MDD202 : Structures algébriques

Benjamin Schraen

7 juillet 2021

Vocabulaire ensembliste

Le langage utilisé en mathématiques est celui des *ensembles*. Nous allons très souvent considérer des objets sont appelés *éléments* et *ensembles*, le mot *ensemble* désignant un ensemble d'*éléments*. Le symbole $\in$ désigne la notion d'appartenance. Si a est un élément et E un ensemble, on note $a \in E$ pour signifier que a est un élément de l'ensemble E. Par exemple $2 \in \mathbb{N}$ mais $-2 \notin \mathbb{N}$. Il faut bien différencier la notion d'appartenance $\in$ de la notion d'inclusion $\subset$. Si A et B sont deux ensembles, on note $A \subset B$ et on dit que A *est inclus dans* B lorsque tous les éléments de A sont des éléments de B. On dit aussi que A est une partie de B.

Si A et B sont deux ensembles, on note $A \cup B$ la *réunion* des ensembles A et B, c'est-à-dire l'ensemble des éléments qui appartiennent à A ou à B :

$$A \cup B = \{a : a \in A \text{ ou } a \in B\}.$$

Par définition, A est donc inclus dans $A \cup B$ et B est inclus dans $A \cup B$:

$$A \subset A \cup B, \quad B \subset A \cup B.$$

On note $A \cap B$ l'*intersection* des ensembles A et B, c'est-à-dire l'ensemble des éléments qui appartiennent à A et à B :

$$A \cap B = \{a : a \in A \text{ et } a \in B\}.$$

Cette fois-ci c'est $A \cap B$ qui est inclus dans A et dans B :

$$A \cap B \subset A, \quad A \cap B \subset B.$$

Si A est une partie de B, on note $B \smallsetminus A$ l'ensemble des éléments de B qui ne sont pas dans A :

$$B \smallsetminus A = \{a \in B : a \notin A\}.$$

On utilise aussi la notion de *différence symétrique*. Si A et B sont deux ensembles, on note $A \triangle B$ pour désigner l'ensemble des éléments qui appartiennent à A ou à B mais pas aux deux à la fois. Ainsi :

$$A \triangle B = \{a \in A \cup B : a \notin A \cap B\} = (A \cup B) \smallsetminus (A \cap B).$$

Si A et B sont deux ensembles, on dit que A et B sont *disjoints* si $A \cap B = \emptyset$. La notation $\emptyset$ désigne l'ensemble vide : c'est l'unique ensemble qui ne contient aucun élément ! Par définition l'ensemble vide est inclus dans tous les autres ensembles et $A \smallsetminus \emptyset = A$.

Un ensemble E est dit *fini* s'il ne contient qu'un nombre fini d'éléments. Le nombre de ses éléments est appelé *cardinal* de cet ensemble et est noté $\operatorname{Card} E$, $|E|$ ou encore $\sharp E$. Voici quelques règles de bon sens concernant les cardinaux des ensembles finis :

— si $A \subset B$ et si B est fini, alors A est fini et $|A| \leqslant |B|$;

— si A et B sont deux ensembles finis, alors $A \cup B$ est fini et $|A \cup B| \leqslant |A| + |B|$. Cette inégalité peut être stricte car les ensembles A et B peuvent avoir des éléments en commun. On a donc

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

En particulier, si A et B sont disjoints, $A \cap B = \emptyset$ et $|A \cup B| = |A| + |B|$.

Chapitre 1

Un peu d'arithmétique

On utilise la lettre $\mathbb{N}$ pour désigner l'ensemble des nombres *entiers naturels* :

$$\mathbb{N} = \{0, 1, 2, \ldots\}, \quad \mathbb{N}^* = \mathbb{N} \setminus \{0\} = \{1, 2, \ldots, \}$$

et la lettre $\mathbb{Z}$ pour désigner l'ensemble des nombres *entiers relatifs* :

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, \ldots\}.$$

Dans ce cours, lorsque l'on parlera d'*entiers* sans plus de précision, il s'agira toujours d'entiers relatifs.

1.1 Divisibilité

On ne peut pas toujours diviser un nombre entier par un autre, ou alors on n'obtient pas nécessairement un nombre entier. On introduit donc la notion de divisibilité.

Définition. *Soient a et b deux entiers relatifs. On dit que b* divise *a s'il existe un entier relatif k tel que $a = kb$. On dit aussi que a* est divisible *par b, ou que a est un* multiple *de b. On note cette relation $b \mid a$.*

Soit $b \in \mathbb{Z}$. On note $\mathbb{Z}b$ l'ensemble des multiples de b, c'est-à-dire l'ensemble des entiers de la forme nb pour $n \in \mathbb{Z}$:

$$\mathbb{Z}b = \{nb,\, n \in \mathbb{Z}\}.$$

Remarquons que si l'on prend $b = 0$, alors pour tout $n \in \mathbb{Z}$, $nb = 0$. Ainsi 0 n'a qu'un seul multiple : lui-même. Autrement dit $\mathbb{Z}0 = \{0\}$.

Si $b \neq 0$, alors b a une infinité de multiples. En effet, si $m \neq n$ sont deux entiers distincts, alors $mb \neq nb$. On dit aussi que l'application

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}b \\ n & \longmapsto & nb \end{array}$$

est injective.

Si $a \in \mathbb{Z}$, on note $\mathcal{D}(a)$ l'ensemble des diviseurs de a.

Proposition. *Soit a un entier non nul. Si $b \in \mathbb{Z}$ est un diviseur de a, alors $|b| \leqslant |a|$. En particulier l'entier a ne possède qu'un nombre fini de diviseurs.*

Démonstration. Soit b un diviseur de a. Par définition, il existe $k \in \mathbb{Z}$ tel que $a = kb$. Comme $a \neq 0$, on a $k \neq 0$ et $b \neq 0$. Ainsi $|k| \geqslant 1$ puisque k est entier. En multipliant cette inégalité par $|b|$, on obtient $|a| = |k||b| \geqslant |b|$. □

Remarquons que l'hypothèse $a \neq 0$ est essentielle. En effet le nombre 0 a une infinité de diviseurs : pour tout $b \in \mathbb{Z}$, on a $b0 = 0$. Ainsi $\mathcal{D}(0) = \mathbb{Z}$.

Exemple. Ainsi les diviseurs de 1 sont dans l'ensemble $\{-1, 0, 1\}$. On peut éliminer 0. De plus $1 = 1.1 = (-1).(-1)$, ainsi l'ensemble des diviseurs de 1 est l'ensemble $\{-1, 1\}$.

Il se trouve que 1 et -1 sont les seuls entiers ayant exactement deux diviseurs. Tous les entiers a non nuls et différents de 1 et -1 ont au moins 4 diviseurs distincts : -1, 1, $-a$, a.

Exemple. Cherchons à déterminer tous les diviseurs de 12. Le théorème nous assure tout de suite qu'il suffit de les chercher dans

$$\{-12, -11, -10, \ldots, 10, 11, 12\}.$$

Il suffit alors d'examiner si chaque élément de cet ensemble est diviseur de 12 (à ce point, une certaine connaissance de ses tables de multiplication est nécessaire). On trouve alors l'ensemble

$$\mathcal{D}(12) = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}.$$

Revenons maintenant aux multiples d'un entier b. Ce sont les nombres de la forme nb où $n \in \mathbb{Z}$. Si $n_1 b$ et $n_2 b$ sont deux multiples de b, on voit par factorisation que $n_1 b + n_2 n = (n_1 + n_2)b$ est aussi un multiple de b (puisque $n_1 + n_2 \in \mathbb{Z}$). De même si $k \in \mathbb{Z}$, $k(nb) = (kn)b$ est toujours un multiple de b. Plus généralement, on a le résultat suivant :

Proposition. *Soit $b \in \mathbb{Z}$. Si u et v sont deux multiples de l'entier b, alors pour tous $\lambda \in \mathbb{Z}$ et $\mu \in \mathbb{Z}$, $\lambda u + \mu v$ est un multiple de b.*

Ce résultat se reformule aussi : si b divise u et b divise v, alors dès que $\lambda \in \mathbb{Z}$ et $\mu \in \mathbb{Z}$, b divise $\lambda u + \mu v$ ou, symboliquement,

$$(b \mid u \text{ et } b \mid v) \Longrightarrow (\forall (\lambda, \mu) \in \mathbb{Z}^2,\ b \mid (\lambda u + \mu v)).$$

Démonstration. Les nombres u et v sont des multiples de b, donc il existe des éléments n_1 et n_2 de $\mathbb{Z}$ tels que $u = n_1 b$ et $v = n_2 b$. Ainsi si λ et μ sont dans $\mathbb{Z}$,

$$\lambda u + \mu v = \lambda n_1 b + \mu n_2 b = (\lambda n_1 + \mu n_2)b.$$

Et comme $\lambda n_1 + \mu n_2 \in \mathbb{Z}$, $\lambda u + \mu v$ est un multiple de b. Le reste s'en déduit. □

On a donc en particulier, si $b \mid u$ et $b \mid v$,

— $b \mid (u+v)$ (avec $\lambda = \mu = 1$) ;

— $b \mid (u-v)$ (avec $\lambda = 1$ et $\mu = -1$) ;

— $b \mid (ku)$ pour tout $k \in \mathbb{Z}$ (avec $\lambda = k$ et $\mu = 0$).

Exemple. Considérons le problème suivant : *déterminer les entiers n tels que $n+2$ divise $7n+3$.*

On commence par faire disparaître le n dans $7n+3$ par combinaison linéaire : on sait que $n+2 \mid n+2$, donc si $n+2 \mid 7n+3$, on a $n+2 \mid (7n+3-7(n+2))$ ce qui donne $n+2 \mid -11$. On se ramène donc à chercher les diviseurs de -11. On obtient : $n+2 \in \mathcal{D}(-11) = \{-11, -1, 1, 11\}$, et donc $n \in \{-13, -3, -1, 9\}$. Cependant à ce stade, on n'a pas encore résolu le problème : on a montré que si n est solution, il est dans l'ensemble $\{-13, -3, -1, 9\}$. Mais est-ce que tous les éléments de cet ensemble sont des solutions ? On pourrait bien sûr vérifier que ces éléments sont tous solutions (il n'y a que quatre vérifications à faire), mais dans un cas où il y a plus de possibilités ce serait fastidieux. Il s'avère en fait qu'ici on peut refaire le raisonnement à l'envers. En effet, si n est dans cet ensemble, $n+2 \mid -11$, donc $n+2 \mid -11+7(n+2) = 7n+3$ et donc n est solution. Finalement on peut bien conclure que l'ensemble des solutions est $\{-13, -3, -1, 9\}$.

1.2 Congruences

Nous avons vu que pour montrer qu'un nombre est divisible par un entier n, on peut se ramener par combinaisons linéaires à étudier la divisibilité par n d'entiers plus petits, et donc à un problème plus simple. Essentiellement, si on considère un entier a, il est équivalent de dire que $n \mid a$ ou que $n \mid a+n$, ou encore que $n \mid a+2n$... Plus généralement $n \mid a$ si et seulement si il existe un entier k tel que $n \mid a+kn$, et dans ce cas $n \mid a+k'n$ pour tout entier k'. Ceci nous montre que tous les entiers a, $a+n, \ldots, a+kn, \ldots$ ont les mêmes propriétés lorsqu'on étudie la divisibilité par n. Dans cette optique, la notion qui va suivre est très utile et est fondamentale en arithmétique.

Définition. *Soit $n \in \mathbb{N}^*$, on dit que deux entiers a et b sont congrus modulo n si $n \mid (a-b)$ et on note alors $a \equiv b\,[n]$ ou $a \equiv b \pmod{n}$.*

Remarquons tout de suite que la notion de congruence est une sorte d'extension de la notion divisibilité. En effet, si $n \in \mathbb{N}^*$, un entier relatif a est divisible par n si et seulement si $a \equiv 0\,[n]$.

Vérifions ensuite quelques propriétés du symbole de congruence, fixons donc un entier $n \in \mathbb{N}^*$.

— Pour tout entier a, $a \equiv a\,[n]$, car on a toujours $n \mid a-a = 0$.

— Si a et b sont deux entiers, $n \mid a-b$ si et seulement si $n \mid b-a$. Il est donc équivalent de dire que $a \equiv b\,[n]$ ou que $b \equiv a\,[n]$.

— Si a, b, c sont trois entiers tels que $a \equiv b\,[n]$ et $b \equiv c\,[n]$, alors $n \mid a-b$ et $n \mid b-c$. D'où $n \mid (a-b)+(b-c) = a-c$ et donc $a \equiv c\,[n]$.

Ces quelques propriétés montrent déjà que le symbole de congruence est une relation assez souple, passons maintenant aux propriétés les plus importantes de ce symbole.

Proposition. *Soit $n \in \mathbb{N}^*$ et a, b, c, d quatre entiers. Alors*

$$a \equiv b\,[n] \text{ et } c \equiv d\,[n] \Rightarrow a+c \equiv b+d\,[n] \text{ et } ac \equiv bd\,[n]$$

Démonstration. On a $n \mid b-a$ et $n \mid d-c$, donc d'après le théorème 3, $n \mid b-a+d-c = (b+d)-(a+c)$ et donc $a+c \equiv b+d\,[n]$. De même $bd-ac = b(d-c)+(b-a)c$. Comme $n \mid b-a$ et $n \mid d-c$, on a bien $n \mid bd-ac$, d'où $ac \equiv bd\,[n]$. □

Ce résultat peut se traduire par la phrase suivante : « la relation de congruence se préserve par addition et multiplication ». Et ceci est très important, nous verrons pourquoi au fur et à mesure. Bien sûr il est aussi vrai que la congruence préserve les combinaisons linéaires, c'est d'ailleurs un cas particulier de ce théorème : soient $a \equiv b\,[n]$, $c \equiv d\,[n]$ et λ et μ deux entiers. Comme $\lambda \equiv \lambda\,[n]$, on a $\lambda a \equiv \lambda b\,[n]$. De même $\mu c \equiv \mu d\,[n]$, et donc $\lambda a + \mu c \equiv \lambda b + \mu d\,[n]$.

Pour terminer cette partie sur les congruences, nous allons montrer l'utilité des congruences sur un exemple bien connu : le critère de divibilité par 3. Il est en général bien connu qu'un entier est divisible par 3 si et seulement la somme des chiffres de son écriture en base 10 est un multiple de 3. Par exemple 135681 est divisible par 3 car $1+3+5+6+8+1 = 24$ qui est divisible par 3. Nous allons montrer d'où vient ce critère.

Soit n un entier naturel. L'écriture de n en base 10 est la donnée d'entiers a_0, …,a_d compris entre 0 et 9 tels que $n = a_d 10^d + a_{d-1}10^{d-1} + \cdots + a_0$. Voyons ce que donne cette égalité modulo 3. On a $10 = 3\times 3+1$ donc $10 \equiv 1\,[3]$. Il en découle que $10^2 \equiv 1\times 1 = 1\,[3]$ et donc, en itérant, pour tout $k \in \mathbb{N}^*$, $10^k \equiv 1\,[3]$. Il faut remarquer que pour écrire tout cela, on doit appliquer la proposition dans le cas multiplicatif. En appliquant maintenant à nouveau la proposition dans le cadre additif, on a $n \equiv a_d + a_{d-1} + \cdots + a_0\,[3]$. On a donc montré que pour étudier la divisibilité par 3 d'un entier, il suffit d'étudier la divisibilité par 3 de la somme des chiffres de son écriture décimale, en particulier un entier est divisible par 3 si et seulement si la somme des chiffres de son écriture décimale est divisible par 3. Comme $10 \equiv 1\,[9]$ le même raisonnement nous donne un critère de divisibilité par 9.

1.3 La division euclidienne

On a vu que la notion de congruence permet de simplifier l'étude de la divisibilité d'un entier en se ramenant à étudier des entiers plus petits. Cependant on ne sait pas encore quelles sont les limites de cette méthode : ne peut-on pas donner un sens plus précis à "petit" ? La division euclidienne répond à cette question. En fait, quand on étudie la divisibilité par un entier n, on peut toujours se ramener à étudier ce qu'il se passe pour des nombres compris entre 0 et n.

Théorème. *Étant donné un entier a et un entier b strictement positif, il existe un unique couple (q, r) où $q \in \mathbb{Z}$ et $0 \leqslant r \leqslant b-1$ tel que*

$$a = bq + r.$$

La recherche de ces entiers q et r consiste à effectuer la *division euclidienne* de a par b. On appelle q le *quotient* de la division euclidienne et r le *reste*.

En terme de congruences, ce théorème peut se reformuler ainsi : tout entier relatif est congru modulo b à un unique entier compris entre 0 et $b-1$.

Démonstration. Comme $b \geqslant 1$, il existe un entier k tel que $kb \geqslant a$ et $kb \geqslant -a$, donc l'ensemble des multiples de b qui sont inférieurs à a est non vide (il contient $-kb$) et majoré (tous ces multiples sont inférieurs ou égaux à kb), il existe donc dans cet ensemble un plus grand élément : qb, où q est un entier. Alors $(q+1)b = qb + b > qb$, donc par définition de q, $qb + b > a$. Posons alors $r = a - qb$. Comme $a \geqslant qb$, on a $r \geqslant 0$ et comme $qb + b > a$, on a $r = a - qb < b$. Comme r est un entier, $r \leqslant b-1$. On a donc démontré l'existence des entiers q et r.

Montrons maintenant leur unicité, c'est à dire que si $a = bq + r$ et $a = q'b + r'$ où q, q', r et r' sont des entiers tels que $0 \leqslant r \leqslant b-1$ et $0 \leqslant r' \leqslant b-1$, alors $q = q'$ et $r = r'$. Pour ce faire, commençons par écrire $qb + r = a = q'b + r'$, donc $r - r' = (q' - q)b$. Ainsi, comme $q - q'$ est un entier, $r - r'$ est un multiple de b. Or on a vu que si a est un multiple non nul de b, alors $|a| \geqslant |b|$, donc si $r - r'$ était non nul, on aurait $|r - r'| \geqslant |b| = b$. Cependant comme $0 \leqslant r \leqslant b-1$ et $0 \leqslant r' \leqslant b-1$, on a $-(b-1) \leqslant r - r' \leqslant b-1$, donc $|r - r'| \leqslant b-1$, ce qui donne une contradiction si $r - r'$ est non nul. On peut donc conclure que $r - r' = 0$, donc $r = r'$. On obtient alors $qb = q'b$ et comme b est non nul, $q = q'$, ce qui achève la preuve de l'unicité. □

Le théorème donne donc une réponse positive à la question : pourra-t-on toujours simplifier l'étude de la congruence d'un entier ? Oui car tout entier est congru modulo n à un unique entier compris entre 0 et $n-1$. Ce qui est très intéressant dans ce résultat, c'est que pour un entier n strictement positif, « il n'y a qu'un nombre fini de congruences modulo n ». Plus précisément, on a démontré le corollaire suivant.

Corollaire. *Soit $n \in \mathbb{N}^*$ un entier naturel non nul. Tout entier relatif a est congru modulo n à un unique élément $r \in \{0, \ldots, n-1\}$. Cet entier est le reste dans la division euclidienne de a par n.*

Démonstration. En effet, dire que a est congru modulo n a un entier $r \in \{0, \dots, n-1\}$ signifie qu'il existe $q \in \mathbb{Z}$ tel que $a = r + bq$. Ainsi r est le reste dans la division euclidienne de a par n. Par existence et unicité du reste, l'entier r existe et est unique. □

Voyons quelques illustrations de ces notions.

Exemple. Démontrer que pour tout entier naturel n, le nombre $n(n+1)(n+2)$ est divisible par 3.

Le théorème nous assure que n est congru à 0, 1 ou 2 modulo 3 : il n'y a donc que 3 cas à étudier.

— Premier cas : $n \equiv 0\,[3]$, cela signifie exactement que n est divisible par 3. Comme $(n+1)(n+2)$ est entier, $n(n+1)(n+2)$ est divisible par 3.
— Deuxième cas : $n \equiv 1\,[3]$. Alors $n+2 \equiv 3 \equiv 0\,[3]$, donc $n+2$ est divisible par 3, et donc $n(n+1)(n+2)$ aussi.
— Troisième cas : $n \equiv 2\,[3]$. Alors $n+1 \equiv 0\,[3]$, et de même $n(n+1)(n+2)$ est divisible par 3.

Tous les cas ont été traités, donc pour tout n entier, $n(n+1)(n+2)$ est divisible par 3. Ici le théorème nous a donc permis de nous ramener à étudier seulement 3 cas.

Exemple. Étant donné un entier n, peut-on l'écrire sous la forme $n = a^2 + b^2$ où a et b sont deux entiers ?

Nous allons voir que ceci n'est pas toujours possible, l'idée est de regarder les classes de conjugaison modulo 4. Si $a \in \mathbb{Z}$, a est congru à 0, 1, 2 ou 3 modulo 4. Quelle est alors la classe de conjugaison de a^2 ? On sait que $a \equiv r\,[4]$ où $r \in \{0, 1, 2, 3\}$. Alors $a^2 \equiv r^2\,[4]$. Il y a ainsi 4 cas à étudier :

— $r = 0$, $r^2 \equiv 0\,[4]$.
— $r = 1$, $r^2 \equiv 1\,[4]$.
— $r = 2$, $r^2 = 4 \equiv 0\,[4]$.
— $r = 3$, $r^2 = 9 = 8 + 1 \equiv 1\,[4]$.

Donc finalement un carré est congru à 0 ou 1 modulo 4. Ainsi si a est une somme de deux carrés, a est congru à 0, 1 ou 2 modulo 4. L'unicité du reste de la division euclidienne prouve alors bien qu'un entier congru à 3 modulo 4 ne peut pas s'écrire comme somme de deux carrés. Par exemple 40003 n'est pas une somme de deux carrés (n'est-ce pas plus facile ainsi que de le vérifier à la main ?).

1.4 Le PGCD

Un nouveau problème qui apparaît souvent en arithmétique est de comparer deux entiers, mais d'une façon particulière : en regardant leurs diviseurs. On peut se poser

cette question : si l'on prend deux entiers a et b, quels sont les diviseurs que ces deux nombres ont en commun ? Il s'agit de l'ensemble $\mathcal{D}(a) \cap \mathcal{D}(b)$. Si a ou b est non nul, cet ensemble est fini, il admet donc un plus grand élément que l'on appelle le *PGCD* de a et b (PGCD signifie Plus Grand Commun Diviseur). Cet élément a des propriétés très intéressantes qui font qu'il caractérise à lui tout seul tous les diviseurs communs à a et b. En fait, un des but de cette partie est de montrer qu'un entier divise à la fois a et b si et seulement si il divise $\mathrm{PGCD}(a, b)$. Ainsi $\mathrm{PGCD}(a, b)$ permet donc à lui seul de connaître tous les diviseurs communs à a et b, puisque ce sont exactement les diviseurs de $\mathrm{PGCD}(a, b)$. On peut encore réécrire ceci de cette façon : $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(\mathrm{PGCD}(a, b))$.

Donnons tout d'abord quelques exemples simples de PGCD.

Proposition. *Si a et b sont deux entiers tels que $b \mid a$ et $b \neq 0$, alors* $\mathrm{PGCD}(a, b) = |b|$.

Démonstration. Le PGCD de a et b est le plus grand diviseur commun à a et b. En particulier, il divise b. En particulier, $\mathrm{PGCD}(a, b) \leqslant |b|$. Mais $|b|$ est un diviseur de b. Et comme b divise a, $|b|$ aussi. Ainsi $|b|$ est un diviseur commun à a et b, et c'est bien le plus grand. □

On peut en déduire que si a est un entier, alors $\mathrm{PGCD}(a, 1) = \mathrm{PGCD}(a, -1) = 1$.

Nous allons à présent démontrer une caractérisation très importante du PGCD. Si a et b sont deux entiers relatifs, on note $\mathbb{Z}a + \mathbb{Z}b$ l'ensemble des *combinaisons linéaire entières* en a et b, plus précisément :

$$\mathbb{Z}a + \mathbb{Z}b = \{\lambda a + \mu b : (\lambda, \mu) \in \mathbb{Z}^2\}.$$

Le rapport avec le PGCD est le suivant. Supposons que $(a, b) \neq (0, 0)$ et posons $d = \mathrm{PGCD}(a, b)$. Alors $d \mid a$ et $d \mid b$. En particulier d divise tout entier de la forme $\lambda a + \mu b$ avec $(\lambda, \mu) \in \mathbb{Z}^2$. Ainsi on a une inclusion

$$\mathbb{Z}a + \mathbb{Z}b \subset \mathbb{Z}d.$$

Nous allons prouver que cette inclusion est en fait une égalité.

Théorème. *Supposons que $(a, b) \neq (0, 0)$ (c'est-à-dire que a et b ne sont pas nuls tous les deux). Alors les combinaisons linéaires entières de a et b sont exactement les multiples de* $\mathrm{PGCD}(a, b)$. *Autrement dit*

$$\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}\,\mathrm{PGCD}(a, b).$$

Démonstration. Comme a et b ne sont pas nuls tous les deux, l'ensemble $\mathbb{Z}a + \mathbb{Z}b$ contient un entier non nul. De plus, si $u \in \mathbb{Z}a + \mathbb{Z}b$ on a $-u \in \mathbb{Z}a + \mathbb{Z}b$. L'ensemble $\mathbb{Z}a + \mathbb{Z}b$ contient donc nécessairement un entier strictement positif. Notons d le plus petit entier strictement positif appartenant à cet ensemble. Nous allons montrer que $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d = \{kd : k \in \mathbb{Z}\}$. Pour ce faire, procédons par double inclusion, c'est-à-dire que l'on prouve dans un premier temps que $\mathbb{Z}a + \mathbb{Z}b \subset \mathbb{Z}d$, puis que $\mathbb{Z}d \subset \mathbb{Z}a + \mathbb{Z}b$.

Commençons par prouver que $\mathbb{Z}a+\mathbb{Z}b \subset \mathbb{Z}d$. Il faut donc montrer que si $x \in \mathbb{Z}a+\mathbb{Z}b$, alors $x \in \mathbb{Z}d$. Supposons que $x \in \mathbb{Z}a + \mathbb{Z}b$ et effectuons la division euclidienne de x par d. On obtient $x = dq + r$ où q et r sont des entiers tels que $0 \leqslant r < h$. Comme x et d sont dans $\mathbb{Z}a + \mathbb{Z}b$, on voit que $x - dq$ y est aussi. Ainsi r est un élément de $\mathbb{Z}a + \mathbb{Z}b$. Mais n'oublions pas que l'on a supposé que d est le plus petit élément de $\mathbb{Z}a + \mathbb{Z}b$ qui est strictement positif. Donc si $r \neq 0$, alors par définition de d, on doit avoir $r \geqslant d$. Ceci est absurde vu que l'on sait que $r < d$. Ainsi $r = 0$, ce qui prouve que $x = dq$ et donc que $x \in \mathbb{Z}d$. On a donc démontré que $\mathbb{Z}a + \mathbb{Z}b \subset \mathbb{Z}d$.

Prouvons à présent que $\mathbb{Z}d \subset \mathbb{Z}a+\mathbb{Z}b$. Puisque $d \in \mathbb{Z}a+\mathbb{Z}b$, on peut écrire $d = \lambda a+\mu b$ avec λ et μ des entiers. Si $k \in \mathbb{Z}$, on a donc $kd = (k\lambda)a + (k\mu)b$ avec $k\lambda \in \mathbb{Z}$ et $k\mu \in \mathbb{Z}$, donc $kd \in \mathbb{Z}a + \mathbb{Z}b$. On en conclut que $\mathbb{Z}d \subset \mathbb{Z}a + \mathbb{Z}b$. Finalement on a bien prouvé que $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d$, c'est-à-dire que $\mathbb{Z}a + \mathbb{Z}b$ est exactement l'ensemble de tous les multiples de d.

Pour conclure la preuve du théorème, il suffit donc de prouver que $d = \mathrm{PGCD}(a, b)$. Comme a et b sont des éléments de $\mathbb{Z}a + \mathbb{Z}b$, l'égalité que nous venons de démontrer implique qu'il existe des entiers u et v tels que $a = ud$ et $b = vd$. Ainsi d est ainsi un diviseur commun à a et b. Par définition du PGCD de a et b, on a donc $d \leqslant \mathrm{PGCD}(a, b)$. D'un autre côté, on sait, puisque $d \in \mathbb{Z}a + \mathbb{Z}b$, qu'il existe des entiers λ et μ tels que $d = \lambda a + \mu b$. Ainsi $\mathrm{PGCD}(a, b)$ divise a et b et donc divise d. On en déduit que $|\mathrm{PGCD}(a, b)| \leqslant |d|$ et comme tous ces nombres sont positifs, ceci donne $\mathrm{PGCD}(a, b) \leqslant d$. Finalement on a montré $\mathrm{PGCD}(a, b) \leqslant d$ et $d \leqslant \mathrm{PGCD}(a, b)$, d'où $d = \mathrm{PGCD}(a, b)$. Ceci achève la démonstration. □

Voici à présent la propriété importante du PGCD dont nous parlions au début de cette section :

Corollaire. *Soient a et b deux entiers non nuls tous les deux. Alors d est un diviseur commun à a et b si et seulement si d divise* $\mathrm{PGCD}(a, b)$.

Démonstration. Si d divise $\mathrm{PGCD}(a, b)$, comme $\mathrm{PGCD}(a, b)$ divise a et b, on voit que d doit également diviser a et b. C'est la partie réciproque qui est moins évidente, mais avec le théorème ci-dessus, cela devient plus facile. Supposons que d divise à la fois a et b. On sait qu'il existe des entiers λ et μ tels que $\mathrm{PGCD}(a, b) = \lambda a + \mu b$. Alors, comme $d \mid a$ et $d \mid b$, on a $d \mid \mathrm{PGCD}(a, b)$ et la preuve est terminée. □

1.5 Équations linéaires à coefficients entiers

Nous allons aussi étudier un autre type de problème auquel le PGCD est fortement lié : les équations linéaires à coefficients entiers. Il s'agit d'équations de la forme $ax+by = c$ où a, b et c sont des entiers fixés, et où on cherche des solutions (x, y) telles que x et y soient des entiers. Voici typiquement le type de problème faisant intervenir ce genre d'équation :

Exemple. On dispose de billets de 20 et 50 euros. Combien y a-t-il de façons, et quelles sont-elles, de réunir la somme de 240 euros ? Cela revient en effet à trouver des entiers naturels m et n tels que $20m + 50n = 240$.
On peut aussi voir ces équations plus géométriquement : si on considère la droite affine d'équation $ax + by = c$. Les solutions (x, y) de l'équation qui sont entières, représentent exactement les points à coordonnées entières qui sont sur la droite.

Fixons donc des entiers a, b et c. Si a et b sont nuls tous les deux, l'équation $ax+by = c$ n'a de solutions que si $c = 0$ et dans ce cas tous les couples (x, y) sont solutions. Ce cas n'a donc pas beaucoup d'intérêt et nous supposons désormais que $(a, b) \neq (0, 0)$. Supposons qu'il existe une solution $(x, y) \in \mathbb{Z}^2$ à l'équation $ax + by = c$. Posons $d = \text{PGCD}(a, b)$. Par définition $d \mid a$ et $d \mid b$, donc $d \mid c$. Ainsi une condition nécessaire pour que l'équation ait des solutions est que c soit un multiple du PGCD de a et b. Nous allons voir que l'assertion réciproque est vraie : si c est un multiple de $\text{PGCD}(a, b)$, alors l'équation a effectivement des solutions.

Théorème. *Soient a et b deux entiers relatifs tels que a ou b soit non nul et $d = \text{PGCD}(a, b)$. L'équation $ax + by = c$ a des solutions entières si et seulement si $d \mid c$.*

Remarque. Le théorème nous donne uniquement une condition pour qu'il existe des solutions, il ne nous donne pas toutes les solutions de l'équation. Nous verrons cependant plus loin que l'on peut déterminer l'ensemble des solutions.

Démonstration. Nous avons déjà vu que pour qu'il y ait des solutions, il est nécessaire que $d \mid c$. Réciproquement, il faut monter que si $d \mid c$, il y a des solutions à cette équation. Nous savons que $c \in \mathbb{Z}d$ et que $\mathbb{Z}d = \mathbb{Z}a + \mathbb{Z}b$. On en conclut que $c \in \mathbb{Z}a + \mathbb{Z}b$, c'est-à-dire qu'il existe des entiers x et y vérifiant $c = ax + by$. On a donc bien prouvé l'existence d'une solution (x, y). □

1.6 Entiers premiers entre eux, théorèmes de Bezout et Gauss

Définition. *Soient a et b deux entiers, on dit qu'ils sont premiers entre eux si leur PGCD vaut* 1.

Dire que deux entiers sont premiers entre eux revient à dire que leurs seuls diviseurs communs sont 1 et -1. Le théorème de Bezout donne une autre caractérisation des entiers premiers eux.

Théorème (Théorème de Bezout)**.** *Deux entiers a et b sont premiers entre eux si et seulements si, il existe des entiers m et n tels que $am + bn = 1$.*

Démonstration. La preuve a essentiellement déjà été faite : supposons que a et b soient premiers entre eux. Il existe des entiers m et n tels que $am + bn = \text{PGCD}(a, b) = 1$.

Réciproquement s'il existe m et n tels que $am + bn = 1$, alors $\mathrm{PGCD}(a, b) \mid 1$, donc $\mathrm{PGCD}(a, b) = 1$, ce qui signifie que a et b sont premiers entre eux. □

On a aussi le résultat suivant, conséquence immédiate du théorème :

Corollaire. *Si a et b sont deux entiers premiers entre eux :*

$$\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}.$$

Autrement dit, tout entier peut d'écrire comme combinaison entières de deux entiers premiers entre eux choisis arbitrairement.

Nous allons maintenant passer à un autre théorème très important. Voici le problème : supposons que l'on sache qu'un entier d divise un produit ab de deux entiers. On ne peut a priori pas dire que d divise a ou que d divise b. L'entier d peut même ne diviser ni a ni b, comme on le voit en prenant $d = 6$, $a = 3$ et $b = 4$. Supposons cependant que d et a soient premiers entre eux, cela signifie que a et d n'ont aucun diviseur en commun (ce n'est pas le cas dans l'exemple précédent où a et d ont 3 comme diviseur commun), alors on peut s'attendre à ce que d divise b, c'est l'objet du théorème suivant :

Théorème (Théorème de Gauss)**.** *Soient a, b et d trois entiers tels que $d \mid ab$ et $\mathrm{PGCD}(a, d) = 1$. Alors $d \mid b$.*

Démonstration. Comme a et d sont premiers entre eux, il existe, d'après le théorème de Bezout, deux entiers u et v tels que $au + dv = 1$. En multipliant cette expression par b, on a $abu + dbv = b$. Or comme $d \mid ab$, on obtient alors bien $d \mid (abu + dbv)$, c'est à dire $d \mid b$. □

Ce théorème est très utile, car il permet souvent de simplifier certaines situations. Par exemple si on sait que $3 \mid 2n$, alors on peut en conclure que $3 \mid n$. Voici d'autres exemples parfois bien utiles :

Corollaire. *Soient a, b, c trois entiers tels que a est premier à c et que b est premier à c. Alors ab est premier à c.*

Démonstration. En effet, soit d le PGCD de ab et de c. Comme d divise c et que c est premier à a, alors d est premier à a (ceci nécessite une petite vérification laissée au lecteur). Ainsi comme $d \mid ab$, d'après le théorème de Gauss, $d \mid b$. Or on sait par hypothèse que d divise aussi c. Comme c et b sont premiers entre eux, $d = 1$. □

Corollaire. *Si a et b sont deux entiers premiers entre eux divisant un entier c, alors ab divise c.*

Démonstration. En effet on peut écrire $c = ak$ où k est un entier. Comme b divise c et que a et b sont premiers entre eux, d'après le théorème de Gauss, b divise k. On peut donc bien en conclure que ab divise $c = ak$. □

Remarque. Ce dernier résultat est encore une fois très intuitif : si a et b divisent c, une raison pour laquelle ab ne doit pas forcément diviser c est que a et b auront peut-être des diviseurs en communs, et le produit ab peut être « trop gros » pour diviser c (par exemple 6 et 3 divisent 12, mais $18 = 3 \times 6$ non). Mais si on suppose a et b premiers entre eux, ils n'ont par définition, aucun diviseur en commun, et on s'attend alors bien à ce que ab divise c.

Plus généralement, on peut facilement généraliser ce résultat par récurrence pour obtenir le résultat, très pratique, suivant.

Corollaire. *Soit n un entier et $a_1, \ldots, a_r$ des entiers premiers entre eux deux à deux, c'est-à-dire* $\mathrm{PGCD}(a_i, a_j) = 1$ *si $i \neq j$ divisant n. Alors n est divisible par $a_1 a_2 \cdots a_r$.*

Revenons un instant dans le cas général où a et b sont deux entiers quelconques, non nécessairement premiers entre eux. Soit d leur PGCD. On peut alors écrire $a = da'$ et $b = db'$ où a' et b' sont deux entiers. Que dire alors de a' et b' ? Souvenons-nous que le PGCD de deux entiers représente tout ce que ces entiers ont en commun d'un point de vue arithmétique. On doit donc s'attendre à ce que a' et b' soient premiers entre eux. Et c'est bien le cas. En effet, d'après le théorème 7, on peut trouver des entiers m et n tels que $am + bn = d$. Mais en écrivant $a = da'$ et $b = db'$, on voit que $a'm + b'n = 1$. D'après le théorème de Bezout, a' et b' sont bien premiers entre eux.

Pour conclure ce chapitre, nous allons achever l'étude des équation linéaires à coefficients entiers que nous avions commencée dans le chapitre précédent, en déterminant toutes les solutions d'une telle équation.

Théorème. *Soient a, b et c des entiers. L'équation $ax + by = c$ a des solutions entières si et seulement si le PGCD de a et b divise c. De plus si cette condition est vérifiée, soit (x_0, y_0) une solution particulière de l'équation et a' et b' tels que $a = \mathrm{PGCD}(a, b)a'$ et $b = \mathrm{PGCD}(a, b)b'$. Alors l'ensemble des solutions est :*

$$\{(x_0 + b'k, y_0 - a'k),\ k \in \mathbb{Z}\}.$$

Démonstration. Nous supposerons tout le temps ici que $a \neq 0$. Soit (x, y) une solution entière de cette équation. Alors $ax + by = c$. Or on sait que $c = ax_0 + by_0$, donc $ax + by = ax_0 + by_0$, donc $a(x - x_0) = b(y_0 - y)$. En simplifiant cette égalité par le PGCD de a et b, on obtient $a'(x - x_0) = b'(y_0 - y)$. Or a' et b' sont maintenant premiers entre eux (voir plus haut), et a' divise $b'(y_0 - y)$. Donc d'après le théorème de Gauss, a' divise $y_0 - y$. On pose alors $y - y_0 = -a'k$ avec $k \in \mathbb{Z}$. On a alors $a'(x - x_0) = b'a'k$ d'où $x - x_0 = b'k$ puisque, a étant non nul, a' est non nul. Ainsi toute solution de l'équation est de la forme annoncée. Vérifions réciproquement que tous les éléments de cet ensemble sont solutions de l'équation.

En effet si $k \in \mathbb{Z}$, $a(x_0 + b'k) + b(y_0 - a'k) = (ax_0 + by_0) + k(ab' - ba') = c + k(ab' - ba') = c$ car $\mathrm{PGCD}(a, b)(ab' - ba') = ab - ba = 0$, et $ab' - ba' = 0$. □

Remarque. L'hypothèse $a \neq 0$ dans la démonstration n'est pas restrictive, puisque si $a = b = 0$, les solutions sont faciles à déterminer, et dans le cas contraire, on peut toujours se ramener à $a \neq 0$, quitte à inverser les rôles de a et b.

1.7 L'algorithme d'Euclide

L'algorithme d'Euclide est un algorithme extrêmement efficace pour calculer le PGCD de deux entiers. Il est base sur l'observation suivante. Supposons que a et b sont deux entiers et que $b \geqslant 1$. Effectuons la division euclidienne de a par b : $a = bq + r$. Alors

$$\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, r).$$

Pour vérifier cette égalité il suffit de montrer que $\mathrm{PGCD}(a, b) \mid \mathrm{PGCD}(b, r)$ et que $\mathrm{PGCD}(b, r) \mid \mathrm{PGCD}(a, b)$. Posons $d = \mathrm{PGCD}(a, b)$. Alors $d \mid a$ et $d \mid b$. Ainsi $d \mid r = a - bq$, on en déduit que $d \mid \mathrm{PGCD}(b, r)$. On démontre de façon analogue que $\mathrm{PGCD}(b, r) \mid \mathrm{PGCD}(a, b)$ (exercice).

L'égalité $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, r)$ est très intéressante car $0 \leqslant r < b$. On obtient donc des nombres strictement plus petit. Décrivons l'algorithme. On considère un couple d'entiers a et b. On suppose que $(a, b) \neq (0, 0)$ pour que $\mathrm{PGCD}(a, b)$ soit bien défini. Quitte à échanger a et b, on peut supposer que $b \neq 0$ et, quitte à changer b en $-b$, on peut même supposer que $b \geqslant 1$. On considère alors l'algorithme suivant :

- on pose $a_0 = a$, $b_0 = b$;
- si $b_i = 0$, on s'arrête et on pose $d = a_i$;
- si $b_i \neq 0$, on fait la division euclidienne de a_i par b_i : $a_i = b_i q_i + r_i$, on pose $a_{i+1} = b_i$ et $b_{i+1} = r_i$ et on revient à l'étape précédente.

On remarque que, pour tout i tels que a_i et b_i sont définis, on a $\mathrm{PGCD}(a_i, b_i) = \mathrm{PGCD}(a_{i+1}, b_{i+1})$. Ainsi, à la fin de l'algorithme :

$$\mathrm{PGCD}(a, b) = \mathrm{PGCD}(a_0, b_0) = \mathrm{PGCD}(d, 0) = d$$

où $d = a_i$ avec i le premier indice tel que $b_i = 0$.

Si $\mathrm{PGCD}(a, b) = 1$, cet algorithme peut être utilisé pour obtenir une solution à l'équation

$$am + bn = 1.$$

Une telle solution (m, n) est parfois appelée *relation de Bezout*. En effet supposons comme précédemment que $b \geqslant 1$ et appliquons l'algorithme d'Euclide. Si i est le premier indice tel que $b_i = 0$, on a $a_i = 1$ et donc

$$1 = a_i = b_{i-1} = a_{i-2} - b_{i-2}q_{i-2} = a_{i-2} - a_{i-1}q_{i-1}.$$

C'est-à-dire que l'on a une relation de Bezout entre a_{i-2} et a_{i-1}. On peut alors remplacer a_{i-1} par $a_{i-3} - a_{i-2}q_{i-2}$ dans la relation précédente pour obtenir une relation de Bezout

entre a_{i-3} et a_{i-2}. En continuant comme cela, on arrive à la fin à une relation de Bezout entre $a_0 = a$ et $a_1 = b$, et on obtient une solution explicite à l'équation

$$am + bn = 1.$$

On en déduit donc une méthode pour obtenir l'ensemble des solutions entières d'une équation linéaire à coefficients entiers du type

$$ax + by = c. \tag{1.1}$$

1. Si $a = b = 0$, et $c \neq 0$, il n'y a pas de solution. Si $a = b = c$, tous les couples $(x, y) \in \mathbb{Z}^2$ sont des solutions.

2. Si $(a, b) \neq (0, 0)$ et $\text{PGCD}(a, b)$ ne divise pas c, il n'y a pas de solution.

3. Si $(a, b) \neq (0, 0)$ et si $d = \text{PGCD}(a, b)$ divise c, il existe des solutions. Pour en trouver une, on pose $a = da'$, $b = db'$, $c = dc'$ de sorte que a' et b' sont premiers entre eux. On utilise alors l'algorithme d'Euclide pour trouver un couple (x_0, y_0) d'entiers tel que $a'x_0 + b'y_0 = 1$. Alors le couple d'entiers $(c'x_0, c'y_0)$ est *une* solution à l'équation $a'x + b'y = c'$. L'ensemble des solutions dans $\mathbb{Z}^2$ est alors l'ensemble

$$\{(c'x_0 + b'k, c'y_0 - a'k) : k \in \mathbb{Z}\}.$$

On remarque alors que $a'x + b'y = c'$ et (1.1) ont les mêmes solutions.

4. Si on demande les solutions dans $\mathbb{N}^2$, il suffit de conserver les couples d'entiers positifs qui sont solutions de (1.1).

1.8 Le PPCM

Dans ce très court chapitre, nous allons étudier le PPCM, de deux entiers, notion très proche du PGCD.

Définition. *Soient a et b deux entiers non nuls. On appelle PPCM de a et b (Plus Petit Commun Multiple), le plus petit entier strictement positif* $\text{PPCM}(a, b)$ *qui est à la fois un multiple de a et un multiple de b.*

Supposons désormais a et b positifs (on peut toujours se ramener à ce cas en multiplicant par -1). Il est déjà clair que ab est toujours un multiple commun à a et b, ce n'est cependant pas toujours le PPCM, il existe souvent des multiples communs à a et b plus petits. Soit en effet d le PGCD de a et b. On peut écrire $a = da'$ et $b = db'$ où a' et b' sont premiers entre eux. Alors $da'b'$ est toujours un multiple de a, car il s'agit de ab'. Mais c'est aussi toujours un multiple de b puisqu'on peut aussi l'écrire ba'. C'est donc un multiple commun à a et b. Or on voit bien qu'il est plus petit que ab vu que $ab = d^2a'b'$. En fait on montre que $da'b'$ est le PPCM de a et b.

Théorème. *Soient a et b deux entiers positifs non tous les deux nuls. On pose $a = \mathrm{PGCD}(a,b)a'$ et $b = \mathrm{PGCD}(a,b)b'$. Alors le PPCM de a et b est $\mathrm{PGCD}(a,b)a'b'$.*

Démonstration. En effet soit m le PPCM de a et b. On sait que a divise m, donc $m = ak = \mathrm{PGCD}(a,b)a'k$ où k est un entier. Or $b = \mathrm{PGCD}(a,b)b'$ divise aussi m, donc on peut affirmer que b' divise $a'k$. Comme a' et b' sont premiers entre eux, le théorème de Gauss nous assure que b' divise k. Ainsi $k = b'k'$ où k' est un entier. Donc $\mathrm{PGCD}(a,b)a'b'$ divise m. Or $\mathrm{PGCD}(a,b)a'b'$ est un multiple commun à a et b comme on l'a vu plus haut. Comme m est le plus petit de ces multiples, on a bien $m = \mathrm{PGCD}(a,b)a'b'$, ce qui achève la démonstration. □

Remarque. Comme $ab = \mathrm{PGCD}(a,b)^2a'b'$, on peut en conclure que ab est le PPCM de a et b si et seulement si a et b sont premiers entre eux.

Plus généralement on a la formule suivante :

Corollaire. *Si a et b sont deux entiers positifs non nuls, on a*

$$\mathrm{PGCD}(a,b)\,\mathrm{PPCM}(a,b) = ab.$$

1.9 Les nombres premiers et le théorème fondamental de l'arithmétique

Dans notre étude des diviseurs des nombres entiers, on peut observer que certains nombres ont un statut bien particulier : ils ont très peu de diviseurs. On a déjà vu qu'un entier n a au moins pour diviseurs 1, -1, n et $-n$. Il existe des entiers qui n'ont aucun autre diviseur : par exemple 2, 3, 5... Mais 6 par exemple en a plus : les entiers 2, 3, -2 et -3 sont aussi des diviseurs de 6. Les entiers ayant cette particularité d'avoir si peu de diviseurs sont appelés nombres premiers.

Définition. *On appelle nombre premier un nombre entier naturel p ayant exactement 4 diviseurs, à savoir 1, -1, p et $-p$.*

On peut tout de suite remarquer qu'avec cette définition, 1 n'est pas considéré comme un nombre premier. En effet, il n'a que 2 diviseurs : 1 et -1. C'est une convention, nous verrons plus loin pourquoi le théorème fondamental de l'arithmétique rend cette convention compréhensible.

Remarquons aussi que si p est un nombre premier et n un entier, soit p divise n, soit p et n sont premiers entre eux (en effet le pgcd de p et n est un diviseur de p, donc est soit 1 soit p).

Donnons quelques exemples de nombres premiers. Nous avons 2, 3, 5, 7, 11, 13... (essayez de trouver tous les nombres premiers jusqu'à 50). Les nombres premiers sont très importants car ils permettent à eux seuls de retrouver tous les autres entiers. Par

exemple on peut écrire $60 = 2 \times 2 \times 3 \times 5$. C'est un produit de nombres premiers. En fait tout entier peut s'écrire comme un tel produit de nombres premiers, et mieux : cette décomposition est unique. Dans notre exemple cela signifie que tout produit d'une séquence de nombres premiers autre que 2, 2, 3, 5, donnerait un autre résultat que 60. Il s'agit de ce qu'on appelle le théorème fondamental de l'arithmétique.

Commençons par démontrer quelques propriétés élémentaires des nombres premiers.

Proposition. *Soient p et q deux nombres premiers.*

(i) Si $p \mid q$, alors $p = q$.

(ii) Si $p \neq q$, alors p et q sont premiers entre eux.

Démonstration. Prouvons (i). Si $p \mid q$, alors $p \in \{1, -1, q, -q\}$. Comme p est positif et $p \neq 1$, on a $p = q$.

Pour (ii), on remarque que

$$\mathrm{PGCD}(p, q) \in \mathbb{N} \cap \mathcal{D}(p) \cap \mathcal{D}(q) = \{1, p\} \cap \{1, q\} = \{1\}$$

puisque $p \neq q$. □

Théorème (Théorème fondamental de l'arithmétique)**.** *Soit n un entier naturel non nul. Il existe des nombres premiers $p_1, \ldots, p_r$ et des entiers naturels $\alpha_1, \ldots, \alpha_r$ tels que $n = p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}$. De plus cette décomposition est unique, c'est à dire que si $n = q_1^{\beta_1} \times \cdots \times q_s^{\beta_s}$ où $q_1, \ldots, q_s$ sont des nombres premiers, alors pour tout $1 \leqslant i \leqslant s$, il existe un $1 \leqslant j \leqslant r$ tel que $q_i = p_j$ et $\alpha_j = \beta_i$.*

Démonstration. Nous allons d'abord démontrer l'existence d'une telle décomposition. Notons E l'ensemble des entiers naturels qui s'écrivent comme un produit de nombres premiers. Ce que l'on veut montrer, c'est que $E = \mathbb{N}^*$. Supposons donc le contraire, et soit n le plus petit entier qui ne soit pas dans E. Alors n n'est pas premier, car sinon n serait dans E. n a donc un diviseur d tel que $1 < d < n$. Par définition de n, d est dans E. Ainsi d est un produit de nombres premiers, et il existe donc un nombre premier p qui divise d. p divise alors aussi n. On peut donc écrire $n = pk$ où k est un entier. Mais comme p est premier, $p \geqslant 2$, ainsi $k < n$. Par définition de n, k est dans E, donc k est un produit de nombres premiers. Ainsi $pk = n$ est aussi un produit de nombres premiers. C'est absurde puisque l'on a supposé que n n'appartient pas à E. Notre hypothèse était donc fausse et on a bien $E = \mathbb{N}^*$.

Démontrons maintenant l'unicité de la décomposition. Soient $p_1, \ldots, p_r$ les nombres premiers divisant n (il n'y en a qu'un nombre fini, car ce sont tous des entiers compris entre 2 et n). Supposons les deux à deux distincts (si i est différent de j alors p_i est différent de p_j). Posons de plus α_i le plus grand entier tel que $p_i^{\alpha_i}$ divise n. Nous aurons besoin ici du résultat suivant :

Lemme. *Si p et q sont deux nombres premiers distincts, m et n deux entiers naturels supérieurs ou égaux à 1, alors p^n et q^m sont premiers entre eux.*

Preuve du lemme. En effet soit d leur pgcd. Supposons d différent de 1 et soit l un diviseur premier de d. Alors l divise p^n. Si l est différent de p, alors l est premier avec p et d'après le théorème de Gauss, l divise p^{n-1}. En continuant ainsi, on arrive à l divise p, et comme p est premier, $l = p$. C'est absurde. On peut donc finalement en conclure que $l = p$. Mais de la même façon on peut montrer que $l = q$, et donc $p = q$, c'est absurde aussi. Ainsi p^n et q^m sont premiers entre eux. □

Revenons à la preuve du théorème : En appliquant le lemme, on obtient que $p_1^{\alpha_1}$ et $p_2^{\alpha_2}$ sont premiers entre eux, donc $p_1^{\alpha_1}p_2^{\alpha_2}$ divise n. De plus $p_3^{\alpha_3}$ est premier avec $p_1^{\alpha_1}$ et avec $p_2^{\alpha_2}$, donc avec $p_1^{\alpha_1}p_2^{\alpha_2}$ d'après le corollaire 3. Ceci nous permet encore de conclure que $p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}$ divise n. En continuant ainsi on trouve que $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}$ divise n. On peut donc écrire $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}k$ avec k entier. Supposons k différent de 1, alors il existe un nombre premier p divisant k. Mais alors p divise aussi n, et donc il existe $1 \leqslant i \leqslant r$ tel que $p = p_i$. On aura alors $p_i^{\alpha_i+1}$ divise n. Mais ceci est impossible puisque α_i est le plus grand entier tel que $p_i^{\alpha_i+1}$ divise n. On en conclut donc que $k = 1$ et que $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}$. Supposons maintenant que $n = q_1^{\beta_1}\times\dots\times q_s^{\beta_s}$. Si $1 \leqslant j \leqslant s$, q_j divise n, il existe donc $1 \leqslant i \leqslant r$ tel que $q_j = p_i$. De plus $q_j^{\beta_j}$ divise n, donc par définition, $\beta_j \leqslant \alpha_i$. Notons donc $q_j = p_{i(j)}$. On a $n = q_1^{\beta_1} \times \dots \times q_s^{\beta_s}$, donc $1 = q_1^{\alpha_{i(1)}-\beta_1} \times \dots \times q_s^{\alpha_{i(s)}-\beta s}$. Ceci impose que $\alpha_{i(j)} - \beta_j = 0$ pour tout $1 \leqslant j \leqslant s$, donc que $\alpha_{i(j)} = \beta_j$, ce qui achève la démonstration de l'unicité de la décomposition. □

Ce théorème s'appelle le théorème fondamental de l'arithmétique car la structure arithmétique d'un entier dépend uniquement de sa décomposition en produit de nombres premiers. Les nombres premiers sont ainsi les briques qui permettent d'étudier l'arithmétique des entiers. L'entier 1 n'est pas un nombre premier, car multiplier un entier par 1 ne change rien, il n'est donc pas considéré comme une « brique » de construction.

Soit n un entier naturel. On a vu au cours de la preuve du théorème que si p est un nombre premier divisant n et si l'on note $v_p(n)$ l'exposant de la plus grande puissance de p divisant n, que n est le produit des $p^{v_p(n)}$ pour p premier divisant n. Si p divise n, $v_p(n)$ est donc un entier supérieur ou égal à 1. Posons alors $v_p(n) = 0$ si p est un nombre premier ne divisant pas n. On a ainsi défini $v_p(n)$ pour tout nombre premier p et tout entier naturel n. On dit que $v_p(n)$ est la valuation de n en p. L'unicité de la décomposition en produit de facteurs premiers nous donne ceci :

Corollaire. *Si p est nombre premier, et si n et m sont deux entiers naturels, alors $v_p(nm) = v_p(n) + v_p(m)$.*

Démonstration. En effet, on en décomposant n et m en produit de facteurs premier, on voit que l'exposant de p dans la décomposition de nm est $v_p(n) + v_p(m)$. □

Les nombre premiers nous permettent alors de déterminer les diviseurs d'un entier n :

Théorème. *Soient n et d deux entiers. d divise n si et seulement si pour tout nombre premier p, $v_p(d) \leqslant v_p(n)$.*

Démonstration. Si d divise n, on peut écrire $n = dk$ où k est un entier, et la formule $v_p(n) = v_p(d) + v_p(k)$ pour tout nombre premier p nous montre que $v_p(d) \leqslant v_p(n)$. Réciproquement si pour tout nombre premier p, $v_p(d) \leqslant v_p(n)$, définissons k comme étant le produit des $p^{v_p(n)-v_p(d)}$ pour p nombre premier divisant n. On voit en décomposant n, d et k en produits de facteurs premiers que $n = dk$. □

Corollaire. *Si n et m sont deux entiers naturels $v_p(\mathrm{PGCD}(n,m)) = \min(v_p(n), v_p(m)$ et $v_p(\mathrm{PPCM}(n,m)) = \max(v_p(n), v_p(m))$ pour tout nombre premier p.*

Démonstration. En effet, soit a l'entier défini par $v_p(a) = \min(v_p(n), v_p(m))$ pour tout p premier. Alors $v_p(a) \leqslant v_p(n)$ et $v_p(a) \leqslant v_p(m)$ pour tout nombre premier p, donc a est un diviseur commun à m et à n. Mais si d est un diviseur commun à n et à m, $v_p(d) \leqslant v_p(n)$ et $v_p(d) \leqslant v_p(m)$, donc $v_p(d) \leqslant \min(v_p(n), v_p(m))$, et ceci pour tout premier p. Ainsi d divise a. On peut bien en conclure que a est le PGCD de n et m. La formule pour le PPCM est laissée en exercice au lecteur. □

On peut remarquer aussi que se donner un diviseur positif de n, c'est se donner, pour chaque nombre premier p, un entier $v_p(d)$ compris entre 0 et $v_p(n)$. Le nombre de diviseurs positifs de n est donc le produit des $v_p(n) + 1$ pour p divisant n. Par exemple $60 = 2^2 \times 3 \times 5$, donc $v_2(60) = 2$, $v_3(60) = v_5(60) = 1$. Ainsi 60 a $3 \times 2 \times 2 = 12$ diviseurs positifs. En comptant les diviseurs négatifs, 60 a en tout 24 diviseurs.

On peut encore se poser une question sur les nombres premiers : y en a-t-il une infinité ? Il semble bien que oui, en essayant de déterminer « à la main » les nombres premiers, il nous semble que l'on puisse trouver des nombres premiers aussi grand que l'on veut. Cependant cette simple observation ne constitue pas une véritable démonstration mathématique. Une démonstration très élégante du fait qu'il existe une infinité de nombres premiers est connue depuis Euclide, la voici :

Théorème. *Il existe une infinité de nombres premiers.*

Démonstration. Supposons par l'absurde qu'il n'y ait qu'un nombre fini de nombres premiers. Notons les $p_1, \ldots, p_r$. Posons alors $N = p_1 \times \cdots \times p_r + 1$. N est un entier naturel non nul et strictement supérieur à 1, donc d'après le théorème fondamental de l'arithmétique, il est divisible par un nombre premier p. p fait donc partie de la liste $p_1, \ldots, p_r$. Ainsi p divise $p_1 \times \cdots \times p_r$. Comme p divise aussi N, on obtient que p divise 1, mais ceci est bien entendu absurde. Notre hypothèse était fausse : il existe bien une infinité de nombres premiers. □

Chapitre 2

Groupes

2.1 Définitions et premiers exemples

2.1.1 Loi de composition interne

On appelle *loi de composition interne* sur un ensemble E toute application $*$ de l'ensemble $E \times E$ dans E. Si la loi est notée $*$, nous notons $x * y$ l'image du couple (x, y). Une loi de composition interne est donc une loi produisant un élément de E à partir de deux éléments de E.

Exemple. 1) L'addition sur $\mathbb{Z}$, la multiplication sur $\mathbb{N}$, la division sur $\mathbb{Q} \setminus \{0\}$ sont des lois de composition internes.

2) Soit X un ensemble et soit $E = \mathcal{F}(X, X)$ l'ensemble des applications de X dans X. Si f et g sont deux éléments de E, on note $f \circ g$ l'application de E dans E définie par $x \mapsto g(x) \mapsto f(g(x))$. La loi $\circ$ est alors une loi de composition interne sur E.

La notion de loi de composition interne est tellement générale qu'on ne peut pas en dire grand chose. Nous allons nous intéresser à des lois de composition internes possédant certaines propriétés particulières. Voici des exemples de telles propriétés.

Une loi de composition interne $*$ sur un ensemble E est dite *associative* si elle vérifie la propriété suivante : si $a, b, c \in E$, alors $a * (b * c) = (a * b) * c$. En termes symboliques :

$$\forall (a, b, c) \in E^3, \quad a * (b * c) = (a * b) * c.$$

Remarque. L'hypothèse d'associativité permet de déparenthéser les expressions. On note ainsi $a * b * c$ l'élément $(a * b) * c = a * (b * c)$. Plus généralement si la loi $*$ est associative et si $x_1, \ldots, x_n$ sont des éléments de E, on définit l'élément $x_1 * x_2 * \cdots * x_n$ de E par une récurrence immédiate sur n.

Exemple. 1) L'addition et la multiplication sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{C} \ldots 0$ sont associatives.

2) La soustraction sur $\mathbb{Z}$ n'est pas associative : $(2-3)-1 \neq 2-(3-1)$.

3) Si X est un ensemble, la composition sur $\mathcal{F}(X,X)$ est une loi associative.

Une loi de composition interne $*$ sur un ensemble E possède un *élément neutre* s'il existe un élément e tel que, pour tout $a \in E$, on a $a * e = e * a = a$.

Remarque. S'il existe un élément neutre pour la loi $*$, celui-ci est unique. En effet, supposons que e et e' sont deux éléments neutres pour la loi $*$, alors on a

$$e = e * e' = e'.$$

Si la loi $*$ possède un élément neutre, celui-ci est unique, on l'appelle donc *l'élément neutre* de la loi $*$ (notez l'utilisation de l'article défini « le » pour désigner cet élément neutre, par opposition à l'article indéfini « un »).

Exemple. 1) La loi d'addition $+$ sur $\mathbb{Z}$ possède un élément neutre, il s'agit de 0.

2) La loi de multiplication $\times$ sur $\mathbb{Z}$ possède aussi un élément neutre, il s'agit de 1 (pourquoi 0 n'est-il pas neutre pour l'addition ?).

3) L'application identité Id_X est neutre pour la composition $\circ$ dans $\mathcal{F}(X,X)$.

4) La loi $+$ ne possède pas d'élément neutre dans $\mathbb{N}^*$.

Considérons à présent un ensemble E muni d'une loi de composition interne $*$ possédant un élément neutre e. On dit qu'un élément a de E est *inversible* s'il existe un élément $b \in E$ tel que $a * b = b * a = e$. Un tel élément b est appelé *inverse* de a.

Remarque. Si la loi $*$ est associative, un élément $a \in E$ possède au plus un inverse dans E. En effet, supposons qu'il existe des éléments b et b' vérifiant $a * b = b * a = e$ et $a * b' = b' * a = e$. Alors

$$b = b * e = b * (a * b') = (b * a) * b' = e * b' = b'.$$

Lorsque $*$ est inversible, un élément b vérifiant $a * b = b * a = e$ est donc unique et on l'appelle *l'inverse de a pour la loi $*$* (notez à nouveau l'utilisation du pronom défini puisqu'il n'y a aucune ambiguïté) et on le note a^{-1}.

Exemple. 1) Pour la loi $+$ dans $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots$ l'inverse de x est $-x$.

2) Pour la loi $\times$ dans $\mathbb{Q}$, l'élément 0 n'est pas inversible. Si $x \in \mathbb{Q}^\times$, x est inversible pour $\times$, d'inverse $\frac{1}{x}$.

Soit E un ensemble muni d'une loi de composition interne $*$. On dit que deux éléments x et y *commutent* si $x * y = y * x$. Si tous les éléments de E commutent deux à deux, on dit que la loi $*$ est *commutative*.

Exemple. 1) Les lois $+$ et $*$ sont commutatives sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots$. La loi $-$ ne l'est pas.

2) Si $E = \mathcal{M}_2(\mathbb{R})$ et $\times$ désigne la multiplication matricielle, alors les éléments $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ ne commutent pas.

3) Si $X = \{a, b\}$, la loi $\circ$ n'est pas commutative sur $\mathcal{F}(X, X)$. En effet définissons f par $f(a) = a$, $f(b) = a$ et g par $f(a) = b$, $g(b) = a$. Alors $g \circ f \neq f \circ g$ puisque $(g \circ f)(a) = b$ et $(f \circ g)(a) = a$.

2.1.2 Rappels de quelques notions ensemblistes

Soient X et Y deux ensembles. Une *application* f de X dans Y, notée $f : X \to Y$, est une loi associant à tout élément x de X un élément $f(x)$ de Y. Une application $f : X \to Y$ est dite *injective* si deux éléments distincts de E sont envoyés sur des éléments distincts de F. Par contraposée cela signifie que, pour tous éléments x et y de E, l'égalité $f(x) = f(y)$ implique $x = y$. Une application f de E dans F est dite *surjective* si tout élément de F est dans l'image de f, autrement dit si pour tout $y \in F$, il existe un élément $x \in E$ tel que $f(x) = y$. Une application *bijective* est une application qui est à la fois injective et surjective, autrement dit, pour tout élément $y \in F$, il existe un *unique* $x \in E$ tel que $f(x) = y$.

Si f est une application bijective de X dans Y, on peut définir une application f^{-1} de Y dans X associant à tout $y \in Y$ l'unique antécédent de y par f, c'est-à-dire l'unique $x \in X$ tel que $f(x) = y$. On a donc par définition $f(f^{-1}(y)) = y$ pour tout $y \in Y$. Remarquons que l'on a également $f^{-1}(f(x)) = x$ pour tout $x \in X$. En effet, on a $f(f^{-1}(y)) = y$ pour tout $y \in Y$ donc, en appliquant cette égalité à $f(x)$, on en déduit $f(f^{-1}(f(x)) = f(x)$ et, par injectivité de f, $f^{-1}(f(x)) = x$.

Si f est bijective, on a donc $f^{-1} \circ f = \mathrm{Id}_X$ et $f \circ f^{-1} = \mathrm{Id}_Y$. L'application f^{-1} est appelée *application réciproque* de f.

Remarque. Si f est bijective, l'application f^{-1} est également bijective et $(f^{-1})^{-1} = f$.

Proposition. *Soit X un ensemble et soit $E = \mathcal{F}(X, X)$. Un élément $f \in E$ est inversible pour la loi de composition $\circ$ si et seulement si f est bijective. Dans ce cas, l'inverse de f est l'application réciproque f^{-1}.*

Démonstration. Supposons dans un premier temps que f est bijective. Par définition de l'application réciproque, on a $f \circ f^{-1} = f^{-1}\circ = \mathrm{Id}_X$. Comme Id_X est l'élément neutre de la loi $\circ$, l'élément f est inversible d'inverse f^{-1}.

Réciproquement supposons f inversible. Il existe alors une application $g \in E$ telle que $g \circ f = f \circ g = \mathrm{Id}_X$. Prouvons alors que f est bijective. Commençons par montrer que f est injective. Si x et x' sont deux éléments de X tels que $f(x) = f(x')$, on obtient, en appliquant g,

$$x = g(f(x)) = g(f(x')) = x'.$$

Ainsi f est injective. L'application f est de plus surjective car si $x \in E$, on a $x = f(g(x))$, ce qui montre que $g(x)$ est un antécédent de x par f. Ainsi f est bijective. Comme $f^{-1} \circ f = f \circ f^{-1} = \mathrm{Id}_X$, l'inverse de f est bien donné par f^{-1}. □

2.1.3 Groupes

Définition. *On appelle* groupe *un couple $(G, *)$ où G est un ensemble muni d'une loi de composition interne $*$ qui est associative, possède un élément neutre et telle que tout élément de G est inversible pour $*$.*

Si la loi $*$ est commutative, on dit que le groupe est commutatif *ou encore* abélien.

On s'autorisera assez souvent à écrire G pour désigner le groupe, la loi de composition étant désignée implicitement par la situation.

Exemple. 1) L'ensemble $(\mathbb{Z}, +)$ des entiers relatifs muni de la loi d'addition est un groupe. En effet, la loi $+$ est associative : on a $a + (b + c) = (a + b) + c$ pour tout triple (a, b, c) de nombres entiers. La loi possède également un élément neutre : l'élément 0. En effet, pour tout entier a, on $a + 0 = 0 + a = a$. Enfin tout élément de $\mathbb{Z}$ est inversible. Si a est un entier relatif, alors

$$a + (-a) = (-a) + a = a - a = 0.$$

Ainsi $-a$ est l'inverse de a pour la loi d'addition.

2) Les couples $(\mathbb{Q}^\times, \times)$ et $(\mathbb{R}^\times, \times)$ sont des groupes abéliens.

3) Le couple $(\mathbb{Z}, \times)$ ne forme pas un groupe : l'élément 2, par exemple, n'est pas inversible.

4) Le couple $(\mathrm{GL}_2(\mathbb{R}), \times)$ est un groupe. Ce groupe n'est pas commutatif.

Nous allons à présent donner une première règle de calcul dans un groupe. Il s'agit des lois de *simplification* à gauche et à droite.

Proposition. *Soit $(G, *)$ un groupe et soient (a, b, c) trois éléments de G.*

- *Si $a * b = a * c$, alors $b = c$ (simplification à gauche).*
- *Si $b * a = c * a$, alors $b = c$ (simplification à droite).*

Démonstration. Supposons que $a * b = a * c$. Comme G est un groupe, l'élément a est inversible. Appliquons l'opération $a^{-1}*$ aux deux côtés de l'égalité, on obtient donc

$$\begin{array}{ccc} a^{-1} * (a * b) & = & a^{-1} * (a * c) \\ \| & & \| \\ (a^{-1} * a) * b & & (a^{-1} * a) * c \\ \| & & \| \\ e * b & & e * c \\ \| & & \| \\ b & & c \end{array}$$

Ainsi on a bien $b = c$. On laisse au lecteur sérieux le soin de vérifier la règle de simplification à droite en appliquant $*a^{-1}$. □

Remarque. Même si vous utilisez cette règle depuis longtemps avec l'addition ou la multiplication, il faut bien se rendre compte qu'elle n'est pas vraie dans le cas général d'une loi de composition interne quelconque. Voici un exemple ou elle est prise en défaut. Considérons l'ensemble $M_2(\mathbb{R})$ des matrices réelles de taille 2×2. On le munit de la loi de composition interne $A * B = AB$ (la multiplication matricielle). Il n'est *pas* vrai que

$$AB = AC \Longrightarrow B = C.$$

Voici un exemple très simple, prenez

$$A = B = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right), \quad C = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$$

et faites le calcul. En particulier, $(M_2(\mathbb{R}), \times)$ n'est pas un groupe.

Proposition. *Soit $(G, *)$ un groupe. Si g et h sont deux éléments de G, alors $(g*h)^{-1} = h^{-1} * g^{-1}$. De plus l'inverse de g^{-1} est égal à g, autrement dit $(g^{-1})^{-1} = g$.*

Démonstration. Il suffit de vérifier que $h^{-1} * g^{-1}$ vérifie les propriétés de l'inverse de gh. On aura alors $(g*h)^{-1} = h^{-1}*g^{-1}$ par unicité de l'inverse. Passons donc à la vérification :

$$(g * h)(h^{-1} * g^{-1}) = g * (h * h^{-1}) * g^{-1} = g * e * g^{-1} = g * g^{-1} = e$$

et de même on vérifie que $(h^{-1} * g^{-1}) * (g * h) = e$. On laisse au lecteur l'exercice de vérifier que $g = (g^{-1})^{-1}$. □

Il faut bien faire attention à l'inversion de l'ordre dans la formule $(gh)^{-1} = h^{-1}g^{-1}$. En effet, si le groupe n'est pas commutatif, il n'est pas toujours vrai que $h^{-1}g^{-1} = g^{-1}h^{-1}$!

Donnons à présent quelques exemples de groupes finis. Les seuls exemples vus jusqu'à présent sont des groupes dont le nombre d'éléments est infini. Il existe cependant des groupes finis. Considérons l'ensemble de nombres complexes suivant :

$$G = \{1, -1, i, -i\}.$$

La loi de multiplication est une loi de composition interne sur G. En effet, si on multiplie deux éléments de G, on obtient un autre élément de G. L'ensemble G muni de la loi de multiplication forme un groupe commutatif. En effet, la loi de multiplication est associative et commutative (puisque la loi de multiplication des nombres complexes l'est). L'élément 1 est bien un élément neutre. Il reste à vérifier que tout élément possède bien un inverse :

$$1 \times 1 = 1, \quad (-1) \times (-1) = 1, \quad i \times (-i) = 1, \quad (-i) \times i = 1.$$

L'ensemble $(G, \times)$ est donc un groupe commutatif ayant 4 éléments.

Si G est un groupe fini, on note $|G|$ le nombre d'éléments de G. Il existe en fait des groupes finis de tous les cardinaux possibles, comme le montre l'exercice suivant.

Exercice. Soit $n \geqslant 1$ un entier. On note $\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$. Montrer que, muni de la loi de multiplication, $\mathbb{U}_n$ est un groupe commutatif de cardinal n.

Notations

1) On utilise souvent d'autres symboles que $*$ pour désigner une loi de groupe. Le symbole $\cdot$ est assez souvent utilisé et, dans ce cas, on omet même souvent de l'écrire, c'est-à-dire que l'on peut écrire ab pour $a \cdot b$.

2) On utilise parfois aussi le symbole $+$ pour désigner une loi de groupe. Cependant l'usage veut que l'on n'utilise ce symbole que dans le cas de lois de groupes commutatives. On note alors $-a$ l'inverse de l'élément a.

3) Soit $(G, \cdot)$ un ensemble muni d'une loi de composition interne associative. Si $g \in G$ et $n \geqslant 1$, on pose

$$g^n = \underbrace{g \cdot g \cdot g \cdots g}_{n}$$

(l'associativité de la loi est nécessaire pour pouvoir déparenthéser cette expression). On peut vérifier (par récurrence) que

$$\forall g \in G, \forall (n, m) \in (\mathbb{N}^\times)^2, \quad g^n g^m = g^{n+m}, \quad (g^n)^m = g^{nm}.$$

pour tout $n \geqslant 1$ et $m \geqslant 1$, on a $g^{n+m} = g^n g^m$.

4) Si de plus la loi possède un élément neutre e_G, on pose $g^0 = e_G$ pour tout $g \in G$.

5) Si enfin $(G, \cdot)$ est un groupe, on peut définir les puissance itérées négatives d'un élément. Si $g \in G$ et si $n \in \mathbb{Z} \smallsetminus \mathbb{N}$, on pose $g^n = (g^{-1})^{-n}$. On vérifie alors que

$$\forall g \in G, \forall (n, m) \in \mathbb{Z}^2, \quad g^n g^m = g^{n+m}, \quad (g^n)^m = g^{nm}.$$

2.2 Sous-groupes d'un groupe

Reprenons l'exemple du groupe $(\{1, -1, i, -i\}, \times)$. Pour vérifier que la loi de composition $\times$ est associative, nous avons utilisé l'associativité de la loi $\times$ sur $\mathbb{C}^\times$ et le fait que $\{1, -1, i, -i\}$ est une partie de $\mathbb{C}^\times$. C'est un exemple de *sous-groupe*.

Définition. *Soit $(G, *)$ un groupe. Une partie H de G est un* sous-groupe *de G si elle possède les propriétés suivantes*

- *pour tout g et h dans H, on a $g * h \in H$ (on dit que H est stable pour la loi $*$) ;*
- *l'élément neutre e de G appartient à H ;*
- *si $g \in H$, alors $g^{-1} \in H$.*

Si H est un sous-groupe de $(G, *)$, alors $(H, *)$ est un groupe.

Exemple. Considérons le groupe $(\mathbb{R}, +)$. Alors $\mathbb{Q}$ et $\mathbb{Z}$ sont des sous-groupes de $(\mathbb{R}, +)$. Cependant $\mathbb{N}$ n'est pas un sous-groupe de $(\mathbb{Z}, +)$. En effet si $a \in \mathbb{N}$ et $a > 0$, alors $-a \notin \mathbb{N}$.

Pour vérifier qu'une partie d'un groupe est un sous-groupe, plutôt que de vérifier les trois propriétés de la définition, il est souvent plus rapide d'utiliser le critère suivant.

Proposition. *Soit $(G, *)$ un groupe et soit H une partie de G. Supposons que $e \in H$ et que pour tous g et h dans H, on a $g * h^{-1} \in H$. Alors H est un sous-groupe de $(G, *)$.*

Démonstration. Tout d'abord $e \in H$ donc la seconde propriété de la définition est vérifiée. Si $h \in H$, alors en prenant $g = e$, on en déduit que $h^{-1} = e * h^{-1} \in H$, donc la troisième propriété de la définition est vérifiée. Enfin si g et h sont dans H, alors $h^{-1} \in H$ d'après ce qui précède. On en déduit que $g * h = g * (h^{-1})^{-1} \in H$. Ainsi la première propriété de la définition est vérifiée. □

Exercice. Vérifier que $\mathbb{U}_n = \{z \in \mathbb{C}^\times \mid z^n = 1\}$ est un sous-groupe de $(\mathbb{C}^\times, \times)$.

2.3 Morphismes

Une fois que l'on a défini la notion de groupe, il est naturel de se demander quelles sont les applications entre des groupes qui préservent la loi de composition. On appelle de telles applications des morphismes de groupes.

Définition. *Soient $(G, *)$ et $(G', *')$ deux groupes. On appelle morphisme de G vers G' une application $\varphi : G \to G'$ qui vérifie, pour tous g et h éléments de G,*

$$\varphi(g * h) = \varphi(g) *' \varphi'(h).$$

De façon plus imagée, un morphisme préserve les lois de compositions.

Exemple. L'application exponentielle est un morphisme de groupes de $(\mathbb{R}, +)$ vers $(\mathbb{R}^\times, \times)$ ou de $(\mathbb{C}, +)$ vers $(\mathbb{C}^\times, \times)$. En effet, on a $e^{a+b} = e^a e^b$.

Proposition. *Soit $\varphi : G \to G'$ un morphisme de groupes.*

(i) On a $\varphi(e_G) = e_{G'}$.

(ii) Si $g \in G$, alors $\varphi(g^{-1}) = \varphi(g)^{-1}$.

(iii) Si $g \in G$ et si $n \in \mathbb{Z}$, on a $\varphi(g^n) = \varphi(g)^n$.

Démonstration. Prouvons (i). Dans G, on a $e_G^2 = e_G$. Comme φ est un morphisme, on a $\varphi(e_G) = \varphi(e_G^2) = \varphi(e_G)^2$. En simplifiant de chaque côté par $\varphi(e_G)$, on en déduit $e_{G'} = \varphi(e_G)$.

Prouvons (ii). Soit $g \in G$. Il faut prouver que $\varphi(g^{-1})$ est l'inverse de $\varphi(g)$. On vérifie que

$$\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e_G) = e_{G'}$$
$$\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(e_G) = e_{G'}.$$

Ainsi $\varphi(g^{-1})$ est l'inverse de $\varphi(g)$ dans G' et donc $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Enfin (iii) se prouve par récurrence pour $n \geqslant 1$ et les cas restants se déduisent de (i) et (ii). □

2.3.1 Image et noyau

Proposition. *Soient $(G, \cdot)$ et $(G', \cdot)$ deux groupes et $\varphi : G \to G'$ un morphisme.*

(i) Si H est un sous-groupe de G, alors $\varphi(H)$ est un sous-groupe de G'.

(ii) Si H' est un sous-groupe de G', alors $\varphi^{-1}(H')$ est un sous-groupe de G.

Démonstration. Prouvons (i). Par définition $\varphi(H) = \{\varphi(g) :\in H\}$. Montrons que c'est un sous-groupe de G'. Comme H est un sous-groupe de G, on a $e_G \in H$, donc $e_{G'} = \varphi(e_G) \in H'$. De plus, si g' et h' sont des éléments de $\varphi(H)$, il existe g et h dans H tels que $g' = \varphi(g)$, $h' = \varphi(h)$ et alors

$$g'(h')^{-1} = \varphi(g)\varphi(h)^{-1} = \varphi(gh^{-1}) \in \varphi(H)$$

puisque $gh^{-1} \in H$.

La preuve du point (ii) est laissée en exercice au lecteur. □

Définition. *Soit $\varphi : G \to G'$ un morphisme de groupe. On appelle* noyau *de φ l'ensemble*

$$\mathrm{Ker}(\varphi) = \varphi^{-1}(\{e_{G'}) = \{g \in G \mid \varphi(g)\} = e_{G'}\}.$$

On appelle image *de φ l'ensemble $\varphi(G) \subset G'$.*

Le noyau d'un morphisme φ est un sous-groupe de G puisque c'est l'image inverse du sous-groupe $\{e_{G'}\} \subset G'$. De même l'image de φ est un sous-groupe de G' puisque c'est l'image directe du sous-groupe $G \subset G$.

Le résultat suivant est très pratique pour vérifier qu'un morphisme est injectif.

Proposition. *Soit $\varphi : G \to G'$ un morphisme de groupes. Alors φ est injectif si et seulement si son noyau est réduit à l'élément neutre de G, c'est-à-dire* $\mathrm{Ker}(\varphi) = \{e_G\}$.

Démonstration. Supposons dans un premier temps que φ est injectif. Alors si $\varphi(g) = e_{G'}$, on a $\varphi(g) = \varphi(e_G)$ donc $g = e_G$ par injectivité. Ceci prouve que $\mathrm{Ker}(\varphi) = \{e_G\}$.

Réciproquement supposons que $\mathrm{Ker}(\varphi) = \{e_G\}$. Montrons que φ est injectif. Soient g et h deux éléments de G tels que $\varphi(g) = \varphi(h)$. On a alors

$$e_{G'} = \varphi(g)\varphi(h)^{-1} = \varphi(gh^{-1})$$

et donc $gh^{-1} \in \mathrm{Ker}(\varphi)$. Comme $\mathrm{Ker}(\varphi) = \{e_G\}$, on en conclut que $gh^{-1} = e_G$ c'est-à-dire $g = h$. On a donc prouvé que φ est injectif. □

2.3.2 Composition

Proposition. *Soient $(G,\cdot)$, $(G',\cdot)$ et $(G'',\cdot)$ trois groupes.*

(i) Si $f : G \to G'$ et $g : G' \to G''$ sont deux morphismes, alors $g \circ f$ est un morphisme de G dans G''.

(ii) Soit $f : G \to G'$ un morphisme bijectif. Alors $f^{-1} : G' \to G$ est un morphisme.

Démonstration. La preuve de ce résultat est laissée en exercice d'application. □

Définition. *On appelle* endomorphisme *du groupe $(G,\cdot)$ tout morphisme de G dans G.*

On appelle isomorphisme *du groupe $(G,\cdot)$ vers le groupe $(G',\cdot)$ tout morphisme bijectif de G sur G'.*

On appelle automorphisme *du groupe $(G,\cdot)$ tout endomorphisme de G qui est aussi un isomorphisme.*

Exemple. L'application $x \mapsto e^x$ est un isomorphisme de $(\mathbb{R},+)$ sur $(\mathbb{R}_+^\times,\times)$. Sa réciproque est l'application ln. Cependant $x \mapsto e^x$ n'est pas un isomorphisme de $(\mathbb{C},+)$ sur $(\mathbb{C}^\times,\times)$ car il n'est pas injectif.

2.4 Quelques exemples de groupes

2.4.1 Groupes finis et tables de groupes

La table d'un groupe fini $(G,\cdot)$ de cardinal n est un tableau à double entrée dont les lignes et les colonnes sont indexées par les éléments de G. Si a et b sont deux éléments de G, la case correspond à la ligne a et à la colonne b contient l'élément ab.

Déterminons par exemple la table d'un groupe à deux éléments. Un groupe à deux éléments est de la forme $G = \{e, a\}$ où e est l'élément neutre et a un autre élément ($a \neq e$). On a nécessairement $ee = e$, $ea = a$ et $ae = a$. On a alors $aa = e$ ou $aa = a$. Dans le deuxième cas, en simplifiant par a, on obtient $a = e$, ce qui est absurde. Ainsi $aa = e$. La table du groupe est donc

	e	a
e	e	a
a	a	e

Remarque. Cette courte analyse nous permet de remarquer que tous les groupes de cardinal 2 sont isomorphes. En effet supposons que G et G' sont deux tels groupes d'éléments neutres e et e'. On a alors $G = \{e, a\}$ et $G' = \{e', a'\}$. Définissons alors une bijection de G sur G' en posant $f(e) = e'$ et $f(a) = a'$. En comparant les deux tables de groupes, on vérifie facilement que f est un morphisme de groupes et donc un isomorphes de groupes.

Prenons l'exemple du groupe $\mathbb{U}_4 = \{1, -1, i, -i\}$. Sa table de groupe est

	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

Remarque. On peut remarquer qu'une table de groupe a la propriété suivante : dans chaque ligne et dans chaque colonne, tout élément du groupe apparaît exactement une fois. Essayez de démontrer cette propriété à partir des axiomes de groupe !

2.4.2 Groupes produits

Soient $(G_1, \cdot)$ et $(G_2, \cdot)$ deux groupes. On considère alors l'ensemble $G = G_1 \times G_2$ muni de la loi de composition interne définie par

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 h_1, g_2 h_2).$$

Proposition. *La loi $\cdot$ ainsi définie muni l'ensemble G d'une structure de groupe dont l'élément neutre est (e_{G_1}, e_{G_2}).*

Démonstration. C'est un bon exercice. □

Muni de la structure de groupe ainsi définie, $G_1 \times G_2$ est appelé le *groupe produit* de G_1 et G_2.

Remarque. Cette construction se généralise immédiatement à un produit fini. Si $G_1, \dots G_n$ sont des groupes, on définit de même une structure de groupe produit sur l'ensemble $G_1 \times G_2 \times \cdots \times G_n$.

Exemple. On peut ainsi définir le groupe $G = U_2 \times U_2$, c'est un groupe à 4 éléments. Ce groupe a la propriété suivante : pour tout $g \in \mathbb{U}_2 \times \mathbb{U}_2$, on a $g^2 = e_G$. Sa table de groupe est

	e=(1,1)	(-1,1)	(1,-1)	(-1,-1)
e=(1,1)	e	(-1,1)	(1,-1)	(-1,-1)
(-1,1)	(-1,1)	e	(-1,-1)	(1,-1)
(1,-1)	(1,-1)	(-1,-1)	e	(-1,1)
(-1,-1)	(-1,-1)	(1,-1)	(-1,1)	e

2.4.3 Exemples de groupes de permutations

Soit X un ensemble. On note $\mathfrak{S}(X)$ l'ensemble des applications bijectives $f : X \to X$. Le couple $(\mathfrak{S}(X), \circ)$ est alors un groupe appelé *groupe des permutations de X*. Son élément neutre est l'application identique Id_X.

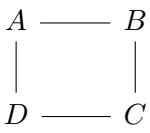
Considérons un cas particulier, celui où X désigne le plan $\mathbb{R}^2$. On peut alors considérer l'ensemble $\mathrm{Iso}(\mathbb{R}^2)$ qui désigne l'ensemble des $f \in \mathfrak{S}(X)$ qui préservent la distance euclidienne, c'est-à-dire telles que

$$\forall P, Q \in \mathbb{R}^2, \quad ||f(P) - f(Q)|| = ||P - Q||.$$

De telles transformations du plan sont appelées *isométries*. On vérifie facilement que $\mathrm{Iso}(\mathbb{R}^2)$ est un sous-groupe de $\mathfrak{S}(\mathbb{R}^2)$ appelé *groupe des isométries du plan*. Nous admettrons pour cet exemple que les isométries du plans sont les translations, les rotations, les symétries orthogonales par rapport à une droite et les symétries glissées (c'est-à-dire la composition d'une symétrie et d'une translation par un vecteur parallèle à l'axe de la symétrie). La démonstration de ce fait sera vue plus tard, lors d'un cours sur les espaces euclidiens.

On peut encore considérer des sous-groupes particuliers du groupe $\mathrm{Iso}(\mathbb{R}^2)$, par exemple le sous-groupe des isométries qui stabilisent une certaine figure du plan. En voici un exemple.

Exemple. On considère le groupe G des isométries de $\mathbb{R}^2$ qui stabilise un carré du plan



Une isométrie qui préserve ce carré doit nécessairement fixer le barycentre de ses quatre sommets, c'est-à-dire le centre O du carré. Une telle isométrie ne peut donc être que l'identité, une rotation ou une symétrie axiale (une translation de vecteur non nul ne fixe aucun point du plan). Les seules rotations qui conviennent sont les rotations de centre O et d'angles 0, $\frac{\pi}{2}$, π et $\frac{3\pi}{2}$. Les seules symétries qui conviennent sont les symétries par rapport aux deux diagonales du carré et par rapports aux médiatrices des côtés du carrés. Le groupe G est donc un groupe fini à 8 éléments. Un bon exercice consiste à écrire la table de ce groupe...

2.5 Groupes cycliques et ordre d'un élément

Soit G un groupe et soit $g \in G$. L'ensemble $H = \{g^n \mid n \in \mathbb{Z}\}$ est un sous-groupe de G. On l'appelle le *sous-groupe engendré par* g et on le note $\langle g \rangle$.

Exemple. Considérons le groupe $(\mathbb{Z}, +)$ est un entier $a \in \mathbb{Z}$. Si $n \geqslant \mathbb{N}$, on a $na = \underbrace{a + \cdots + a}_{n}$ et comme l'inverse de a est $-a$, on a

$$\langle a \rangle = \{na \mid n \in \mathbb{Z}\} = \{\cdots, -2a, -a, 0, a, 2a, 3a, \cdots\}.$$

Ainsi le sous-groupe engendré par a est l'ensemble des multiples de a. Rappelons qu'il s'agit dans l'ensemble noté $\mathbb{Z}a$ dans le chapitre précédent. L'ensemble $\mathbb{Z}a$ est donc le sous-groupe de $(\mathbb{Z}, +)$ engendré par a. Notez qu'il s'agit d'un ensemble infini.

Exemple. Soit $n \geqslant 1$ un entier. Posons $\zeta = e^{\frac{2\pi i}{n}} \in \mathbb{C}^\times$. On s'intéresse au sous-groupe de $(\mathbb{C}^\times, \times)$ engendré par ζ. Comme $\zeta^n = 1$, on a

$$\zeta^r = \zeta^s \text{ si } r \equiv s\,[n].$$

Ainsi

$$\langle \zeta \rangle = \{\zeta^0, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}.$$

Enfin les propriétés de l'exponentielle complexe nous assurent que si $m \in \mathbb{Z}$, on a $\zeta^m = 1$ si et seulement si $n \mid m$. Ainsi

$$\zeta^{m_1} = \zeta^{m_2} \Leftrightarrow \zeta^{m_1 - m_2} \Leftrightarrow n \mid (m_1 - m_2) \Leftrightarrow m_1 \equiv m_2\,[n].$$

On en conclut que les éléments ζ^i pour $0 \leqslant i \leqslant n-1$ sont deux à deux distincts et donc que $\langle \zeta \rangle$ est un groupe fini de cardinal n. Remarquons également que $\langle \zeta \rangle$ est le sous-groupe $\mathbb{U}_n$ que l'on a déjà rencontré.

Ainsi un sous-groupe engendré par un élément peut-être de cardinal infini ou fini selon les cas.

Définition. *Soit G un groupe. On dit que G est* cyclique *si G est engendré par un élément, c'est-à-dire s'il existe $g \in G$ tel que $G = \langle g \rangle$ et si G est fini.*

Supposons que le groupe G soit cyclique. Il existe donc un élément g tel que $G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$. Comme G est de plus fini, tous les éléments g^n ne peuvent pas être distincts. Il existe donc deux entiers $m_1 > m_2$ tels que $g^{m_1} = g^{m_2}$. Ainsi $g^{m_1 - m_2} = e$. Une puissance positive de l'élément g est égale à l'élément neutre, on dit que g est un élément d'ordre fini.

Définition. *Soit G un groupe. On dit qu'un élément g est* d'ordre fini *si il existe un entier $n \geqslant 1$ tel que $g^n = e$. L'*ordre *d'un élément $g \in G$ est alors le plus petit entier $n \geqslant 1$ tel que $g^n = e$.*

Un élément qui n'est pas d'ordre fini et dit d'ordre infini.

Exemple. Le groupe $(\mathbb{C}^\times, \times)$ possède des éléments d'ordre fini. Si $n \geqslant 1$, l'élément $e^{\frac{2\pi i}{n}}$ est d'ordre n.

Exemple. Le seul élément du groupe $(\mathbb{Z}, +)$ qui est d'ordre fini est 0. En effet si $a \neq 0$, on a $na \neq 0$ pour tout $n \geqslant 0$.

Proposition. *Soit G un groupe et g un élément de G d'ordre n. Pour tout entier $m \in \mathbb{Z}$, on a $g^m = e$ si et seulement si n divise m. Plus généralement, on a*

$$g^{m_1} = g^{m_2} \Leftrightarrow m_1 \equiv m_2\,[n].$$

Démonstration. Un sens est facile. Supposons que n divise m. Il existe alors un entier k tel que $m = nk$. On peut alors écrire $g^m = (g^n)^k = e^k = e$. Donc $g^m = e$.

Réciproquement supposons que $g^m = e$. Effectuons la division euclidienne de m par n. On a donc $m = nk + r$ avec $k \in \mathbb{Z}$ et $0 \leqslant r < n$. Alors

$$g^m = g^{nk+r} = (g^n)^k g^r = g^r.$$

Or n est par définition le plus petit entier $\geqslant 1$ tel que $g^n = e$. Comme $0 \leqslant r < n$, on en conclut que $r = 0$. Ainsi n divise m. □

Théorème. *Soit G un groupe cyclique et soit $g \in G$ un élément tel que $G = \langle g \rangle$. Soit n l'ordre de g. Alors G est de cardinal n et*

$$G = \{g^0 = e, g, g^2, \ldots, g^{n-1}\}.$$

Démonstration. Remarquons tout d'abord que, puisque g est d'ordre n, on a $g^{m_1} = g^{m_2}$ si et seulement si $m_1 \equiv m_2 \,[n]$. Soit $h \in G$ un élément quelconque. Par définition de $G = \langle g \rangle$, il existe un entier m tel que $h = g^m$. De plus il existe un unique $0 \leqslant r < n$ tel que $m \equiv r \,[n]$ et donc tel que $h = g^r$. On en conclut que

$$G = \{g^r \mid r = 0, 1, 2, \ldots, n-1\}$$

et que les éléments $e, g, \ldots, g^{n-1}$ sont deux à deux distincts. En particulier G est de cardinal n. □

2.6 Le théorème de Lagrange, relations d'équivalence

2.6.1 Relations d'équivalence

Soit E un ensemble et $\mathcal{R}$ une relation binaire sur E (c'est-à-dire une relation telle que $=$, $\leqslant$, $<$,etc.). On dit que $\mathcal{R}$ est

1) *réflexive* si $\forall a \in E$, $a\mathcal{R}a$;
2) *symétrique* si $a\mathcal{R}b \Leftrightarrow b\mathcal{R}a$;
3) *antisymétrique* si $a\mathcal{R}b$ et $b\mathcal{R}a$ impliquent $a = b$;
4) *transitive* si $a\mathcal{R}b$ et $b\mathcal{R}c$ impliquent $a\mathcal{R}c$.

Définition. *Une relation binaire $\mathcal{R}$ sur un ensemble E est appelée* relation d'équivalence *si elle est réflexive, symétrique et transitive.*

Exemple. a) La relation d'égalité est une relation d'équivalence.

b) Si $E = \mathbb{Z}$ et $n \in \mathbb{N}^*$, la relation de congruence modulo n est une relation d'équivalence.

c) Si E désigne l'ensemble des droites du plan, la relation « être parallèle à » est une relation d'équivalence.

Si $\mathcal{R}$ est une relation d'équivalence sur un ensemble E, on appelle *classe d'équivalence* de l'élément $a \in E$ l'ensemble $\mathrm{Cl}_{\mathcal{R}}(a) = \{x \in E : a\mathcal{R}x\}$.

Les classes d'équivalence vérifient les propriétés suivantes :

— par réflexivité de $\mathcal{R}$,
$$\forall a \in E, \quad a \in \mathrm{Cl}_{\mathcal{R}}(a)$$

— si $b \in \mathrm{Cl}_{\mathcal{R}}(a)$, alors $\mathrm{Cl}_{\mathcal{R}}(b) = \mathrm{Cl}_{\mathcal{R}}(a)$. En effet on a $a\mathcal{R}b$ et, pour $c \in \mathrm{Cl}_{\mathcal{R}}(b)$, $b\mathcal{R}c$. La transitivité implique alors que $a\mathcal{R}c$, c'est-à-dire $c \in \mathrm{Cl}_{\mathcal{R}}(a)$. On en conclut que $\mathrm{Cl}_{\mathcal{R}}(b) \subset \mathrm{Cl}_{\mathcal{R}}(a)$. Par symétrie, on a aussi $b\mathcal{R}a$, c'est-à-dire $a \in \mathrm{Cl}_{\mathcal{R}}(b)$ et, d'après le résultat ci-dessus, $\mathrm{Cl}_{\mathcal{R}}(a) \subset \mathrm{Cl}_{\mathcal{R}}(b)$. On a donc bien $\mathrm{Cl}_{\mathcal{R}}(a) = \mathrm{Cl}_{\mathcal{R}}(b)$.

— deux classes d'équivalence sont soit égales soit disjointes :
$$\forall (a,b) \in E^2, \quad \mathrm{Cl}_{\mathcal{R}}(a) = \mathrm{Cl}_{\mathcal{R}}(b) \text{ ou } \mathrm{Cl}_{\mathcal{R}}(a) \cap \mathrm{Cl}_{\mathcal{R}}(b) = \emptyset.$$
En effet supposons $\mathrm{Cl}_{\mathcal{R}}(a) \cap \mathrm{Cl}_{\mathcal{R}}(b) \neq \emptyset$ et montrons que $\mathrm{Cl}_{\mathcal{R}}(a) = \mathrm{Cl}_{\mathcal{R}}(b)$. Comme $\mathrm{Cl}_{\mathcal{R}}(a) \cap \mathrm{Cl}_{\mathcal{R}}(b) \neq \emptyset$, il existe $c \in \mathrm{Cl}_{\mathcal{R}}(a) \cap \mathrm{Cl}_{\mathcal{R}}(b)$. On a donc $\mathrm{Cl}_{\mathcal{R}}(a) = \mathrm{Cl}_{\mathcal{R}}(c)$ et $\mathrm{Cl}_{\mathcal{R}}(b) = \mathrm{Cl}_{\mathcal{R}}(c)$, d'où $\mathrm{Cl}_{\mathcal{R}}(a) = \mathrm{Cl}_{\mathcal{R}}(b)$.

On note alors $E/\mathcal{R}$ l'ensemble des classes d'équivalence de E pour la relation $\mathcal{R}$.

Exemple. Soit $E = \mathbb{Z}$ et soit $\mathcal{R}$ la relation $\equiv [n]$ pour un certain $n \geqslant 1$. Les classes d'équivalence sont les parties de $\mathbb{Z}$ de la forme $a + n\mathbb{Z}$. En effet, si $a \in \mathbb{Z}$, on a
$$x \in \mathrm{Cl}_{\mathcal{R}}(a) \Leftrightarrow a \equiv x\,[n] \Leftrightarrow x \in a + n\mathbb{Z}.$$

Définition. *Soit E un ensemble. On appelle* partition *de E toute famille $(A_i)_{i\in I}$ de parties de E telle que*

(i) $\forall i \in I, \quad A_i \neq \emptyset$;

(ii) $\forall (i,j) \in I^2,\ i \neq j, \quad A_i \cap A_j = \emptyset$;

(iii) $\bigcup_{i\in I} A_i = E$.

Si $(A_i)_{i\in I}$ est une parition de E, on utilise la notation $E = \coprod_{i\in I} A_i$.

Remarque. Si E est un ensemble fini et $(A_i)_{i\in I}$ alors I est un ensemble fini et
$$|E| = \sum_{i\in I} |A_i|.$$

Une relation d'équivalence $\mathcal{R}$ sur un ensemble E fournit une partition de cet ensemble en classes d'équivalence.

Proposition. *Soit E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E, la famille $(\mathrm{Cl}_{\mathcal{R}}(a))$ est une partition de E.*

Démonstration. Pour tout $a \in E$, on a $a \in \mathrm{Cl}_{\mathcal{R}}(a)$, donc $\mathrm{Cl}_{\mathcal{R}}(a) \neq \emptyset$ et $E = \bigcup_{a\in E} \mathrm{Cl}_{\mathcal{R}}(a)$. De plus si $\mathrm{Cl}_{\mathcal{R}}(a) \neq \mathrm{Cl}_{\mathcal{R}}(b)$, on a $\mathrm{Cl}_{\mathcal{R}}(a) \neq \mathrm{Cl}_{\mathcal{R}}(b)$, on a donc bien une partition de E. □

2.6.2 Le théorème de Lagrange

Théorème (Théorème de Lagrange)**.** *Soit G un groupe fini et soit H un sous-groupe de G. Alors le cardinal de H divise le cardinal de G.*

Démonstration. Considérons la relation binaire sur G

$$a\mathcal{R}b \Leftrightarrow a^{-1}b \in H.$$

Il s'agit d'une relation d'équivalence sur G. En effet, puisque $e_G \in H$, on a $a\mathcal{R}a$ pour tout $a \in G$, la relation est donc réflexive. La relation est symétrique :

$$a\mathcal{R}b \Leftrightarrow a^{-1}b \in H \Leftrightarrow (a^{-1}b)^{-1} = b^{-1}a \in H \Leftrightarrow b\mathcal{R}a.$$

Enfin la relation est transitive : si $a\mathcal{R}b$ et $b\mathcal{R}c$, on a $a^{-1}b \in H$ et $b^{-1}c \in H$ donc $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$, ce qui signifie $a\mathcal{R}c$. Déterminons les classes d'équivalence de cette relation. Si $a \in G$,

$$a\mathcal{R}x \Leftrightarrow a^{-1}x \in H \Leftrightarrow x \in aH = \{ah : h \in H\}.$$

Ainsi G est l'union disjointe de ses classes d'équivalence, c'est-à-dire

$$G = \coprod (aH).$$

Comme G est fini, il y a un nombre fini de classes d'équivalences $a_1H, \ldots, a_rH$ et

$$|G| = \sum_{i=1}^{r} |a_iH|.$$

Il reste à déterminer le cardinal d'une classe d'équivalence aH. L'application $f : H \to aH$ définie par $f(h) = ah$ est une bijection de H sur aH. En effet si $b \in aH$, b s'écrit sous la forme $b = ah$ pour un certain $h \in H$ et h est l'unique antécédent de b pr f. En effet, d'après la règle de simplification à gauche, $ah = ah'$ implique $h = h'$. Il existe donc une bijection entre les deux ensembles finis H et aH, ils ont donc le même cardinal. Finalement

$$|G| = \sum_{i=1}^{r} |H| = r|H|$$

ce qui montre que $|H|$ est un diviseur de $|G|$. □

Corollaire. *Soit G un groupe fini et soit g un élément de G. Alors l'ordre $\omega(g)$ de g est un diviseur de $|G|$.*

Démonstration. On applique le théorème de Lagrange au sous-groupe $H = \langle g \rangle$ engendré par g. Ce sous-groupe est cyclique de cardinal $\omega(g)$, donc $\omega(g)$ divise $|G|$. □

Voici un exemple d'application : la classification des groupes de cardinal premier à isomorphisme près.

Théorème. *Soit p un nombre premier. Tout groupe fini d'ordre p est cyclique est isomorphe à $\mathbb{U}_p$.*

Démonstration. Soit G un groupe fini de cardinal p. Soit $x \neq e_G$ un élément de G. Alors $\omega(x) \mid |G| = p$ donc $\omega(x) = 1$ ou $\omega(x) = p$. Comme $x \neq e$, on a $\omega(x) \neq 1$ donc x est d'ordre p. Le sous-groupe $\langle x \rangle$ engendré par x est donc de cardinal p, on a donc $\langle x \rangle = G$. Ceci implique que le groupe G est cyclique de cardinal p. On a déjà prouvé qu'un tel groupe est isomorphe à $\mathbb{U}_p$. □

2.7 Le groupe $\mathbb{Z}/N\mathbb{Z}$

Soit $N \geqslant 1$ un entier et soit $\mathcal{R}$ la relation de congruence modulo N. C'est une relation d'équivalence dont les classes d'équivalence sont les ensembles de la forme

$$a + N\mathbb{Z} = \{a + kN \mid k \in \mathbb{Z}\}.$$

Comme tout entier est congruent à un unique élément de $\{0, \ldots, N-1\}$ (par division euclidienne), il ya exactement N classes d'équivalences qui sont

$$N\mathbb{Z}, 1 + N\mathbb{Z}, \ldots, (N-1) + \mathbb{Z}.$$

Définition. *On note $\mathbb{Z}/N\mathbb{Z}$ l'ensemble des classes d'équivalence de $\mathbb{Z}$ pour la relation de congruence modulo N. Ses éléments sont donc les classes $a + N\mathbb{Z}$ où $a \in \mathbb{Z}$. On notera simplement $\overline{a}$ la classe $a + N\mathbb{Z}$.*

Si a et b sont deux entiers relatifs, on a donc

$$\overline{a} = \overline{b} \Leftrightarrow a \equiv b\,[N] \Leftrightarrow b \in a + N\mathbb{Z}.$$

L'existence et l'unicité du reste dans la division euclidienne par N nous donnent alors

$$\mathbb{Z}/N\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{N-1}\}.$$

Il faut bien comprendre que $\overline{N+1}$ est aussi un élément de $\mathbb{Z}/N\mathbb{Z}$, mais on a $\overline{N+1} = \overline{1}$ (car $N + 1 \equiv 1\,[N]$).

Nous allons à présent munir l'ensemble $\mathbb{Z}/N\mathbb{Z}$ d'une structure de groupe abélien. Soient x et y deux éléments de $\mathbb{Z}/N\mathbb{Z}$. On peut alors les écrire $x = \overline{a}$ et $y = \overline{b}$ où a et b sont deux éléments de $\mathbb{Z}/N\mathbb{Z}$. Il est alors tentant de poser $x + y = \overline{a+b}$. Cependant il y a un point auquel il faut faire attention : il faut bien vérifier que $\overline{a+b}$ ne dépend pas du choix de a et b. En effet, on a $\overline{a} = \overline{a+N} = x$ et il est possible de choisir $a + N$ à la place de a. Notre définition n'a un sens que si $\overline{a+N+b}$ et $\overline{a+b}$ donnent le même élément de $\mathbb{Z}/N\mathbb{Z}$.

Plus généralement supposons donc $x = \overline{a} = \overline{a'}$ et $y = \overline{b} = \overline{b'}$. On a alors $a \equiv a'\,[N]$ et $b \equiv b'\,[N]$. Les propriétés d'addition des congruences nous assurent alors que $a + b \equiv$

$a' + b'\,[N]$ et donc que $\overline{a+b} = \overline{a'+b'}$. Autrement dit, la quantité $\overline{a+b}$ ne dépend pas du choix de a et b mais uniquement de x et y. On pose alors

$$x + y = \overline{a+b}.$$

Proposition. *L'ensemble $\mathbb{Z}/N\mathbb{Z}$ muni de la loi de composition interne $+$ est un groupe commutatif. Son élément neutre est $\overline{0}$ et l'inverse $\overline{a}$ et $\overline{-a}$.*

Démonstration. Laissée en exercice. □

Proposition. *Le groupe $(\mathbb{Z}/N\mathbb{Z}, +)$ est cyclique de cardinal N.*

Démonstration. Nous avons déjà vu que $\mathbb{Z}/N\mathbb{Z}$ est un ensemble fini de cardinal N. En effet pour tout $a \in \mathbb{Z}$, il existe un unique $0 \leqslant r \leqslant N-1$ tel que $\overline{a} = \overline{r}$. Vérifions donc qu'il est engendré par un élément. Nous allons en fait vérifier qu'il est engendré par $\overline{1}$. Soit $r \geqslant 1$ un entier, en utilisant la relation $\overline{a} + \overline{b} = \overline{a+b}$, on vérifie facilement par récurrence que

$$\overline{r} = \underbrace{\overline{1} + \cdots + \overline{1}}_{r} = r\overline{1}.$$

Ceci prouve que $\mathbb{Z}/N\mathbb{Z} = \{r\overline{1} : 1 \leqslant r \leqslant N\}$ et est donc engendré par $\overline{1}$. Il s'agit donc d'un groupe monogène. Comme il est fini de cardinal n, c'est un groupe cyclique de cardinal n. □

Corollaire. *Tout groupe cyclique de cardinal n est isomorphe à $(\mathbb{Z}/N\mathbb{Z}, +)$.*

Chapitre 3

Le groupe symétrique

Nous allons ici étudier une famille de groupes de nature combinatoire.

3.1 Définition

3.1.1 Permutations d'un ensemble

Soit X un ensemble. Une *permutation* de X est une application bijective $f : X \to X$. L'ensemble des permutations de X est noté $\mathfrak{S}(X)$. Comme la composition de deux applications bijectives est encore bijective, si f et g sont deux permutations de X, leur compoée $f \circ g$ est encore une permutation de X. On munit ainsi l'ensemble $\mathfrak{S}(X)$ d'une loi de composition interne $(f, g) \mapsto f \circ g$.

Proposition. *Muni de la loi $\circ$, l'ensemble $\mathfrak{S}(X)$ est un groupe.*

Démonstration. Nous avons déjà remarqué que la loi $\circ$ est associative. L'application identité Id_X est une permutation de X et vérifie bien $f \circ \mathrm{Id}_X = f = \mathrm{Id}_X \circ f$ pour tout $f \in \mathfrak{X}(X)$, donc $\circ$ possède un élément neutre. Enfin, si $f \in \mathfrak{S}(X)$, l'application réciproque f^{-1} est une bijection de X dans X et $f \circ f^{-1} = f^{-1} \circ f = \mathrm{Id}_X$. Ainsi tout élément possède un inverse et $(\mathfrak{S}(X), \circ)$ est un groupe. □

3.1.2 Le cas d'un ensemble fini

Soit $n \geqslant 1$ un entier. On note $\mathfrak{S}_n$ le groupe des permutations de l'ensemble $\{1, \ldots, n\}$. Un élément σ est donc une permutation $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$. La loi de groupe est la loi de composition des permutations

$$\sigma\sigma' = \sigma \circ \sigma'.$$

Rappelons que $\sigma \circ \sigma'$ est la permutation de $\{1, \ldots, n\}$ obtenue en appliquant d'abord σ', puis σ. Autrement dit, pour $1 \leqslant i \leqslant n$, on a

$$\sigma\sigma'(i) = \sigma(\sigma'(i)).$$

Une façon standard de décrire une permutation σ est de l'écrire sous la forme d'un tableau à deux lignes, la première ligne étant la liste $1, 2, \ldots, n$ et la deuxième la liste $\sigma(1), \sigma(2), \ldots, \sigma(n)$. Voici un exemple si $n = 4$. La permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

est la permutation

$$\begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 4 \\ 4 \mapsto 3 \end{cases}$$

Exemple. Considérons les éléments de $\mathfrak{S}_3$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma' = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

et calculons $\sigma\sigma'$. On a $\sigma\sigma'(1) = \sigma(2) = 3$ et $\sigma\sigma'(2) = \sigma(1) = 2$. Comme $\sigma\sigma'$ est une permutation, on a nécessairement $\sigma\sigma'(3) = 1$:

$$\begin{cases} 1 \overset{\sigma'}{\longmapsto} 2 \overset{\sigma}{\longmapsto} 3 \\ 2 \mapsto 1 \mapsto 2 \\ 3 \mapsto 3 \mapsto 1 \end{cases}$$

et donc $\sigma\sigma' = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

À titre d'exercice, vérifier que $\sigma'\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. On remarque que $\sigma\sigma' \neq \sigma'\sigma$, le groupe S_3 n'est donc pas commutatif ! L'ordre de composition est donc très important.

Théorème. *Le groupe $\mathfrak{S}_n$ est un groupe fini de cardinal $n!$.*

Démonstration. Il faut compter combien de permutations de l'ensemble fini $\{1, \ldots, n\}$ sont possibles. Se donner une permutation de $\{1, \ldots, n\}$ revient à se donner n entiers $\sigma(1), \ldots, \sigma(n)$ deux à deux distincts et compris entre 1 et n. Il y a donc n choix possibles pour $\sigma(1)$. Une fois $\sigma(1)$ choisi, il n'y a plus que $n - 1$ choix pour $\sigma(2)$, puis $n - 2$ choix pour $\sigma(3)$ etc. et une unique possibilité pour $\sigma(n)$. Au final, il y a donc $n(n-1)(n-2)\cdots 1$ choix possibles de permutations de $\{1, \ldots, n\}$. □

3.1.3 Exemples d'éléments

Si $1 \leqslant i < j \leqslant n$, on note (i, j) l'unique permutation de $\{1, \dots, n\}$ qui échange i et j et fixe tous les autres éléments. Une telle permutation s'appelle une *transposition*.

Si $2 \leqslant k \leqslant n$ et si $a_1, \dots, a_k$ sont des éléments distincts de $\{1, \dots, n\}$, on note $(a_1, \dots, a_k)$ la permutation σ définie par

$$\begin{aligned} \sigma(a_1) &= a_2 \\ \sigma(a_2) &= a_3 \\ &\vdots \\ \sigma(a_k) &= a_1 \\ \sigma(x) &= x \text{ si } x \notin \{a_1, \dots, a_k\}. \end{aligned}$$

Une telle permutation est appelée un *k-cycle*.

Remarque. Les 2-cycles sont exactement les transpositions.

Exemple.

$$(2,3) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad (1,3,2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad (1,2)(2,3) = (1,2,3).$$

Proposition. *Tout élément de $\mathfrak{S}_n$ s'écrit comme un produit de transpositions.*

Démonstration. Pour $n \geqslant 2$, soit H_n l'hypothèse de récurrence « toute permutation de $\{1, \dots, n\}$ est un produit de transpositions ». Alors H_2 est vrai car $\mathfrak{S}_2 = \{\mathrm{Id}, (12)\}$. Supposons H_n vrai et démontrons H_{n+1}. Soit $\sigma \in \mathfrak{S}_{n+1}$ et posons

$$\sigma' = \begin{cases} \sigma & \text{si } \sigma(n+1) = n+1 \\ (n, \sigma(n+1)) \circ \sigma & \text{si } \sigma(n+1) \neq n+1. \end{cases}$$

Alors $\sigma'(n+1) = n+1$. La restriction de σ' à $\{1, \dots, n\}$ est un élément de $\mathfrak{S}_n$ et s'écrit comme un produit de transpositions par H_n. Comme $\sigma = (n, \sigma(n+1)) \circ \sigma'$, on en conclut que σ est un produit de transpositions. □

3.2 Décomposition d'une permutation

Soit $\sigma \in \mathfrak{S}_n$. On appelle *support* de la permutation σ l'ensemble $\{x \in \{1, \dots, n\} : \sigma(x) \neq x\}$. On le note $\mathrm{Supp}(\sigma)$.

Proposition. *(i) Les ensembles* $\mathrm{Supp}(\sigma)$ *et* $\{1, \dots, n\} \smallsetminus \mathrm{Supp}(\sigma)$ *sont stables par* σ.

(ii) Si $\mathrm{Supp}(\sigma_1) \cap \mathrm{Supp}(\sigma_2) = \emptyset$, *alors* $\sigma_1 \sigma_2 = \sigma_2 \sigma_1$.

Démonstration. Supposons que $x \notin \mathrm{Supp}(\sigma)$. Alors $\sigma(x) = x$. On en conclut que $\sigma(\sigma(x)) = \sigma(x)$ et donc que $\sigma(x) \notin \mathrm{Supp}(\sigma)$. Ainsi le complémentaire de $\mathrm{Supp}(\sigma)$ est stable par σ. Comme σ est une permutation de $\{1, \dots, n\}$, on en conclut que $\mathrm{Supp}(\sigma)$ est également stable par σ.

Supposons désormais que σ_1 et σ_2 sont deux permutations à supports disjoints. Si $x \notin \mathrm{Supp}(\sigma_1) \cup \mathrm{Supp}(\sigma_2)$, alors $\sigma_1(\sigma_2(x)) = \sigma_1(x) = x = \sigma_2(\sigma_1(x))$. Si $x \in \mathrm{Supp}(\sigma_1)$, on a donc $x \notin \mathrm{Supp}(\sigma_2)$, ce qui implique $\sigma_2(x) = x$. Comme $\mathrm{Supp}(\sigma_1)$ est stable par σ_1, on a $\sigma_1(x) \in \mathrm{Supp}(\sigma_1)$ et donc $\sigma_2(\sigma_1(x)) = \sigma_1(x)$. On a donc

$$\sigma_2(\sigma_1(x)) = \sigma_1(x) = \sigma_1(\sigma_2(x)).$$

De façon identique, on montre la même égalité si $x \in \mathrm{Supp}(\sigma_2)$. On en conclut que

$$\forall x \in \{1, \dots, n\}, \quad \sigma_2(\sigma_1(x)) = \sigma_1(x) = \sigma_1(\sigma_2(x)),$$

c'est-à-dire $\sigma_2\sigma_1 = \sigma_1\sigma_2$. □

Théorème. *Toute permutation $\sigma \in \mathfrak{S}_n$ se décompose comme un produit de cycles à support disjoints.*

Démonstration. Soit H_n l'hypothèse de récurrence « pour tout $k \leqslant n$, toute élément de $\mathfrak{S}_k$ est un produit de cycles à supports disjoints ». L'hypothèse H_2 est trivialement vraie. Supposons H_n. Soit $\sigma \in \mathfrak{S}_{n+1}$. On pose $E = \{\sigma^k(1) : k \in \mathbb{N}\}$. Dans le cas contraire, σ est d'ordre fini et il existe $m \geqslant 1$ tel que $\sigma^m = \mathrm{Id}$. Soit $p = \min\{k \geqslant 1; \sigma^k(1) = 1\}$. Alors $E = \{1, \sigma(1), \dots, \sigma^{p-1}(1)\}$. On montre facilement que $\sigma^k(1) = \sigma^{k'}(1)$ si et seulement si $k \equiv k'\,[p]$ et donc que E contient p éléments. Si $p = n + 1$, alors $E = \{1, \dots, n + 1\}$ et on a gagné car $\sigma = (1, \sigma(1), \dots, \sigma^{p-1}(1))$ est un $(n + 1)$-cycle. Sinon on pose $c = (1, \sigma(1), \dots, \sigma^{p-1}(1))$. C'est un p-cycle. On pose $\sigma' = c^{-1}\sigma$ de sorte que $\sigma'(k) = k$ si $k \in E$. Ainsi σ' induit une permutation de l'ensemble $\{1, \dots, n + 1\} \smallsetminus E$ qui est de cardinal inférieur à n. Par H_n, on en déduit que σ' se décompose comme un produit de cycles à supports disjoints, contenus dans $\{1, \dots, n + 1\} \smallsetminus E$. Comme $\mathrm{Supp}(c) = E$ et que $\sigma = c\sigma'$, on en conclut que σ est un produit de cycles à supports disjoints. □

Remarque. Une telle décomposition est unique à l'ordre près mais nous ne le démontrerons pas.

Exemple. Le théorème montre donc que les éléments de $\mathfrak{S}_5$ sont de la forme suivante

- l'identité ;
- les transpositions ;
- les 3-cycles ;
- les 4-cycles ;
- les 5-cycles ;
- les produits d'un 3-cycle et d'une transposition dont les supports sont disjoints.

À titre d'exercice, on pourra dénombrer les éléments de chaque type ci-dessus.

Corollaire. *Soit $\sigma \in \mathfrak{S}_n$ et soit $\sigma = \sigma_1\sigma_2\cdots\sigma_r$ une décomposition de σ en produit de cycles à supports disjoints. Alors*

$$\omega(\sigma) = \mathrm{PPCM}(\omega(\sigma_1), \ldots, \omega(\sigma_r)).$$

Remarque. On note $\mathrm{PPCM}(n_1, \ldots, n_r)$ le plus petit commun multiple aux entiers $n_1, \ldots, n_r$. On vérifie facilement que le calcul de ce ppcm se ramène au cas de deux entiers par la formule suivante

$$\mathrm{PPCM}(n_1, \ldots, n_r) = \mathrm{PPCM}(n_1, \mathrm{PPCM}(n_2, \ldots, n_r)).$$

Démonstration. On considère uniquement le cas où $r = 2$. Le cas général s'en déduit par récurrence. Posons $\sigma = \sigma_1\sigma_2$ où σ_1 et σ_2 sont à supports disjoints. Soit n l'ordre de σ. On a donc $\sigma^n = \mathrm{Id}$. Si $x \in \mathrm{Supp}(\sigma_2)$, on a $\sigma^n(x) = \sigma_2^n(x)$. Si $x \notin \mathrm{Supp}(\sigma_2)$, alors $\sigma_2(x) = x$ donc $\sigma_2^n = \mathrm{Id}$. On en conclut que $\omega(\sigma_2) \mid n$. De même, on prouve que $\omega(\sigma_1) \mid n$. Ainsi $\mathrm{PPCM}(\omega(\sigma_1), \omega(\sigma_2)) \mid n$. Réciproquement si $\mathrm{PPCM}(\omega(\sigma_1), \omega(\sigma_2)) \mid n$, on a $\sigma_1^n = \mathrm{Id}$ et $\sigma_2^n = \mathrm{Id}$. Comme σ_1 et σ_2 commutent, on en déduit que $\sigma^n = \sigma_1^n\sigma_2^n = \mathrm{Id}$. On en déduit que $n = \mathrm{PPCM}(\omega(\sigma_1), \omega(\sigma_2))$. □

3.3 Signature d'un élément, groupe alterné

3.3.1 Définition

Soit $\varepsilon : \mathfrak{S}_n \to (\mathbb{C}^\times, \times)$ un morphisme de groupes. Quelle peut être la forme de ε ? Remarquons déjà que si σ est une transposition, alors $\sigma^2 = \mathrm{Id}$ et donc $\varepsilon(\sigma)^2 = 1$ d'où $\varepsilon(\sigma) \in \{\pm 1\}$. Comme tout élément de $\mathfrak{S}_n$ est un produit de transposition et que ε est un morphisme de groupes, on en déduit que

$$\forall \sigma \in \mathfrak{S}_n, \quad \varepsilon(\sigma) \in \{\pm 1\}.$$

Cependant il n'est pas clair qu'il existe un tel morphisme qui soit non trivial. On peut donc se demander s'il est possible de construire un tel morphisme de groupe. La *signature* en est un exemple.

Si $\sigma \in \mathfrak{S}_n$, on pose

$$\ell(\sigma) = |\{(i,j) \in \{1, \ldots, n\}^1 : i < j \text{ et } \sigma(i) > \sigma(j)\}|.$$

Il s'agit du nombre d'inversions de σ. On pose alors $\varepsilon(\sigma) = (-1)^{\ell(\sigma)}$. Le nombre $\varepsilon(\sigma)$ s'appelle la *signature* de σ.

Théorème. *La signature $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ est un morphisme de groupes tel que $\varepsilon(\tau) = -1$ si τ est une transposition.*

Démonstration. Soient σ_1 et σ_2 deux éléments de $\mathfrak{S}_n$. Il faut vérifier que $\varepsilon(\sigma_1\sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)$. On utilise la formule suivante

$$\varepsilon(\sigma) = \prod_{i<j} \operatorname{sgn}(\sigma(j) - \sigma(i)).$$

On a

$$\begin{aligned}
\varepsilon(\sigma_1\sigma_2)\varepsilon(\sigma_2) &= \prod_{i<j}(\sigma_1\sigma_2(j) - \sigma_1\sigma_2(i)) \prod_{i<j}(\sigma_2(j) - \sigma_2(i)) \\
&= \prod_{i<j} \underbrace{\operatorname{sgn}(\sigma_1(\sigma_2(j)) - \sigma_1(\sigma_2(j)))\operatorname{sgn}(\sigma_2(j) - \sigma_2(i))}_{\text{symétrique en } i \text{ et } j} \\
&= \prod_{\sigma_2(i)<\sigma_2(j)} \operatorname{sgn}(\sigma_1(\sigma_2(j)) - \sigma_1(\sigma_2(j)))\operatorname{sgn}(\sigma_2(j) - \sigma_2(i)) \\
&= \prod_{i<j} \operatorname{sgn}(\sigma_2(j) - \sigma_2(i)) = \varepsilon(\sigma_2).
\end{aligned}$$

Il reste à vérifier si τ est une transposition, on a $\varepsilon(\tau) = -1$. Supposons que $\tau = (i, j)$ avec $i < j$ et soient $k < \ell$.

$$\begin{cases}
k, \ell \notin \{i, j\} & \tau(k) = k < \ell = \tau(\ell) \\
k = i,\ \ell \neq j & \tau(k) < \tau(\ell) \text{ si } \ell > j,\ \tau(k) > \tau(\ell) \text{ si } i < \ell < j \\
k \neq i,\ \ell = j & \tau(k) < \tau(\ell) \text{ si } k < i,\ \tau(k) > \tau(\ell) \text{ si } i < k < j \\
(k, \ell) = (i, j) & \tau(k) > \tau(\ell).
\end{cases}$$

Ainsi $\ell(\tau) = 2(j - i - 1) + 1$ et donc $\varepsilon(\tau) = -1$. □

3.3.2 Le groupe alterné

On note $\mathfrak{A}_n$ le noyau de la signature ε. Il s'agit d'un sous-groupe de $\mathfrak{A}_n$ appelé *sous-groupe alterné* de $\mathfrak{S}_n$. Il s'agit de l'ensemble des permutations de signature $+1$.

Proposition. *Le groupe $\mathfrak{A}_n$ est un groupe de cardinal $\frac{n!}{2}$.*

Démonstration. Soit $\tau \in \mathfrak{S}_n$ une transposition. Comme $\varepsilon(\tau) = -1$ et comme ε est un morphisme de groupes, on a $\varepsilon(\sigma) = -1$ si et seulement s $\sigma \in \tau\mathfrak{A}_n$. Ainsi $\mathfrak{S}_n$ est l'union disjointe de $\mathcal{A} - n$ et de $\tau\mathcal{A}_n$. Comme ces deux parties sont de cardinal $|\mathcal{A}_n|$, on en déduit que $|\mathfrak{S}_n| = 2|\mathcal{A}_n|$ et le résultat. □

Exemple. Le sous-groupe alterné de $\mathfrak{S}_2$ est de cardinal 1, il est réduit à l'identité. Le sous-groupe alterné de $\mathfrak{S}_3$ est de cardinal 3. Il contient les 3-cycles. Comme $\mathfrak{S}_3$ possède exactement deux 3-cycles, on a

$$\mathcal{A}_3 = \{\mathrm{Id}, (1, 2, 3), (1, 3, 2)\}.$$

De plus comme 3 est un nombre premier, le groupe $\mathcal{A}_3$ est automatique cyclique de cardinal 3. On peut aussi remarque qu'un 3-cycle est un élément d'ordre 3 dans $\mathfrak{S}_3$.

Chapitre 4

Anneaux

4.1 Structure d'anneau

4.1.1 Définitions

Soit A un ensemble muni de deux lois de composition internes $+$ et $\times$. On dit que le triplet $(A, +, \times)$ est un *anneau* s'il vérifie les propriétés suivantes

1) le couple $(A, +)$ est un groupe abélien ;
2) la loi $\times$ est associative ;
3) la loi $\times$ est distributive par rapport à $+$, ce qui signifie que

$$\forall (a, b, c) \in A, \quad \begin{aligned} a \times (b + c) &= (a \times b) + (a \times c) \\ (a + b) \times c &= (a \times c) + (b \times c); \end{aligned}$$

4) il existe un élément neutre pour la loi $\times$.

On dit qu'un anneau $(A, +, \times)$ est *commutatif* si la loi $\times$ est commutative.

Remarque. 1) On note 0_A l'élément neutre pour la loi $+$ et on l'appelle l'*élément nul* de A. On note 1_A l'élément neutre pour la loi $\times$ et on l'appelle l'*unité* de A.

2) Comme dans $\mathbb{C}$, on omet parfois le signe $\times$ dans les calculs et on écrit ab pour $a \times b$.

Exemple. 1) Les triplets $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des anneaux.

2) Soit E un ensemble et soit $\mathcal{F}$ l'ensemble des fonctions de E dans $\mathbb{R}$. On peut définir deux lois $+$ et $\times$ sur $\mathcal{F}$. Si f et g sont deux éléments de $\mathcal{F}$, on peut définir une fonction $f + g$ en posant, pour $x \in E$, $(f + g)(x) = f(x) + g(x)$. On définit de même une fonction $f \times g$ en posant, pour $x \in E$, $(f \times g)(x) = f(x) \times g(x)$. Le triplet $(\mathcal{F}, +, \times)$ est alors un anneau. Son élément nul est la fonction constante prenant la valeur 0 en tout point et son unité est la fonction constante prenant la valeur 1 en tout point.

3) Soit $\mathcal{M}_n(\mathbb{R})$ l'ensemble des matrices carrées de taille n à coefficients dans $\mathbb{R}$. L'addition et la multiplication matricielles font de $\mathcal{M}_2(\mathbb{R})$ un anneau. Cet anneau n'est pas commutatif. En effet, on a

$$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\times\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)\neq\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)\times\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right).$$

Proposition. *Soit $(A,+,\times)$ un anneau. On a alors*

1) $\forall a\in A,\quad a\times 0_A=0_A\times a=0_A$ *;*

2) $\forall (a,b)\in A^2,\quad a\times(-b)=(-a)\times b=-(a\times b)$ *;*

3) $\forall (a,b)\in A^2,\quad (-a)\times(-b)=a\times b.$

Démonstration. Comme 0_A est un élément neutre pour la loi $+$, on a $0_A=0_A+0_A$. Ainsi en multipliant cette égalité par a et en utilisant la distributivité, on a

$$0_A\times a=(0_A+0_A)\times a=(0_A\times a)+(0_A\times a)$$

et en remarquant que $(A,+)$ est un groupe, on en déduit $0_A=0_A\times a$. On montre de façon similaire que $0_A=a\times 0_A$, ce qui fournit 1).

Si a et b sont dans A, on a

$$(a\times b)+(a\times(-b))=a\times(b-b)=a\times 0_A=0_A$$

par 1). On en déduit que $a\times(-b)$ est l'inverse de $a\times b$ pour la loi $+$, c'est-à-dire $a\times(-b)=-(a\times b)$. On montre de façon similaire que $(-a)\times b=-(a\times b)$ et on obtient 2).

Si a et b sont dans A, on utilise deux fois 2) et on a

$$(-a)\times(-b)=-(a\times(-b))=-(-(a\times b))=a\times b.$$ □

4.1.2 Calcul dans les anneaux

On rappelle que dans le groupe $A,+$, on note $na=\underbrace{a+\cdots a}_{n}$ si $n\in\mathbb{N}$. De même, si $n\in\mathbb{N}^*$ et $a\in A$, on note a^n pour l'élément $\underbrace{a\times\cdots\times a}_{n}$ et $a^0=1_A$. On a les relations habituelles $a^{n+m}=a^n\times a^m$, $a^{nm}=(a^n)^m$. Il faut noter que, puisque l'élément a n'est pas toujours inversible dans A, la notation a^n n'a pas toujours de sens si $n<0$.

Rappelons que si $n\in\mathbb{N}$ et $0\leqslant m\leqslant n$ est un entier naturel inférieur ou égal à n, on note $\binom{n}{m}$ (ou parfois C_n^m) l'entier

$$\binom{n}{m}=\frac{n!}{m!(n-m)!}=\frac{n(n-1)(n-2)\cdots(n-m+1)}{m!}.$$

On vérifie facilement que ces entiers vérifient la relation de récurrence suivante

$$\binom{n+1}{m+1} = \binom{n}{m} + \binom{n}{m+1}.$$

On peut représenter graphiquement cette relation sous la forme du triangle de Pascal :

$$\begin{array}{ccccccc} 1 & & & & & & \\ 1 & 1 & & & & & \\ 1 & 2 & 1 & & & & \\ 1 & 3 & 3 & 1 & & & \\ 1 & 4 & 6 & 4 & 1 & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \end{array}$$

Remarque. L'entier $\binom{n}{m}$ est très important en combinatoire et en probabilités : il s'agit du nombre de parties à m éléments dans un ensemble à n éléments.

Proposition (Formule du binôme de Newton)**.** *Soit A un anneau. Si a et b sont deux éléments de A tels que $ab = ba$ et si $n \in \mathbb{N}$, on a*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + b^n.$$

Démonstration. Si $n = 0$, la relation est vraie car $\binom{0}{0} = 1$ (par convention, on pose toujours $0! = 1$). Supposons la relation vraie pour n et montrons qu'elle est vraie pour $n+1$. On a en effet

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)^n a + (a+b)^n b \\
&= \left(\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k\right) a + \left(\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k\right) b \\
&= \left(\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k a\right) + \left(\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^{k+1}\right) \\
&= \left(\sum_{k=0}^{n} \binom{n}{k} a^{n-k+1}b^k\right) + \left(\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^{k+1}\right) \\
&= \left(\sum_{k=0}^{n} \binom{n}{k} a^{n+1-k}b^k\right) + \left(\sum_{k=1}^{n+1} \binom{n}{k-1} a^{n-k+1}b^k\right) \\
&= a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k} + \binom{n}{k-1}\right) a^{n+1-k}b^k \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k}b^k.
\end{aligned}$$

Ce qui prouve la formule. □

Remarque. Dans la démonstration précédente, on a utilisé le fait que a et b commutatent pour transformer l'expression $a^{n-k}b^k a$ en $a^{n+1-k}b^k$. L'hypothèse de commutativité de a et b est essentielle. En effet, on a général

$$(a+b)^2 = a^2 + ab + ba + b^2$$

et on ne peut pas remplacer $ab + ba$ par $2ab$, sauf si a et b commutent.

4.1.3 Sous-anneaux

Soit $(A, +, \times)$ un anneau. Un *sous-anneau* de $(A, +, \times)$ est une partie B de A telle que

1) B est un sous-groupe de $(A, +)$;
2) pour tous a et b dans B, on a $a \times b \in B$;
3) $1_A \in B$.

Proposition. *Si B est un sous-anneau de $(A, +, \times)$, le triplet $(B, +, \times)$ est un anneau.*

Démonstration. La vérification est laissée au lecteur. □

Exemple. L'ensemble $\mathbb{Z}$ est un sous-anneau de $(\mathbb{C}, +, \times)$.

4.1.4 Morphismes d'anneaux

Soient A et A' deux anneaux. Un *morphisme d'anneaux* de A vers A' est une application $f : A \to A'$ telle que

1) $\forall (a, b) \in A^2, \quad f(a+b) = f(a) + f(b)$;
2) $\forall (a, b) \in A^2, \quad f(a \times b) = f(a) \times f(b)$;
3) $f(1_A) = 1_{A'}$.

Un *endomorphisme d'anneaux* d'un anneau A est un morphisme d'anneaux de A vers A. Un *isomorphisme d'anneaux* d'un anneau A vers un anneau A' est un morphisme d'anneaux qui est de plus bijectif. Un *automorphisme d'anneaux* de A est un endomorphisme de A qui est aussi un isomorphisme.

Exemple. 1) Soit $a \in \mathbb{Z}$ et définissons $f : \mathbb{Z} \to \mathbb{Z}$ en posant $f(x) = ax$. Alors f est un morphismes de groupes $(\mathbb{Z}, +) \to (\mathbb{Z}, +)$, cependant, si $a \neq 1$, ce n'est pas un morphisme d'anneaux car, en général, $f(xy) \neq f(x)f(y)$.

2) L'application $z = x + iy \mapsto \overline{z} = x - iy$ est un morphisme d'anneaux. C'est même un automorphisme de l'anneau $\mathbb{C}$.

Si $f : A \to A'$ est un morphisme d'anneaux, on appelle *noyau* de f l'ensemble

$$\mathrm{Ker}(f) = \{a \in A : f(a) = 0_{A'}\}$$

et *image* de f l'ensemble $f(A)$.

Remarque. On peut vérifier que l'image d'un morphisme d'anneaux $f : A \to A'$ est toujours un sous-anneau de A'. Attention, en général, le noyau d'un tel morphisme n'est pas un sous-anneau de A : il ne contient pas toujours 1_A.

4.1.5 Idéaux

Soit $(A, +, \times)$ commutatif. Un *idéal* de A est une partie $I \subset A$ telle que
1) $(I, +)$ est un sous-groupe de A ;
2) pour tout $a \in A$ et $x \in I$, on a $a \times x \in I$.

4.1.6 Produit d'anneaux

Soient $A_1, \ldots, A_n$ des anneaux. On peut munir l'ensemble $A_1 \times \cdots \times A_n$ de deux lois de composition internes en posant

$$(a_1, \ldots, a_n) + (b_1, \ldots,_n) = (a_1 + b_1, \ldots, a_n + b_n)$$
$$(a_1, \ldots, a_n) \times (b_1, \ldots, b_n) = (a_1 \times b_1, \ldots, a_n \times b_n).$$

Proposition. *Muni des lois $+$ et $\times$ ainsi définies, l'ensemble $A_1 \times \cdots \times A_n$ est muni d'une structure d'anneau. Son élément nul est $(0_{A_1}, \ldots, 0_{A_n})$ et son unité est $(1_{A_1}, \ldots, 1_{A_n})$.*

Démonstration. La vérification est laissée en exercice au lecteur. □

4.2 Anneaux intègres et corps

4.2.1 Anneaux intègres

Un anneau $(A, +, \times)$ est dit *intègre* si, pour tous a et b dans A, la relation $ab = 0_A$ implique $a = 0_A$ ou $b = 0_A$. Autrement dit, dans un anneau intègre, si $a \neq 0_A$ et $b \neq 0_A$, on a $ab \neq 0_A$.

Proposition. *Dans un anneau intègre, on a les règles de simplification suivantes :*
(i) si $a \neq 0_A$, alors $ab = ac \Rightarrow b = c$;
(ii) si $c \neq 0_A$, alors $ac = bc \Rightarrow a = b$.

Démonstration. Prouvons la relation (i), (ii) est similaire. Supposons que $ab = ac$. Alors, comme $(A, +)$ est un groupe, on a $ab - ac = 0_A$. Comme $-ac = a(-c)0$, on déduit de la distributivité de $\cdot$ que $a(b - c) = 0_A$. Comme $a \neq 0_A$ et que A est intègre, on en déduit $b_c = 0_A$, c'est-à-dire $b = c$. □

Exemple. 1) L'anneau $(\mathbb{Z}, +, \times)$ est intègre.

2) L'anneau $(\mathcal{M}_2(\mathbb{R}), +, \times)$ n'est pas intègre. En effet, si $M = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, on a $M \neq 0$ mais $M^2 = M \times M = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

4.2.2 Corps

Un *corps* est un anneau $(A, +, \times)$ tel que $1_A \neq 0_A$ et tel que $(A \setminus \{0\}, \times)$ est un groupe. De façon équivalente, un corps est un anneau ayant au moins deux éléments et tel que tout élément non nul est inversible.

Exemple. 1) Les anneaux $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps.

2) L'anneau $\mathbb{Z}$ n'est pas un corps : l'élément 2, par exemple, n'est pas inversible pour la loi $\times$.

Proposition. *Un corps est un anneau intègre.*

Démonstration. Soit K un corps. Soient a et b deux éléments de K tels que $ab = 0_K$. Supposons $a \neq 0_K$. Alors, puisque K est un corps, l'élément a est inversible. Il existe donc $a^{-1} \in K$ tel que $a^{-1}a = aa^{-1} = 1_A$. De l'égalité $ab = 0_K$, on déduit $a^{-1}(ab) = a^{-1}0_A$. Ainsi $(a^{-1}a)b = 0_K$ et donc $b = 1_A b = 0_K$. On montre de même que si $b \neq 0_K$, alors $a = 0_K$. L'anneau K est donc bien intègre. □

Les anneaux finis ont des propriétés très particulières, il se trouve que tout anneau fini et intègre est en fait déjà un corps.

Théorème. *Un anneau A qui est intègre, de cardinal fini et non nul (c'est-à-dire tel que $1_A \neq 0_A$) est un corps.*

Démonstration. Rappelons que si E est un ensemble fini et que f est une application de E dans E, alors les trois propriétés suivantes sont équivalentes :

— f est injective ;

— f est surjective ;

— f est bijective.

Nous allons à présent démontrer le théorème. Soit $(A, +, \times)$ un anneau intègre, fini et non nul. Comme A est non nul, il possède au moins 2 éléments. Montrons donc que tout élément non nul de A est inversible. Soit $a \in A \setminus \{0\}$. On définit l'application

$$\varphi : \begin{array}{ccc} A & \to & A \\ x & \mapsto & ax \end{array}$$

L'application φ est un endomorphisme du *groupe* $(A, +)$. En effet, si $(x, y) \in A^2$, on a

$$\varphi(x + y) = a(x + y) = (ax) + (ay) = \varphi(x) + \varphi(y).$$

Montrons à présent que φ est injective. Comme φ est un morphisme de groupes, il suffit de vérifier que son noyau est l'ensemble $\{0_A\}$. C'est le cas puisque :

$$\varphi(x) = 0_A \Leftrightarrow ax = 0_A \Leftrightarrow x = 0_A.$$

La dernière équivalence est une conséquence du fait que A est intègre et que $a \neq 0$. L'application φ est donc une application injective de A dans A. Comme A est fini, l'application φ est également surjective. Cela signifie qu'il existe $x \in A$ tel que $\varphi(x) = 1_A$, c'est-à-dire $ax = 1_A$.

En utilisant l'application $x \mapsto xa$, on montre de même qu'il existe un élément $y \in A$ tel que $ya = 1_A$. Pour conclure que a est inversible, il reste à vérifier que $x = y$. Pour ce faire, on remarque que

$$y = y1_A = y(ax) = (ya)x = 1_A x = x.$$

Ainsi $x = y = a^{-1}$ et a est bien un élément inversible de A. On a montré que tout élément non nul de A est inversible, donc A est bien un corps. □

4.2.3 Groupe des inversibles

Si A est un anneau, et si A n'est pas un corps, l'ensemble $A \setminus \{0\}$ n'est pas un groupe pour la loi $\times$. Dans le cas général, on peut considérer un ensemble plus petit qui, lui, est un groupe.

Rappelons qu'un élément $a \in A$ est *inversible* s'il est inversible pour la loi $\times$, c'est-à-dire s'il existe $a^{-1} \in A$ tel que $a^{-1}a = aa^{-1} = 1_A$. On note alors $A^\times$ l'ensemble des éléments inversibles pour la loi $\times$.

Remarquons que si a et b sont inversibles, alors ab est inversible. En effet $b^{-1}a^{-1}$ est alors un inverse de ab. On en conclut que la loi $\times$ induit une loi de composition interne sur $A^\times$.

Proposition. *Le couple $(A^\times, \times)$ est un groupe.*

Démonstration. La loi $\times$ est associative sur A, elle l'est donc également sur $A^\times$. L'élément 1_A est tautologiquement inversible, on a donc $1_A \in A^\times$ et 1_A est un élément neutre pour $\times$. Enfin, tout élément de $A^\times$ est inversible. Il suffit en effet de vérifier que si $a \in A^\times$, alors $a^{-1} \in A^\times$. C'est clair car, si a^{-1} est l'inverse de a, alors a est l'inverse de a^{-1} et on a bien $a^{-1} \in A^\times$. □

Pour cette raison, on nomme le groupe $(A^\times, \times)$, *groupe des inversibles* de l'anneau A.

Remarque. Si A_1 et A_2 sont deux anneaux, on vérifie facilement que l'on a $(A_1 \times A_2)^\times = A_1^\times \times A_2^\times$.

4.3 L'anneau $\mathbb{Z}/n\mathbb{Z}$

4.3.1 Définition

Soit $n \geqslant 1$ un entier. Rappelons que la relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$. L'ensemble de ses classes d'équivalence est noté $\mathbb{Z}/n\mathbb{Z}$. Nous avons déjà vu comment munir $\mathbb{Z}/n\mathbb{Z}$ d'une structure de groupe abélien. Nous allons enrichir cette structure en une structure d'anneau. Rappelons également que les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont de la forme $\overline{a}$ pour $a \in \mathbb{Z}$.

Si x et y sont deux éléments de $\mathbb{Z}/n\mathbb{Z}$, il existe des entiers a et b tels que $x = \overline{a}$ et $y = \overline{b}$. On a envie de définir le produit xy comme étant la classe $\overline{ab}$ du produit ab mais il faut vérifier auparavant que $\overline{ab}$ ne dépend pas des choix particuliers de a et b dans les classes x et y. Soient donc a' et b' deux entiers tels que $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$. On a donc $a \equiv a'\,[n]$ et $b \equiv b'\,[n]$. Les lois d'opérations sur les congruences nous apprennent que $ab \equiv a'b'\,[n]$, c'est-à-dire $\overline{ab} = \overline{a'b'}$. La quantité $\overline{ab}$ ne dépend donc pas du choix de a et b mais uniquement de $\overline{a}$ et $\overline{b}$. On peut donc définir sans ambigüité

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

Proposition. *Le triplet $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif.*

Démonstration. On a déjà vu que le couple $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif. Il faut donc vérifier que la loi $\cdot$ est commutatif, associative, distributive par rapport à $+$ et possède un élément neutre. Vérifions la commutativité : si x et y sont deux éléments de $\mathbb{Z}/n\mathbb{Z}$, il existe des entiers a et b tels que $x = \overline{a}$ et $y = \overline{b}$. On a alors

$$xy = \overline{a}\overline{b} = \overline{ab} = \overline{ba} = yx,$$

l'égalité de la deuxième ligne se déduisant de la commutativité de la multiplication dans $\mathbb{Z}$. L'associativité se déduit de façon analogue de l'associativité de la multiplication de $\mathbb{Z}$. Comme la loi $\cdot$ est commutative, il suffit de vérifier la distributivité à gauche pour avoir également la distributivité à droite. Si x, y et z sont trois éléments de $\mathbb{Z}/n\mathbb{Z}$ et a, b, c trois entiers tels que $x = \overline{a}$, $y = \overline{b}$ et $z = \overline{c}$, on a

$$\begin{aligned} x(y+z) &= \overline{a}(\overline{b} + \overline{c}) = \overline{a}\overline{b+c} \\ &= \overline{a(b+c)} = \overline{ab+ac} \\ &= \overline{ab} + \overline{ac} = \overline{a}\overline{b} + \overline{a}\overline{c} \\ &= xy + xz. \end{aligned}$$

Il reste à vérifier que $\cdot$ possède un élément neutre. L'élément $\overline{1}$ fait parfaitement l'affaire car, pour tout $a \in \mathbb{Z}$, on a $\overline{1}\overline{a} = \overline{1a} = \overline{a}$ et par commutativité, $\overline{a}\overline{1} = \overline{a}$. □

Exemple. Voici par exemple, la table de multiplication dans $\mathbb{Z}/6\mathbb{Z}$:

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Théorème. *Les assertions suivantes sont équivalentes :*

(i) n est premier ;

(ii) l'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre ;

(iii) l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Démonstration. Nous allons démontrer ces équivalences en prouvant que $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$.

Montrons $(i) \Rightarrow (ii)$. Supposons donc que n est un nombre premier. En particulier $n \geqslant 2$, donc $\overline{1} \neq \overline{0}$ et l'anneau a au moins deux éléments. Montrons que si x et y sont deux éléments de $\mathbb{Z}/n\mathbb{Z}$ tels que $xy = \overline{0}$, alors $x = \overline{0}$ et $y = \overline{0}$. Soient a et b deux entiers tels que $x = \overline{a}$ et $y = \overline{b}$. L'égalité $xy = \overline{0}$ se traduit par $\overline{ab} = \overline{a}\overline{b} = \overline{0}$, c'est-à-dire $n \mid ab$. Comme n est un nombre premier, on a $n \mid a$ ou $n \mid b$, c'est-à-dire $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$. Ainsi l'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre et $(ii =$ est vérifié.

Montrons $(ii) \Rightarrow (iii)$. On suppose donc que l'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est donc un anneau intègre et de cardinal fini. On a déjà vu qu'un tel anneau est automatiquement un corps. On a donc (iii).

Montrons $(iii) \Rightarrow (i)$. Supposons que $\mathbb{Z}/n\mathbb{Z}$ est un corps. Remarquons déjà que $\mathbb{Z}/n\mathbb{Z}$ est un corps, il a donc plus de deux éléments, ce qui implique $n \geqslant 2$. Soit $a \in \mathbb{Z}$ un entier tel que $n \nmid a$. Alors $\overline{a} = \overline{0}$. Comme $\mathbb{Z}/n\mathbb{Z}$ est un corps, l'élément $\overline{a}$ est inversible et il existe donc $b \in \mathbb{Z}$ tel que $\overline{a}\overline{b} = \overline{1}$ autrement dit $ab \equiv 1\,[n]$. Il existe donc un entier $k \in \mathbb{Z}$ tel que $ab = 1 + kn$. Il s'agit d'une relation de Bezout entre a et n et donc $a \wedge n = 1$. Si $d \geqslant 1$ est un diviseur de n tel que $d < n$, on a alors $n \mid d$ et d'après ce qui précède, $d \wedge n = 1$. Comme par ailleurs $d \mid n$, on a $d \wedge n = 1$ donc $d = 1$. On en conclut que n est un élément de $\mathbb{N}$ ayant exactement deux diviseurs positifs, c'est donc un nombre premier. □

Exemple. L'anneau $\mathbb{Z}/5\mathbb{Z}$ est un corps. On a en effet $\overline{2}^{-1} = \overline{3}$, $\overline{3}^{-1} = \overline{2}$, $\overline{4}^{-1} = \overline{4}$.

De façon générale, on a une caractérisation des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Théorème. *Soit $n \geqslant 2$ et soit $a \in \mathbb{Z}$. L'élément $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si a et n sont premiers entre eux.*

Démonstration. En effet, on a

$$\begin{aligned}\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times &\Leftrightarrow \exists b \in \mathbb{Z}, \quad \overline{a}\overline{b} = \overline{1} \\ &\Leftrightarrow \exists b \in \mathbb{Z}, \quad \overline{ab} = \overline{1} \\ &\Leftrightarrow \exists b \in \mathbb{Z}, \quad ab \equiv 1\,[n] \\ &\Leftrightarrow \exists (b,k) \in \mathbb{Z}^2, \quad ab + kn = 1\end{aligned}$$

AInsi $\overline{a}$ est inversible si et seulement si a et n sont premiers entre eux. □

Remarque. Déterminer l'inverse de $\overline{a}$ dans $\mathbb{Z}/n\mathbb{Z}$ se fait donc en recherchant une relation de Bezout entre a et n : si b et k sont deux entiers tels que $ab + kn = 1$, on a alors $\overline{a}^{-1} = \overline{b}$.

4.3.2 Le petit théorème de Fermat

Nous allons utiliser la structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$ pour démontrer quelques résultats d'arithmétique.

Théorème. *Soit p un nombre premier et soit $a \in \mathbb{Z}$ un entier non multiple de p. On a alors $a^{p-1} \equiv 1\,[p]$.*

Démonstration. Le nombre p est premier. On sait donc que l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps. Le goupe $((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ est donc un groupe fini de cardinal $p-1$. Comme $p \nmid a$, on a $\overline{a} \neq 0$ et donc, puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps, $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$. Or il découle du corollaire au théorème de Lagrange que l'ordre de tout élément de $(\mathbb{Z}/p\mathbb{Z})^\times$ divise $p-1$. On en déduit que $\overline{a}^{p-1} = \overline{1}$. Cette dernière égalité est bien équivalente à la congruence $a^{p-1} \equiv 1\,[p]$. □

Corollaire. *Si $a \in \mathbb{Z}$ et si p est un nombre premier, on a $a^p \equiv a\,[p]$.*

Démonstration. Si $p \mid a$, la congruence est immédiate car $a \equiv 0\,[p]$. Si $p \nmid a$, le petit théorème de Fermat implique que $a^{p-1} \equiv 1\,[p]$. En multipliant cette congruence par a, on a donc $a^p \equiv a\,[p]$. □

Exemple. Détermions le reste de la division de 5^{400} par 397. Comme 397 est premier, le petit théorème de Fermat implique que $5^{396} \equiv 1\,[397]$. On a donc

$$5^{400} \equiv 5^4 = 625 \equiv 328\,[397].$$

Comme $328 < 397$, le reste recherché est 328.

Remarque. Si p est un nombre premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps ayant exactement p éléments. Les seuls autres exemples de corps vus jusqu'à présent étaient $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. On voit donc qu'il existe également des corps finis. Le corps $\mathbb{Z}/p\mathbb{Z}$ a des propriétés très étranges car, d'après le corollaire au petit théorème de Fermat, on a $x^p = x$ pour tout élément de $\mathbb{Z}/p\mathbb{Z}$. Ces corps finis sont pourtant des objets très important en arithmétique et sont même au cœur de la plupart des procédés de cryptographie actuels.

4.3.3 Le théorème des restes chinois

Dans cette section nous allons comparer différents anneaux $\mathbb{Z}/n\mathbb{Z}$. Nous allons donc utiliser la convention suivante. Si $a \in \mathbb{Z}$, on note $\overline{a}_n$ sa classe dans $\mathbb{Z}/n\mathbb{Z}$. Si $d \geqslant 1$ est un diviseur de n et $\overline{a}_n \in \mathbb{Z}/n\mathbb{Z}$, l'élément $\overline{a}_d \in \mathbb{Z}/d\mathbb{Z}$ ne dépend que de $\overline{a}_n$ et non de a. En effet si a et a' sont deux entiers tels que $\overline{a}_n = \overline{a'}_n$, on a $a \equiv a'$, c'est-à-dire $n \mid (a - a')$ et, puisque $d \mid n$, $d \mid (a - a')$. On en déduit que $\overline{a}_d = \overline{a'}_d$. On a donc défini une application

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/d\mathbb{Z} \\ \overline{a}_n & \longmapsto & \overline{a}_d \end{array}$$

Théorème. *Soient $m \geqslant 1$ et $n \geqslant 1$ deux entiers premiers entre eux. L'application*

$$\varphi : \begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \overline{a}_{mn} & \longmapsto & (\overline{a}_m, \overline{a}_n) \end{array}$$

est un isomorphisme d'anneaux.

Démonstration. Commençons par vérifier que φ est un morphisme d'anneaux. Il faut vérifier que, pour tout a et b dans $\mathbb{Z}$, on a

$$\varphi(\overline{a}_{mn} + \overline{b}_{mn}) = \varphi(\overline{a}_{mn}) + \varphi(\overline{b}_{mn}) \text{ et } \varphi(\overline{a}_{mn}\overline{b}_{mn}) = \varphi(\overline{a}_{mn})\varphi(\overline{b}_{mn}).$$

Vérifions-le pour l'addition, le cas de la multiplication est similaire.

$$\begin{aligned} \varphi(\overline{a}_{mn} + \overline{b}_{mn}) &= \varphi(\overline{a+b}_{mn}) = (\overline{a+b}_m, \overline{a+b}_n) \\ &= (\overline{a}_m + \overline{b}_m, \overline{a}_n + \overline{b}_n) = (\overline{a}_m, \overline{a}_n) + (\overline{b}_m, \overline{b}_n) \\ &= \varphi(\overline{a}_{mn}) + \varphi(\overline{b}_{mn}) \end{aligned}$$

Il faut ensuite montrer que φ est une bijection. Comme les deux ensembles $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ont le même nombre d'éléments : mn, l'application φ est bijective si et seulement si elle est injective. Il suffit donc de prouver qu'elle est injective. Comme φ est en particulier un morphisme de groupes additifs, il suffit de prouver que $\mathrm{Ker}(\varphi)$ est l'ensemble $\{\overline{0}_{mn}\}$. Vérifions-le ! Soit $x \in \mathrm{Ker}(\varphi)$ et soit $a \in \mathbb{Z}$ tel que $x = \overline{a}_{mn}$. On a alors $\varphi(\overline{a}_{mn}) = (\overline{0}_m, \overline{0}_n)$, c'est-à-dire $(\overline{a}_m, \overline{a}_n) = (\overline{0}_m, \overline{0}_n)$. Ainsi $m \mid a$ et $n \mid a$. Comme m et n sont premiers entre eux, on en déduit que $mn \mid a$, c'est-à-dire $x = \overline{a}_{mn} = \overline{0}_{mn}$. On a donc bien montré que $\mathrm{Ker}(\varphi) = \{\overline{0}_{mn}\}$ et donc que φ est injective. Comme expliqué plus haut, ceci implique que φ est bijective et est donc un isomorphisme d'anneaux. □

Remarque. 1) Si $m \wedge n = 1$, on en déduit en particulier que les groupes $(\mathbb{Z}/mn\mathbb{Z}, +)$ et $(\mathbb{Z}/m\mathbb{Z}, +) \times (\mathbb{Z}/n\mathbb{Z}, +)$ sont isomorphes. On en conclut que le produit de deux groupes cycliques de cardinaux premiers entre eux est un groupe cyclique.

2) On peut reformuler la surjectivié de l'application φ de la façon suivante : si $(a, b) \in \mathbb{Z}^2$ et si m et n sont deux entiers naturels premiers entre eux, il existe $c \in \mathbb{Z}$ tel que

$$\begin{cases} c \equiv a\,[m]; \\ c \equiv b\,[n]. \end{cases}$$

De plus, l'entier c est unique modulo mn.

3) Il existe une méthode pour déterminer explicitement un entier c comme ci-dessus. Commençons par rechercher des entiers α et β tels que

$$\begin{cases}\alpha \equiv 1\,[m] \\ \alpha \equiv 0\,[n]\end{cases} \qquad \begin{cases}\beta \equiv 0\,[m] \\ \beta \equiv 1\,[n]\end{cases}$$

On peut alors poser $c = a\alpha + b\beta$ et c convient. Trouver α revient à déterminer un multiple de n congru à 1 modulo m, c'est-à-dire un entier k tel que $kn \equiv 1\,[m]$, ou encore un entier k et un entier ℓ tels que $kn = 1 + \ell m$. Il s'agit donc de déterminer une relation de Bezout, ce que l'on sait faire explicitement en remontant l'algorithme d'Euclide. On peut déterminer un entier β comme ci-dessus de façon analogue en inversant les rôles de m et n.

4.3.4 La fonction indicatrice d'Euler

On définit une fonction $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ en posant $\varphi(1) = 1$ et, si $n \geqslant 2$,

$$\varphi(n) = |\{0 \leqslant k \leqslant n-1 : k \wedge n = 1\}|$$

le nombre d'entiers premiers à n entre 0 et n. Remarquons que, puisque $k \wedge n = (k+n) \wedge n$, $\varphi(n)$ est aussi égal au nombre d'entiers premiers avec n et compris entre a et $a + n - 1$, et ceci quelque soit la valeur de a.

Exemple. On a $\varphi(6) = 2$.

Remarque. 1) Si $n \geqslant 2$, l'entier $\varphi(n)$ est égal au cardinal du groupe fini $(\mathbb{Z}/n\mathbb{Z})^\times$. En effet, on a $k \wedge n = 1$ si et seulement si $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

2) Si p est premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps, on a donc

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{\overline{1}, \ldots, \overline{p-1}\}$$

et donc $\varphi(p) = p - 1$.

Le résultat suivant permet de calculer rapidement $\varphi(n)$.

Théorème. *1) Si m et n sont dans $\mathbb{N}^*$ et vérifient $m \wedge n = 1$, on a $\varphi(mn) = \varphi(m)\varphi(n)$.*

2) Si p est un nombre premier et $\alpha \in \mathbb{N}^*$, on a $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Démonstration. Si m et n sont premiers entre eux, les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes. On en déduit que les groupes $(\mathbb{Z}/mn\mathbb{Z})^\times$ et $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times$ sont isomorphes. Ils ont en particulier le même cardinal. Comme $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$, on en conclut que les groupes $(\mathbb{Z}/mn\mathbb{Z})^\times$ et $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ ont le même cardinal, c'est-à-dire $\varphi(mn) = \varphi(m)\varphi(n)$. Ceci nous donne 1).

Soit maintenant p un nombre premier et $\alpha \geqslant 1$. Un entier $1 \leqslant k \leqslant p^\alpha$ n'est pas premier à p^α si et seulement si il est divisible par p. Il y a exactement $p^{\alpha-1}$ multiples de p compris entre 1 et p^α. On en conclut qu'il y a $p^\alpha - p^{\alpha-1}$ entiers premiers à p^α compris entre 1 et p^α, c'est-à-dire $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. On a démontré le point 2). □

Exemple. On a $63 = 9 \times 7$, donc $\varphi(63) = \varphi(9)\varphi(7) = 6 \times 6 = 36$.

Le résultat suivant est une généralisation du petit théorème de Fermat.

Théorème (Euler)**.** *Soit $n \geqslant 2$ un entier et soit $a \in \mathbb{Z}$ premier avec n. On a alors $a^{\varphi(n)} \equiv 1\,[n]$.*

Démonstration. Comme a est premier avec n, on a $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ et ce groupe est par définition de cardinal $\varphi(n)$. On déduit donc du corollaire au théorème de Lagrange que $\overline{a}^{\varphi(n)} = \overline{1}$ c'est-à-dire $a^{\varphi(n)} \equiv 1\,[n]$. □

Chapitre 5

Polynômes

5.1 L'anneau des polynômes

Soit $(A, +, \times)$ un anneau commutatif. Le but de ce chapitre est de donner un sens puis d'étudier des sommes formelles du type $X^3 - X^2 + aX + b$ où a et b sont des éléments de A. Nous les appellerons des *polynômes*. Commençons par en donner une définition formelle.

On note $A[X]$ l'ensemble des suites $(a_n)_{n\geqslant 0}$ qui sont presque nulles, c'est-à-dire pour lesquelles il existe un entier $N \geqslant 0$ tel que que $a_n = 0$ pour $n \geqslant N$. On définit deux lois de composition internes sur cet ensemble.

— Une addition, définie par

$$(a_n)_{n\geqslant 0} + (b_n)_{n\geqslant 0} = (a_n + b_n)_{n\geqslant 0}.$$

— Une multiplication, définie par

$$(a_n)_{n\geqslant 0} \cdot (b_n)_{n\geqslant 0} = (c_n)_{n\geqslant 0}, \text{ avec } c_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

Remarquons que cette opération est bien définie, c'est-à-dire que la suite $(c_n)_{n\geqslant 0}$ est effectivement presque nulle. Il existe en effet des entiers N_1 et N_2 tels que $a_n = 0$ si $n \geqslant N_1$ et $b_n = 0$ si $n \geqslant N_2$. On en déduit que $a_i b_{n-i} = 0$ si $n \geqslant N_1 + N_2 - 1$ et $0 \leqslant i \leqslant n$, ce qui implique $c_n = 0$ pour $n \geqslant N_1 + N_2 - 1$. La suite $(c_n)_{n\geqslant 0}$ est donc presque nulle.

Proposition. *Le triplet $(A[X], +, \times)$ est un anneau commutatif.*

Démonstration. La loi $+$ est associative et commutative. La suite nulle est un élément neutre pour $+$ et tout élément $(a_n)_{n\geqslant 0}$ a pour inverse $(-a_n)_{n\geqslant 0}$ pour la loi $+$. Ainsi $(A[X], +)$ est un groupe commutatif.

La loi de multiplication est visiblement commutative. Vérifions qu'elle est associative. Pour cela il suffit de vérifier que, pour toutes suites presque nulles $(a_n)_{n\geqslant 0}$, $(b_n)_{n\geqslant 0}$ et $(c_n)_{\geqslant 0}$, on a

$$\sum_{i=0}^{n} a_i \left(\sum_{j=0}^{n-i} b_j c_{n-i-j} \right) = \sum_{i=0}^{n} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) c_{n-i}.$$

Cela se vérifie en développant ces sommes et en remarquant qu'elles sont toutes deux égales à la somme finie

$$\sum_{\substack{i\geqslant 0, j\geqslant 0, k\geqslant 0 \\ i+j+k=n}} a_i b_j c_k.$$

La loi de multiplication est distributive à gauche et à droite par rapport à la loi d'addition. Comme on sait qu'elle est commutative, il suffit de vérifier la distributivité à gauche. Si $(a_n)_{n\geqslant 0}$, $(b_n)_{n\geqslant 0}$ sont trois éléments de $A[X]$, on a bien

$$\sum_{i=0}^{n} a_i (b_{n-i} + c_{n-i}) = \left(\sum_{i=0}^{n} a_i b_{n-i} \right) + \left(\sum_{i=0}^{n} a_i c_{n-i} \right).$$

Enfin la loi $\times$ possède un élément neutre, il s'agit de la suite

$$A_{A[X]} = (1_A, 0_A, \dots, 0_A, \dots).$$

Ainsi le triplet $(A[X], +, \dot{})$ est un anneau. □

Nous allons maintenant changer définitivement de notation pour désigner les éléments de $A[X]$. On pose

$$X = (0_A, 1_A, 0_A, \dots, 0_A, \dots).$$

On vérifie immédiatement que, pour tout $m \geqslant 0$, l'élément $X^m \in A[X]$ est la suite $(a_n)_{n\geqslant 0}$ où $a_m = 1_A$ et $a_n = 0$ si $n \neq m$.

Si $a \in A$, on note simplement a l'élément $(a, 0_A, 0_A, \dots) \in A[X]$. Ainsi la suite $(a_n)_{n\geqslant 0}$ telle que $a_n = a$ si $n = m$ et $a_n = 0_A$ si $n \neq m$ peut encore s'écrire sous la forme $a \cdot X^m$.

On en conclut qu'un élément $(a_n)_{n\geqslant 0}$ de $A[X]$ peut s'écrire sous la forme

$$\sum_{n\geqslant 0} a_n X^n = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n + \cdots$$

cette somme étant finie, car si $a_n = 0_A$, on a $a_n X^n = 0_{A[X]}$.

Un élément de $A[X]$ est appelé un *polynôme* à coefficients dans A et de variable X.

Exemple. Si $A = \mathbb{Z}$, l'élément $2X + X^2$ est un polynôme à coefficients dans $\mathbb{Z}$.

Remarque. 1) L'application de A dans $A[X]$ envoyant a sur l'élément $aX^0 = (a, 0_A, \dots)$ est un morphisme injectif d'anneaux. On utilise ce morphisme pour identifier A a un sous-anneau de $A[X]$. C'est une raison supplémentaire pour noter simplement a l'élément $(a, 0_A, 0_A, \dots)$. Les éléments de ce sous-anneau de $A[X]$ sont appelés *polynômes constants*.

2) Si $P \in A[X]$ est un polynôme, on désignera parfois P par la notation $P(X)$ si on veut mettre en valeur la variable du polynôme.

5.2 Le degré d'un polynôme

Soit $P = \sum_{n \geqslant 0} a_n X^n$ un polynôme. Si $P \neq 0_{A[X]}$, l'ensemble $\{n \in \mathbb{N} : a_n \neq 0_A\}$ est une partie non vide et finie de $\mathbb{N}$. Cette partie possède donc un plus grand élément appelé *degré* de $P(X)$ et noté $\deg(P)$. L'élément $a_{\deg(P)}$ est alors appelé *coefficient dominant* du polynôme P.

Exemple. Si $A = \mathbb{Z}$, le polynôme $P = 2X^3 + 1$ est de degré 3 et de coefficient dominant 2.

Par convention, on pose $\deg(0_{A[X]} = -\infty$. Les polynômes constants sont donc les polynômes de degré 0 ou $-\infty$.

Proposition. *Supposons que l'anneau A est intègre. Si P et Q sont deux éléments de $A[X]$, on a alors*

$$\deg(PQ) = \deg(P) + \deg(Q)$$

(avec la convention que $-\infty + x = -\infty$ pour tout $x \in \mathbb{N} \cup \{-\infty\}$).

Démonstration. Supposons P et Q tous les deux non nuls, la formule étant immédiate dans le cas contraire. Posons $m = \deg(P)$ et $n = \deg(Q)$. On peut donc écrire

$$P = \sum_{i=0}^{m} a_i X^i \text{ et } Q = \sum_{i=0}^{n} b_i X^i.$$

Posons $PQ = \sum_{i \geqslant 0} c_i X^i$ avec, par définition, $c_i = \sum_{j=0}^{i} a_j b_{i-j}$.

Si $i \geqslant m + n + 1$ et $i = j + k$ avec $j, k \geqslant 0$, on a nécessairement $j \geqslant m + 1$ ou $k \geqslant n + 1$, donc $a_j b_{i-j} = 0_A$. Ceci implique que $c_i = 0$ pour $i \geqslant m + n + 1$. On en conclut déjà que $\deg(PQ) \leqslant m + n$.

Si $(j, k) \in \mathbb{N}^2$ vérifie $j + k = m + n$, on a alors $a_j b_k = 0_A$ lorsque $(j, k) \neq (m, n)$. On en conclut que $c_{m+n} = a_m b_n$. Comme l'anneau A est intègre et que $a_m \neq 0_A$ et $b_n \neq 0_A$, on a $a_m b_n \neq 0_A$ et donc $\deg(PQ) = m + n = \deg(P) + \deg(Q)$. □

Remarque. 1) La preuve précédente montre plus précisément que si l'anneau est intègre, le coefficient dominant d'un produit de polynômes non nuls est le produit des coefficients dominants.

2) Le résultat de la proposition est faux si l'anneau A n'est pas supposé intègre. Considérons par exemple le cas où $A = \mathbb{Z}/6\mathbb{Z}$ et

$$P = \overline{2}X + \overline{1}, \quad Q = \overline{3}X^2 + \overline{A}.$$

On a alors $PQ = \overline{6}X^3 + \overline{3}X^2 + \overline{2}X + \overline{1} = \overline{3}X^2 + \overline{2}X + \overline{1}$ et donc $\deg(PQ) = 2 < \deg(P) + \deg(Q)$.

Corollaire. *Si l'anneau A est intègre, l'anneau $A[X]$ est intègre.*

Démonstration. En effet supposons que P et Q sont deux éléments non nuls de $A[X]$. Alors la proposition montre que $\deg(PQ) \neq -\infty$, donc que $PQ \neq 0_{A[X]}$. □

Corollaire. *Si A est un anneau intègre, les éléments inversibles de $A[X]$ sont les polynômes constants de la forme aX^0 où a est inversible dans A.*

Démonstration. Soit $P \in A[X]^\times$. Il existe alors un polynôme $Q \in A[X]$ tel que $PQ = 1_{A[X]} = 1_A X^0$. On a donc $\deg(P) + \deg(Q) = 0$, ce qui implique $\deg(P) = \deg(Q) = 0$. Il existe donc a et b dans A tels que $P = aX^0$ et $Q = bX^0$ tels que $ab = 1_A$. On en conclut que $a \in A^\times$.

Réciproquement, si $a \in A^\times$ le polynôme aX^0 est inversible d'inverse $a^{-1}X^0 \in A[X]$. □

Corollaire. *Si K est un corps, les éléments inversibles de $K[X]$ sont exactement les polynômes constants non nuls.*

Démonstration. C'est une conséquence immédiate du corollaire précédent en tenant compte du fait que les éléments inversibles de K sont exactement les éléments non nuls de K. □

Nous allons désormais essentiellement considérer des polynômes à coefficients dans des corps.

5.3 Division euclidienne dans $K[X]$

Soit K un corps commutatif.

5.3.1 Division dans $K[X]$

Si A et B sont deux éléments de $K[X]$, on dit que B *divise* A et on note $B \mid A$ s'il existe un élément $C \in K[X]$ tel que $A = BC$. Dans ce cas on dit aussi que B est un *diviseur* de A ou encore que A est un *multiple* de B.

Exemple. Dans l'anneau $\mathbb{R}[X]$, le polynôme $X+1$ divise X^2-1 car on peut écrire

$$X^2-1=(X-1)(X+1).$$

Par contre le polynôme X ne divise pas $X+1$, on ne peut pas trouver de polynôme C tel que $X+1=XC$.

Remarque. En fait la notion de division ne fait appel à aucune propriété particulière de l'anneau $K[X]$. On pourrait, de façon plus générale, définir la notion de divisibilité dans tout anneau commutatif. Dans un anneau non commutatif, il faudrait distinguer la notion de divisibilité à droite et de divisibilité à gauche.

5.3.2 La division euclidienne

Comme dans $\mathbb{Z}$, si on ne peut pas toujours diviser par un polynôme non nul dans $K[X]$, on peut néanmoins faire une division euclidienne.

Théorème. *Soient P et D deux éléments de $K[X]$ tels que $D\neq 0_{K[X]}$. Il existe alors un unique couple $(Q,R)\in K[X]^2$ tel que $P=QD+R$ et $\deg(R)<\deg(D)$.*

L'élément Q est appelé le *quotient* de la division euclidienne de P par D et R le *reste*.

Démonstration. Commençons par prouver l'existence de (Q,R). Remarquons déjà que si $\deg(P)<\deg(D)$, alors on peut prendre $Q=0_{K[X]}$ et $R=P$.

Raisonnons alors par récurrence généralisée sur le degré de P. Si $\deg(P)=-\infty$, on est dans le cas où $\deg(P)<\deg(D)$ qui a déjà été traité.

Supposons donc l'existence de la division euclidienne de P par D prouvée pour tout polynôme P de degré $\leqslant N$. Soit P un polynôme de degré $N+1$. Le cas où $\deg(P)<\deg(D)$ a déjà été vu, on peut donc supposer de plus que $\deg(P)\geqslant\deg(D)$. Notons $n=\deg(D)$, p_{N+1} le coefficient dominant de P et d_n le coefficient dominant de D. Comme $d_n\in K\setminus\{0\}$, l'élément d_n est inversible dans K et on peut donc poser

$$P_1=P-p_{N+1}d_n^{-1}X^{N+1-n}D.$$

Le polynôme $p_{N+1}d_n^{-1}X^{N+1-n}D$ est de degré $N+1$ et de coefficient dominant p_{N+1}, on en conclut que P et $p_{N+1}d_n^{-1}X^{N+1-n}D$ ont même degré $N+1$ et mêmes coefficients dominants, donc que leur différence P_1 est de degré $\leqslant N$. Par récurrence, il existe $(Q_1,R_1)\in K[X]^2$ tel que $P_1=Q_1D+R_1$ et $\deg(R_1)<\deg(D)$. On peut donc écrire

$$P=P_1+p_{N+1}d_n^{-1}X^{N+1-n}D=Q_1D+R_1+p_{N+1}d_n^{-1}X^{N+1-n}D=(Q_1+p_{N+1}d_n^{-1}X^{N+1-n})D+R_1.$$

On peut donc prendre $Q=Q_1+p_{N+1}d_n^{-1}X^{N+1-n}$ et $R=R_1$.

Montrons à présent l'unicité de la division euclidienne. Supposons qu'il existe des couples (Q_1,R_1) et (Q_2,R_2) tels que

$$P=Q_1D+R_1=Q_2D+R_2$$

et $\deg(R_1), \deg(R_2) < \deg(D)$. On a alors

$$R_1 - R_2 = (Q_2 - Q_1)D.$$

Supposons par l'absurde que $Q_2 - Q_1 \neq 0$. On a alors

$$\deg(R_1 - R_2) = \deg(D) + \deg(Q_2 - Q_1) \geqslant \deg(R_1 - R_2).$$

Comme par ailleurs $\deg(R_1 - R_2) < \deg(D)$, on aboutit à une contradiction. On en conclut que $Q_2 = Q_1$ et donc que $R_1 = R_2$. □

Remarque. Pour effectuer une division euclidienne dans $K[X]$, on peut la poser comme dans $\mathbb{Z}$. Donnons l'exemple en effectuant la division euclidienne de X^3+1 par X^2+X+1 dans $\mathbb{R}[X]$.

$$\begin{array}{c|c} X^3+1 & X^2+X+1 \\ \cline{2-2} -X(X^2+X+1) & X-1 \\ = -X^2-X+1 & \\ -(-X^2-X-1) & \\ = 2 & \end{array}$$

Ainsi $X^3 + 1 = (X - 1)(X^2 + X + 1) + 2$.

5.3.3 Idéaux de $K[X]$

On rappelle qu'un idéal de $K[X]$ est une partie $I \subset K[X]$ telle que $(I, +)$ est un sous-groupe de $(K[X], +)$ et telle que, pour tout $A \in I$ et $B \in K[X]$, $AB \in I$.

Exemple. Si $D \in K[X]$, on note $DK[X]$ l'ensemble des multiples de D, c'est-à-dire

$$DK[X] = \{DA : A \in K[X]\}.$$

Un tel idéal est appelé un *idéal principal* de $K[X]$.

Remarquons que $D \mid P$ si et seulement si $P \in DK[X]$, ainsi $DK[X]$ est l'ensemble des multiples de D.

Remarque. La notion de divisibilité dans $K[X]$ peut encore se reformuler en termes d'idéaux. Si A et B sont dans $K[X]$, on a $B \mid A$ si et seulement si $AK[X] \subset BK[X]$. En effet, on a

$$B \mid A \Leftrightarrow A \in BK[X] \Leftrightarrow AK[X] \subset BK[X].$$

Théorème. *Soit I un idéal de $K[X]$. Alors I est un idéal principal. Autrement dit il existe $D \in K[X]$ tel que $I = DK[X]$.*

Démonstration. Si $I = \{0\}$, alors $I = 0_{K[X]}K[X]$. Supposons donc $I \neq \{0\}$. On peut donc choisir $D \in I \setminus \{0_{K[X]}\}$ de degré minimal. Montrons alors que $I = DK[X]$.

Comme $D \in I$ et que I est un idéal, on a $DK[X] \subset I$. Montrons l'inclusion réciproque. Soit $P \in I$. Effectuons la division euclidienne de P par D. On a $P = QD + R$ avec $\deg(R) < \deg(R)$. Mais alors $P \in I$ et, puisque I est un idéal, $QD \in I$. On en conclut que $R \in I$. Comme $\deg(R) < \deg(D)$ et que D est de degré minimal parmi les polynômes non nuls de I, on a nécessairement $R = 0$ et donc $P = QD \in I$. Ainsi $I \subset DK[X]$ et finalement $I = DK[X]$. □

Soient A et B deux polynômes non nuls de $K[X]$. On dit que A et B sont associés s'il existe un élément $\lambda \in K^\times$ tel que $B = \lambda A$.

Remarque. 1) La relation « A est associé à B » est une relation d'équivalence sur l'ensemble $K[X] \setminus \{0_{K[X]}\}$.

2) Deux polynômes A et B sont associés si et seulement si $A \mid B$ et $B \mid A$.

3) Tout polynôme $P \in K[X] \setminus \{0_{K[X]}\}$ est associé à un unique polynôme unitaire, c'est-à-dire un polynôme de coefficient dominant égal à 1_K. En effet si λ est le coefficient dominant de P, alors $\lambda^{-1}P$ est unitaire. L'unicité provient du fait que si A et B sont associés et unitaire, on peut écrire $B = \lambda A$, mais en comparant les coefficients dominants, on trouve $\lambda = 1_K$ et donc $B = A$.

4) Deux polynômes A et B sont associés si et seulement si $AK[X] = BK[X]$.

Corollaire. *Soit I un idéal de $K[X]$ différent de $\{0\}$. Il existe alors un unique polynôme unitaire D tel que $I = DK[X]$.*

5.3.4 PGCD de deux polynômes

Nous allons maintenant appliquer les résultats précédents à l'étude du PGCD dans $K[X]$.

Soient A et B deux polynômes de $K[X]$ tels que $(A, B) \neq (0_{K[X]}, 0_{K[X]})$. On peut considérer l'ensemble

$$I = AK[X] + BK[X] = \{AP + BQ : (P, Q) \in K[X]^2\}.$$

On vérifie facilement que c'est un idéal de $K[X]$. De plus, puisque $(A, B) \neq (0_{K[X]}, 0_{K[X]})$, on a $I \neq \{0_{K[X]}\}$ et il existe un unique polynôme unitaire D tel que

$$AK[X] + BK[X] = DK[X].$$

Le polynôme D est alors appelé PGCD de A et B et noté $A \wedge B$.

Proposition. *Soit $C \in K[X]$. On a $C \mid A$ et $C \mid B$ si et seulement si $C \mid A \wedge B$.*

Démonstration. En effet si $C \mid A$, on a $AK[X] \subset CK[X]$. De même $C \mid B$ implique $BK[X] \subset CK[X]$. Ainsi, si $C \mid A$ et $C \mid B$, on a $AK[X] + BK[X] \subset CK[X]$ et donc $(A \wedge B)K[X] \subset CK[X]$, c'est-à-dire $C \mid (A \wedge B)$. Réciproquement, puisque $AK[X] +$

$BK[X] = (A \wedge B)K[X]$, on a $A \in (A \wedge B)K[X]$ et $B \in (A \wedge B)K[X]$, donc $A \wedge B \mid A$ et $A \wedge B \mid B$. On en conclut que tout diviseur de $A \wedge B$ est un diviseur commun à A et B. □

Remarque. De même que dans $\mathbb{Z}$, on peut utiliser l'algorithme d'Euclide dans $K[X]$ pour calculer explicitement le PGCD de deux polynômes.

Définition. *Soient A et B deux polynômes de $K[X]$ tels que $(A, B) \neq (0, 0)$. On dit que A et B sont* premiers entre eux *si $A \wedge B = 1_{K[X]}$.*

On voit que

$$A \wedge B = 1 \Leftrightarrow 1 \in AK[X] + BK[X] \Leftrightarrow AK[X] + BK[X] = K[X]$$

ainsi $A \wedge B = 1$ si et seulement si il existe des polynômes U et V de $K[X]$ tels que $AU + BV = 1$. Une paire (U, V) vérifiant cette propriété est appelée *relation de Bezout*. Pour déterminer une relation de Bezout dans $K[X]$, la méthode est exactement la même que dans $\mathbb{Z}$, au moyen de l'algorithme d'Euclide et de la division euclidienne.

Proposition (Lemme de Gauss)**.** *Soient A, B, C des éléments de $K[X]$ tels que $A \neq 0$, $A \mid BC$ et $A \wedge B = 1$. On a alors $A \mid C$.*

Démonstration. Comme $A \wedge B = 1$, il existe U et V dans $K[X]$ tels que $AU + BV = 1$. On en déduit qu $C = ACU + BCV$. Comme A divise AC et BC, on en conclut que $A \mid C$. □

Corollaire. *Soient A, B, C trois éléments de $K[X]$ tels que A et B sont non nuls, $A \wedge B = 1$, $A \mid C$ et $B \mid C$. Alors $AB \mid C$.*

Démonstration. Comme $A \mid C$, on a $C = AU$ avec $U \in K[X]$. Ainsi $B \mid AU$. Comme $A \wedge B = 1$, le lemme de Gauss implique que $B \mid U$ et donc $AB \mid AU = C$. □

5.3.5 Polynômes irréductibles

Soit $P \in K[X]$. On dit que P est *irréductible* dans $K[X]$ si P est non constant et si les seuls diviseurs de P sont les polynômes constants non nuls et les polynômes associés à P.

Remarque. La notion de polynôme irréductible dans $K[X]$ est l'analogue de la notion de nombre premier dans $\mathbb{Z}$.

Exemple. 1) Les polynômes de degré 1 sont toujours irréductibles. En effet, si $\deg(P) = 1$ et si $Q \mid P$, on a $\deg(Q) = 0$ et Q est constant non nul ou $\deg(Q) = 1$. Dans ce cas on peut écrire $P = QR$ avec $\deg(R) = 0$ de sorte que R est constant non nul et donc que Q est associé à P.

2) Le polynôme X^2+1 est irréductible dans $\mathbb{R}[X]$. En effet si Q est un diviseur de X^2+1 qui n'est de degré ni 0 ni 2, alors $\deg(Q)=1$. On peut donc écrire $P=(X-a)(X-b)$ avec a et b dans $\mathbb{R}$. En développant cette égalité, on a $a+b=0$ et $ab=1$. Ceci implique $a\in\{i,-i\}$, ce qui est absurde.

3) Dans $\mathbb{C}[X]$, on a $X^2+1=(X-i)(X+i)$. Le polynôme X^2+1 n'est donc pas irréductible dans $\mathbb{C}[X]$: il est divisible par $X-i$ qui n'est pas constant ni associé à X^2+1.

Proposition. *Soit $P\in K[X]$ un polynôme irréductible.*

(i) Si $A\in K[X]$ et $P\nmid A$, on a $A\wedge P=1$.

(ii) Si $A,B\in K[X]$ et $P\mid AB$, alors $P\mid A$ ou $P\mid B$.

Démonstration. Le PGCD $A\wedge P$ est un diviseur de P. Si $P\nmid A$, alors $A\wedge P$ n'est pas associé à P et donc que $A\wedge P$ est une constante non nulle. Comme $A\wedge P$ est par ailleurs unitaire, on a $A\wedge P=1$.

Si $P\mid AB$ et si $P\nmid A$, alors $A\wedge P=1$ et, d'après le lemme de Gauss, $P\mid B$. □

5.3.6 Factorisation en produit d'irréductibles

Théorème. *Tout polynôme non constant de $K[X]$ se décompose de façon unique, à l'ordre près, sous la forme $\lambda\prod_{i=1}^r P_i^{\alpha_i}$ où $\lambda\in K^\times$, les P_i sont des polynômes irréductibles distincts et les α_i des éléments de $\mathbb{N}^*$.*

5.4 Racines d'un polynôme

Soit K un corps.

5.4.1 Fonction polynomiale

Soit $P=\sum_{i=0}^r a_iX^i\in K[X]$. On appelle *fonction polynomiale* associée à P la fonction

$$\widetilde{P}:\begin{array}{ccc}K&\longrightarrow&K\\ x&\longmapsto&\sum_{i=0}^r a_ix^i.\end{array}$$

Ainsi, si $P\in K[X]$ et $x\in K$, $\widetilde{P}(x)$ est un élément de K.

Proposition. *Si $P,Q\in K[X]$, on a*

$$\forall x\in K,\quad \widetilde{P+Q}(x)=\widetilde{P}(x)+\widetilde{Q}(x)$$
$$\widetilde{PQ}(x)=\widetilde{P}(x)\widetilde{Q}(x).$$

Démonstration. Nous prouvons uniquement la deuxième inégalité, la première étant plus simple. On écrit $P = \sum_{i=0}^{m} a_i X^i$ et $Q = \sum_{j=0}^{n} b_j X^j$. Si $x \in K$, on a

$$\begin{aligned}\widetilde{P}(x)\widetilde{Q}(x) &= \left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{j=0}^{n} b_j X^j\right) = \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j x^{i+j} \\ &= \sum_{k=0}^{m+n}\left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k = \widetilde{PQ}(x).\end{aligned}$$

□

Remarque. Si le corps K est fini, il est possible que $\widetilde{P} = \widetilde{Q}$ alors que $P \neq Q$. Considérons par exemple $K = \mathbb{Z}/p\mathbb{Z}$ avec p un nombre premier et $P = X$, $Q = X^p$. On a alors, par le petit théorème de Fermat,

$$\forall x \in \mathbb{Z}/p\mathbb{Z}, \quad \widetilde{Q}(x) = x^p = x\widetilde{P}(x).$$

La notation $\widetilde{P}$ est utile pour bien différencier la fonction polynomiale $\widetilde{P}$ du polynôme P. Elle est cependant un peu lourde. On notera donc désormais $P(x) = \widetilde{P}(x)$ pour $x \in K$.

5.4.2 Racines

Soit $P \in K[X]$ et $x \in K$. On dit que x est une *racine* de P si $P(x) = 0_K$.

Exemple. L'élément a est une racine du polynôme $X - a$. Dans $\mathbb{C}$, i est une racine du polynôme $X^2 + 1$.

Proposition. *Soit $x \in K$ et $P \in K[X]$. Alors x est une racine de P si et seulement si $(X - x) \mid P$ dans $K[X]$.*

Démonstration. On effectue la division euclidienne de P par $X - x$. On a donc $P = (X - x)Q + R$ avec $\deg(R) < \deg(X - x) = 1$. Ainsi R est un polynôme constant. Comme $P(x) = R(x)$, le polynôme R est constant de valeur $P(x)$. Alors $(X - x)$ divise P si et seulement si $R = 0$n c'est-à-dire si et seulement si $P(x) = 0_K$. □

Théorème. *Soit $P \in K[X]$ un polynôme non constant de degré n. Alors le nombre de racines de P est $\leqslant n$.*

Démonstration. On montre le résultat par récurrence sur $n \geqslant 1$. Si $n = 1$, P est de la forme $aX + b$ avec $a \neq 0_K$. Alors P a une unique racine, donnée par $-\frac{b}{a}$. Supposons le résulat démontré pour une valeur n. Soit P un polynôme de degré $n + 1$. Si P n'a pas de racine dans K, le résultat est vrai. Si P a une racine $x \in K$, alors $(X - x)$ divise P et on peut écrire $P = (X - x)Q$. Le polynôme Q est alors de degré n et, pour $y \in K$, on a

$$P(y) = 0_K \Leftrightarrow (y - x)Q(y) = 0_K \Leftrightarrow y - x = 0_K \text{ ou } Q(y) = 0_K$$

(noter que l'on a utilisé ici l'intégrité de K). Ainsi l'ensemble des racines de P est inclus dans l'union de l'ensemble des racines de Q et de $\{x\}$. Par récurrence, l'ensemble des racines de Q est de cardinal $\leqslant n$ donc l'ensemble des racines de P est de cardinal $\leqslant n+1$. □

Corollaire. *Soient P et Q dans $K[X]$ de degrés $\leqslant n$. S'il existe $n+1$ éléments $x_1, \ldots, x_{n+1} \in K$ tels que $P(x) = Q(x)$, alors $P = Q$.*

Démonstration. Comme P et Q sont de degrés $\leqslant n$, on a $\deg(P-Q) \leqslant n$. Le polynôme $P-Q$ est donc de degré $\leqslant n$ et possède au moins $n+1$ racines dans P. Il est donc de degré $\leqslant 0$, c'est-à-dire constant. Comme il s'annule en au moins un élément de K, c'est le polynôme nul, c'est-à-dire $P = Q$. □

Corollaire. *Si K est infini et si $\widetilde{P} = \widetilde{Q}$, alors $P = Q$.*

Démonstration. Soit $n \geqslant \max(\deg(P), \deg(Q))$. Comme K est infini, il existe au moins $n+1$ éléments distincts $x_1, \ldots, x_{n+1}$dans K. Comme $\widetilde{P} = \widetilde{Q}$, on a $P(x_i) = Q(x_i)$ pour $1 \leqslant i \leqslant n+1$ et donc $P = Q$. □

5.5 Polynômes irréductibles de $\mathbb{R}[X]$, $\mathbb{C}[X]$, corps algébriquement clos

5.5.1 Corps algébriquement clos

Commençons par quelques remarques générales sur les polynômes irréductibles.

1) Un polynôme de degré 1 est toujours irréductible.

2) Un polynôme irréductible P ayant une racine est de degré 1. En effet, si x est une racine de P, on a $(X-x) \mid P$. Comme $(X-x)$ n'est pas constant et P est irréductible, $(X-x)$ est associé à P et $\deg(P) = \deg(X-x) = 1$.

3) Si $\deg(P) = 2$, alors P est irréductible si et seulement si P n'a pas de racine dans K. En effet, d'après le point précédent, on sait que si P est irréductible, alors P n'a pas de racine dans K (puisque $\deg(P) > 1$). Réciproquement si P est réductible, il est divisible par Q avec $0 < \deg(Q) < 2$, donc $\deg(Q) = 1$. Mais alors $Q = aX + b$ avec $a \neq 0$ et donc $-\frac{b}{a}$ est racine de Q donc de P.

Proposition. *Les deux assertions suivantes sont équivalentes !*

(i) tout polynôme non constant admet une racine dans K ;

(ii) les polynômes irréductibles de $K[X]$ sont exactement les polynômes de degré 1.

Démonstration. Montrons que $(i) \Rightarrow (ii)$. Supposons donc (i). Soit P un polynôme irréductible de $K[X]$. D'après (i), le polynôme P possède une racine $x \in K$. On a déjà vu que ceci implique $\deg(P) = 1$ et donc (ii).

Réciproquement supposons (ii). Si P est un polynôme non constant, alors P est divisible par un polynôme irréductible Q. D'après (ii), on a $\deg(Q) = 1$. Le polynôme Q étant de la forme $aX + b$ possède un racine dans K, donc P également. Ceci prouve (i). □

Définition. *On dit qu'un corps est* algébriquement clos *s'il vérifie l'une des deux propriétés ci-dessus (et donc automatiquement l'autre). Autrement dit, un corps K est algébriquement clos si et seulement si tout polynôme non constant $P \in K[X]$ possède au moins une racine dans K.*

Dans ce cours, on ne verra qu'un seul exemple de corps algébriquement clos.

Nous admettons le résultat suivant.

Théorème (d'Alembert-Gauss)**.** *Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.*

Corollaire. *Tout polyôme $P \in \mathbb{C}[X]$ non constant s'écrit de façon unique sous la forme*

$$P = \lambda \prod_{i=1}^{r} (X - x_i)^{\alpha_i}$$

où $\lambda \in K^\times$, $x_1, \dots, x_r$ sont des nombres complexes distincts et les α_i des éléments de $\mathbb{N}^*$.

Exemple.

$$X^n - 1 = \prod_{k=0}^{n-1} (X - e^{\frac{2\pi i k}{n}})$$

5.5.2 Irréductibles de $\mathbb{R}[X]$

Soit $P \in \mathbb{R}[X]$ de degré $\geqslant 1$. Soit $z \in \mathbb{C}$ une racine de P dans $\mathbb{C}$, qui existe puisque $\mathbb{C}$ est algébriquement clos. Alors $\overline{z}$ est aussi une racine de P. En effet, on peut écrire $P = \sum_{i=0}^{n} a_i X^i$ avec $a_i \in \mathbb{R}$. On a donc

$$\begin{aligned} P(\overline{z}) &= \sum_{i=0}^{n} a_i \overline{z}^i = \sum_{i=0}^{n} \overline{a_i z^i} \\ &= \overline{\sum_{i=0}^{n} a_i z^i} = \overline{P(z)} = \overline{0} = 0. \end{aligned}$$

En conséquence, soit $z \in \mathbb{R}$ et $(X - z) \mid P$ dans $\mathbb{R}[X]$, soit $z \in \mathbb{C} \smallsetminus \mathbb{R}$ et $z \neq \overline{z}$ de sorte que $(X - z) \wedge (X - \overline{z}) = 1$. Ainsi $(X - z)(X - \overline{z}) \mid P$ dans $\mathbb{C}[X]$.

Lemme. *Si P et Q sont dans $\mathbb{R}[X]$ et si $Q \mid P$ dans $\mathbb{C}[X]$, alors $Q \mid P$ dans $\mathbb{R}[X]$.*

Démonstration. Effectuons la division euclidienne de P par Q dans $\mathbb{R}[X]$. On a donc $P = QQ' + R$ avec $\deg(R) < \deg(R)$. L'unicité de la division euclidienne montre que cette décomposition est également la division euclidienne de P par Q dans $\mathbb{C}[X]$. Ainsi, puisque $Q \mid P$, on a $R = 0$. Ainsi $Q \mid P$ dans $\mathbb{R}[X]$. □

Théorème. *Les polynômes irréductibles de $\mathbb{R}[X]$ sont exactement les polynômes suivants :*

1) *les polynômes de degré 1 ;*
2) *les polynômes de degré 2 sans racine dans $\mathbb{R}$.*

Démonstration. Nous avons déjà vu que tous ces polynômes sont irréductibles. Montrons que ce sont les seuls. Soit $P \in \mathbb{R}[X]$ un polynôme irréductible de $\mathbb{R}[X]$. Si P a une racine dans $\mathbb{R}$, alors, puisque P est irréductible, le polynôme P est de degré 1 et appartient à la première famille. Si P n'a pas de racine dans $\mathbb{R}$, il suit de la discussion précédant le théorème qu'il existe $z \in \mathbb{C} \smallsetminus \mathbb{R}$ tel que $(X - z)(X - \overline{z})$ divise P dans $\mathbb{C}[X]$. Mais alors $(X - z)(X - \overline{z}) = X^2 - (z + \overline{z})X + |z|^2$. Comme $z + \overline{z} = 2\,\mathrm{Re}(z) \in \mathbb{R}$ et $|z|^2 \in \mathbb{R}$, le polynôme $Q = X^2 - (z + \overline{z})X + |z|^2$ est dans $\mathbb{R}[X]$ et il suit du lemme ci-dessus que $Q \mid P$ dans $\mathbb{R}[X]$. Comme Q n'est pas constat et P est irréductible, le polynôme Q est associé à P et donc $\deg(P) = \deg(Q) = 2$. Ainsi P est dans la seconde famille. □

Remarque. Le polynôme $X^2 + bX + c \in \mathbb{R}[X]$ n'a pas de racine réelle si et seulement si $b^2 - 4c < 0$.

Corollaire. *Soit $P \in \mathbb{R}[X]$ non constant. La décomposition de P en produit d'irréductibles a la forme suivante*

$$P = \lambda \prod_{i=1}^{r} (X - a_i)^{\alpha_i} \prod_{j=1}^{s} (X^2 + b_j X + c_j)^{\beta_j}$$

où $\lambda \in \mathbb{R}^\times$, les a_i sont des réels distincts, les (b_j, c_j) sont des couples de réels distincts tels que $b_j^2 - 4c_j < 0$, et les α_j, β_j des entiers $\geqslant 1$.

5.5.3 Un exemple dans $\mathbb{Q}[X]$

Les polynômes irréductibles de $\mathbb{Q}[X]$ sont beaucoup plus difficiles à classifier. Voici un exemple montrant qu'il existe des polynômes de tous degrés dans $\mathbb{Q}[X]$.

Proposition. *Si $n \in \mathbb{N}^*$, le polynôme $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$.*

Démonstration. Supposons que $X^n - 2$ possède un diviseur unitaire $P \in \mathbb{Q}[X]$ tel que $1 \leqslant d = \deg(P) \leqslant n - 1$. Comme $X^n - 2 = \prod_{\zeta \in \mathbb{U}_n} (X - 2^{1/n}\zeta)$ dans $\mathbb{C}[X]$, il existe $\zeta_1, \ldots, \zeta_d$ dans $\mathbb{U}_n$ tels que $P = \prod_{i=1}^{d} (X - 2^{1/n}\zeta_i)$ dans $\mathbb{C}[X]$. Le terme de degré 0 de P est alors

$$P(0) = (-1)^d 2^{d/n} \prod_{i=1}^{d} \zeta_i$$

et ce terme est un élément de $\mathbb{Q}$. En prenant sa valeur absolue, on en conclut que $2^{d/n} \in \mathbb{Q}$. Montrons que ce n'est pas possible. En effet, il existe alors deux entiers $a \wedge b = 1$ tels que $2^{d/n} = \frac{a}{b}$, et donc $a = 2^{d/n} b$, ce qui implique $a^n = 2^d b^n$. Comme $d \geqslant 1$, on a $2 \mid a$. Comme $a \wedge b = 1$, on a donc $2 \nmid b$. On a donc $2^n \mid a^n \mid 2^d b^n$ et, puisque $2 \wedge b = 1$, $2^n \mid 2^d$. C'est absurde puisque $d < n$.

Ainsi il n'existe pas de $P \in \mathbb{Q}[X]$ divisant $X^n - 2$ et de degré $1 \leqslant d \leqslant n-1$, le polynôme $X^n - 2$ est donc irréductible dans $\mathbb{Q}[X]$. □

5.6 Dérivarions

Soit K un corps.

5.6.1 Définitions

Soit $P = \sum_{i=0}^{n} a_i X^i \in K[X]$. On appelle *polynôme dérivé de P* le polynôme

$$P' = \sum_{i=0}^{n-1} (i+1) a_{i+1} X^i = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \cdots + a_1.$$

Remarque. Si $K = \mathbb{R}$, la fonction $\widetilde{P} : \mathbb{R} \to \mathbb{R}$ est dérivable de dérivée $\widetilde{P'}$. Le nom de l'opération ainsi définie est donc bien justifié.

On définit alors par récurrence le polynôme $P^{(n)}$ pour tout $n \geqslant 1$ en posant $P^{(1)} = P'$ et $P^{(n+1)} = (P^{(n)})'$.

Proposition. *Si P et Q sont deux éléments de $K[X]$, on a les propriétés suivantes :*
- $(P+Q)' = P' + Q'$;
- *pour $\lambda \in K$, on a* $(\lambda P)' = \lambda P'$;
- $(PQ)' = P'Q + PQ'$;
- *pour $n \geqslant 1$,* $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$.

Démonstration. C'est un calcul immédiat. La dernière formule se démontre par récurrence sur n. □

Proposition. *Si $P \in K[X]$, on a* $\deg(P') \leqslant \deg(P) - 1$. *Si le corps K est $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, on a même* $\deg(P') = \deg(P) - 1$ *dès que P est non constant.*

Démonstration. Si P est de degré n, alors par définition P' est de degré $n-1$. Supposons maintenant que P est degré $n \geqslant 1$ et que K est $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. Alors $P' = n a_n X^{n-1} + Q$ où Q est un polynôme de degré inférieur ou égal à $n-2$. On en conclut que, si $n a_n \neq 0$, le terme dominant de P' est $n a_n$ et que P' est de degré $n-1$. Comme P est de degré n, on a $a_n \neq 0$ et $n a_n = \underbrace{a_n + \cdots + a_n}_{n} \neq 0$ dans $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. □

Remarque. L'hypothèse $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ est importante. Considérons par exemple p un nombre premier et $P = X^p + X$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. Alors $P' = pX^{p-1} + 1 = 1$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. On a donc

$$\deg(P') = 0 < \deg(P) - 1 = p - 1.$$

5.6.2 Formule de Taylor

On suppose dans cette partie que K est $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

Théorème. *Soit $P \in K[X]$ et soit $x_0 \in K$. Alors, si $\deg(P) = n$, on a*

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!}(X - x_0)^k.$$

Démonstration. Commençons par démontrer le cas où $x_0 = 0$. Posons $P = \sum_{i=0}^{n} a_i X^i$. Il suffit de prouver que $P^{(k)}(0) = k!a_k$. Cela se vérifie en prouvant par récurrence que $(X^m)^{(k)} = 0$ si $k > m$ et $(X^m)^{(m)} = m(m-1)\cdots(m-k+1)X^{m-k}$ si $k \leqslant m$.

Pour traiter le cas général, on pose $Q = P(X + x_0)$. On vérifie alors que $Q' = P'(X + x_0)$ et, pour tout $n \geqslant 1$, $Q^{(n)} = P^{(n)}(X + x_0)$. Ainsi, d'après le cas $x_0 = 0$, on a

$$Q = \sum_{k=0}^{n} \frac{P^{(k)}(x_0)}{k!} X^k$$

et donc

$$P = Q(X - x_0) = \sum_{k=0}^{n} \frac{P^{(k)}(x_0)}{k!}(X - x_0)^k.$$

□

5.6.3 Multiplicité d'une racine

Soit $P \in K[X]$ non nul et soit $x_0 \in K$ une racine de P. On appelle *multiplicité de x_0* l'entier

$$m_{x_0}(P) = \max\{k \geqslant 1 : (X - x_0)^k \mid P\}.$$

On appelle *racine simple* de P une racine de P qui est de multiplicité 1.

Proposition. *Supposons que le corps K est $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. On a alors*

$$(X - x_0)^k \mid P \Leftrightarrow P(x_0) = P'(x_0) = \cdots = P^{(k-1)}(x_0) = 0.$$

Démonstration. Remarquons que la formule de Taylor nous dit que le reste de la division euclidienne de P par $(X - x_0)^k$ est le polynôme

$$\sum_{i=0}^{k-1} \frac{P^{(i)}(x_0)}{i!}(X - x_0)^i.$$

Ce reste est nul si et seulement si $P^{(i)}(x_0) = 0$ pour $0 \leqslant i \leqslant k-1$. □

On en déduit qu'une racine x_0 de P est une racine simple si et seulement si $P'(x_0) \neq 0$.

Chapitre 6

Fractions rationnelles

Dans tout ce chapitre, K désigne un corps commutatif.

6.1 Le corps des fractions d'un anneau commutatif et intègre

Soit A un anneau commutatif et intègre. On définit une relation binaire sur $A \times A \setminus \{0_A\}$ en posant

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc.$$

Vérifions qu'il s'agit d'une relation d'équivalence :

- elle est réflexive car $(a,b) \sim (a,b)$ pour tout $(a,b) \in A \times A \setminus \{0_A\}$ puisque $ab = ba$ (l'anneau est commutatif) ;
- elle est symétrique car

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc \Leftrightarrow cb = da \Leftrightarrow (c,d) \sim (a,b).$$

- elle est transitive, si $(a,b) \sim (c,d)$ et $(c,d) \sim (e,f)$, on $ad = bc$ et $cf = de$. On en déduit $adf = bcf = bde$, donc $afd = bed$. Comme $d \neq 0_A$ et A est intègre, on en déduit $af = be$, c'est-à-dire $(a,b) \sim (e,f)$.

On note alors $\mathrm{Frac}(A)$ l'ensemble des classes d'équivalence de $A \times A \setminus \{0_A\}$. Pour des raisons qui vont très vite devenir claires, on note $\frac{a}{b}$ la classe de l'élément (a,b).

Nous allons maintenant définir deux lois de composition internes sur $\mathrm{Frac}(A)$. Si (a,b) et (c,d) sont deux éléments de $A \times A \setminus \{0_1\}$, on pose

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

Il faut vérifier que cette définition est bien cohérente, c'est-à-dire que $\frac{a}{b} + \frac{c}{d}$ défini ainsi ne dépend que des classes de (a,b) et (c,d) et non des choix particuliers (a,b) de (c,d)

dans leurs classes. Il s'agit donc de vérifier que si $(a,b) \sim (a',b')$ et $(c,d) \sim (c',d')$, alors $(ad+bc,bc) \sim (a'd'+b'c',b'c')$. Vérifions-le ! On a $ab' = a'b$ et $ad' = c'd$, donc

$$(ad+bc)b'c' = adb'c' + bcb'c' = ab'dc' + b'c'bc = a'bcd' + b'c'bc = (a'd'+b'c')bc$$

de sorte que $(ad+bc,bc) \sim (a'd'+b'c',b'c')$. On fait de même pour la loi $\cdot$.

Proposition. *Le triplet* $(\mathrm{Frac}(A),+,\cdot)$ *est un corps commutatif de neutre* $\frac{0}{1}$ *et d'unité* $\frac{1}{1}$.

Démonstration. La preuve est laissée en exercice. □

On remarque que si $(a,b) \in A \times A \setminus \{0_1\}$ et $\lambda \in A \setminus \{0_A\}$, on a $(\lambda a, \lambda b) \sim (a,b)$ de sorte que $\frac{\lambda a}{\lambda b} = \frac{a}{b}$.

Proposition. *L'anneau* $\mathrm{Frac}(A)$ *est un corps commutatif.*

Démonstration. On remarque que $\frac{a}{b} = 0$ si et seulement si $(a,b) \sim (0,1)$ c'est-à-dire si et seulement si $a = 0$. Soit donc $\frac{a}{b} \neq 0_{\mathrm{Frac}(A)}$, c'est-à-dire $a \neq 0$. L'élément $\frac{b}{a}$ est donc bien défini dans $\mathrm{Frac}(A)$, vérifions qu'il s'agit de l'inverse de $\frac{a}{b}$. On a

$$\frac{a}{b}\frac{b}{a} = \frac{ab}{ba} = \frac{1}{1} = 1_{\mathrm{Frac}(A)}.$$

□

On considère l'application φ de A dans $\mathrm{Frac}(A)$ définie par $\varphi(a) = \frac{a}{1}$. On vérifie facilement qu'il s'agit d'un morphisme d'anneaux qui est injectif car $\frac{a}{1} = 0_{\mathrm{Frac}(A)}$ si et seulement si $a = 0_A$. On utilise cette application pour identifier A à un sous-anneau de $\mathrm{Frac}(A)$ et on utilise la notation a pour désigner $\frac{a}{1}$ si $a \in A$.

Le corps $\mathrm{Frac}(A)$ est appelé *corps des fractions* de l'anneau intègre A.

Exemple. Le corps des fractions de l'anneau intègre $\mathbb{Z}$ est le corps $\mathbb{Q}$.

Définition. *Si K est un corps commutatif, l'anneau des polynômes $K[X]$ est intègre et commutatif, on peut donc construire son anneau de fractions que l'on note $K(X)$. Ses éléments sont appelés des* fractions rationnelles.

Une fractions rationnelle à coefficients dans K est donc un élément de la forme $\frac{A}{B}$ où A et B sont des polyômes à coefficients dans K et $B \neq 0$. Notons tout de suite que, puisque l'on peut définir un PGCD dans $K[X]$ et que tout polynôme non nul est associé à un unique polynôme unitaire, on peut écrire une fraction rationnelle de façon unique sous la forme $\frac{A}{B}$ où A et B sont deux polynômes premiers entre eux et B est unitaire. On appelle cette écriture *forme réduite* de la fraction rationnelle. Les racines du numérateur de la forme réduite sont appelés les *zéros* de la fractions rationnelles et les racines du dénominateur ses *pôles*.

Si $F \in K(X)$, on appelle *degré* de la fraction rationnelle l'entier relatif $\deg(A) - \deg(B)$ où A et B sont deux polynômes vérifiant $F = \frac{A}{B}$. Notons que le degré de F ne dépend pas du choix des polynômes A et B, car si $\frac{A}{B} = \frac{C}{D}$, on a $AD = BC$ et donc

$$\deg(A) - \deg(B = \deg(C) - \deg(D).$$

6.2 Décomposition en éléments simples

6.2.1 Partie entière

Proposition. *Soit $F \in K(X)$, il existe alors un unique polynôme $E \in K[X]$ et une unique fraction rationnelle G tels que $F = E + G$ et $\deg(G) < 0$.*

Le polynôme E s'appelle alors la *partie entière* de F et G sa *partie rationnelle.*

Démonstration. Posons $F = \frac{A}{B}$ avec A et B dans $K[X]$. Effectuons la division euclidienne de A par B. On a donc $A = BQ + R$ avec $\deg(R) < \deg(B)$ de sorte que

$$F = Q + \frac{R}{B}.$$

On peut alors poser $E = Q$ et $G = \frac{R}{B}$. Prouvons l'unicité. Si $F = E + G$ avec $E \in K[X]$ et $\deg(G) < 0$, en multipliant par B, on obtient $A = BE + BG$. Ainsi $BG \in K[X]$ et $\deg(BG) < \deg(B)$, on en déduit que E est nécessairement le quotient de la division euclidienne de A par B et BG le reste. L'unicité suit de l'unicité du quotient et du reste dans la division euclidienne de polynômes. □

6.2.2 Éléments simples

Lemme. *Soient A et B deux éléments de $K[X]$ tels que $\deg(A) < \deg(B)$. Supposons que $B = B_1B_2$ avec $B_1 \wedge B_2 = 1$. Il existe alors un unique couple $(A_1, A_2) \in K[X]^2$ tel que $\frac{A}{B} = \frac{A_1}{B_1} + \frac{A_2}{B_2}$ et $\deg(A_i) < \deg(B_i)$ pour $i = 1, 2$.*

Démonstration. L'égalité $\frac{A}{B} = \frac{A_1}{B_1} + \frac{A_2}{B_2}$ est équivalente à l'égalité $A = A_1B_2 + A_2B_1$. Comme $B_1 \wedge B_2 = 1$, le théorème de Bezout implique l'existence d'un couple (U_0, V_0) vérifiant $U_0B_2 + V_0B_1 = A$.

Déterminons toutes les autres solutions de cette équation. Si $UB_2 + VB_1 = A$, on a $(U - U_0)B_2 + (V - V_0)B_1 = 0$ et donc $B_1 \mid (U - U_0)$ puisque $B_1 \wedge B_2 = 1$. On peut donc écrire $U = U_0 + B_1P$, pour $P \in K[X]$ et on en déduit $V = V_0 - B_2P$. Comme un couple de la forme $(U_0 + B_1P, V_0 - B_2P)$ est visiblement solution de l'équation $UB_2 + VB_1 = A$, on en déduit que

$$UB_2 + VB_1 = A \Leftrightarrow (U, V) = (U_0 + B_1P, V_0 - B_2P),\ P \in K[X].$$

Il existe une unique valeur de P pour laquelle $\deg(U_0 + B_1P) < \deg(B_1)$, il s'agit du quotient de la division euclidienne de $-U_0$ par B_1. Posons alors $A_1 = U_0 + B_1P$ pour cette valeur de P et $A_2 = V_0 - B_2P$. Il reste à vérifier que $\deg(A_2) < \deg(B_2)$. On remarque pour cela que $A_2B_1 = A - A_1B_2$. Comme $\deg(A) < deg(B) = \deg(B_1) + \deg(B_2)$ et $\deg(A_1B_2) < \deg(B_1) + \deg(B_2)$, on en conclut que $\deg(A_2B_1) < \deg(B_1) + \deg(B_2)$ et donc que $\deg(A_2) < \deg(B_2)$. L'unicité du couple (A_1, A_2) est claire car, d'après ce qui précède, A_1 est unique, donc A_2 également. □

Une conséquence de ce lemme est la suivante. Suppsons que A et B sont deux polynômes avec $\deg(A) < \deg(B)$. Décomposons $B = B_1^{\alpha_1} \cdots B_r^{\alpha_r}$ où les $B_1, \ldots, B_r$ sont des polynômes irréductibles non associés deux à deux. Il existe un unique r-uple $(A_1, \ldots, A_r) \in K[X]^r$ tel que

$$\frac{A}{B} = \frac{A_1}{B_1^{\alpha_1}} + \cdots + \frac{A_r}{B_r^{\alpha_r}}$$

et $\deg(A_i) < \deg(B_i^{\alpha_i})$ pou $i = 1, \ldots, r$. La preuve se fait par récurrence sur r.

Lemme. *Soit $A \in K[X]$, soit $P \in K[X]$ un polynôme irréductible et soit $\alpha \in \mathbb{N}^*$ tel que $\deg(A) < \deg(P^r)$. Il existe alors un unique α-uplet $(A_1, \ldots, A_r) \in K[X]^r$ tel que*

$$\frac{A}{P^r} = \frac{A_1}{P} + \frac{A_2}{P^2} + \cdots + \frac{A_r}{P^r}$$

avec $\deg(A_i) < \deg(P)$ pour $i = 1, \ldots, \alpha$.

Démonstration. L'égalité recherchée est équivalente à la décomposition

$$A = A_1P^{r-1} + A_2P^{r-1} + \cdots + A_{\alpha-1}P + A_\alpha.$$

L'existence et l'unicité des A_i provient encore de la division euclidienne appliquée plusieurs fois. Le polynôme A_α est le reste de la division euclidienne de A par P. Notons Q_α le quotient. Le polynôme $A_{\alpha-1}$ est alors le reste de la division de Q_α par P. On itère le processus jusqu'à obtenir $A_\alpha, \ldots, A_1$. □

En regroupant les deux lemmes prouvés précédemment, on obtient le théorème de décomposition en éléments simples.

Théorème. *Soient A et B deux polynômes avec $B \neq 0$ unitaire. On décompose B en produit d'irréductibles $P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ où les P_i sont irréductibles unitaires et distincts. On peut alors écrirede façon unique*

$$\frac{A}{B} = E + \sum_{i=1}^{r} \sum_{j=1}^{\alpha_i} \frac{A_{i,j}}{P_i^j}$$

avec $E \in K[X]$ et $A_{i,j} \in K[X]$ vérifiant $\deg(A_{i,j}) < \deg(P_i)$.

Discutons quelques cas particuliers.

a) Si $K = \mathbb{C}$, les polynômes P_i sont de la forme $(X - a_i)$ avec $a_i \in \mathbb{C}$. La décomposition en éléments simples prend donc la forme

$$\frac{A}{B} = E + \sum_{i=1}^{r} \sum_{j=1}^{\alpha_i} \frac{\lambda_{i,j}}{(X - a_i)^{\alpha_i}}$$

où les $\lambda_{i,j}$ sont des polynômes de degré 0, c'est-à-dire des éléments de $\mathbb{C}$.

b) Si $K = \mathbb{R}$, les polynômes P_i sont de la forme $X - a_i$ avec $a_i \in \mathbb{R}$ ou $X^2 + b_i X + c_i$ avec $b_i^2 - 4c_i < 0$. La décomposition en éléments simples prend donc la forme

$$\frac{A}{B} = E + \sum_{i=1}^{r} \sum_{j=1}^{\alpha_i} \frac{\lambda_{i,j}}{(X - a_i)^j} + \sum_{k=1}^{s} \sum_{\ell=1}^{\alpha_k} \frac{\mu_{k,\ell} X + \nu_{k,\ell}}{(X^2 + b_k X + c_k)^\ell}$$

où les $\lambda_{i,j}$, $\mu_{k,\ell}$ et $\nu_{k,\ell}$ sont des éléments de $\mathbb{R}$.

6.3 Quelques méthodes de décomposition

Donnons à présent quelques méthodes de décomposition. Si $F = \frac{A}{B}$, il faut commencer par mettre F sous forme réduite, c'est-à-dire telle que $A \wedge B = 1$, cela permet de réduire le degré des polynômes qui vont apparaître. Si $\deg(A) \geqslant \deg(B)$, on effectue la division euclidienne de A par B pour extraire la partie rationnelle. On est donc ramené au cas où $\deg(A) < \deg(B)$. Il existe alors des méthodes plus directes que la division euclidienne pour déterminer les coefficients $\lambda_{i,j}$, $\mu_{k,\ell}$ et $\nu_{k,\ell}$ de la décomposition en éléments simples.

6.3.1 Exemple d'un pôle simple

Posons $F = \frac{1}{X^3 - 3X^2 + 2X}$. On commence par factoriser le dénominateur, on trouve $X(X-1)(X-2)$, tous les diviseurs irréductibles sont simples. La décomposition de F en éléments simples est donc de la forme

$$F = \frac{\alpha}{X} + \frac{\beta}{X-1} + \frac{\gamma}{X-2}.$$

Pour déterminer α, on peut alors multiplier F par X et évaluer XF en 0. On obtient alors $\alpha = \frac{1}{2}$. En multipliant F par $(X-1)$ et en évaluant en 1, on trouve $\beta = -1$ et de même $\gamma = \frac{1}{2}$.

6.3.2 Exemple avec un pôle multiple

Posons $F = \frac{X^2+1}{X(X-1)^2}$. On cherche donc une décomposition en éléments simple de la forme

$$F = \frac{\alpha}{X} + \frac{\beta}{(X-1)} + \frac{\gamma}{(X-1)^2}.$$

On détermine α par la méthode précédente puisque 0 est un pôle simple. On peut également déterminer γ en multipliant F par $(X-1)^2$ et en évaluant $(X-1)^2F$ en 1. Il reste alors à déterminer β. On peut alors évaluer F en un point différent de 0 et 1, ceci fournit une relation entre α, β et γ qui permet de déduire β de notre connaissance de α et β. On peut également multiplier F par $(X-1)$, évaluer la fraction rationnelle en $t \in \mathbb{R} \setminus \{0,1\}$ et faire tendre t vers $+\infty$. On obtient ici

$$\alpha = 1, \quad \beta = 0, \quad \gamma = 2.$$

Lorsque la multiplicité des pôles devient plus grande, on peut évaluer la fraction rationnelle en un plus grand nombre de points afin d'obtenir un système linéaire satisfait par les coefficients.

6.3.3 Exemple avec des facteurs irréductibles de degré 2

Lorsque $K = \mathbb{R}$ et que des facteur irréductibles de degré 2 apparaissent au dénominateur, on peut effectuer la décomposition en éléments simples dans $\mathbb{C}$ et regrouper les termes conjugués. Voici un exemple avec $F = \frac{1}{X^4-1} = \frac{1}{(X-1)(X+1)(X^2+1)}$. Dans $\mathbb{C}(X)$, on recherche une décomposition de la forme

$$F = \frac{\alpha}{(X-i)} + \frac{\beta}{X+1} + \frac{\gamma}{X-i} + \frac{\delta}{X+i}.$$

Les méthodes précédentes nous donnent

$$\alpha = \frac{1}{4}, \quad \beta = -\frac{1}{4}, \gamma = \frac{i}{4}, \delta = -\frac{i}{4}.$$

On regroupe alors les termes conjugués :

$$\frac{\gamma}{(X-i)} + \frac{\delta}{X+i} = \frac{(\gamma+\delta)X + (\gamma-\delta)i}{X^2+1} = \frac{1}{2}\frac{1}{(X^2+1)}.$$

Pour conclure, on a

$$\frac{1}{X^4+1} = \frac{1}{4}\left(\frac{1}{X-1} - \frac{1}{X+1} + \frac{2}{X^2+1}\right).$$