

- ① l'alignement
- ② l'orthogonalité
- ③ le parallélisme
- ④ le contact entre deux objets (droites, polygone, cercles...)
- ⑤ le barycentre

Démonstration. ①, ② et ③ proviennent de la conservation des angles orientés. ④ est admise.

⑤ Signifie que l'image d'un barycentre est le barycentre des images munies des mêmes masses. On fait la preuve pour un barycentre G de deux points pondérés (A, α) et (B, β) , d'images respectives G', A' et B' par une similitude directe d'écriture complexe $z' = az + b$. Prouvons que G' est barycentre de (A', α) et (B', β) . Comme :

$$z_G = \frac{\alpha z_A + \beta z_B}{\alpha + \beta}$$

Alors G' l'image de G par a pour affixe :

$$z' = az_G + b = a \times \frac{\alpha z_A + \beta z_B}{\alpha + \beta} + b = \frac{\alpha}{\alpha + \beta}(az_A + b) + \frac{\beta}{\alpha + \beta}(az_B + b) = \frac{\alpha z_{A'} + \beta z_{B'}}{\alpha + \beta}$$

Ce qui est finalement l'affixe du barycentre de (A', α) et (B', β) .

Autre méthode (sans ruse) : l'affixe du barycentre de (A', α) et (B', β) est :

$$\frac{\alpha z_{A'} + \beta z_{B'}}{\alpha + \beta} = \frac{\alpha}{\alpha + \beta}(az_A + b) + \frac{\beta}{\alpha + \beta}(az_B + b) = a \times \frac{\alpha z_A + \beta z_B}{\alpha + \beta} + b \times \frac{\alpha + \beta}{\alpha + \beta} = az_G + b$$

\square

3 Étude générale des similitudes

Ici on va chercher à caractériser les similitudes qui ne sont pas des similitudes directes.

3.1 Similitudes et points fixes

Propriété 38. Une similitude plane qui admet trois points fixes non alignés est l'identité.

Démonstration. Guide :

On note Σ une similitude admettant trois points fixes non alignés, mettons A , B , et C .

1. On a donc $\Sigma(\dots) = \dots$, $\Sigma(\dots) = \dots$ et $\Sigma(\dots) = \dots$.
2. En déduire que Σ est une isométrie :
3. On finit la preuve par l'absurde. Supposons que Σ ne soit pas l'identité, i.e. il existe un point M tel que $\Sigma(M) = M'$ avec $M' \dots$
 - a. On a $AM = AM'$ car
 - b. De la même manière on a $BM = BM'$ et $CM = CM'$. Ainsi les trois points A , B , et C appartiennent à la
 - c. Ceci est impossible car
4. Conclusion :

□

Propriété 39. Une similitude plane qui admet deux points fixes distincts est soit l'identité soit la symétrie d'axe (AB) .

Démonstration. Guide :

On note Σ une similitude admettant deux points fixes distincts A et B . Comme dans la preuve précédente, on prouve que Σ est une isométrie.

Soit C un point non aligné avec A et B . On note $C' = \Sigma(C)$.

1. Si $C = C'$ alors
2. Si $C \neq C'$ alors $AC' = \dots$ et $BC' = \dots$ donc A et B appartiennent à
 - a. On note s la symétrie d'axe (AB) . Alors $s^{-1} = \dots$
 - b. On pose $t = s \circ \Sigma$. Alors $t(A) = s(\Sigma(\dots)) = s(\dots) = \dots$ de même $t(B) = \dots$. On a aussi : $t(C) = s(\Sigma(\dots)) = s(\dots) = \dots$
 - c. Ainsi t a ... points fixes donc $t = \dots$
 - d. On a donc $s \circ \Sigma = Id$. En composant à gauche par s^{-1} on a : $\Sigma = \dots$ et donc par le 2a, on obtient : $\Sigma = \dots$

□

3.2 Caractérisation des similitudes non directes

Propriété 40. Une similitude non directe peut s'écrire sous la forme $\sigma \circ s$ où σ est une similitude directe et s une symétrie axiale.

Démonstration. Soit Σ une similitude non directe, A et B deux points distincts d'images respectives A' et B' par Σ .

1. Il existe une unique similitude directe σ telle que $\sigma(\dots) = \dots$ et $\sigma(\dots) = \dots$ car
2. On considère la similitude $s = \sigma^{-1} \circ \Sigma$. Alors $s(A) = \dots$
3. De même $s(B) = \dots$. Or s ne peut pas être l'identité car cela signifie que $\Sigma = \dots$ or Σ n'est pas une similitude
4. Par la propriété 39, s est donc
5. Or $s = \sigma^{-1} \circ \Sigma$ donc en composant par σ on a : $\sigma \circ s = \dots$

□