Université de Bordeaux, année 2020-21
Licence de Sciences et Technologies mention mathématiques
Parcours Math-Fonda, Math-Info, CMI OPTIM, Semestre 4.

Structures algébriques 1 :
Résumé de cours

Ces notes sont un support de cours ; elles ne s'y substituent pas. On y trouve les résultats principaux, non commentés et non illustrés la plupart du temps. Les démonstrations sont le plus souvent simplement esquissées, voire absentes. Les détails, explications, et illustrations, indispensables à la compréhension, sont donnés en cours et en TD.

Table des matières

Chapitre 1

Rappels d'arithmétique dans $\mathbb{Z}$

1 Addition et multiplication dans $\mathbb{Z}$

L'ensemble $\mathbb{Z}$ des entiers relatifs est muni d'une addition et d'une multiplication qui vérifient les propriétés suivantes :

1) L'addition est une *loi de composition interne* :

$$\forall (a,b) \in \mathbb{Z}^2 \ , \ a+b \in \mathbb{Z}$$

2) L'addition est *associative* :

$$\forall (a,b,c) \in \mathbb{Z}^3 \ , \ a+(b+c) = (a+b)+c$$

3) 0 est un *élément neutre* pour l'addition :

$$\forall a \in \mathbb{Z} \ , \ a+0 = 0+a = a$$

4) *Tout élément admet un opposé* pour l'addition :

$$\forall a \in \mathbb{Z} \ , \ a+(-a) = (-a)+a = 0$$

Qui plus est :

5) L'addition est *commutative* :

$$\forall (a,b) \in \mathbb{Z}^2 \ , \ a+b = b+a$$

Pour ce qui est de la multiplication, elle possède les propriétés suivantes :

1) C'est une loi de composition interne : $\forall (a,b) \in \mathbb{Z}^2 \ , \ a \cdot b \in \mathbb{Z}$

2) Elle est associative : $\forall (a,b,c) \in \mathbb{Z}^3 \ , \ a \cdot (b \cdot c) = (a \cdot b) \cdot c$

3) Elle possède un élément neutre (l'entier 1) : $\forall a \in \mathbb{Z} \ , \ a \cdot 1 = 1 \cdot a = a$

4) Elle est *distributive par rapport à l'addition*, ce qui signifie que

$$\forall (a,b,c) \in \mathbb{Z}^3 \ , \ a \cdot (b+c) = a \cdot b + a \cdot c.$$

2 Division euclidienne et relation de divisibilité dans $\mathbb{Z}$

2.1 Division euclidienne

Théorème 1
Pour tout couple d'entiers relatifs (a, b) avec $b \neq 0$, il existe un unique couple (q, r) d'entiers relatifs tels que

$$\begin{cases} a = bq + r \\ 0 \leq r < |b|. \end{cases} \tag{1.1}$$

Les entiers q et r sont respectivement le quotient et le reste de la division euclidienne de a par b.

Preuve. Commençons par supposer $b > 0$. Pour l'existence, on considère l'ensemble $E = \{k \in \mathbb{Z} \mid bk \leq a\}$; comme partie non vide et majorée de $\mathbb{Z}$, il admet un plus grand élément q (E est majoré par a et comme $a + b|a| \geq 0$, $-|a| \in E$). On pose alors $r := a - bq$. Clairement, on a $0 \leq a - bq < b = |b|$ (par maximalité de q), donc le couple (q, r) satisfait 1.3. Pour l'unicité, on suppose qu'il existe un autre couple (q', r') tel que

$$\begin{cases} a = bq' + r' \\ 0 \leq r' < b. \end{cases} \tag{1.2}$$

En particulier, $a = bq + r = bq' + r'$ et $-b < r - r' < b'$ donc $-b < b(q' - q) < b$ i.e. $b|q - q'| < b$ ce qui entraîne $q = q'$ et par conséquent $r = r'$.
Si $b < 0$, on applique le raisonnement précédent à a et $-b$, donc il existe $(q, r) \in \mathbb{Z}^2$ unique tel que $a = (-b)q + r = b(-q) + r$ et $0 \leq r \leq -b = |b|$ ce qui donne également le résultat dans ce cas.

□

La division euclidienne s'étend sans difficulté à l'ensemble $\mathbb{Z}$ des entiers relatifs :

Théorème 2
Pour tout couple d'entiers naturels (a, b) avec $b \neq 0$, il existe un unique couple (q, r) d'entiers naturels tels que

$$\begin{cases} a = bq + r \\ 0 \leq r < b. \end{cases} \tag{1.3}$$

2.2 Divisibilité

Définition 1
Soit a et b deux entiers relatifs, avec b non nul. On dit que "b divise a", que "b est un diviseur de a", ou encore que "a est un multiple de b" et on écrit " $b \mid a$ " s' il existe $q \in \mathbb{Z}$ tel que $a = bq$.

Remarque : b divise a si et seulement si le reste de la division euclidienne de a par b est nul.

Proposition 1
La relation de divisibilité restreinte à $\mathbb{N}_{\geq 1}$ est une relation d'ordre.

Preuve. Bien sûr la relation est réflexive car tout entier non nul a est diviseur de lui-même. La relation est antisymétrique car si $a, b \geq 1$ sont des entiers tels que $a \mid b$ et $b \mid a$, alors $a = bc$ et $b = ad$ pour certains entiers $c, d \geq 1$. On déduit $a = acd$ puis $cd = 1$ car $a \neq 0$. Ainsi $c = d = 1$ puisque $c, d \in \mathbb{N}_{\geq 1}$. Donc $a = b$. Enfin la transitivité est évidente : si $a \mid b$ et $b \mid c$, avec $a, b, c \in \mathbb{N}_{\geq 1}$, alors $a \mid c$. □

Définition 2 (Nombre premier)
Un entier naturel $p \geq 2$ est dit premier *si l'ensemble de ses diviseurs dans $\mathbb{N}$ est exactement $\{1, p\}$.*

Remarque : Par convention 1 **n'est pas** un nombre premier. Cela permet en particulier d'avoir factorisation *unique* (à l'ordre des facteurs près) de tout entier naturel non nul en produit de facteurs premiers

La suite croissante des nombres premiers a donc pour premiers termes $2, 3, 5, 7, 11, ...$ Rappelons deux propriétés fondamentales relatives aux nombres premiers.

Théorème 3
1) *Tout entier n distinct de ± 1 admet un diviseur premier.*

2) *(*Euclide*) Il existe une infinité de nombres premiers.*

Preuve. Pour le point 1, fixons un entier n tel que $|n| \geq 2$ (la propriété est triviale pour $n = 0$). L'ensemble des diviseurs > 1 de n est non-vide (car $|n|$ est un tel diviseur) et donc admet un plus petit élément p comme partie non vide de $\mathbb{N}$. On a $p > 1$ et donc, si p n'est pas premier, p admet un diviseur positif autre que 1 et p. On aurait alors trouvé un entier p' satisfaisant $1 < p' < p$ tel que $p' \mid n$ (on utilise la transitivité de la relation "divise"). Cela contredit la minimalité de p. Donc p est premier.
Pour le second point, on raisonne par l'absurde : si $p_1 = 2, p_2 = 3, \ldots, p_N$ est la liste complète des nombres premiers alors considérons $n = 1 + \prod_{i=1}^{N} p_i$. L'entier n est bien sûr ≥ 2. On peut lui appliquer le point 1 : il existe un nombre premier p_0 divisant n. Ce nombre premier n'est pas un des p_i, sinon ce serait un diviseur de $n - \prod_{i=1}^{N} p_i = 1$. On a donc contredit le fait que $p_1, \ldots, p_N$ est la liste complète des nombres premiers. □

2.3 PGCD, PPCM

Définition 3

1) *Le PGCD de deux entiers relatifs a et b non tous les deux nuls est l'entier d défini par :*

$$d := \max\{k \in \mathbb{N}^* \mid k \text{ divise } a \text{ et } b\} .$$

Lorsque $d = 1$, on dit que a et b sont premiers entre eux *ou que a* est premier à *b.*

2) *Le PPCM de deux entiers relatifs a et b non nuls est l'entier m défini par :*

$$m := \min\{k \in \mathbb{N}^* \mid k \text{ est un multiple commun à } a \text{ et } b\} .$$

Notation : On notera parfois $a \wedge b$ ou (a, b) le pgcd des entiers a et b et $a \vee b$ leur ppcm .

Remarque : Notons que par définition, si p est premier alors pour tout $a \in \mathbb{Z}$, $\text{pgcd}(a, p) = 1$ ou p.

2.4 Théorème de Bézout

Notation : si a est un entier (quelconque), on note $a\mathbb{Z}$ l'ensemble de ses multiples. Autrement dit

$$a\mathbb{Z} = \{am \colon m \in \mathbb{Z}\} = \{n \in \mathbb{Z} \colon \exists m \in \mathbb{Z}, n = am\} .$$

De même, si a et b sont deux entiers, on définit

$$a\mathbb{Z} + b\mathbb{Z} = \{ax + by \colon x, y \in \mathbb{Z}\} = \{n \in \mathbb{Z} \colon \exists x, y \in \mathbb{Z}, n = ax + by\} .$$

Proposition 2
Si a et b sont des entiers, on a l'équivalence : $a\mathbb{Z} \subset b\mathbb{Z} \Leftrightarrow$ b divise a.

Théorème 4
Soient a et b deux entiers non tous les deux nuls. On note d leur PGCD et m leur PPCM.

1) *$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.*

2) *(Théorème de Bézout) Si $\text{pgcd}(a, b) = d$ alors il existe deux entiers u et v tels que*

$$au + bv = d.$$

3) *$d = \text{pgcd}(a, b)$ équivaut à*

$$(d \mid a, d \mid b) \text{ et } \big((c \in \mathbb{Z}, c \mid a, c \mid b) \Rightarrow c \mid d\big) .$$

Le PGCD de a et b est le "plus grand diviseur commun" à a et b au sens de la relation d'ordre usuelle sur $\mathbb{Z}$, mais également au sens de la relation de divisibilité.

4) $m = \text{ppcm}(a,b)$ *équivaut à*

$$(a \mid m, b \mid m) \text{ et } \big((c \in \mathbb{Z}, a \mid c, b \mid c) \Rightarrow m \mid c\big).$$

Le PPCM de a et b est le "plus petit multiple commun" à a et b au sens de la relation d'ordre usuelle sur $\mathbb{Z}$ et au sens de la relation de divisibilité.

Notons que la preuve du point 1 donnée ci-dessous se généralise pour caractériser les *sous-groupes* de $\mathbb{Z}$ (cf le chapitre suivant).

Preuve. (1) On donne la preuve de la première assertion, on laisse la preuve de la seconde en exercice (c'est exactement le même schéma).
Comme a et b ne sont pas tous les deux nuls, alors $a\mathbb{Z} + b\mathbb{Z}$ contient un élément non nul x, ainsi que son opposé $-x$ (on voit immédiatement que si $z \in a\mathbb{Z} + b\mathbb{Z}$ alors $-z \in a\mathbb{Z} + b\mathbb{Z}$). Ainsi $a\mathbb{Z} + b\mathbb{Z}$ contient un élément strictement positif. Par conséquent, l'ensemble $F_+ = \{x \in a\mathbb{Z} + b\mathbb{Z} : x > 0\} \subset \mathbb{N}$ est non vide. Il admet donc, comme toute partie non vide de $\mathbb{N}$, un plus petit élément noté g. Clairement, g ainsi que tous ses multiples appartiennent à $a\mathbb{Z} + b\mathbb{Z}$, donc $g\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$. Inversement, si x est un élément (quelconque) de $a\mathbb{Z} + b\mathbb{Z}$, on peut effectuer la division euclidienne de x par g :

$$x = gq + r\ , \ \text{ avec } q, r \in \mathbb{Z} \text{ et } 0 \leq r < g.$$

On en déduit que $r = x - gq$ appartient à $a\mathbb{Z} + b\mathbb{Z}$, comme différence de deux éléments de $a\mathbb{Z} + b\mathbb{Z}$. S'il était > 0, cela contredirait la définition de g, donc $r = 0$, ce qui signifie que $x \in g\mathbb{Z}$.
Montrons enfin que $g = d$. Bien sûr $a \in g\mathbb{Z}$ et $b \in g\mathbb{Z}$ donc $g > 0$ est un diviseur commun de a et b. Par ailleurs si $c \in \mathbb{Z}$ divise a et b, il divise tout entier de la forme $an + bm$ $(n, m \in \mathbb{Z})$. On a montré que g est un entier de cette forme ; en particulier $c \mid g$ donc $c \leq g$. Ainsi g est le plus grand diviseur commun de a et b.
(2) c'est une conséquence facile du point (1).
(3) Le sens réciproque est immédiat d'après la définition de PGCD. Pour le sens direct, fixons un entier c diviseur commun à a et b. Alors c divise toute combinaison $\mathbb{Z}$-linéaire $am + bn$ de a et b. Prenant $(m, n) = (u, v)$ où le couple (u, v) satisfait à la relation de Bézout de (2), on déduit que $c \mid d$.
(4) exercice ; la preuve est identique à celle de (3). □

Corollaire 1
Soient a et b deux entiers non tous les deux nuls. Alors $\text{pgcd}(a,b) = 1$ *ssi il existe deux entiers u et v tels que* $au + bv = 1$.

Preuve. Le sens direct est une conséquence du théorème de Bézout. Réciproquement, tout diviseur positif commun de a et b divise $au + bv = 1$ et donc vaut 1. □

Remarque : Le point 2 du théorème n'admet pas de réciproque en général : on ne peut bien sûr pas déduire du fait que $3 \times u + 5 \times v = 29$, pour le choix $u = -2$, $v = 7$, que le pgcd de de 3 et 5 vaut 29.

2.5 Complément : Algorithme d'Euclide

Proposition 3
Soient a et b deux entiers, avec $b \neq 0$. Si r est le reste de la division euclidienne de a par b alors

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

Voici le principe de l'algorithme d'Euclide : soient a et b deux entiers positifs ; on pose $r_0 = a$ et $r_1 = b$, puis pour $k \geq 1$, **tant que** $r_k > 0$, on définit r_{k+1} comme le reste de la division euclidienne de r_{k-1} par r_k, $r_{k-1} = r_k q_k + r_{k+1}$. En particulier, on a $r_{k+1} < r_k$ si r_k est non nul. La suite ainsi construite est donc strictement décroissante, ce qui garantit que l'algorithme s'arrête. On vérifie alors, en utilisant la Proposition 3, que le dernier terme non nul de la suite est le PGCD de a et b.

Entrées : a,b entiers naturels
Sorties : PGCD de a et b
tant que $b > 0$ **faire**
  $r \leftarrow a\%b$ `/* reste de la division euclidienne de a par b */`
  $a \leftarrow b$
  $b \leftarrow r$
fin
retourner a

Algorithme 1 : Algorithme d'Euclide

Voici maintenant une variante de l'algorithme d'Euclide qui permet de déterminer le PGCD de deux entiers a et b ainsi que deux entiers u et v tels que $au + bv = \mathrm{PGCD}(a, b)$. Cette variante est généralement appelée *algorithme d'Euclide étendu*.
On définit récursivement des entiers u_k et v_k de la façon suivante : on pose $u_0 = 1$, $v_0 = 0$, $u_1 = 0$, $v_1 = 1$ et pour $k \geq 1$

$$\begin{cases} u_{k+1} = u_{k-1} - u_k q_k \\ v_{k+1} = v_{k-1} - v_k q_k \end{cases}$$

On vérifie alors par récurrence sur k, que les entiers u_k et v_k ainsi définis vérifient la relation

$$r_k = au_k + bv_k$$

pour tout $k \geq 0$. En effet, cette relation est vraie pour $k = 0, 1$ et si elle est vérifiée pour deux entiers consécutifs $k-1$ et k, alors

$$r_{k+1} = r_{k-1} - r_k q_k = au_{k-1} + bv_{k-1} - q_k(au_k + bv_k) = a(u_{k-1} - u_k q_k) + b(v_{k-1} - v_k q_k).$$

En particulier, si n est l'indice du dernier reste non nul, on obtient

$$d = r_n = au_n + bv_n.$$

Entrées : a,b entiers naturels
Sorties : $d = \text{PGCD}(a,b)$ et $(u,v) \in \mathbb{Z}^2$ tel que $d = au + bv$
$u \leftarrow 1$
$v \leftarrow 0$
$s \leftarrow 0$
$t \leftarrow 1$
tant que $b > 0$ **faire**
  $q \leftarrow a/b$ `/* quotient de la division euclidienne de` a `par` b `*/`
  $r \leftarrow a\%b$ `/* reste de la division euclidienne de` a `par` b `*/`
  $a \leftarrow b$
  $b \leftarrow r$
  $X \leftarrow s$
  $s \leftarrow u - qs$
  $u \leftarrow X$
  $X \leftarrow t$
  $t \leftarrow v - qt$
  $v \leftarrow X$
fin
retourner a, u, v

Algorithme 2 : Algorithme d'Euclide étendu

Remarque : l'algorithme précédent fournit une preuve *constructive* du théorème de Bézout, à l'inverse de l'approche de §2.4 qui prouve l'existence d'une relation de Bézout mais ne donne aucun moyen d'en déterminer une.

3 Lemme de Gauss et décomposition en produit de facteurs premiers

Dans ce paragraphe, on notera $a \wedge b$ le PGCD de deux entiers a et b, et $a \vee b$ leur PPCM.

Proposition 4 (Lemme de Gauss)
Soient a, b et c trois entiers. Si a divise bc et $a \wedge b = 1$ alors a divise c.

Preuve. Comme a est premier à b, on a une relation de Bézout $au + bv = 1$, $u, v \in \mathbb{Z}$. Ainsi $acu + bcv = c$. Comme $a \mid bc$, alors a divise le membre de gauche de cette dernière égalité, donc $a \mid c$. □

Proposition 5
Soient a, b et c trois entiers.
a) *Si a divise c et b divise c et si $a \wedge b = 1$ alors ab divise c.*
b) (Lemme d'Euclide) *Si p est un nombre premier et si p divise ab alors p divise a ou p divise b.*
c) *Si $a \wedge b = 1$ et $a \wedge c = 1$ alors $a \wedge bc = 1$.*

Preuve. a) Écrivons $c = an_1 = bn_2$, $n_1, n_2 \in \mathbb{Z}$. Aussi on a une relation de Bézout $au + bv = 1$, $u, v \in \mathbb{Z}$. Ainsi $c = acu + bcv = abn_2u + abn_1v$ est divisible par ab.
b) On combine le lemme de Gauss et le fait que si p est premier, alors pour tout entier a, soit $p \mid a$, soit $p \wedge a = 1$.
c) Si a a un diviseur commun > 1 avec bc, alors, d'après le théorème 3, ce diviseur admet un facteur premier qui divise a et bc. On conclut avec le lemme d'Euclide. □

On conclut ce paragraphe avec le résultat fondamental suivant.

Théorème 5
Tout entier $a > 1$ s'écrit de manière unique

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

où $\begin{cases} \text{les entiers } p_i \text{ sont premiers et vérifient } p_1 < p_2 < \dots < p_k \\ \text{les entiers } \alpha_i \text{ sont strictement positifs} \end{cases}$

La preuve de l'unicité de la décomposition en facteurs premiers repose sur le lemme de Gauss.

4 Congruences

Dans ce paragraphe, n désigne un entier naturel non nul fixé.

Définition 4
On dit que deux entiers relatifs a et b sont congrus modulo n ou encore que a est congru à b modulo n si n divise $a - b$. On notera $a \equiv b \mod n$ ou $a \equiv b\ [n]$.

Proposition 6
La relation de congruence modulo n vérifie les propriétés suivantes

1) $\forall a \in \mathbb{Z} \quad a \equiv a \mod n$ *("Réflexivité"),*

2) $\forall (a, b) \in \mathbb{Z}^2 \quad a \equiv b \mod n \iff b \equiv a \mod n$ *("Symétrie"),*

3) $\forall (a, b, c) \in \mathbb{Z}^3 \quad (a \equiv b \mod n \wedge b \equiv c \mod n) \Rightarrow a \equiv c \mod n$ *("Transitivité").*

On dit que la relation de congruence est une ***relation d'équivalence*** *(cf chapitre suivant pour un rappel de la définition générale) sur l'ensemble des entiers.*

Proposition 7
Pour tout entier relatif a, il existe un unique entier naturel $r \in \{0, \dots, n-1\}$ tel que $a \equiv r \mod n$

Preuve. Il suffit de considérer le reste de la division euclidienne de a par n. □

Définition 5
Pour tout $a \in \mathbb{Z}$, on note $a + n\mathbb{Z}$ ou $\overline{a}$ la classe de congruence de a modulo n, c'est-à-dire

$$a + n\mathbb{Z} = \overline{a} := \{b \in \mathbb{Z} \mid b \equiv a \mod n\}.$$

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes de congruence modulo n.

La Proposition 7 admet le corollaire suivant :

Corollaire 2
$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

On souhaite munir l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes de congurence modulo n d'une addition et d'une multiplication. Le point de départ de la construction est le résultat suivant.

Proposition 8
Soit n un entier naturel non nul. On note a, b, a' et b' quatre entiers relatifs. On a les propriétés suivantes : si $a \equiv b \mod n$ et $a' \equiv b' \mod n$ alors

$$a + a' \equiv b + b' \mod n \qquad a - a' \equiv b - b' \mod n \qquad aa' \equiv bb' \mod n$$

Remarque : On dit que la relation de congruence est compatible avec l'addition, la soustraction et la multiplication définies sur $\mathbb{Z}$.

La Proposition 8 permet en particulier de munir l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ d'une addition et d'une multiplication définies comme suit.

Définition 6
Soient $\overline{x}$ et $\overline{y}$ deux éléments de $\mathbb{Z}/n\mathbb{Z}$. On pose :

1) *(Addition) $\overline{x} + \overline{y} := \overline{s}$, où s désigne le reste de la division euclidienne de $x + y$ par n,*

2) *(Multiplication) $\overline{x}\ \overline{y} := \overline{p}$, où p désigne le reste de la division euclidienne de xy par n.*

Pour illustrer la construction ci-dessus, on donne ci-dessous les tables d'addition et de multiplication de $\mathbb{Z}/3\mathbb{Z}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Chapitre 2

Théorie des groupes

1 Définition et premiers exemples

Définition 1
Un groupe est la donnée d'un ensemble G et d'une ***loi de composition interne*** $*$

$$\begin{array}{ccc} G \times G & \to & G \\ (x,y) & \mapsto & x*y \end{array}$$

qui vérifie les propriétés suivantes :

1) *la loi $*$ est associative : $\forall (x,y,z) \in G^3$, $x*(y*z) = (x*y)*z$*

2) *il existe un élément $e \in G$, qu'on appelle* ***élément neutre****, qui est tel que : $\forall x \in G$, $x*e = e*x = x$*

3) *tout élément de G admet un* ***inverse*** *: $\forall x \in G$, $\exists y \in G$: $x*y = y*x = e$.*

Si en outre la loi $*$ est commutative (i.e. $x*y = y*x$ pour tout $x,y \in G$), on dit que G est un groupe abélien *ou* commutatif.

Proposition 1
Dans un groupe $(G,*)$:

1) *l'élément neutre est unique,*

2) *tout élément x admet un unique inverse, que l'on note x^{-1},*

3) *$e^{-1} = e$, $(x^{-1})^{-1} = x$ pour tout élément x de G, et $(x*y)^{-1} = y^{-1}*x^{-1}$ pour tout couple (x,y) d'éléments de G.*

Notation : Dans la suite on adoptera en général la *notation multiplicative* pour un groupe abstrait G : on notera xy au lieu de $x*y$. De même on notera x^{-1} l'inverse de

$x \in G$ et 1 le neutre de G (on conservera parfois la notation e pour le neutre, pour insister sur le caractère "général" d'une notion abordée).
Si G est un groupe abélien, on préférera souvent la notation *additive* : $x * y$ est noté $x + y$; l'inverse de x est noté $-x$ et le neutre est noté 0.

Définition 2
L'ordre *d'un groupe G est son nombre d'éléments. On dit queG est fini si son ordre est fini.*

Définition 3
Dans un groupe G, pour tout $x \in G$ et $n \in \mathbb{N}_{\geq 1}$, on définit par récurrence

- $x^0 = e$;
- $x^n = (x^{n-1})x$;
- $x^{-n} = (x^{-1})^n$.

Si $n, m \in \mathbb{Z}$, en utilisant l'associativité de la multiplication, on montre facilement que $x^{n+m} = x^n x^m$.

Exemples:

- $(\mathbb{Z}, +)$ est un groupe infini abélien.
- $(\mathbb{R}^\times, \times)$ est un groupe infini abélien.
- $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien fini d'ordre n. L'addition est définie comme à la fin du chapitre précédent.
- L'ensemble des permutations de n symboles muni de la composition des applications $(S_n, \circ)$ est un groupe fini d'ordre $n!$. C'est un groupe non-abélien dès que $n \geq 3$.
- $(\mathrm{GL}_n(\mathbb{R}), \times)$ est groupe infini non-abélien dès que $n \geq 2$.
- Les racines de l'unité dans $\mathbb{C}$ forment un groupe abélien infini.
- Si $(G, \star_G)$ et $(H, \star_H)$ sont des groupes alors le produit direct $G \times H$ est un groupe pour la loi $\star$ définie par

$$(g_1, h_1) \star (g_2, h_2) = (g_1 \star_G g_2, h_1 \star_H h_2)\,.$$

2 Sous-groupes

2.1 Définitions

Définition 4
Soit G un groupe noté multiplicativement. Une partie H de G est un sous-groupe *si*

1) $H \neq \emptyset$,

2) $\forall (x,y) \in H^2\ ,\ xy \in H$,

3) $\forall x \in H\ ,\ x^{-1} \in H$.

Remarquons en particulier qu'un sous-groupe d'un groupe G contient nécessairement l'élément neutre de G. Aussi, pour tout groupe G, les parties $\{e\}$ et G de G sont de sous-groupes (les sous-groupes *triviaux*).
Clairement, la loi de groupe de G, quand on la restreint à un sous-groupe H, induit une structure de groupe sur H. En pratique, on montrera souvent qu'un ensemble, muni d'une loi de composition interne est un groupe en l'identifiant à un sous-groupe d'un groupe connu.
La proposition suivante fournit une caractérisation très utile pour un sous-groupe :

Proposition 2
Soit H une partie d'un groupe G noté multiplicativement. Alors H est un sous-groupe si et seulement si

$$H \neq \emptyset \ \text{ et } \forall (x,y) \in H^2\ ,\ xy^{-1} \in H.$$

On termine ce paragraphe en donnant la description des sous-groupes de $\mathbb{Z}$.

Proposition 3
Les sous-groupes de $(\mathbb{Z},+)$ sont les $a\mathbb{Z}$ pour $a \in \mathbb{N}$.

Preuve. On reprend la preuve du théorème 4 du chapitre 1. Soit $H \subset \mathbb{Z}$ un sous-groupe. Si $H = \{0\}$, $H = 0\mathbb{Z}$. Sinon, H contient un élément non nul x, ainsi que son opposé $-x$. Ainsi H contient un élément strictement positif. Par conséquent, l'ensemble $F_+ = \{x \in H : x > 0\} \subset \mathbb{N}$ est non vide. Il admet donc, comme toute partie non vide de $\mathbb{N}$, un plus petit élément noté a. Clairement, a ainsi que tous ses multiples appartiennent à H, donc $a\mathbb{Z} \subset H$. Inversement, si x est un élément (quelconque) de H, on peut effectuer la division euclidienne de x par a :

$$x = aq + r\ ,\ \text{ avec } q, r \in \mathbb{Z} \text{ et } 0 \leq r < a.$$

On en déduit que $r = x - aq$ appartient à H, comme différence de deux éléments de H. S'il était > 0, cela contredirait la définition de a, donc $r = 0$, ce qui signifie que $x \in a\mathbb{Z}$.

□

2.2 Sous-groupe engendré par une partie

Proposition 4
L'intersection de deux sous-groupes, ou plus généralement d'une famille de sous-groupes, d'un groupe G est un sous-groupe de G.

⚠ La réunion de deux sous-groupes n'est en revanche pas un sous-groupe en général. Ce n'est même essentiellement "jamais" le cas, comme le montre l'énoncé suivant (exercice)

> *"Si H et K deux sous-groupes d'un groupe G. Alors $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$."*

La proposition 4 permet de définir la notion de sous-groupe engendré par une partie :

Définition 5
Soit S une partie d'un groupe G. On appelle sous-groupe engendré par S, et on note $\langle S \rangle$ le plus petit sous-groupe de G contenant S. C'est l'intersection de tous les sous-groupes de G qui contiennent S. On dit alors que S est une partie génératrice *de $\langle S \rangle$ ou que S* engendre *$\langle S \rangle$.*

⚠ La définition ci-dessus permet de considérer le sous-groupe $\langle \emptyset \rangle$ de G (le "sous-groupe engendré par le vide"). On définit $\langle \emptyset \rangle = \{e\}$, ce qui est compatible avec la définition ci-dessus.

La définition ci-dessus est peu exploitable en pratique. On dispose de la description plus explicite suivante :

Proposition 5
Soit G un groupe. Alors le sous-groupe engendré par une partie non vide S de G est l'ensemble des éléments de la forme $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_r^{\varepsilon_r}$ où :

- *r est un entier naturel non nul,*
- *les x_i sont des éléments de S,*
- *$\varepsilon_i = \pm 1$ pour tout i.*

En faisant la convention qu'un produit vide d'élements de G est égal au neutre de G et en autorisant $r = 0$ dans la proposition ci-dessus, on peut se débarrasser de la restriction $S \neq \emptyset$ dans l'énoncé.

3 Ordre d'un élément

Définition 6
Soit G un groupe dont la loi est notée multiplicativement. On dit qu'un élément x de G est **d'ordre fini** *s'il existe un entier naturel non nul k tel que $x^k = e$. Si tel est le cas on appelle* **ordre de** *x le plus petit entier $k \in \mathbb{N}^\star$ tel que $x^k = e$. Sinon, on dit que x est* **d'ordre infini**.

Donnons un premier énoncé reliant l'ordre d'un élément à l'ordre du sous-groupe qu'il engendre.

Proposition 6
Soit G un groupe noté multiplicativement et de neutre e. Soit $x \in G$. Alors l'ordre de l'élément x de G est égal à l'ordre du sous-groupe engendré par $\{x\}$ dans G.

Preuve. Notons n l'ordre de x (on a soit $n \in \mathbb{N}_{\geq 1}$, soit $n = \infty$). D'après la proposition 5, le sous-groupe de G engendré par $S = \{x\}$ est :

$$\langle S \rangle = \{x^k : k \in \mathbb{Z}\}.$$

Deux cas se présentent : soit $n = \infty$ et alors $|\langle S \rangle| = \infty$ puisque si on a des entiers $k < \ell$ tels que $x^k = x^\ell$, alors $x^{\ell-k} = e$, ce qui contredit $n = \infty$ car $\ell - k \in \mathbb{N}_{\geq 1}$. Sinon $n \in \mathbb{N}_{\geq 1}$; montrons alors que

$$\langle S \rangle = \{e, x, \dots x^{n-1}\}.$$

L'inclusion $\supset$ est évidente. Réciproquement si $y = x^k \in \langle S \rangle$ pour un $k \in \mathbb{Z}$ alors, en écrivant la division euclidienne $k = qn + r$, $0 \leq r < n$, de k par n, on voit que $y = x^{qn+r} = (x^n)^q \cdot x^r = x^r$, ce qui achève de démontrer l'égalité souhaitée.
Enfin, si $n \in \mathbb{N}_{\geq 1}$, alors dès que $0 \leq i < j \leq n-1$, on a $x^i \neq x^j$, car sinon la relation $x^{j-i} = e$ contredirait le fait que n est l'ordre de x. Ainsi l'ordre du sous-groupe engendré par $S = \{x\}$ est $|\langle S \rangle| = n$. □

On souhaite maintenant établir la caractérisation de l'ordre d'un élément donnée par le corollaire 1 ci-dessous. On donne d'abord la forme un peu plus générale suivante de ce résultat.

Proposition 7
Avec les mêmes hypothèses que précédemment, on définit, pour tout x de G, l'ensemble

$$E(x) = \left\{k \in \mathbb{Z} : x^k = e\right\}.$$

Alors $E(x)$ est un sous-groupe de $\mathbb{Z}$, qui est différent de $\{0\}$ si et seulement si x est d'ordre fini, auquel cas l'ordre de x est le générateur positif de $E(x)$.

Preuve.
L'ensemble $E(x)$ contient 0 et si k, ℓ sont dans $E(x)$ alors $x^{k-\ell} = e$ de sorte que $k - \ell \in E(x)$. Donc $E(x)$ est un sous-groupe de $\mathbb{Z}$ et, d'après la proposition 3, il existe $k_x \in \mathbb{N}$

tel que $E(x) = k_x\mathbb{Z}$. On a $k_x \neq 0$ si et seulement si $E(x) \neq 0$ si et seulement si il existe $k \in \mathbb{N}_{>0}$ tel que $x^k = e$. Cela équivaut par définition au fait que x est d'ordre fini. Si tel est le cas, on a vu dans la preuve de la proposition 3 que $k_x = \min\{k > 0 : k \in E(x)\}$ qui est par définition l'ordre de x. □

On déduit immédiatement le résultat suivant.

Corollaire 1
Soit x un élément d'ordre n de G. Alors on a, pour tout $m \in \mathbb{Z}$, l'équivalence

$$x^m = e \Leftrightarrow n \text{ divise } m.$$

4 Groupes monogènes et groupes cycliques

Pour alléger les notations, on note généralement $\langle x \rangle$ (au lieu de $\langle \{x\} \rangle$) le sous-groupe engendré par une partie $S = \{x\}$ réduite à un élément. Ce cas particulier important conduit à la notion de *groupe monogène*.

Définition 7
Un groupe G est dit monogène *s'il coïncide avec le sous-groupe engendré par un de ses éléments, autrement dit s'il existe $x \in G$ tel que $G = \langle x \rangle = \{x^k : k \in \mathbb{Z}\}$. Si de plus x est d'ordre fini n, on dit que G et* cyclique *d'ordre n, et on a alors $\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}$ (*cf *la preuve de la proposition 6).*

Exercice : Montrer que pour tout $n \geq 1$ le groupe $\mathbb{Z}/n\mathbb{Z}$ et le groupe des racines n-èmes de 1 dans $\mathbb{C}$ sont cycliques.

Remarque :

1) Un groupe monogène (en particulier un groupe cyclique) est automatiquement abélien.

2) L'ordre d'un groupe cyclique engendré par un élément x est égal à l'ordre de x, comme on l'a vu dans la preuve de la proposition 6.

Lemme 1
Soit $G = \langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}$ un groupe cyclique d'ordre n. Alors, pour tout $\ell \in \mathbb{Z}$, l'élément x^ℓ est d'ordre $\dfrac{n}{n \wedge \ell}$ où l'on rappelle la notation $n \wedge \ell = \text{pgcd}(n, \ell)$.

Preuve. Si D désigne le PGCD de ℓ et de n, on a

$$\begin{cases} n &= Dn' \\ \ell &= D\ell' \\ n' \wedge \ell' &= 1 \end{cases}.$$

On a alors les équivalences :

$$\left(x^{\ell}\right)^{m} = e \Leftrightarrow x^{\ell m} = e \Leftrightarrow n \mid \ell m \Leftrightarrow Dn' \mid D\ell' m \Leftrightarrow n' \mid \ell' m \Leftrightarrow n' \mid m \text{ (Gauss)}$$

ce qui signifie précisément que x^{ℓ} est d'ordre $n' = \dfrac{n}{n \wedge \ell}$. □

Théorème 1

1) *Les sous-groupes d'un groupe monogène sont monogènes.*

2) *Si G est un groupe cyclique d'ordre n, alors tous ses sous-groupes sont cycliques et leur ordre divise n. Inversement, pour tout diviseur d de n il existe un unique sous-groupe G_d de G d'ordre d et on a*

$$G_d = \left\langle x^{\frac{n}{d}} \right\rangle = \left\{ g \in G \mid g^d = e \right\}.$$

Preuve.

1) C'est la même démonstration que pour montrer que les sous-groupes de $\mathbb{Z}$ sont les $a\mathbb{Z}$, $a \in \mathbb{N}$.

Si $G = \langle x \rangle$ est un groupe monogène engendré par un élément x et si H est un sous-groupe de G alors ses éléments sont des puissances de x. Si H est réduit à l'élément neutre e, alors il est monogène (engendré par e). Sinon, il existe un exposant k non nul tel que x^k appartienne à H, auquel cas $x^{-k} = (x^k)^{-1}$ appartient aussi à H. L'un des deux entiers k ou $-k$ est strictement positif, et il existe donc un plus petit entier naturel non nul k_0 tel que x^{k_0} appartienne à H. On vérifie alors que $H = \left\langle x^{k_0} \right\rangle$: l'inclusion $\left\langle x^{k_0} \right\rangle \subset H$ est évidente et en sens inverse, si x^k appartient à H, on effectue la division euclidienne de k par k_0 ($k = k_0 q + r$, $0 \leq r < k_0$) et on constate que $x^r = x^k \left(x^{k_0}\right)^{-q}$ appartient à H, comme produit d'éléments de H, ce qui n'est possible que si $r = 0$, en vertu de la minimalité de k_0 (r est strictement inférieur à k_0), c'est-à-dire si k_0 divise k.

2) Soit $G = \langle x \rangle$ un groupe cyclique d'ordre n, ce qui signifie en particulier que x est d'ordre n. Comme G est monogène, ses sous-groupes sont monogènes d'après la première partie du théorème, donc cycliques puisqu'ils sont finis.

Si d est un diviseur de n, c'est-à-dire si $n = qd$ pour un certain entier q, alors le sous-groupe engendré par x^q est cyclique d'ordre d.

Montrons enfin l'unicité : pour cela considérons l'ensemble

$$G_d = \left\{ g \in G \mid g^d = e \right\}.$$

Pour qu'un élément $y = x^k$ de G appartienne à G_d, il faut et il suffit que $x^{kd} = e$, ce qui équivaut, par le corollaire 1, à la propriété que $n = qd$ divise kd, ou encore

q divise k. Par conséquent, $G_d = \langle x^q \rangle$ est un sous-groupe de G et il est d'ordre d. En outre, il est unique car tout sous-groupe d'ordre d de G est nécessairement cyclique d'après la première partie du théorème, donc engendré par un élément de G_d qui contient par définition tous les éléments d'ordre d de G.

Il reste à montrer que l'ordre d'un sous-groupe de G est nécessairement un diviseur de n. Soit H un tel sous groupe. Il existe donc un entier ℓ tel que

$$H = \left\langle x^\ell \right\rangle = \left\{ x^{\ell k}, k \in \mathbb{Z} \right\}$$

et l'ordre de H est égal à l'ordre de l'élément $y = x^\ell$, qui vaut $\dfrac{n}{n \wedge \ell}$ d'après le lemme précédent. En particulier, c'est un diviseur de n.

□

5 Classes modulo un sous-groupe et théorème de Lagrange

5.1 Classes modulo un sous-groupe

On débute par des rappels sur la notion de relation d'équivalence.

Définition 8
Une relation binaire $\mathcal{R}$ sur un ensemble E est une relation d'équivalence *si elle est*

- ***réflexive*** *:*
$$\forall x \in E, \qquad x \mathcal{R} x \tag{2.1}$$
- ***symétrique*** *:*
$$\forall x, y \in E, \qquad (x \mathcal{R} y) \Rightarrow (y \mathcal{R} x) \tag{2.2}$$
- ***transitive***
$$\forall x, y, z \in E, \qquad (x \mathcal{R} y \text{ et } y \mathcal{R} z) \Rightarrow x \mathcal{R} z \tag{2.3}$$

La classe d'équivalence d'un élément x de E , notée $\mathrm{Cl}_\mathcal{R}(x)$, est l'ensemble des éléments de E qui sont en relation avec x.

$$\mathrm{Cl}_\mathcal{R}(x) = \{ y \in E \mid x \mathcal{R} y \}. \tag{2.4}$$

L'ensemble quotient de E par la relation d'équivalence $\mathcal{R}$, noté $E/\mathcal{R}$, est l'ensemble des classes d'équivalence de E relativement à $\mathcal{R}$:

$$E/\mathcal{R} = \{ \mathrm{Cl}_\mathcal{R}(x) \mid x \in E \} \tag{2.5}$$

Proposition 8
L'ensemble des classes d'équivalence de E relativement à une relation d'équivalence $\mathcal{R}$ forme une partition de E, c'est-à-dire que les classes sont deux à deux disjointes *et que leur réunion est égale à E.*

Exemple: Soient A et B deux ensembles non vides et $f : A \to B$ une application. Sur A on a la relation d'équivalence $\mathcal{R}_f$ définie par $x\mathcal{R}_f y$ si $f(x) = f(y)$. Les classes d'équivalence pour $\mathcal{R}_f$ sont les images réciproques $f^{-1}(\{b\})$, où b parcourt l'image $f(A)$ de f. Sur l'ensemble quotient $A/\mathcal{R}_f$, on peut définir $\tilde{f}\colon A/\mathcal{R}_f \to B$ par $\tilde{f}(\bar{a}) = f(a)$, où $\bar{a}$ est la classe d'équivalence de $a \in A$ pour $\mathcal{R}_f$. On vérifie (exercice) que $\tilde{f}$ est bien définie (*i.e.* sa définition ne dépend pas d'un choix de représentant pour $\bar{a}$) et injective.

Étant donné un groupe G et un sous-groupe H de G, l'énoncé suivant donne la définition et les premières propriétés de deux relations d'équivalence sur G définies grâce à H.

Définition et proposition 1
Soit H un sous-groupe d'un groupe G.

1) *La relation $\mathcal{R}_H$ définie par*

$$x\mathcal{R}_H y \text{ si } x^{-1}y \in H$$

est une relation d'équivalence sur G. La classe d'équivalence d'un élément x est égale à $xH := \{xy \in G\colon y \in H\}$ ("classe ***à gauche*** *de x modulo H"). L'ensemble quotient est noté G/H.*

2) *De même, la relation $\mathcal{R}'_H$ définie par*

$$x\mathcal{R}'_H y \text{ si } yx^{-1} \in H$$

est une relation d'équivalence sur G, dont les classes d'équivalence sont les "classes ***à droite***" *$Hx := \{yx \in G\colon y \in H\}$, dont l'ensemble est noté $H\backslash G$.*

3) *La bijection $G \to G$, $x \mapsto x^{-1}$ induit une bijection de G/H sur $H\backslash G$; ces ensembles ont donc même cardinal. Quand ce cardinal commun est fini on le note $(G : H)$ et on l'appelle* indice *de H dans G.*

Preuve.

1) La relation $\mathcal{R}_H$ est réflexive puisque pour tout $x \in G$, $x^{-1}x = e \in H$ qui est un groupe. Elle est symétrique car $x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} = y^{-1}x \in H$ qui est un groupe. Enfin, elle est transitive puisque $x^{-1}y \in H, y^{-1}z \in H \Rightarrow (x^{-1}y)(y^{-1}z) = x^{-1}z \in H$ qui est un groupe.

2) Preuve similaire à celle de 1).

3) Il est clair que $x \mapsto x^{-1}$ est une bijection de G et que $z \in xH \Leftrightarrow z^{-1} \in Hx^{-1}$.

□

Exemple: Soit $n \in \mathbb{N}_{\geq 1}$. Dans le cas $G = \mathbb{Z}$, $H = n\mathbb{Z}$, on a pour $x, y \in \mathbb{Z}$:

$$x\mathcal{R}_H y \Leftrightarrow x\mathcal{R}'_H y \Leftrightarrow (x - y) \in n\mathbb{Z} \Leftrightarrow x \equiv y (\mathrm{mod}\ n)\,.$$

Le quotient $G/H = \mathbb{Z}/n\mathbb{Z}$ correspond donc comme attendu aux classes de congruence modulo n. On a $(G : H) = (\mathbb{Z} : n\mathbb{Z}) = |\mathbb{Z}/n\mathbb{Z}| = n$.

5.2 Théorème de Lagrange

Il s'agit du résultat très important suivant.

Théorème 2 (Lagrange)
Soit G un groupe fini, et H un sous-groupe de G. Alors on a la relation :

$$(G : H) = \frac{|G|}{|H|}\,.$$

En particulier l'ordre de H et l'indice de H dans G divisent l'ordre de G.

Preuve. Soit $a \in G$. L'application $H \to aH$ qui à h associe ah est une bijection. On déduit que deux classes à gauche quelconques de G sont toujours en bijection. Comme G est réunion disjointe de ses classes à gauche modulo H, on déduit le résultat. □

Corollaire 2
Si G est un groupe fini, alors son ordre est un multiple de l'ordre de chacun de ses éléments.

Corollaire 3
Tout groupe G d'ordre p premier est cyclique.

Preuve. En effet, l'ordre du sous-groupe de G engendré par tout élément $x \in G$ différent de e divise p et a au moins deux éléments. Ce sous-groupe est donc d'ordre p et x engendre G. □

On a la généralisation suivante du théorème de Lagrange (qui correspond à $K = \{e_G\}$).

Théorème 3
Soient G un groupe fini, H un sous-groupe de G et K un sous-groupe de H i.e. des groupes $K \subset H \subset G$. Alors on a la relation :

$$(G : K) = (G : H)\,(H : K)\,.$$

Preuve. On considère l'application $\varphi : G/K \to G/H, gK \mapsto gH$. Cette application est clairement bien définie car K est un sous-groupe de H. Elle est évidemment surjective. En outre, pour tout $gH \in G/H$, nous avons une bijection $H/K \to \varphi^{-1}(gH)$ donnée par $hK \mapsto ghK$ (et dont la réciproque est $xK \mapsto g^{-1}xK$). On en déduit immédiatement le résultat. □

6 Morphismes

6.1 Définitions

Définition 9
Une application φ d'un groupe G dans un groupe H est un morphisme de groupes *(ou* homomorphisme*) si*

$$\forall x \in G, \forall y \in G, \varphi(xy) = \varphi(x)\varphi(y).$$

Exercice : Décrire les morphismes de groupe $\varphi\colon \mathbb{Z} \to \mathbb{Z}$.

Exemples:

a) Si G est un groupe (quelconque) et x un élément fixé de G, l'application

$$\begin{array}{rccc} \varphi_x : & \mathbb{Z} & \longrightarrow & G \\ & k & \longmapsto & x^k. \end{array}$$

est un morphisme de groupes.

b) Notons $\zeta_n = \exp(2i\pi/n)$ et $U_n = \{z \in \mathbb{C} : z^n = 1\}$, pour $n \in \mathbb{N}_{>0}$. L'application $\mathbb{Z}/n\mathbb{Z} \to U_n$ définie par $\bar{k} \mapsto \zeta_n^k$ est un morphisme de groupes.

c) La signature $\varepsilon\colon S_n \to \{\pm 1\}$ est un morphisme de groupes.

Proposition 9
Soit $\varphi : G \to H$ un morphisme de groupes. Alors

1) $\varphi(e_G) = e_H$.

2) $\forall x \in G, \varphi(x^{-1}) = \varphi(x)^{-1}$.

Proposition 10

1) *La composée de deux morphismes est un morphisme.*

2) *Soit $\varphi : G \to H$ un morphisme de groupes* bijectif *alors φ^{-1} est un morphisme. On dit alors que φ est un* isomorphisme *; si de plus $G = H$, on dit que φ est un* automorphisme *de G.*

Donnons une application de la notion d'isomorphisme dans le cadre des groupes cycliques.

Proposition 11
Soit G un groupe cyclique d'ordre n, alors G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, i.e. il existe un isomorphisme $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to G$.

Preuve. Soit x un générateur de G. On définit φ comme étant le morphisme de groupes $\mathbb{Z}/n\mathbb{Z} \to G$ tel que $\varphi(\bar{k}) = x^k$ (vérifier qu'il est bien défini et que c'est un morphisme de groupes). Par définition de l'ordre, φ est une surjection et comme les deux groupes ont même ordre ; c'est un isomorphisme. □

Proposition 12
Soit $\varphi : G \to H$ un morphisme de groupes. Alors

1) *l'image d'un sous-groupe de G est un sous-groupe de H.*

2) *l'image inverse d'un sous-groupe de H est un sous-groupe de G.*

Remarque. Soit $\varphi\colon G \to H$ un morphisme de groupes, alors :

- Si $G = \langle x \rangle$ est monogène, son image par φ est un sous-groupe monogène de H (engendré par $\varphi(x)$).
- Si $G = \langle S \rangle$, pour une partie $S \subseteq G$, décrire φ, c'est déterminer l'image par φ des éléments $s \in S$.

6.2 Noyau, image

Définition 10
Soit $\varphi : G \to H$ un morphisme de groupes.

- *On appelle* noyau de φ *et on note* $\ker \varphi$ *l'ensemble des antécédents par φ de l'élément neutre e_H de H*

$$\ker \varphi = \{g \in G \mid \varphi(g) = e_H\}.$$

- *On appelle* image de φ *et on note* $\operatorname{Im} \varphi$ *l'ensemble des éléments de H admettant un antécédent par φ*

$$\operatorname{Im} \varphi = \{h \in H \mid \exists g \in G, \varphi(g) = h\}.$$

On obtient, comme corollaire immédiat de la proposition 12 :

Corollaire 4
Soit $\varphi : G \to H$ un morphisme de groupes. Le noyau de φ est un sous-groupe de G, et son image est un sous-groupe de H.

Proposition 13
Soit $\varphi : G \to H$ un morphisme de groupes. Alors φ est injectif si et seulement si $\ker \varphi = \{e_G\}$.

Remarque.

1) Si x est un élément fixé dans un groupe G, le noyau du morphisme

$$\begin{array}{rccc} \varphi_x : & \mathbb{Z} & \longrightarrow & G \\ & k & \longmapsto & x^k \end{array}$$

est un sous-groupe de $\mathbb{Z}$, donc de la forme $k_x\mathbb{Z}$ pour un entier naturel k_x convenable. C'est le groupe $E(x)$ de la proposition 7. Comme on l'a vu :

- $k_x = 0 \Leftrightarrow \varphi_x$ injectif $\Leftrightarrow x$ d'ordre infini.
- $k_x \neq 0 \Leftrightarrow x$ d'ordre fini égal à k_x.

2) Le morphisme de l'exemple b) de §6.1 est un isomorphisme.

3) Dès que $n \geq 2$ la signature (exemple c) de §6.1) est un morphisme surjectif de groupes.

Chapitre 3

Le groupe des permutations

1 Définitions et premières propriétés

Définition 1
Soit n un entier naturel non nul. L'ensemble des bijections de $\{1, \ldots, n\}$ dans lui-même s'appelle le groupe symétrique sur n éléments. On le note S_n. Ses éléments s'appellent des permutations.

Plus généralement, l'ensemble des bijections d'un ensemble fini E dans lui-même s'appelle le groupe des permutations de E.
Il y a exactement $n!$ façons de permuter les entiers de 1 à n. On a donc

$$|S_n| = n!$$

Remarque : on ne définit pas "S_0", moyennant quoi, dans la suite, l'écriture S_n sous-entendra toujours que n est un entier naturel non nul.

Une façon commode de noter les éléments de S_n est d'utiliser un tableau à 2 lignes, la première contenant les entiers de 1 à n, et la seconde leurs images.
Exemple :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix}$$

désigne la permutation de $\{1, \cdots, 5\}$ dans lui-même définie par

$$\sigma(1) = 5,\ \sigma(2) = 2,\ \sigma(3) = 4,\ \sigma(4) = 1 \text{ et } \sigma(5) = 3.$$

Sa bijection réciproque s'écrit

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}.$$

La composition des applications munit S_n d'une structure de groupe : la composée de deux permutations est une permutation, la composition est associative, S_n possède

un élément neutre (l'application "identité" qui applique chaque entier $i \in \{1, \dots, n\}$ sur lui-même), tout élément a un "inverse" (bijection réciproque).
Pour alléger les notations, on omettra le symbole "$\circ$" de la composition, c'est-à-dire qu'on écrira $\sigma\gamma$ pour désigner la composée $\sigma \circ \gamma$.
Si $n \geq 3$ ce groupe *n'est pas commutatif* : par exemple, les deux éléments

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ et } \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

de S_3 ne commutent pas (on a $\sigma_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ et $\sigma_2\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$).

Définition 2 (support)
Le support *d'une permutation $\sigma \in S_n$ noté* $\operatorname{Supp}\sigma$ *est le complémentaire dans* $\{1, \cdots, n\}$ *de l'ensemble* $\operatorname{Fix}\sigma$ *de ses points fixes. Autrement dit*

$$\operatorname{Supp}\sigma = \{i \in \{1, \dots, n\} \mid \sigma(i) \neq i\} \ , \ \operatorname{Fix}\sigma = \{i \in \{1, \dots, n\} \mid \sigma(i) = i\} \, .$$

Remarque : le support d'une permutation σ et son complémentaire sont stables par σ

$$\sigma(\operatorname{Supp}\sigma) = \operatorname{Supp}\sigma \, , \ \sigma(\operatorname{Fix}\sigma) = \operatorname{Fix}\sigma.$$

La notion de support apparait dans la proposition (fondamentale) suivante.

Proposition 1
Soient σ et γ deux éléments de S_n de supports disjoints. Alors $\sigma\gamma = \gamma\sigma$. Autrement dit, "deux permutations de supports disjoints commutent".

⚠ La réciproque est fausse : il se peut que deux permutations de supports non disjoints commutent. Par exemple, toute permutation commute avec elle-même !
Preuve. Comparons les images par $\sigma\gamma$ et $\gamma\sigma$ d'un élément x de $\{1, \dots, n\}$.

- Si x appartient au support de σ, alors il n'appartient pas au support de γ puisque ces deux supports sont disjoints, par hypothèse. Par conséquent, $\gamma(x) = x$ et

  $$\sigma\gamma(x) = \sigma(x). \tag{3.1}$$

  Par ailleurs $\sigma(x)$ appartient lui aussi au support de σ, puisque celui-ci est stable par σ (*cf.* remarque précédente), et n'appartient donc pas au support de γ. Par conséquent,

  $$\gamma(\sigma(x)) = \sigma(x). \tag{3.2}$$

  En comparant (3.1) et (3.2) on conclut que $\sigma\gamma(x) = \gamma(\sigma(x))$.

- Le raisonnement serait le même, en échangeant les rôles de σ et γ, si on supposait que x appartient au support de γ.

- Enfin, si x n'appartient à aucun des deux supports, alors $\sigma\gamma(x) = \gamma\sigma(x) = x$.

□

Définition 3 (orbite)
Soit $x \in \{1, \dots, n\}$ et $\sigma \in S_n$. On appelle orbite de x sous l'action de σ l'ensemble

$$\mathrm{Orb}_\sigma(x) := \left\{ \sigma^k(x) : k \in \mathbb{Z} \right\}.$$

Proposition 2
Soit $\sigma \in S_n$. Pour tout $x \in \{1, \dots, n\}$, il existe un plus petit entier naturel non nul k tel que $\sigma^k(x) = x$. On a alors $\mathrm{Orb}_\sigma(x) = \{x, \sigma(x), \dots, \sigma^{k-1}(x)\}$, en particulier les éléments $\sigma^\ell(i)$, $0 \leq \ell \leq k-1$, sont deux à deux distincts.

Preuve. Le groupe S_n est d'ordre fini donc σ est d'ordre fini. Si l'on note d cet ordre on a bien sûr $\sigma^d(x) = x$. L'ensemble $\{k \geq 1 : \sigma^k(x) = x\}$ est donc non vide et minoré car inclus dans $\mathbb{N}$. Cet ensemble admet un plus petit élément k.
Soit $m \in \mathbb{Z}$ un entier. La division euclidienne de m par k s'écrit $m = kq + r$, avec $0 \leq r < k$. On a $\sigma^m(x) = \sigma^r(x)$ ce qui démontre que $\mathrm{Orb}_\sigma(x)$ ne contient pas d'autres éléments que $x, \sigma(x), \dots, \sigma^{k-1}(x)$. Enfin s'il existe des entiers $k-1 \geq i > j \geq 0$ avec $\sigma^i(x) = \sigma^j(x)$ on déduit $\sigma^{i-j}(x) = x$ ce qui contredit la minimalité de k. Cela démontre la seconde partie de l'assertion. □

Exercice : Montrer que le cardinal de l'orbite d'un élément de $\{1, \dots, n\}$ sous l'action d'une permutation $\sigma \in S_n$ divise l'ordre de σ comme élément de S_n.

2 Cycles

2.1 Définitions et propritétés

Définition 4
Soient n un entier naturel non nul, et k un entier compris entre 2 et n. Un élément σ de $S_n \setminus \{\mathrm{Id}\}$ s'appelle un cycle de longueur k (ou k-cycle) s'il existe une partie $\{a_1, a_2, \dots, a_k\}$ de $\{1, \dots n\}$ telle que

- $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3, \dots, \sigma(a_{k-1}) = a_k$, $\sigma(a_k) = a_1$
- $\mathrm{Supp}\,\sigma = \{a_1, a_2, \dots, a_k\}$.

Un tel cycle se note : $\sigma = (a_1, a_2, \dots, a_k)$.

Autrement dit, un k-cycle est un élément de S_n qui permute circulairement les éléments d'une partie à k éléments de $\{1, \dots n\}$ et fixe les autres :

$$a_1 \to a_2 \to \cdots a_{k-1} \to a_k \to a_1.$$

Exemple: Dans S_4 le cycle $(1,2,4)$ désigne la permutation

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

⚠ Un même k-cycle peut s'écrire de k façons distinctes. Plus précisement, les k écritures suivantes

$$(a_1, a_2, \ldots, a_k)\,,\ (a_2, a_3, \ldots, a_k, a_1)\,,\ \ldots,\ (a_k, a_1, a_2 \ldots, a_{k-1})$$

désignent toutes le même cycle.

À l'inverse, le support d'un cycle ne suffit pas à le définir : dans S_4, les cycles $(1,2,4)$ et $(1,4,2)$ ont même support mais sont distincts (exercice : combien y a-t-il de cycles distincts de support donné ? Combien y a-t-il de cycles de longueur k dans S_n ?).

Proposition 3
L'ordre d'un k-cycle est égal à k.

Un cas particulier important est celui des cycles de longueur 2, que l'on appelle *transpositions*.

Proposition 4
Toute permutation peut s'écrire comme produit de transpositions.

⚠ cette décomposition n'est pas unique !

Preuve. Récurrence sur le cardinal du support de σ : si $x \in \operatorname{Supp}\sigma$ et si τ désigne la transposition $(x, \sigma(x))$ alors le support de $\sigma' := \tau\sigma$ est contenu strictement dans celui de σ. En effet, comme x et $\sigma(x)$ appartiennent à $\operatorname{Supp}\sigma$, $\operatorname{Fix}\sigma \subset \operatorname{Fix}\sigma'$. Mais par ailleurs, par construction, $x \in \operatorname{Fix}\sigma' \setminus \operatorname{Fix}\sigma$. □

2.2 Conjugué d'un cycle par une permutation

On conclut la section en débutant, dans le cas du groupe S_n, l'étude de la *conjugaison* dans un groupe. Il s'agit là d'un aspect très important en théorie des groupes. Il reviendra fréquemment dans la suite du cours.

Définition 5 (Conjugaison)
Dans un groupe G noté multiplicativement le conjugué *d'un élément $x \in G$ par un élément $g \in G$ est l'élément gxg^{-1} de G.*
La classe de conjugaison *de $x \in G$ est l'ensemble des conjugués de x dans G : c'est la partie $\{gxg^{-1} : g \in G\}$ de G.*

Remarque. La propriété, pour 2 éléments de G, d'être conjugués, est une relation déquivalence sur G.

Exercice. Montrer que pour tout groupe G et tout $g \in G$, l'application $\gamma_g \colon G \to G$ définie par $\gamma_g(x) = gxg^{-1}$ est un automorphisme de G. Un tel automorphisme est dit *intérieur*.

Remarque. Notons que dans un groupe abélien, la conjugaison est une opération triviale puisque dans ce cas, pour tous $x, g \in G$, $gxg^{-1} = xgg^{-1} = x$. En particulier, pour tout g, $\gamma_g = \mathrm{Id}$.

On dispose d'une formule commode pour la conjugaison d'un cycle par une permutation de S_n.

Proposition 5
Soit $2 \leq k \leq n$ des entiers et soit $(a_1, a_2, \ldots, a_k)$ un k-cycle de S_n. Pour tout $\gamma \in S_n$, on a

$$\gamma(a_1, a_2, \ldots, a_k)\gamma^{-1} = (\gamma(a_1), \gamma(a_2), \ldots, \gamma(a_k)) .$$

En particulier le conjugué d'un k-cycle est encore un k-cycle.

Preuve. On évalue les membres de gauche et de droite en $\gamma(a_i)$. Dans les deux cas cela donne $\gamma(a_{i+1})$ (resp. $\gamma(a_1)$) si $i < k$ (resp. si $i = k$). Pour un indice $\ell \in \{1, \ldots, n\} \setminus \{a_1, \ldots, a_k\}$, l'évaluation des membres de gauche et de droite en $\gamma(\ell)$ donne $\gamma(\ell)$. On a donc l'égalité de permutations annoncée. □

3 Décomposition en cycles disjoints

Proposition 6
Les orbites sous l'action d'une permutation σ de S_n fournissent une partition de l'ensemble $\{1, \ldots, n\}$. Plus précisément, il existe des éléments x_1, x_2, …, x_r dans $\{1, \ldots, n\}$ tels que $\{1, \ldots, n\}$ soit la réunion disjointe *des orbites* $\mathrm{Orb}_\sigma(x_1)$, …, $\mathrm{Orb}_\sigma(x_r)$ *:*

$$\{1, \ldots, n\} = \bigsqcup_{i=1}^{r} \mathrm{Orb}_\sigma(x_i).$$

Preuve. On remarque que la relation "appartenir à la même orbite sous l'action de σ" est une relation d'équivalence sur $\{1, \ldots, n\}$. La réflexivité et la symétrie sont évidentes. La transitivité est une conséquence du fait que deux orbites sont soit confondues, soit disjointes. En effet, si $\mathrm{Orb}_\sigma(x) \cap \mathrm{Orb}_\sigma(y) \neq \emptyset$, il existe $i, j \in \mathbb{Z}$ tels que $\sigma^i(x) = \sigma^j(y)$, d'où $y = \sigma^{i-j}(x)$, dont on déduit immédiatement $\mathrm{Orb}_\sigma(x) = \mathrm{Orb}_\sigma(y)$. Les orbites sont donc par définition les classes d'équivalence modulo cette relation et on en déduit la proposition. □
Le théorème suivant est fondamental. Il fournit une décomposition "canonique" pour toute permutation.

Théorème 1
Toute permutation différente de l'identité se décompose de façon essentiellement unique comme produit commutatif *de cycles disjoints. Autrement dit, pour tout $\sigma \in S_n \setminus \{\mathrm{Id}\}$ il existe des cycles $c_1, \ldots, c_s$ à supports disjoints tels que*

$$\sigma = c_1 c_2 \ldots c_s$$

et cette décomposition est unique à l'ordre près des facteurs.

Preuve.

- **Existence :** soient $\Omega_1 = \mathrm{Orb}_\sigma(x_1), \Omega_2 = \mathrm{Orb}_\sigma(x_2), \ldots, \Omega_s = \mathrm{Orb}_\sigma(x_s)$ les orbites de σ *non réduites à un point*. Elles forment une partition du support de σ, dont on note les cardinaux $k_1, k_2, \ldots, k_s$ respectivement. On considère alors les cycles

$$\begin{aligned} c_1 &= \left(x_1, \sigma(x_1), \cdots, \sigma^{k_1-1}(x_1)\right), \\ c_2 &= \left(x_2, \sigma(x_2), \cdots, \sigma^{k_2-1}(x_2)\right), \\ &\vdots \\ c_s &= \left(x_s, \sigma(x_s), \cdots, \sigma^{k_s-1}(x_s)\right) \end{aligned}$$

  et on vérifie immédiatement que $\sigma = c_1 c_2 \cdots c_s$.

- **Unicité :** elle est claire car les cycles sont déterminés par σ. □

Corollaire 1
L'ordre d'une permutation est égale au ppcm des longueurs des cycles à supports disjoints qui la composent.

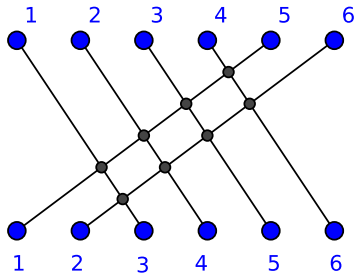
4 Signature et groupe alterné

Définition 6
Soit $\sigma \in S_n$. On dit que σ réalise une inversion *sur le couple (i, j) si $i < j$ et $\sigma(i) > \sigma(j)$. On note $I(\sigma)$ le nombre d'inversions réalisées par σ. La signature de σ est le nombre*

$$\epsilon(\sigma) = (-1)^{I(\sigma)}.$$

Autrement dit, $\epsilon(\sigma)$ vaut $+1$ ou -1 selon que σ réalise un nombre pair ou impair d'inversions.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$$



$$\varepsilon(\sigma) = (-1)^8 = +1$$

Proposition 7

1) *La signature d'une permutation $\sigma \in S_n$ est donnée par la formule*

$$\varepsilon(\sigma) = \prod_{\{i,j\} \in \mathcal{P}} \frac{\sigma(i) - \sigma(j)}{i - j}$$

où le produit est pris sur l'ensemble $\mathcal{P}$ des paires $\{i, j\}$ d'éléments de $\{1, \ldots, n\}$.

2) *Une transposition est de signature -1.*

3) *La signature est un morphisme de groupes $S_n \to \{\pm 1\}$:*

$$\forall \sigma \in S_n, \forall \gamma \in S_n, \ \varepsilon(\sigma\gamma) = \varepsilon(\sigma)\varepsilon(\gamma).$$

Ce morphisme est surjectif dès que $n \geq 2$; son noyau est alors un sous-groupe d'indice 2 de S_n appelé groupe alterné. *On note ce sous-groupe A_n.*

Preuve.

1) On voit que le membre de droite est

- bien défini car $\dfrac{\sigma(i) - \sigma(j)}{i - j} = \dfrac{\sigma(j) - \sigma(i)}{j - i}$, donc indépendant de l'ordre de la paire $\{i, j\}$;

- par définition du même signe que $\varepsilon(\sigma)$;
- de valeur absolue 1 car, puisque σ est une bijection, l'ensemble des couples $\{\sigma(i), \sigma(j)\}$ est égal à l'ensemble des couples $\{i, j\}$.

2) Notons $i < j$ les termes échangés par la transposition, de sorte qu'elle est égale à

$$\begin{pmatrix} 1 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & n \\ 1 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & n \end{pmatrix}.$$

Les paires en inversion sont les paires de la forme $\{i, k\}$ avec k compris entre $i+1$ et j et celles de la forme $\{k, j\}$ avec k compris entre $i+1$ et $j-1$. Au total, il y a $(j-i)+(j-i-1)$ soit un nombre impair d'inversions, et l'imparité de la permutation en découle.

3) Il suffit d'écrire

$$\begin{aligned} \varepsilon(\sigma\gamma) &= \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma\gamma(i) - \sigma\gamma(j)}{i-j} \\ &= \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma\gamma(i) - \sigma\gamma(j)}{\gamma(i) - \gamma(j)} \prod_{\{i,j\}\in\mathcal{P}} \frac{\gamma(i) - \gamma(j)}{i-j} \\ &= \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma(i) - \sigma(j)}{i-j} \prod_{\{i,j\}\in\mathcal{P}} \frac{\gamma(i) - \gamma(j)}{i-j} \end{aligned}$$

la dernière égalité étant justifiée par le fait que γ induit une bijection de $\mathcal{P}$ sur lui-même.

Ainsi $\varepsilon\colon S_n \to \{\pm 1\}$ est un morphisme de groupes. Comme la signature d'une transposition vaut -1, ce morphisme est surjectif pour $n \geq 2$. Enfin si τ est une transposition de S_n, les classes à gauche A_n et τA_n de S_n modulo A_n sont distinctes et leur réunion vaut S_n (en effet, si $\varepsilon(\sigma) = -1$, alors $\sigma = \tau(\tau\sigma)$ avec $\tau\sigma \in A_n$). Donc A_n est d'indice 2 dans S_n.

□

Proposition 8

1) *La signature d'un k-cycle est égale à* $(-1)^{k-1}$.

2) *Soit* $c_1 c_2 \dots c_s$ *la décomposition en cycles à supports disjoints d'une permutation* $\sigma \in S_n$. *On note r le nombre de points fixes de* σ. *On a alors*

$$\varepsilon(\sigma) = (-1)^{n-(s+r)}.$$

Preuve.

1) On remarque que tout k-cycle peut se décomposer (de manière non canonique) comme produit de $k-1$ transpositions

$$(i_1, i_2, \ldots, i_k) = (i_1, i_k) \circ (i_1, i_{k-1}) \circ \cdots \circ (i_1, i_2) \ .$$

La signature étant un morphisme de groupes dont la valeur en toute transposition est -1, on conclut.

2) C'est un corollaire immédiat du point précédent et de la multiplicativité de la signature (i.e. du fait que la signature est un morphisme) : en notant k_i la longueur du cyle c_i, on a

$$\varepsilon(\sigma) = (-1)^{(\sum_{i=1}^{s} k_i)-s} = (-1)^{n-r-s}.$$

□

Remarques : en combinant les propositions 4 et 7, on constate que la signature d'une permutation σ est égale à $+1$ (resp. -1) si σ se décompose en un produit d'un nombre *pair* (resp. *impair*) de transpositions. Ceci constitue un moyen de calcul efficace de la signature si l'on dispose d'une décomposition en produit de transpositions.
En combinant le théorème 1 et la preuve du point 1) de la proposition précédente, on retrouve le fait qu'une permutation se décompose en produit de transpositions (proposition 4).

Chapitre 4

Actions de groupes

Dans ce chapitre, on généralise la notion d'action d'un groupe sur un ensemble telle qu'entrevue au chapitre précédent avec l'action de S_n sur $\{1, \dots, n\}$, ainsi que divers concepts qui s'y rapportent, comme celui d'orbite.

1 Définition et exemples

Définition 1
Soit X un ensemble et G un groupe (noté multiplicativement et de neutre noté e). Une action de G sur X *est la donnée d'une application :*

$$G \times X \to X, \qquad (g, x) \mapsto g \cdot x$$

vérifiant

(a) $\forall g, h \in G, \forall x \in X,\ g \cdot (h \cdot x) = (gh) \cdot x,$

(b) $\forall x \in X,\ e \cdot x = x.$

Exemples. 1. La définition du groupe S_n des permutations de $\{1, \dots, n\}$ induit une action évidente de S_n sur $X = \{1, \dots, n\}$.
2. Le groupe $\mathrm{GL}_n(\mathbb{R})$ agit (par multiplication à gauche) sur les vecteurs colonnes de taille n à coefficients réels.
3. Tout groupe G agit sur l'ensemble de ses sous-groupes par conjugaison : étant donné $g \in G$ et H un sous-groupe de G, le conjugué gHg^{-1} de H est encore un sous-groupe de G.
4. Étant donné un groupe G quelconque et un sous-groupe H de G fixé, le groupe G agit sur l'ensemble quotient G/H (classes à gauche de G modulo H) via $(g, aH) \mapsto (ga)H$.

Donnons une caractérisation très utile de la notion d'action de groupes en termes de morphismes. Si X est un ensemble quelconque, on note $\mathrm{Sym}(X)$ le groupe des

bijections $f : X \to X$ muni de la composition des applications.

Proposition 1
Avec les mêmes notations que dans la définition, la donnée d'une action de G sur X est équivalente à la donnée d'un morphisme de groupes $\rho : G \to \mathrm{Sym}(X)$.

Preuve. Il s'agit d'une simple réécriture des axiomes (a) et (b) définissant ce qu'est une action. En effet à partir de la donnée d'une action de G sur X, on peut définir une application :

$$\rho : G \to \mathrm{Sym}(X), \qquad g \mapsto (x \mapsto g \cdot x).$$

Remarquons que G est bien à valeurs dans $\mathrm{Sym}(X)$ car les axiomes (a) et (b) impliquent que $(x \mapsto g \cdot x)$ est bijective, de bijection réciproque $(x \mapsto g^{-1} \cdot x)$. L'axiome (a) de la définition implique que ρ est un morphisme de groupes. Réciproquement étant donné un morphisme $\rho : G \to \mathrm{Sym}(X)$, on a une action de G sur X définie pour $g \in G$ et $x \in X$ par :

$$g \cdot x = \rho(g)(x).$$

Le fait que ρ est un morphisme implique que (a) et (b) de la définition sont satisfaits. □

Exercice. Montrer que le noyau du morphisme correspondant à l'action par multiplication à gauche de G sur ses classes gauche G/H modulo un sous-groupe H fixé est $\cap_{a \in G} aHa^{-1}$.

2 Orbite et stabilisateur

On fixe un groupe G (noté multiplicativement) et un ensemble X sur lequel G agit.

Définition 2
Étant donné $x \in X$, on appelle orbite de x sous l'action de G *l'ensemble :*

$$\mathrm{Orb}(x) = \{g \cdot x : g \in G\}.$$

Il s'agit d'un sous-ensemble de X.
On appelle stabilisateur de x *le sous-groupe de G :*

$$\mathrm{Stab}(x) = \{g \in G : g \cdot x = x\}.$$

Exercice. Soit G un groupe agissant sur un ensemble X. Montrer que si $x, y \in X$ sont dans la même orbite alors leurs stabilisateurs sont conjugués. Que dire de l'assertion réciproque ?

Proposition 2
Si un groupe G agit sur un ensemble X alors X est réunion disjointe des orbites pour cette action.

Preuve. On procède comme pour la preuve de la proposition 6 du chapitre 3. La relation sur X définie par $x\mathcal{R}y$ ssi $y \in \mathrm{Orb}(x)$ est une relation d'équivalence. En effet, elle est réflexive car $x = e \cdot x$ et elle est symétrique car $y = g \cdot x$ ssi $x = g^{-1} \cdot y$. Enfin, elle est transitive car si $y = g \cdot x$ et $z = g' \cdot y$ alors $z = (g'g) \cdot x$. Les classes d'équivalence pour $\mathcal{R}$ sont donc les orbites de l'action et le résultat se déduit immédiatement de la proposition 8 du chapitre 2. □
Remarque. Si $G = S_n$ est le groupe symétrique et si l'on se donne $\sigma \in S_n$ et $i \in \{1, \ldots, n\}$ alors la partie $\mathrm{Orb}_\sigma(i)$ de $\{1, \ldots, n\}$ définie dans le chapitre précédent est l'orbite de i sous l'action du sous-groupe $\langle\sigma\rangle$ de S_n.

Définition 3
S'il n'y a qu'une seule orbite dans l'action d'un groupe G sur un ensemble X, on dit que l'action est transitive.

On note par exemple que S_n (et aussi A_n si $n \geq 3$) agit transitivement sur $\{1, \ldots, n\}$. On note également que, dans le cas général, si G agit sur X, alors l'action induite sur chaque orbite est transitive.

Le résultat suivant énonce une propriété fondamentale des actions de groupes.

Théorème 1 (Relation orbite-stabilisateur et équation des classes)
Soit G un groupe agissant sur un ensemble X alors pour tout $x \in X$ l'application

$$\varphi_x \colon G/\mathrm{Stab}(x) \to \mathrm{Orb}(x)\,, \qquad g\mathrm{Stab}(x) \mapsto g \cdot x$$

est une bijection. En particulier si G est fini, on a la relation orbite-stabilisateur *:*

$$|\,\mathrm{Orb}(x)| \times |\mathrm{Stab}(x)| = |G|\,,$$

c'est-à-dire l'indice de $\mathrm{Stab}(x)$ *dans G est* $|\,\mathrm{Orb}(x)|$.
*Enfin, si G et X sont finis, on déduit l'égalité suivante (*équation des classes*) :*

$$|X| = \sum_{i=1}^{r} \frac{|G|}{|\mathrm{Stab}(x_i)|}\,,$$

où les orbites dans l'action de G sur X sont $\mathrm{Orb}(x_1), \ldots, \mathrm{Orb}(x_r)$.

Preuve. Montrons déjà que φ_x est bien définie. Si $g\mathrm{Stab}(x) = h\mathrm{Stab}(x)$ alors il existe $s \in \mathrm{Stab}(x)$ tel que $g = hs$. On a alors $g \cdot x = (hs) \cdot x$. Cette dernière quantité vaut $h \cdot (s \cdot x) = h \cdot x$ car s stabilise x. Donc $\varphi_x(g\mathrm{Stab}(x)) = \varphi_x(h\mathrm{Stab}(x))$.
La surjectivité de φ_x est évidente. Quant à l'injectivité, l'égalité $g \cdot x = h \cdot x$ implique $(h^{-1}g) \cdot x = x$ i.e. $h^{-1}g \in \mathrm{Stab}(x)$. Donc $g \in h\mathrm{Stab}(x)$ i.e. $g\mathrm{Stab}(x) = h\mathrm{Stab}(x)$.

L'assertion concernant l'indice de $\mathrm{Stab}(x)$ dans G se déduit alors du théorème de Lagrange puisque

$$\frac{|G|}{|\mathrm{Stab}(x)|} = |G/\mathrm{Stab}(x)| = |\,\mathrm{Orb}(x)|.$$

Quant à l'équation des classes, elle provient de la relation orbite-stabilisateur combinée avec la proposition 2. □

Remarque. Dans le cas où G est infini, la relation orbite-stabilisateur prend la forme suivante : pour tout $x \in X$, soit $\mathrm{Orb}(x)$, soit $\mathrm{Stab}(x)$ est infini.

Exemple. Soit G un groupe. On considère son action sur lui-même par conjugaison (cf la définition 5 du chapitre précédent) : étant donné $g, x \in G$, on définit

$$g \cdot x = gxg^{-1}\,.$$

Pour cette action, l'orbite de $x \in G$ est sa classe de conjugaison. On remarque que $\mathrm{Orb}(x) = \{x\}$ si et seulement si x commute avec tous les éléments de G. Cette propriété donne lieu à la définition suivante.

Définition 4 (Centre d'un groupe)
Soit G un groupe (noté multiplicativement). Le centre *de G est l'ensemble de tous les éléments de $x \in G$ tels que*

$$\forall g \in G,\ gxg^{-1} = x\,,$$

de manière équivalente c'est l'ensemble des $x \in G$ dont la classe de conjugaison est réduite à $\{x\}$. Le centre de G, noté $Z(G)$ est un sous-groupe abélien de G.

Pour conclure avec l'exemple, on écrit l'équation des classes pour l'action par conjugaison d'un groupe fini G sur lui-même :

$$|G| = |Z(G)| + \sum_{i=1}^{k} |\mathrm{Cl}_{\mathrm{conj}}(x_i)| = |Z(G)| + \sum_{i=1}^{k} \frac{|G|}{|\mathrm{Stab}(x_i)|}\,,$$

où $\{x_1, \ldots, x_k\}$ est un ensemble de représentants pour les classes de conjugaison (notées $\mathrm{Cl}_{\mathrm{conj}}$) de G ayant > 1 éléments (si G est abélien, cette somme, alors vide, vaut 0).

On conclut ce chapitre avec un théorème donnant une forme de "réciproque faible" au théorème de Lagrange.

Théorème 2 (Cauchy)
Soit G un groupe fini d'ordre divisible par un nombre premier p. Alors il existe dans G un élément d'ordre p.

Preuve. Notons $n = |G|$. On a par hypothèse $p \mid n$. On considère

$$X = \{(g_1, \ldots, g_p) \in G^p : g_1 \cdots g_p = e\}\,.$$

On a $|X| = n^{p-1}$: en effet la donnée d'un élément de X est la donnée d'un $(p-1)$-uplet quelconque $(g_1, \cdots, g_{p-1})$ d'éléments de G. L'élément g_p correspondant est alors l'inverse du produit $g_1 \cdots g_{p-1}$.
Soit σ la permutation de X définie par

$$\sigma(g_1, \ldots, g_p) = (g_2, \cdots, g_p, g_1)\,.$$

Il s'agit bien d'une permutation de X, comme on voit en conjugant les 2 membres de l'égalité $g_1 \cdots g_p = e$ par g_1^{-1}. Il est par ailleurs facile d'expliciter la permutation réciproque de σ. On a bien sûr $\sigma^p = \mathrm{Id}$ de sorte que l'on a une action de $\mathbb{Z}/p\mathbb{Z}$ sur X *via* le morphisme de groupes :

$$\mathbb{Z}/p\mathbb{Z} \to \mathrm{Sym}(X)\,, \qquad \bar{r} \mapsto \sigma^r\,.$$

Le stabilisateur d'un élément quelconque de X est un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$. Ce stabilisateur est donc soit $\mathbb{Z}/p\mathbb{Z}$ tout entier, soit trivial. Si $(g_1, \ldots, g_p) \in X$ a pour stabilisateur $\mathbb{Z}/p\mathbb{Z}$, cela signifie que $g_1 = g_2 = \ldots = g_p$ et donc l'orbite de cet élément est réduite à lui-même. En particulier $(e, \ldots, e)$ est un tel élément. D'après la relation orbite-stabilisateur, les éléments de X dont le stabilisateur est trivial ont une orbite à p éléments. En notant s le nombre d'orbites ponctuelles et r le nombre d'orbites à p éléments on obtient

$$n^{p-1} = pr + s\,.$$

Comme $p \mid n$, on déduit $p \mid s$. Or on a vu que $s \geq 1$: ainsi $s \geq p$ et il existe donc un élément de X distinct de $(e, \ldots, e)$ de stabilisateur trivial, i.e. il existe $g \in G \setminus \{e\}$ tel que $(g, \ldots, g) \in X$.

□

Chapitre 5

Sous-groupes distingués, groupes quotients et théorème de factorisation

1 Sous-groupes distingués et groupes quotients

On a vu comment définir dans un groupe G l'ensemble des classes à gauche G/H (resp. à droite $H\backslash G$) modulo un sous-groupe H. Le fait d'associer à un élément quelconque $g \in G$ sa classe à gauche gH modulo H définit une application surjective $\pi\colon G \to G/H$, appelée *surjection canonique*. (On pourrrait aussi considérer la surjection analogue $G \to H\backslash G$.)

Deux questions naturelles, et apparemment indépendantes, se posent :

1) À quelle condition a-t-on coïncidence entre "classes à gauche" et "classes à droite" ?

2) À quelle condition peut-on munir l'ensemble quotient G/H (resp. $H\backslash G$) d'une structure de groupe ? Peut-on assurer de plus que $\pi\colon G \to G/H$ devient alors un morphisme de groupes ?

Les deux questions admettent la même réponse, qui repose sur la notion de sous-groupe *distingué* (ou *normal*).
Pour commencer, examinons la situation de $\mathbb{Z}/n\mathbb{Z}$ que nous avons pu munir d'une addition (voir le premier chapitre). À cette occasion, il est apparu que si la définition choisie pour l'addition de $\mathbb{Z}/n\mathbb{Z}$ avait bien un sens, c'était grâce à la propriété fondamentale suivante :

$$\left\{ \begin{array}{rcll} x' & \equiv & x & \mod n \\ y' & \equiv & y & \mod n \end{array} \right. \Rightarrow x' + y' \equiv x + y \mod n$$

Pour imiter cette démarche dans le cas général, on a envie, pour définir une loi de groupe sur G/H, de poser $xHyH := xyH$ (de sorte que $G \to G/H$ soit un morphisme). Mais cette définition est-elle bien indépendante d'un choix de représentants ?

Précisément, à quelle(s) condition(s) a-t-on, pour tout $x, x', y, y' \in G$:

$$\begin{cases} x'H &= xH \\ y'H &= yH \end{cases} \Rightarrow x'y'H = xyH \text{ ?}$$

Définition et proposition 1
On dit que H est distingué *ou* normal *dans G si l'une des 4 assertions équivalentes suivantes est satisfaite*

1) $\forall y \in G, \forall h \in H, y^{-1}hy \in H$

2) $\forall y \in G, y^{-1}Hy \subset H$

3) $\forall y \in G, y^{-1}Hy = H$

4) $\forall y \in G, Hy = yH$

Notation : $H \triangleleft G$.

Preuve. 1) $\Rightarrow$ 2) et 3) $\Rightarrow$ 4) $\Rightarrow$ 1) sont triviales.
Quant à 2) $\Rightarrow$ 3), il suffit de remplacer y par y^{-1} dans 2) pour obtenir $yHy^{-1} \subset H$ i.e. $H \subset y^{-1}Hy$. □

Clairement, cette propriété apporte une réponse à la première question posée en préambule de cette section : si $H \triangleleft G$, alors les classes à droite et à gauche de tout élément de G coïncident, c'est-à-dire que les relations d'équivalence $\mathcal{R}$ et $\mathcal{R}'$ du chapitre 2 sont égales. En particulier les ensembles de classes d'équivalence correspondants G/H et $H\backslash G$ sont les mêmes.

Si l'on revient au problème de munir G/H d'une structure de groupe (telle que $\pi : G \to G/H$ soit un morphisme de groupes), on voit que si H est distingué dans G alors en supposant

- $x'H = xH$, c'est-à-dire s'il existe $h \in H$ tel que $x' = xh$,
- $y'H = yH$, c'est-à-dire s'il existe $k \in H$ tel que $y' = yk$,

on déduit

$$x'y' = xhyk = xy(y^{-1}hy)k \in xyH \text{ et donc } x'y'H = xyH\,.$$

On obtient donc une loi de composition interne bien définie sur G/H en posant

$$\forall x \in G,\ \forall y \in G,\ xHyH := xyH$$

Il reste à voir que la loi ainsi définie est bien une loi de groupe :

- la loi est associative,

- elle possède un élément neutre, à savoir la classe de e, c'est-à-dire H, puisque $H\,(xH) = (xH)\,H = xH$ pour tout $x \in G$. En résumé, $e_{G/H} = H$,
- tout élément de G/H admet un inverse : pour tout $x \in G$ on a $(xH)\left(x^{-1}H\right) = \left(x^{-1}H\right)(xH) = (xx^{-1})H = H = e_{G/H}$, autrement dit, $(xH)^{-1} = x^{-1}H$.

En résumé, la propriété pour H d'être distingué dans G est donc une condition *suffisante* pour que G/H admette un structure de groupe compatible avec la loi de groupe de G (i.e telle que la surjection canonique $\pi\colon G \to G/H$ soit un morphisme de groupes).

Définition 1
Si H est un sous-groupe distingué de G, on appelle groupe quotient *de G par H l'ensemble des classes à gauche G/H muni de la loi de groupe :*

$$(xH)\cdot(yH) := (xyH),\ (x, y \in G)\,.$$

On montre facilement que cette condition est également nécessaire. En effet, pour pouvoir munir G/H d'une loi de groupe, il faut en particulier que pour tous $x, y \in G$, et tout $h \in H$, on ait $xhy = xyk$ avec $k \in H$ ou encore $y^{-1}hy \in H$.
On résume tout cela dans l'énoncé suivant :

Théorème 1
Soit G un groupe et H un sous-groupe de G.
• Si $H \triangleleft G$, il existe sur G/H une unique structure de groupe telle que la surjection canonique $\pi\colon G \to G/H$ soit un morphisme. Elle est définie par $xH \cdot yH = xyH$.
• Réciproquement si G/H admet une structure de groupe telle que la surjection canonique $\pi\colon G \to G/H$ est un morphisme de groupes, alors $H \triangleleft G$.

Exemples :

- Si G est abélien, tous ses sous-groupes sont distingués.
- Dans S_3, le sous-groupe engendré par (123) est distingué. En revanche, le sous-groupe engendré par (12) ne l'est pas.

Proposition 1 (Un sous-groupe d'indice 2 est toujours distingué)
Si G est un groupe et H est un sous-groupe de G tel que $(G : H) = 2$ alors $H \triangleleft G$.

Preuve. Par hypothèse il y a deux classes à gauche de G modulo H : la classe triviale H et une classe s'écrivant aH pour un $a \notin H$. Comme $a \notin H$ on a également exactement deux classes *à droite* : H et Ha. Par disjonction des classes (à droite ou à gauche) distinctes, on déduit $aH = Ha$. Prenons maintenant un $x \in G$ quelconque. Soit $x \in H$ et alors $xH = Hx = H$ car H est un sous-groupe. Sinon $x \in aH = Ha$ et donc $xH = Hx$. Dans tous les cas on a montré $xH = Hx$. □

Application : le groupe alterné A_n, d'ordre $n!/2$, est distingué dans le groupe symétrique S_n d'ordre $n!$.

Remarque. Si G est fini on a plus généralement : si H est un sous-groupe de G d'indice p, le plus petit diviseur premier de $|G|$, alors $H \triangleleft G$. (Cf TD.)

> **Proposition 2**
> *Si $H \triangleleft G$ et π est la surjection canonique associée, alors l'ensemble des sous-groupes de G qui contiennent H est en bijection avec l'ensemble des sous-groupes de G/H via l'application $K \mapsto \pi(K)$, l'application réciproque étant donnée par $K' \mapsto \pi^{-1}(K')$.*

Preuve.
Comme π est un morphisme de groupes, on a : si K est un sous-groupe de G alors $\pi(K)$ est un sous-groupe de G/H et si K' est un sous-groupe de G/H alors $\pi^{-1}(K')$ est un sous-groupe de G.
Ensuite, on a toujours $\pi(\pi^{-1}(K')) = K'$ et d'autre part, $\pi^{-1}(\pi(K)) = KH = \{kh \,|\, k \in K,\, h \in H\}$ puisque $\pi(x) = \pi(y)$ ssi il existe $h \in H$ tel que $y = xh$. Mais si $H \subset K$, $KH = K$. □

2 Sous-groupes distingués et morphismes

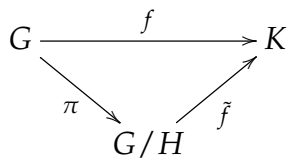
2.1 Le théorème de factorisation

La preuve de la proposition suivante est immédiate.

> **Proposition 3**
> *Soit $\varphi : G \to H$ un morphisme de groupes. Si $K \triangleleft H$ est un sous-groupe distingué de H alors $\varphi^{-1}(K) \triangleleft G$ est un sous-groupe distingué de G. En particulier, le noyau d'un morphisme de groupe $\varphi : G \to H$ est un sous-groupe distingué dans G.*
> *Si $L \triangleleft G$ est un sous-groupe distingué de G alors $\varphi(L) \triangleleft \operatorname{Im}\varphi$ est un sous-groupe distingué de $\operatorname{Im}\varphi$. En particulier, si φ est surjectif, on a $\varphi(L) \triangleleft H$.*

En particulier on retrouve le fait que $A_n \triangleleft S_n$. Aussi, en considérant le morphisme "déterminant" $\mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$, on déduit que $\mathrm{SL}_n(\mathbb{R}) \triangleleft \mathrm{GL}_n(\mathbb{R})$.
On en déduit aussi que dans la proposition 2, l'ensemble des sous-groupes distingués de G qui contiennent H est en bijection avec l'ensemble des sous-groupes distingués de G/H par la même application.

> **Théorème 2**
> *Soit $f : G \longrightarrow K$ un morphisme de groupes et H un sous-groupe normal de G. On suppose $H \subset \ker f$. Alors il existe un unique morphisme de groupes $\tilde{f} : G/H \longrightarrow K$ tel que $f = \tilde{f} \circ \pi$, où π désigne la projection canonique de G sur G/H.*



- *En particulier, f induit un isomorphisme $G/\ker f \to \operatorname{Im} f$.*

Preuve. On définit $\tilde{f}$ par $\tilde{f}(xH) = f(x)$. Comme $H \subset \ker f$, $\tilde{f}$ est bien définie puisque pour tout $h \in H$, $f(xh) = f(x)f(h) = f(x)e_K = f(x)$. On voit facilement que $\tilde{f}$ est un morphisme de groupes puisque

$$\tilde{f}(xHyH) = \tilde{f}(xyH) = f(xy) = f(x)f(y) = \tilde{f}(xH)\tilde{f}(yH).$$

On a évidemment $\operatorname{Im}\tilde{f} = \operatorname{Im} f$.
En outre, si $H = \ker f$, on a $\tilde{f}(xH) = e_K \Leftrightarrow f(x) = e_K \Leftrightarrow x \in \ker f \Leftrightarrow xH = H$ i.e. $\tilde{f}$ est injective. Donc dans ce cas, $\tilde{f}$ est un *isomorphisme* de $G/\ker f$ sur $\operatorname{Im} f$.

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & K \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ G/\ker f & \xrightarrow[\tilde{f}]{\sim} & \operatorname{Im} f \end{array}$$

□

Exemples :

- Le morphisme
$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{C}\setminus\{0\} \\ & x & \longmapsto & e^{2i\pi x} \end{array}$$
a pour noyau
$$\ker f = \mathbb{Z},$$
pour image
$$\operatorname{Im} f = U = \{z \in \mathbb{C} \mid |z| = 1\}$$
et induit donc un isomorphisme $\tilde{f} : \mathbb{R}/\mathbb{Z} \longrightarrow U$.

- Si x est un élément d'ordre n dans un groupe G, le morphisme
$$\begin{array}{rccc} \varphi_x: & \mathbb{Z} & \longrightarrow & G \\ & k & \longmapsto & x^k \end{array},$$
de noyau $\ker\varphi_x = n\mathbb{Z}$, induit un isomorphisme $\mathbb{Z}/n\mathbb{Z} \simeq \langle x\rangle$.

- *Via* le morphisme de signature ε, on a $S_n/A_n \simeq \{\pm 1\}$ pour $n \geq 2$, et *via* le morphisme "déterminant" on a $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \simeq \mathbb{R}^\times$.

Corollaire 1
Soient G un groupe et K, H deux sous-groupes distingués de G avec $K \subset H$. Alors $(G/K)/(H/K)$ est isomorphe à G/H.

Preuve. Remarquons que d'une part, K étant distingué dans G, il est a fortiori distingué dans H et d'autre part, d'après la proposition 3, H/K est un sous-groupe distingué de G/K. Le morphisme $G/K \to G/H$, $gK \mapsto gH$ est évidemment surjectif, et son noyau est H/K, d'où le résultat par le théorème 2. □

2.2 Groupes quotients et actions de groupes

• Rappelons que la donnée d'une action d'un groupe G sur un ensemble X est équivalente à la donnée d'un morphisme de groupes $\rho\colon G \to \mathrm{Sym}(X)$ (cf chapitre précédent). En combinant cela au théorème de factorisation, on obtient

Théorème 3 (Théorème de Cayley)
Tout groupe fini G à n éléments est isomorphe à un sous-groupe du groupe symétrique S_n.

Preuve. On fait agir G sur lui-même par multiplication à gauche : $g \cdot x = gx$ pour tout $g, x \in G$. Notons ρ le morphisme correspondant à cette action. Alors $\rho\colon G \to \mathrm{Sym}(G)$ passe au quotient (d'après le théorème 2) par $\ker\rho$ et induit un morphisme injectif de groupes

$$G/\ker\rho \to \mathrm{Sym}(G)\,.$$

De plus $\ker\rho$ est trivial puisque seul $\rho(e)$ a des points fixes. Par ailleurs G a n éléments et donc le groupe $\mathrm{Sym}(G)$ est isomorphe à S_n, ce qui conclut la preuve. □

• Une autre conséquence du théorème de factorisation est la suivante : la donnée d'une action d'un groupe G quelconque sur un ensemble fini X est équivalente à la donnée de l'action d'un quotient *fini* de G sur X. En effet, en notant ρ le morphisme correspondant à l'action de G sur X, on a, par le même argument que dans la preuve du théorème de Cayley, un morphisme injectif $G/\ker\rho \to \mathrm{Sym}(X)$. Comme X est fini, $\mathrm{Sym}(X)$ est fini et donc $(G : \ker\rho)$ est fini.

• Les actions de groupes ont une importance centrale en théorie des groupes, mais aussi en géométrie, en théorie des nombres, etc... On illustre ici dans le cadre d'un exercice la puissance de la notion d'action de groupe en démontrant une généralisation du théorème de Cauchy (théorème 2 du chapitre précédent). Soit G un groupe fini d'ordre $p^a m$ où p est premier et $a, m \in \mathbb{N}$ sont tels que $m \geq 1$ et $p \nmid m$. Un *p-sous-groupe de Sylow* de G est un sous-groupe de G d'ordre p^a.

Exercice. On souhaite montrer, en conservant les notations ci-dessus, que G admet toujours un p-sous-groupe de Sylow (on notera que l'on peut supposer $a \geq 1$, puisque le résultat est trivialement vrai dans le cas contraire).

1) Soit $\mathcal{S}$ l'ensemble des parties de G à p^a éléments. Montrer que G agit sur S par multiplication à gauche et que le cardinal de $\mathcal{S}$ est premier à p.

2) Soit $\mathcal{S}_1$ une orbite dans l'action de G sur $\mathcal{S}$ de cardinal non divisible par p. Justifier l'existence de $\mathcal{S}_1$ et montrer que pour un élément quelconque $X \in \mathcal{S}_1$ le stabilisateur $P := \mathrm{Stab}(X)$ est d'ordre divisible par p^a.

3) Fixons un $X \in \mathcal{S}_1$. Justifier que P agit sur X par multiplication à gauche et que l'orbite d'un élément quelconque $x \in X$ dans cette action est de cardinal $|P|$.

4) Déduire $p^a \geq |P|$, puis conclure.

Chapitre 6

Anneaux

On débute dans ce chapitre l'étude d'une structure relative à *deux* lois de composition interne. Le point de départ est un groupe abélien dont on note "$+$" la loi. Si l'ensemble en question est muni d'une seconde loi vérifiant certains axiomes et compatibilités vis à vis de la loi "$+$", on dit alors que c'est un *anneau*. On croise ce type de structure en permanence en mathématiques : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $M_n(\mathbb{R})$, $\mathbb{Z}/n\mathbb{Z}$, $\mathrm{End}(E)$, $\mathbb{Q}[X]$,... sont des anneaux.

1 Définitions

Définition 1
Un anneau est la donnée d'un triplet $(A, +, \cdot)$ *où* A *est un ensemble et* $+$ *et* $\cdot$ *sont deux lois de composition internes telles que*

1) $(A, +)$ *est un* groupe abélien *d'élément neutre noté* 0.

2) *La multiplication est* associative *:* $\forall (a, b, c) \in A^3$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

3) *La multiplication est* distributive par rapport à l'addition*, ce qui signifie que pour tout* $(a, b, c) \in A^3$

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad et \qquad (b + c) \cdot a = b \cdot a + c \cdot a\,.$$

4) *La multiplication possède un* élément neutre *noté* 1 *(on dit que l'anneau* A *est* unitaire*) caractérisé par la propriété*

$$\forall a \in A\ ,\ a \cdot 1 = 1 \cdot a = a.$$

De plus, l'anneau A *est dit* **commutatif** *si la multiplication est commutative.*

Remarque : dans certains ouvrages, seuls les trois premiers axiomes ci-dessus sont demandés pour définir un anneau (*i.e.* on n'exige pas qu'il y ait un élément neutre

pour la multiplication). Dans ce cas, un anneau vérifaint l'axiome 4) ci-dessus est appelé anneau *unitaire*.

Proposition 1
$(A, +, \cdot)$ un anneau.

1) *$\forall x \in A,\ 0 \cdot x = x \cdot 0 = 0$.*

2) *L'élément neutre pour $\cdot$ est unique.*

3) *Si $A \neq \{0\}$ alors $0 \neq 1$.*

4) *$\forall x, y \in A, x \cdot (-y) = (-x) \cdot y = -x \cdot y$.*

Preuve.

1) $x = (1+0)x = 1x + 0x = x + 0x \Rightarrow 0x = 0$. On montre de même $x \cdot 0 = 0$.

2) Si 1 et $1'$ sont éléments neutres pour la multiplication alors $1 \cdot 1' = 1$ et $1 \cdot 1' = 1'$.

3) Si $0 = 1$ alors $\forall x \in A$, $x = 1x = 0x = 0$.

4) $(-x)y + xy = (-x + x)y = 0$. De même $x \cdot (-y) + xy = x \cdot (-y + y) = 0$.

□

Dans la suite on omettra le plus souvent de préciser les lois relatives à la structure d'anneau : on écrira "soit A un anneau" et l'on sous-entendra alors que les lois correspondantes sont notées "$+$" et "$\cdot$".
Une différence majeure entre $+$ et $\cdot$: tous les éléments ne sont pas nécessairement inversibles pour la multiplication. Cette remarque induit la définition suivante.

Définition 2
Un élément a de A est dit inversible *s'il existe $b \in A$ tel que $ab = ba = 1$. L'ensemble des éléments inversibles (aussi appelés* unités*) de A est noté $A^\times$ ou $U(A)$.*

Remarque : certains auteurs parlent d'inverse à droite et à gauche (un élément peut avoir un inverse à droite mais pas à gauche...).

Exercice : Montrer que si $a \in A$ admet un inverse à droite et un inverse à gauche alors ils sont uniques et sont égaux (mieux : si $a \in A$ admet un unique inverse à droite, alors il admet un inverse à gauche...).

Proposition 2
Si A est un anneau, $A^\times$ est un groupe multiplicatif de neutre 1.

Exercice. Déterminer $A^\times$ lorsque $A = \mathbb{Z}, \mathbb{R}, \mathbb{Q}[X], \mathbb{Z}/n\mathbb{Z}, \{a + ib \colon a, b \in \mathbb{Z}\}$.

Définition 3 (Éléments nilpotents, diviseurs de zéros, anneaux intègres)
Soit A un anneau.

1) *Un élément $a \in A$ est dit* nilpotent *s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$.*

2) *Un élément $a \in A$ est* diviseur de zéro *s'il est non nul et s'il existe soit un élément $b \in A \setminus \{0\}$ tel que $ab = 0$ (on dit que a est* diviseur de zéro à gauche*), soit un élément $c \in A \setminus \{0\}$ tel que $ca = 0$ (on dit que a est* diviseur de zéro à droite*).*

3) *L'anneau A est* intègre *s'il est commutatif, si $1 \neq 0$, et s'il n'admet pas diviseur de zéro.*

4) *Un anneau commutatif est un* corps *si $1 \neq 0$ et si tout élément non nul est inversible pour la multiplication.*

Exemples. • Les anneaux $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}[X]$ sont intègres. Les anneaux $\mathbb{Z}/6\mathbb{Z}$ (cf propositon ci-dessous), $M_n(\mathbb{R})$ ($n \geq 2$) ne sont pas intègres.
• $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps. $\mathbb{Z}$ n'est pas un corps.

Remarque. Les éléments nilpotents et les diviseurs de zéro ne sont bien sûr jamais inversibles. Un corps est intègre, mais la réciproque n'est pas toujours vraie. En revanche cette réciproque est vraie pour un anneau fini : un anneau fini est intègre si et seulement si c'est un corps. (Exercice : démontrer toutes les affirmations contenues dans cette remarque.)

Exercice. Montrer que si A est intègre alors, pour $f, g \in A[X]$, on a $\deg(fg) = \deg(f) + \deg(g)$. En déduire que $A[X]$ est intègre et que $(A[X])^\times = A^\times$.

Proposition 3
Soit $n \in \mathbb{Z}_{\geq 1}$, alors $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ où les lois sont définies par

$$\bar{a} + \bar{b} = \overline{a+b}\,,$$
$$\bar{a} \times \bar{b} = \overline{ab}\,,$$

est un anneau. De plus on a les équivalences :

$$\mathbb{Z}/n\mathbb{Z} \text{ est intègre } \Leftrightarrow \mathbb{Z}/n\mathbb{Z} \text{ est un corps } \Leftrightarrow n \text{ est premier.}$$

Définition 4 (Sous-anneau et produit cartésien d'anneaux)
1) *Un sous-anneau d'un anneau A est une partie B de A telle que*

(a) $(B, +)$ est un sous-groupe de $(A, +)$,

(b) B est stable pour la multiplication,

(c) 1_A appartient à B.

2) *Si A et B sont deux anneaux, leur produit cartésien $A \times B$ est canoniquement muni d'une structure d'anneau en posant :*

- $(x, y) + (x', y') = (x + x', y + y')$,
- $(x, y) \cdot (x', y') = (xx', yy')$

les éléments neutres pour l'addition et la multiplication étant définis respectivement par $0_{A\times B} = (0_A, 0_B)$ et $1_{A\times B} = (1_A, 1_B)$.

Proposition 4
Si A est un anneau et B est un sous-anneau de A alors B est un anneau pour les lois induites par celles de A.

Tout comme dans le cas des groupes, il est souvent commode, pour montrer qu'un ensemble est un anneau, de montrer que c'est un sous-anneau d'un anneau le contenant (exemple : pour montrer que $\mathbb{Z}[i] := \{a + ib : a, b \in \mathbb{Z}\}$ est un anneau, on peut commencer par remarquer que $\mathbb{Z}[i] \subseteq \mathbb{C}$).
On conclut cette section avec deux formules calculatoires souvent utiles dans les exercices.

Proposition 5 (Binôme de Newton)
Soit A un anneau et a, b des éléments de A dont on suppose qu'ils commutent *i.e. $ab = ba$. Alors pour tout $n \in \mathbb{Z}_{\geq 1}$, on a :*

1) $(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$,

2) $a^n - b^n = (a - b) \sum_{j=1}^{n} a^{n-j} b^{j-1}$.

2 Morphismes d'anneaux

De même que pour les groupes, les espaces vectoriels... on porte un intérêt particulier aux applications respectant la structure d'anneaux.

Définition 5
Soient A et B deux anneaux. Une application $f : A \to B$ est un morphisme d'anneaux *si*

1) *c'est un morphismes de groupes additifs de $(A, +)$ dans $(B, +)$,*

2) $\forall (x, y) \in A^2$, $f(xy) = f(x)f(y)$,

3) $f(1_A) = 1_B$.

Exemples.

1) Pour $n \geq 1$, la surjection canonique $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est un morphisme d'anneaux.

2) La conjugaison complexe $a + ib \mapsto a - ib$ est un morphisme d'anneaux $\mathbb{C} \to \mathbb{C}$.

3) Soit $\alpha = 2^{1/3}$ l'unique solution réelle à l'équation $x^3 = 2$. On note $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_r\alpha^r : a_i \in \mathbb{Q}, r \in \mathbb{N}\} = \{a_0 + a_1\alpha + a_2\alpha^2 : a_i \in \mathbb{Q}\}$; c'est un sous-anneau de $\mathbb{C}$ (et même de $\mathbb{R}$). L'application d'évaluation

$$\mathrm{eval}_\alpha : \mathbb{Q}[X] \to \mathbb{Q}[\alpha], \qquad f(X) \mapsto f(\alpha),$$

est un morphisme d'anneaux.

4) Soit $P \in \mathrm{GL}_n(\mathbb{R})$. L'application $A \mapsto P^{-1}AP$ de $M_n(\mathbb{R})$ dans lui-même est un morphisme d'anneaux.

Définition 6
Soit $f : A \to B$ un morphisme d'anneaux. Le noyau *de f est*

$$\ker f := \{x \in A : f(x) = 0\}$$

et l'image de f est $\mathrm{Im}(f) := f(A)$.
Si f est injectif (i.e. $\ker f = \{0\}$*) et surjectif (i.e.* $\mathrm{Im}(f) = B$*), on dit que f est un* isomorphisme *d'anneaux.*

⚠ Si $f : A \to B$ est un morphisme d'anneaux, $\mathrm{Im}(f)$ est un sous-anneau de B, mais $\ker f$ n'est pas un sous-anneau de A en général, puisque f doit vérifier $f(1_A) = 1_B$.

3 L'anneau $\mathbb{Z}/n\mathbb{Z}$ et le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$

3.1 Théorème chinois et l'indicatrice d'Euler

Donnons pour commencer l'énoncé du théorème des restes chinois.

Proposition 6 (Th. des restes chinois)
Soit a, b deux entiers premiers entre eux alors l'application

$$\mathbb{Z}/ab\mathbb{Z} \to (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z}), \qquad x \bmod ab \mapsto (x \bmod a, x \bmod b),$$

est un isomorphisme d'anneaux.

Preuve. Il est facile de vérifier que l'application est un morphisme d'anneaux. Elle est en outre injective car si x est divisible par a et par b, il est divisible par ab en vertu du lemme de Gauss puisque a et b sont premiers entre eux. Enfin $\mathbb{Z}/ab\mathbb{Z}$ et $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$ ont même cardinal ab donc l'application est bijective.

Remarquons cependant que l'on peut expliciter la réciproque de cette application. En effet, puisque $\text{pgcd}(a,b) = 1$ il existe par le théorème de Bézout $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. On vérifie alors immédiatement que pour tout $(y \bmod a, z \bmod b) \in (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$, l'image de $x = ybv + zau \bmod ab \in \mathbb{Z}/ab\mathbb{Z}$ dans $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$ est égale à $(y \bmod a, z \bmod b)$.

□

Soit $n \in \mathbb{Z}_{\geq 1}$. Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, on s'intéresse maintenant au groupe des unités $(\mathbb{Z}/n\mathbb{Z})^\times$. Rappelons les caractérisations déjà vues de l'inversibilité d'une classe modulo n.

Proposition 7
Soit n un entier naturel non nul. Alors, pour tout entier relatif k, les propriétés suivantes sont équivalentes :

1) *la classe de k modulo n est inversible pour la multiplication.*

2) *la classe de k modulo n est un générateur du groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$.*

3) *k est premier à n.*

Preuve. Les trois propriétés sont toutes des conséquences du fait que $\text{pgcd}(k,n) = 1$ ssi il existe $(u,v) \in \mathbb{Z}^2$ tel que $ku + nv = 1$ (corollaire du théorème de Bézout). □

On rappelle la définition de *l'indicatrice d'Euler* d'un entier $n \geq 1$: il s'agit de la fonction φ définie par $\varphi(1) = 1$, et pour tout $n \geq 2$:

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times .$$

On commence par établir une formule qui d'une part permet en principe de calculer $\varphi(n)$ récursivement, et jouera d'autre part un rôle important dans la démonstration de la cyclicité de $(\mathbb{Z}/p\mathbb{Z})^\times$ pour p premier (voir la section 3.2).

Proposition 8
Soit $n \in \mathbb{Z}_{\geq 1}$. On a l'égalité :

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

Preuve. Comme $\mathbb{Z}/n\mathbb{Z}$ est cyclique, il y a pour tout diviseur d de n, un unique sous-groupe (nécessairement cyclique) d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$. Ce sous-groupe est donc isomorphe à $\mathbb{Z}/d\mathbb{Z}$ et admet donc $\varphi(d)$ générateurs d'après la proposition 7. On partitionne $\mathbb{Z}/n\mathbb{Z}$ en :

$$\bigcup_{d|n} S_d , \qquad S_d := \{\bar{a} : |\langle \bar{a} \rangle| = d\} ,$$

et l'on obtient donc l'égalité annoncée. □

La proposition 6 permet de retrouver très facilement la multiplicativité de la fonction indicatrice d'Euler, modulo le lemme suivant :

Lemme 1

1) *Si $f : A \longrightarrow B$ est un isomorphisme d'anneaux, alors $B^\times = f(A^\times)$.*

2) *Si A et B sont deux anneaux, alors $(A \times B)^\times = A^\times \times B^\times$.*

Preuve. Exercice □

Appliqué à l'isomorphisme $\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ **(pour a et b premiers entre eux)**, ce lemme entraîne que

$$(\mathbb{Z}/ab\mathbb{Z})^\times \simeq (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times \text{ si } a \wedge b = 1$$

(on aurait pu également utiliser la proposition 7 et le fait que $c \wedge a = 1$ et $c \wedge b = 1$ ssi $c \wedge ab = 1$).
On en déduit immédiatement, en comparant les cardinaux, la formule

$$\varphi(ab) = \varphi(a)\varphi(b) \text{ si } a \wedge b = 1.$$

On déduit une formule explicite pour la valeur de $\varphi(n)$ lorsque l'on connait la factorisation en produit de nombres premiers de n.

Proposition 9

1) *Si p est un nombre premier et k un entier naturel non nul, on a*

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

2) *Si n est un entier naturel non nul et si P_n désigne l'ensemble des nombres premiers qui le divisent, on a*

$$\varphi(n) = n \prod_{p \in P_n} (1 - \frac{1}{p}).$$

Preuve.

1) Comme p est premier, les entiers compris entre 1 et p^k qui ne sont *pas* premiers avec p^k sont ceux qui s'écrivent $p\ell$ avec $1 \leq \ell \leq p^{k-1}$. Ils sont donc au nombre de p^{k-1} et $\varphi(p^k) = p^k - p^{k-1}$.

2) Si $n = p_1^{k_1} \dots p_r^{k_r}$ avec les p_i premiers et deux à deux distincts, et les $k_i \geq 1$, il suffit d'utiliser la multiplicativité de la fonction φ pour obtenir

$$\varphi(n) = \varphi(p_1^{k_1}) \dots \varphi(p_r^{k_r}) = p_1^{k_1-1}(p_1-1) \dots p_r^{k_r-1}(p_r-1)$$

$$= p_1^{k_1} \dots p_r^{k_r} \frac{p_1-1}{p_1} \dots \frac{p_r-1}{p_r} = n \prod_{i=1}^{r} (1 - \frac{1}{p_i}).$$

□

3.2 Corps finis, sous-groupes multiplicatifs finis d'un corps

On a vu précédemment que, si p est premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps, que l'on note traditionnellement $\mathbb{F}_p$. L'étude systématique des corps finis dépasse le cadre de ce cours. Signalons simplement, sans aucune démonstration, que le cardinal d'un corps fini est nécessairement une puissance d'un nombre premier, et que réciproquement, pour tout entier $q = p^k$ (p premier, k entier ≥ 1), il existe, à isomorphisme près, un unique corps de cardinal q, noté $\mathbb{F}_q$.
On va démontrer un résultat de structure très important.

Théorème 1
*Soit K un corps commutatif et G un sous-groupe **fini** du groupe multiplicatif $K^\times$. Alors G est cyclique. En particulier, pour tout nombre premier p, le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$.*

Preuve. On note $n = |G|$. Soit d un diviseur de n et soit $\psi(d)$ le nombre d'éléments de G d'ordre d. Supposons que G admette un élément a d'ordre d et soit $H = \langle a \rangle$. Chaque élément de H est une puissance de a et donc satisfait l'équation $x^d = 1$. Comme G est une partie d'un corps, il y a au plus d solutions dans G à l'équation $x^d = 1$ (cf corollaire 1 du chapitre suivant). Ainsi par cardinalité $H = \{x \in G : x^d = 1\}$. Ainsi, si $\psi(d) \neq 0$, H contient tous les éléments d'ordre d de G. Il y a $\varphi(d)$ tels éléments (c'est le nombre de générateurs d'un groupe cyclique d'ordre d). En écrivant, d'après le théorème de Lagrange et la proposition 8,

$$n = \sum_{d|n} \psi(d) = \sum_{d|n} \varphi(d)\,,$$

on déduit que $\psi(d) = \varphi(d)$ pour tout diviseur d de n. En particulier $\psi(n) \neq 0$. □

4 Idéal d'un anneau

On définit maintenant la notion très importante d'idéal : les idéaux jouent, pour les anneaux, le rôle que les sous-groupes distingués jouent en théorie des groupes. Dans cette section A désigne un anneau *commutatif*.

Définition 7
Un idéal *I de A est un sous-groupe additif de A vérifiant :*

$$\forall a \in A,\ \forall x \in I,\ a \cdot x \in I\,.$$

Exemples. • Les idéaux de $\mathbb{Z}$ sont les $d\mathbb{Z}$, pour $d \in \mathbb{N}$. En effet les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les $d\mathbb{Z}$ et l'on vérifie immédiatement que pour tout $n \in \mathbb{Z}$ et tout $x \in d\mathbb{Z}$, on a encore $nx \in d\mathbb{Z}$.

• Soit $P \in \mathbb{Q}[X]$: l'ensemble des multiples de P (i.e. l'ensemble $\{P \cdot Q \colon Q \in \mathbb{Q}[X]\}$ est un idéal de $\mathbb{Q}[X]$). On dit qu'il s'agit de *l'idéal engendré* par P (cf définition suivante).

Remarque. On peut définir la notion d'idéal dans le cadre plus général d'un anneau non nécessairement commutatif. Dans ce cas la définition 7 correspond à la notion d'idéal *à gauche*. On obtient la défintion *d'idéal à droite* en remplaçant la seconde condition par : "pour tout $a \in A$ et tout $x \in I$, on a $x \cdot a \in I$".

Proposition 10
Soit B un anneau commutatif et $f \colon A \to B$ un morphisme d'anneaux. Alors l'image réciproque de tout idéal de B est un idéal de A. En particulier $\ker f$ *est un idéal de A. D'autre part, l'image directe d'un idéal de A est un idéal de* $\operatorname{Im} f$*. En particulier, si f est surjectif, l'image d'un idéal est un idéal.*

Exemple. On reprend un exemple vu plus haut : soit $\alpha = 2^{1/3}$ l'unique solution réelle à l'équation $x^3 = 2$. On note $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_r\alpha^r \colon a_i \in \mathbb{Q}, r \in \mathbb{N}\}$. L'application d'évaluation

$$\operatorname{eval}_\alpha \colon \mathbb{Q}[X] \to \mathbb{Q}[\alpha]\,, \qquad f(X) \mapsto f(\alpha)\,,$$

est un morphisme d'anneaux. Son noyau est un idéal de $\mathbb{Q}[X]$; c'est l'ensemble des polynômes à coefficients rationnels qui s'annulent en α :

$$\ker \operatorname{eval}_\alpha = \{P \in \mathbb{Q}[X] \colon P(\alpha) = 0\}\,.$$

Définition et proposition 1 (Idéal engendré)
Soit Λ un ensemble d'indices et $(I_\lambda)_{\lambda\in\Lambda}$ une famille d'idéaux de A, alors l'intersection $\cap_{\lambda\in\Lambda} I_\lambda$ est encore un idéal de A.
Soit S une partie de A ; l'idéal engendré par *S est l'intersection des idéaux de A contenant S. Au sens de l'inclusion, c'est le plus petit idéal de A contenant S. On note en général $\langle S\rangle$ (ou bien $(x_1, \ldots, x_s)$ lorsque $S = \{x_1, \ldots, x_s\}$ est fini) l'idéal engendré par S et on peut décrire ses éléments :*

$$\langle S\rangle = \left\{ \sum_{\text{finie}} a_i x_i \colon a_i \in A,\ x_i \in S \right\}\,.$$

Dans le cas où $S = \{x\}$ pour un $x \in A$, l'idéal $\langle S\rangle$ est alors noté (x) ou Ax. Il est appelé idéal principal *engendré par x. On a*

$$(x) = \{ax \colon a \in A\}\,.$$

On accorde une attention particulière aux idéaux principaux ; il sont notamment au cœur du chapitre suivant. Notons déjà que si $u \in A^\times$, alors $(u) = A$. En particulier A est un idéal principal de A engendré par 1. Donnons tout de suite une première utilisation des idéaux principaux (0) et $(1) = A$.

Proposition 11
Un anneau commutatif A est un corps si et seulement si il contient exactement deux idéaux distincts : (0) *et* $(1) = A$.

Preuve. Supposons que A est un corps et soit I un idéal de A alors, si $I \neq (0)$, il existe dans I un $x \neq 0$. C'est un élément de $A^\times$ et donc $A = (x) \subseteq I$.
Réciproquement si (0) et (1) sont les seuls idéaux de A (et s'ils sont distincts), alors fixons $x \in A \setminus \{0\}$. Bien sûr $(x) \neq (0)$, et donc $(x) = (1)$. Ainsi $1 \in (x)$ i.e. il existe $y \in A$ tel que $xy = 1$. On a montré que x est inversible. □

Outre l'intersection d'idéaux, utilisée dans la notion d'idéal engendré, on définit la somme et le produit d'idéaux.

Définition et proposition 2
Soit I, J des idéaux de A.

1) *L'ensemble $I + J := \{a + b : a \in I, b \in J\}$,* somme des idéaux I et J *est encore un idéal de A. C'est l'idéal de A engendré par $I \cup J$ (une telle réunion n'est pas un idéal en général).*

2) *L'idéal engendré par $\{xy : x \in I, y \in J\}$ est noté IJ ; il est appelé* idéal produit de I et J.

Remarques. On a toujours $IJ \subseteq I \cap J$. Dans le cas $A = \mathbb{Z}$ la somme d'idéaux $a\mathbb{Z} + b\mathbb{Z}$ (resp. l'intersection $a\mathbb{Z} \cap b\mathbb{Z}$) est l'idéal $d\mathbb{Z}$ où $d = \text{pgcd}(a, b)$ (resp. $m\mathbb{Z}$ où $m = \text{ppcm}(a, b)$).
Notons enfin que si $a, b \in A$ alors l'idéal produit $(a)(b)$ est l'idéal engendré par ab.

5 Anneaux quotients

On développe et on justifie, dans cette section, le fait que les idéaux jouent, dans la théorie des anneaux, le rôle joué par les sous-groupes distingués en théorie des groupes. Dans cette section A désigne un anneau commutatif dont on note, comme précédemment "$+$" et "$\cdot$" les lois. L'hypothèse simplificatrice "A commutatif" n'est en fait pas nécessaire à la construction d'anneaux quotients : dans le cas général où A n'est pas supposé commutatif, l'idéal I relativement auquel on construit le quotient est alors supposé *bilatère* (i.e. I est simultanément un idéal à gauche et à droite).

5.1 Structure quotient et théorème de factorisation

Soit I un idéal de A. La relation binaire $\mathcal{R}_I$ sur A :

$$x \mathcal{R}_I y \text{ si } x - y \in I$$

est une relation d'équivalence. C'est en effet une conséquence du fait que I est un sous-groupe additif de A. On note A/I l'ensemble des classes d'équivalence pour la relation $\mathcal{R}_I$. Un élément de A/I (qu'on appelle *classe de A modulo I*) est une partie de A de la forme

$$x + I := \{x + b \colon b \in I\}\,.$$

Comme dans le cas des groupes, on a une application surjective évidente (que l'on appelle encore *surjection canonique*)

$$\pi \colon A \to A/I\,, \qquad x \mapsto x + I\,.$$

On a alors le résultat fondamental suivant.

Proposition 12
Avec les notations comme ci-dessus, les lois "$+$" et "$\cdot$" définies sur A/I, pour $x, y \in A$, par

$$(x + I) + (y + I) := (x + y) + I\,, \qquad (x + I) \cdot (y + I) := (x \cdot y) + I$$

confèrent à A/I une structure d'anneau commutatif appelé anneau quotient de A par I. *Le neutre pour l'addition est la classe triviale $I = 0 + I$ et le neutre pour la multiplication est la classe $1 + I$ de l'élément $1 \in A$.*
Pour cette structure, la surjection canonique $\pi \colon A \to A/I$ est un morphisme d'anneaux.

Preuve. Il faut vérifier l'indépendance de la défintion des lois "$+$" et "$\cdot$" relativement à un choix de représentants. Si $x\mathcal{R}_I x'$ et $y\mathcal{R}_I y'$, alors il existe $z_x, z_y \in I$ tels que $x' = x + z_x$ et $y' = y + z_y$. Ainsi $x' + y' = x + y + z_x + z_y$, et comme I est un groupe additif, on a bien $x' + y' \in (x + y) + I$. Aussi $x'y' = xy + xz_y + yz_x + z_xz_y$. Or I est un idéal donc les éléments xz_y, yz_x, z_xz_y ainsi que leur somme sont dans I. On déduit $x'y' \in xy + I$.
On laisse en exercice la vérification du fait que ces deux lois confèrent bien une structure d'anneau à A/I. □

Exercice. Dans les notations de la proposition, vérifier que $1 + I = 1_{A/I}$.

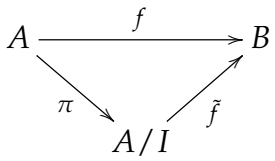
Exemples. • Tout anneau $\mathbb{Z}/n\mathbb{Z}$ est un anneau quotient de l'anneau $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$.
• Si K est un corps et P est un élément de $K[X]$ alors le quotient $K[X]/(P)$ de $K[X]$ par l'idéal principal (P) s'identifie à l'ensemble des restes possibles dans la division euclidienne par P si $P \neq 0$ (cf chapitre suivant).

On décrit l'ensemble des idéaux d'un anneau quotient A/I *via* l'analogue suivant de la proposition 2 du chapitre 5.

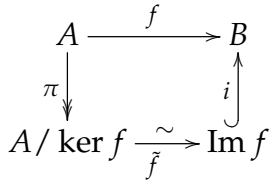
Proposition 13
Si I est un idéal de A et π est la surjection canonique associée, alors l'ensemble des idéaux de A/I est en bijection avec l'ensemble des idéaux de A qui contiennent I via l'application $J \mapsto \pi^{-1}(J)$.

L'analogue du théorème de factorisation 2 du chapitre 5 existe pour les anneaux. C'est le résultat suivant.

Théorème 2
Soit $f\colon A \longrightarrow B$ un morphisme d'anneaux commutatifs. Soit I un idéal de A tel que $I \subset \ker f$. Alors il existe un unique morphisme d'anneaux $\tilde{f}\colon A/I \longrightarrow B$ tel que $f = \tilde{f} \circ \pi$, où π désigne la projection canonique de A sur A/I.



En particulier si $I = \ker f$, le morphisme d'anneaux f induit un isomorphisme d'anneaux $A/\ker f \to \operatorname{Im} f$:



Les exemples suivants donnent des illustrations importantes du théorème de factorisation pour les anneaux.

Exemples. 1. (*Caractéristique d'un anneau*) Soit A un anneau commutatif dont on note 1_A le neutre pour la multiplication. On considère le morphisme d'anneaux :

$$\varphi\colon \mathbb{Z} \to A\,, \qquad n \geq 1 \mapsto 1_A + \cdots + 1_A\,,$$

où 1_A apparait n fois dans la somme (et donc $\varphi(0) = 0_A$, $\varphi(-n) = -\varphi(-n)$). Le noyau de φ est un idéal de $\mathbb{Z}$, il est donc de la forme $d\mathbb{Z}$ pour un $d \in \mathbb{N}$. L'entier d s'appelle la *caractéristique* de l'anneau A. Le théorème de factorisation affirme que φ induit un isomorphisme d'anneaux :

$$\mathbb{Z}/d\mathbb{Z} \simeq \operatorname{Im}\varphi \subseteq A\,.$$

On déduit que la caractéristique d'un anneau intègre (et en particulier la caractéristique d'un corps) vaut soit 0, soit un nombre premier. [Exercice : quelle est la caractéristique de $\mathbb{R}$, de $\mathbb{Z}/n\mathbb{Z}$, de $\mathbb{Z}[i] = \{a + ib\colon a, b \in \mathbb{Z}\}$?]
2. On reprend l'exemple déjà considéré à deux reprises. Soit $\alpha = 2^{1/3}$ l'unique solution réelle à l'équation $x^3 = 2$. On note $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_r\alpha^r\colon a_i \in \mathbb{Q}, r \in \mathbb{N}\}$; c'est un sous-anneau de $\mathbb{C}$. L'application d'évaluation

$$\operatorname{eval}_\alpha\colon \mathbb{Q}[X] \to \mathbb{Q}[\alpha]\,, \qquad f(X) \mapsto f(\alpha)\,,$$

est un morphisme d'anneaux de noyau $\ker \mathrm{eval}_\alpha = \{P \in \mathbb{Q}[X] : P(\alpha) = 0\}$. L'application eval_α, qui est évidemment surjective, induit donc un isomorphisme d'anneaux :

$$(\mathbb{Q}[X]/\{P \in \mathbb{Q}[X] : P(\alpha) = 0\}) \simeq \mathbb{Q}[\alpha]\,.$$

On a bien sûr $\ker \mathrm{eval}_\alpha \supseteq (X^3 - 2)$. Dans le chapitre suivant on verra que cette inclusion est en fait une égalité.

5.2 Idéaux premiers, maximaux

Pour les anneaux commutatifs généraux, on a vu les notions d'intégrité et de corps. Puisque l'on sait maintenant construire des anneaux quotients A/I d'un anneau commutatif A par un idéal I, on se demande à quelle condition sur I, l'anneau A/I est intègre (resp. est un corps). La notion d'idéal premier (resp. d'idéal maximal) répond à cette question, comme on va le voir.

Définition 8 (Idéal premier, idéal maximal)
Soit A un anneau commutatif et I un idéal de A, distinct de A.

1) *On dit que I est un idéal* premier *de A si pour $a, b \in A$ on a l'implication :*

$$ab \in I \Rightarrow (a \in I \text{ ou } b \in I)\,.$$

2) *On dit que I est un idéal* maximal *de A si pour tout idéal J de A on a l'implication :*

$$I \subseteq J \subseteq A \Rightarrow (J = I \text{ ou } J = A)\,.$$

Exemples. L'idéal $6\mathbb{Z}$ n'est pas premier dans $\mathbb{Z}$; en revanche l'idéal $5\mathbb{Z}$ est premier (et même maximal, ce qui est plus fort comme le montre la proposition suivante). Plus généralement les idéaux premiers non nuls de $\mathbb{Z}$ coïncident avec les idéaux maximaux de $\mathbb{Z}$: ce sont les $p\mathbb{Z}$, pour p premier. On note que (0) est un idéal premier non maximal de $\mathbb{Z}$ (car $\mathbb{Z}/(0) \simeq \mathbb{Z}$ est intègre, mais ce n'est pas un corps).
L'idéal $I = (X)$ est premier dans $A = \mathbb{Z}[X]$ mais il n'est pas maximal car on a par exemple la chaine d'inclusions strictes $I \subset (2, X) \subset A$.

Proposition 14
Soit A un anneau commutatif et I un idéal de A. On a les équivalences :

1) *A/I est intègre si et seulement si I est premier.*

2) *A/I est un corps si et seulement si I est maximal.*

On déduit immédiatement le fait que tout idéal maximal est premier.

Preuve. (1) Soit $\bar{a}, \bar{b}$ des éléments de A/I. On a

$$\bar{a} \cdot \bar{b} = \bar{0} \Leftrightarrow \overline{ab} = \bar{0} \Leftrightarrow ab \in I\,.$$

L'équivalence annoncée s'en déduit immédiatement.
(2) Si A/I est un corps alors d'après la proposition 11, A/I ne contient que deux idéaux, $(\bar{0})$ et $(\bar{1})$. Soit $I \subset J \subset A$ un idéal de A. Alors $\pi(J) = J/I$ est un idéal de A/I et donc $\pi(J) = (\bar{0})$ ce qui est équivalent à $J = I$, ou $\pi(J) = (\bar{1}) = A/I$ ce qui est équivalent à $J = A$.
Réciproquement, si I est maximal, soit $\bar{x} \in A/I$, $\bar{x} \neq \bar{0}$. On a alors $(\bar{x}) = (\bar{1})$. En effet, $\pi^{-1}((\bar{x}))$ est un idéal de A qui contient I et qui est différent de I. On a donc $\pi^{-1}((\bar{x})) = A$ par maximalité de I et $(\bar{x}) = \pi(\pi^{-1}((\bar{x}))) = A/I$. Enfin, $(\bar{x}) = (\bar{1})$ est équivalent à $\bar{x}$ inversible.

□

Chapitre 7

Anneaux principaux et anneaux euclidiens

1 Anneaux principaux

Soit A un anneau, que l'on supposera, dans toute la suite de ce chapitre, *commutatif*. On peut généraliser dans A la notion de divisibilité vue au chapitre 1 dans la cas $A = \mathbb{Z}$.

1.1 Divisibilité

Définition 1
Soit $a, b \in A$, $b \neq 0$. On dit que b divise *a (ou que b est un diviseur de a, ou encore que a est multiple de b) s'il existe $c \in a$ tel que $a = bc$.*
Si l'on suppose de plus que A est intègre, on dit que des éléments a et b de $A \setminus \{0\}$ sont associés *s'ils se divisent l'un l'autre i.e. $b \mid a$ et $a \mid b$. Cette proriété équivaut à l'existence d'une unité $u \in A^\times$ telle que $a = ub$.*

Pour démontrer l'assertion contenue dans la définition écrivons $a = bc$ et $b = ad$. On déduit $a = adc$ puis $a(1 - dc) = 0$. Comme $a \neq 0$ par hypothèse et que A est intègre, on déduit $cd = 1$ et donc $u = c$ est l'unité cherchée.

Exemple. Dans $\mathbb{Q}[X]$ on a $(2X + 2) \mid (X^2 + X)$, en revanche cette divisibilité n'a pas lieu dans $\mathbb{Z}[X]$.

Définition et proposition 1 (Idéal principal, anneau principal)
Un idéal I de A est dit principal *s'il existe $a \in A$ tel que $I = (a)$. L'idéal (a) est l'ensemble des multiples de a dans A. On le note parfois Aa.*
On dit que l'anneau A est principal *s'il est intègre et si tous ses idéaux sont principaux.*

Remarque. Si A est intègre, 2 éléments de A sont associés si et seulement si ils engendrent le même idéal principal. En particulier le générateur d'un idéal principal est toujours déterminé à multiplication par une unité près.

La proposition suivante est évidente.

Proposition 1
Soit $a, b \in A$. On a l'équivalence $b \mid a \Leftrightarrow (a) \subseteq (b)$.

Donnons deux exemples fondamentaux d'anneaux principaux.

Théorème 1
• *L'anneau $\mathbb{Z}$ est principal.*
• *Soit K un corps. L'anneau $K[X]$ des polynômes en une indéterminée à coefficients dans K est principal.*

Pour $\mathbb{Z}$, nous avons déjà vu au chapitre précédent que ses idéaux sont exactement les $d\mathbb{Z}$, $d \geq 0$ qui sont donc tous principaux. Ce théorème est en fait une conséquence du fait que $\mathbb{Z}$ et $K[X]$ sont des anneaux ayant une propriété plus remarquable encore que le principalité : ce sont des anneaux *euclidiens* (voir le théorème 3 de la section 2).

1.2 Arithmétique dans les anneaux principaux : PGCD, PPCM, éléments premiers entre eux

Dans toute cette section A désigne un anneau intègre (donc commutatif). La notion de divisibilité dans les anneaux (§1.1) permet d'étendre au cas des anneaux principaux les notions de pgcd et de ppcm.

Définition 2
Soient a et b deux éléments (non nuls) d'un anneau A principal (en particulier commutatif et intègre).

1) *On appelle PGCD de a et b tout élément d de A tel que $(d) = (a) + (b)$.*

2) *On appelle PPCM de a et b tout élément m de A tel que $(m) = (a) \cap (b)$.*

On dit que a et b sont premiers entre eux *s'ils admettent* 1 *pour PGCD, en d'autres termes si $(a) + (b) = A$.*

Remarques.

1) Ces définitions sont compatibles avec les définitions classiques de PGCD et PPCM dans $\mathbb{Z}$ (voir le théorème 4 du chapitre 1).

2) Deux PGCDs (resp. PPCMs) d'un même couple d'éléments sont associés (c'est-à-dire se déduisent l'un de l'autre par multiplication par un inversible de A ; voir la remarque précédant la proposition 1).

3) On peut définir plus généralement un PGCD (resp. un PPCM) d'une famille d'éléments $(a_1, \ldots, a_n)$ comme étant un générateur de l'idéal $(a_1) + \cdots + (a_n)$ (resp. $(a_1) \cap \cdots \cap (a_n)$)

4) La relation "être associés" est une relation d'équivalence sur $A^\star := A \setminus \{0\}$, qu'on note $\sim$ dans la suite :

$$x \sim y \Leftrightarrow \exists u \in A^\times, y = xu.$$

Sur le quotient $\overline{A} := A^\star / \sim$, la relation de divisibilité est alors une relation d'ordre (ce ne serait pas le cas sur $A \setminus \{0\}$, où l'on n'a pas, en général, l'antisymétrie).

Proposition 2 (Bézout, Gauss)
Soient a, b et c des éléments d'un anneau principal A.

1) *(Bézout) a et b de A sont premiers entre eux si et seulement s'il existe u et v éléments de A tels que $au + bv = 1$.*

2) *(Gauss) Si a et b sont premiers entre eux et si a divise bc, alors a divise c.*

3) *(Gauss 2) Si a et b sont premiers entre eux et divisent tous les deux c, alors ab divise c*

4) *Si a est premier avec b et avec c, alors a est premier avec bc.*

Preuve.

1) Par définition, a et b sont premiers entre eux si et seulement si $1 \in (a) + (b)$

2) Si $au + bv = 1$, alors $acu + bcv = c$. Or, si a divise bc, il divise le membre de gauche, et donc celui de droite.

3) Si $a \mid c$ alors $ab \mid bc$ et de même, si $b \mid c$ alors $ab \mid ac$. Mais par ailleurs, si $au + bv = 1$, $acu + bcv = c$. On vient de voir que ab divise le membre de gauche, donc aussi celui de droite.

4) Il existe (u, v) et (u', v') tels que $au + bv = 1$ et $au' + cv' = 1$ et en multipliant ces deux égalités, $a(auu' + cuv' + bvu') + bc(vv') = 1$ d'où le résultat par le théorème de Bézout.

□

Proposition 3
Si a et b sont deux éléments d'un anneau principal A, et si d et m désignent respectivement un PGCD et un PPCM de a et b, alors :

1) *Pour tout $x \in A$, on a : x divise a et $b \Leftrightarrow x$ divise d.*

2) *Pour tout $y \in A$, on a : a et b divisent $y \Leftrightarrow m$ divise y.*

3) $(ab) = (dm)$.

Preuve. On utilise la proposition 1.

1) Si $(a) \subset (x)$ et $(b) \subset (x)$, alors $(a) + (b) \subset (x)$ i.e. $(d) \subset (x)$. Réciproquement, si $(d) \subset (x)$, comme $(a) \subset (d)$ et $(b) \subset (d)$, on a $(a) \subset (x)$ et $(b) \subset (x)$.

2) On raisonne de façon similaire.

3) On écrit $a = da'$ et $b = db'$ et on a $(a') + (b') = A$ (en effet, il existe $u, v \in A$ tels que $au + bv = d$, donc $a'u + b'v = 1$). On a alors $da'b' = ab' = a'b$, donc $da'b'$ est un multiple commun de a et de b donc de m, ou autrement dit

$$(m) \supset (da'b').$$

Inversement, en écrivant

$$\begin{aligned} m &= xa = xda' \\ &= yb = ydb' \end{aligned}$$

on obtient que $xa' = yb'$, d'où l'on conclut (Gauss) que a' divise y (et b' divise x). Il suit que $da'b'$ divise m, c'est-à-dire $(m) \subset (da'b')$.

□

1.3 Décomposition en produit d'irréductibles

Définition 3
Un élément $x \neq 0$ d'un anneau A commutatif et intègre est dit irréductible *s'il n'est ni inversible, ni produit de deux éléments non inversibles. Autrement dit, x est irréductible s'il n'est pas inversible et si*

$$\forall (a, b) \in A \times A \ , \ x = ab \Rightarrow \left(a \in A^\times \text{ ou } b \in A^\times\right).$$

Exemple : Dans $\mathbb{Z}$, un élément irréductible est, au signe près, un nombre premier.

Lemme 1
Dans un anneau principal, toute suite croissante d'idéaux est stationnaire. Autrement dit, il n'existe pas de suite infinie d'idéaux strictement *croissante.*

Preuve. Soit $I_0 \subset I_1 \subset I_2 \subset \cdots$ une suite croissante d'idéaux. Alors $I := \bigcup_{n\in\mathbb{N}} I_n$ est un idéal de A (attention : ce serait en général faux si la suite n'était pas croissante). Il existe donc $x \in I$ tel que $I = (x)$. Mais alors, il existe $k \in \mathbb{N}$ tel que $x \in I_k$, auquel cas $I_k \subset I = Ax \subset I_k$, donc $I_k = I$ et $I_\ell = I_k$ pour tout $\ell \geq k$. □

Remarque. On peut reformuler ce lemme en disant que toute suite décroissante (au sens de la divisibilité) d'éléments de $\overline{A}$ est stationnaire (voir remarque ci-dessus pour la définition de $\overline{A}$).

Proposition 4
Soit a un élément non nul d'un anneau principal A. Alors

1) *Si a est non inversible, alors il admet un diviseur irréductible.*

2) *Pour tout élément irréductible p, l'ensemble $\{k \in \mathbb{N} \mid p^k \text{ divise } a\}$ est majoré.*

3) *L'ensemble des éléments irréductibles deux à deux non associés qui divisent a est fini.*

Preuve.

1) Si a est irréductible, c'est clair. Sinon, $a = a_1 b_1$ avec a_1 et b_1 non inversibles. Si a_1 est irréductible, on obtient bien un diviseur irréductible de a. Sinon, $a_1 = a_2 b_2$ avec a_2 et b_2 non inversibles, etc. Si le processus ne s'arrêtait jamais, on construirait ainsi une suite d'éléments $a_0 = a$, a_1, a_2, ... tels que a_i divise strictement a_{i-1} pour tout $i \geq 1$. La suite des idéaux (a_i) serait donc strictement croissante, ce qui est impossible en vertu du lemme 1. Donc le processus s'arrête, et le dernier terme a_k construit est irréductible.

2) Supposons, par l'absurde, que a soit divisible par p^k pour tout $k \in \mathbb{N}$. Il existe alors, pour tout $k \in \mathbb{N}$, un élément a_k de A tel que $a = p^k a_k$ et la suite (a_k) est strictement croissante, ce qui est impossible.

3) Si l'ensemble des diviseurs irréductibles de a deux à deux non associés est infini, on construit par récurrence une suite infinie $(p_n)_{n\in\mathbb{N}}$ d'irréductibles deux à deux non associés et une suite strictement croissante d'idéaux de la façon suivante :

$$a = p_1 a_1 = p_1 p_2 a_2 = p_1 p_2 p_3 a_3 = \cdots$$

(attention : on utilise Gauss à chaque étape !) et on a alors $(a_1) \subsetneq (a_2) \subsetneq \cdots$.

□

Pour conclure cette section on déduit de la proposition précédente l'énoncé d'une généralisation du théorème fondamental de l'arithmétique affirmant que tout entier $n \geq 2$ est, de manière unique, produit de nombres premiers.

Définition 4
À tout élément irréductible p d'un anneau principal A est associée une application $v_p : A \setminus \{0\} \to \mathbb{N}$ définie par

$$v_p(a) = \max\left\{k \in \mathbb{N} \mid p^k \text{ divise } a\right\}.$$

Le fait que v_p est bien définie est une conséquence de la proposition 4 2).

Théorème 2
Soit a un élément non nul et non inversible d'un anneau principal A. On note $\mathbb{P}(a)$ un ensemble de représentants pour ses diviseurs irréductibles à association près. Alors il existe $u \in A^\times$ et des entiers strictement positifs $v_p(a)$ tels que

$$a = u \prod_{p \in \mathbb{P}(a)} p^{v_p(a)}.$$

Cette factorisation est unique à une unité près et au choix de représentants dans $\mathbb{P}(a)$ près.

Remarque. Un anneau intègre dans lequel tout élément non nul admet une factorisation unique en produit d'irréductibles (comme dans le théorème) est dit factoriel.

Preuve. D'après la proposition 4 3), $\mathbb{P}(a)$ est fini. Par définition, a est divisible par chacun des $p^{v_p(a)}$ pour $p \in \mathbb{P}(a)$ et comme ils sont deux à deux premiers entre eux, par le théorème de Gauss 2, a est divisible par $\prod_{p\in\mathbb{P}(a)} p^{v_p(a)}$. Le quotient de a par ce produit n'admet pas de diviseur irréductible car un tel diviseur p serait aussi un diviseur irréductible de a et on aurait une contradiction avec soit la définition de $v_p(a)$, soit celle de $\mathbb{P}(a)$. Par conséquent, d'après la proposition 4 1) ce quotient est inversible.
En ce qui concerne l'unicité, remarquons tout d'abord que si p est irréductible et divise un produit bc, alors $p \mid b$ ou $p \mid c$. En effet, si $p \nmid b$, $\mathrm{PGCD}(p, a) = 1$ car p est irréductible et on conclut par Gauss.
Supposons que $a = u\prod_{i=1}^n p_i = v\prod_{j=1}^m q_j$ où $u, v \in A^\times$ et les p_i, q_j sont irréductibles (remarquons que la décomposition du théorème s'écrit ainsi, avec des répétitions éventuelles des facteurs p_i). Puisque p_1 qui est irréductible divise le membre de droite, p_1 divise un des facteurs que l'on peut supposer être q_1 après renumérotation. Ce dernier étant lui aussi irréductible, on a $q_1 = v_1 p_1$ avec $v_1 \in A^\times$ et on peut donc simplifier par p_1 les deux membres et obtenir $u\prod_{i=2}^n p_i = vv_1\prod_{j=2}^m q_j$. En poursuivant de même pour p_i, $i = 2, \ldots, n$, on obtient l'unicité (en particulier, $m = n$ et quitte à réordonner, $q_i = v_i p_i$, $v_i \in A^\times$, pour tout i). □

2 Anneaux euclidiens

Définition 5
L'anneau A est dit euclidien *s'il est intègre et s'il existe une fonction (appelée stathme euclidien)*

$$\phi\colon A \setminus \{0\} \to \mathbb{N}$$

telle que pour tout couple (a,b) d'éléments de A, avec $b \neq 0$, il existe $q, r \in A$ tels que

$$a = bq + r\,, \qquad (r = 0 \text{ ou } \phi(r) < \phi(b))\,.$$

Exemples. • L'anneau des entiers $\mathbb{Z}$ est euclidien pour le choix $\phi = |\cdot|$.
• Si K est un corps, l'anneau $K[X]$ est euclidien pour le choix $\phi = \deg$; la fonction degré. Aussi K lui-même est euclidien pour la fonction ϕ constante égale à 1. (Cela dit, faire des divisions euclidiennes dans un corps ne présente pas grand intérêt.)
• L'anneau des *entiers de Gauss* $\mathbb{Z}[i] = \{a + ib\colon a, b \in \mathbb{Z}\}$ est euclidien relativement à la restriction de la fonction "carré du module" $z \in \mathbb{C} \mapsto |z|^2$ (cf TD).

Dans $\mathbb{Z}$ et $K[X]$, on effectue la division euclidienne pour trouver q et r. Dans $\mathbb{Z}[i]$, c'est un peu plus compliqué (cf TD).

Donnons une conséquence importante du second exemple ci-dessus.

Corollaire 1
Soit K un corps et $P \in K[X]$ un polynôme non nul. Pour tout corps L contenant K, le nombre de racines du polynôme P dans L est inférieur ou égal à $\deg P$.

Preuve. Remarquons tout d'abord que $a \in L$ est racine de P (i.e. $P(a) = 0$) ssi P est divisible par $X - a$ dans $L[X] \supset K[X]$. Il suffit pour cela d'effectuer la division euclidienne de P par $X - a$ et d'évaluer en a (cf proposition 3 du chapitre suivant). Remarquons également que $X - a$ est irréductible, donc apparaît comme facteur irréductible de P dans $L[X]$ si a est racine.
Écrivons la décomposition de P en produits de facteurs irréductibles dans $L[X]$ (théorème 2),

$$P(X) = u \prod_{i=1}^{k} (X - a_i)^{\alpha_i} \prod_{j=1}^{\ell} Q_j^{\beta_j}$$

où $u \in K^\times$, les $a_i \in L$ et les $Q_j \in L[X]$ sont deux à deux distincts, $\alpha_i = v_{X-a_i}(P) \geq 1$ est la multiplicité de la racine a_i dans P, $\deg Q_j \geq 2$ et $\beta_j = v_{Q_j}(P)$. On a alors, en considérant les degrés, $k \leq \sum_{i=1}^{k} \alpha_i \leq \deg P$. On obtient donc que P a au plus $\deg P$ racines dans L (y compris en tenant compte des multiplicités). □

Le théorème 1 est une conséquence du résultat général suivant.

Théorème 3
Tout anneau euclidien est principal.

Preuve. Soit I un idéal de A différent de $\{0\} = (0)$ qui est évidemment principal. On choisit $b \in I\backslash\{0\}$ tel que $\phi(b) = \min\{\phi(x) \mid x \in I\backslash\{0\}\}$.
Soit maintenant $a \in I$ arbitraire, on a alors $a = bq + r$ avec $q, r \in A$ et $\phi(r) < \phi(b)$ ou $r = 0$. Cependant, comme I est un idéal, $r = a - bq \in I$ et par conséquent, par minimalité de $\phi(b)$, on a $r = 0$, ce qui montre que $I = (b)$. □
Exercice. Montrer que l'anneau $\mathbb{Z}[X]$ n'est pas euclidien.

Application. On conclut en reprenant l'exemple vu plusieurs fois dans le chapitre précédent. Soit $\alpha = 2^{1/3}$ l'unique solution réelle à l'équation $x^3 = 2$. On note $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_r\alpha^r : a_i \in \mathbb{Q}, r \in \mathbb{N}\}$. L'application d'évaluation

$$\mathrm{eval}_\alpha : \mathbb{Q}[X] \to \mathbb{Q}[\alpha]\,, \qquad f(X) \mapsto f(\alpha)\,,$$

est un morphisme surjectif d'anneaux de noyau $\ker \mathrm{eval}_\alpha = \{P \in \mathbb{Q}[X] : P(\alpha) = 0\}$. On a bien sûr $\ker \mathrm{eval}_\alpha \supseteq (X^3 - 2)$ et, comme $\mathbb{Q}[X]$ est principal, il existe $P_0 \in \mathbb{Q}[X]$ non constant tel que $\ker \mathrm{eval}_\alpha = (P_0)$. Ainsi $P_0 \mid (X^3 - 2)$ dans $Q[X]$. Si $\deg P_0 < 3$, alors on déduit, par division euclidienne de $X^3 - 2$ par P_0, que $X^3 - 2$ admet un facteur de degré 1 dans $\mathbb{Q}[X]$ et donc une racine rationnelle. Or l'unique racine rélle α de $X^3 - 2$ est irrationnelle (exercice : le démontrer). Donc $\deg P_0 = 3$; comme $P_0 \mid (X^3 - 2)$, on déduit que P_0 et $X^3 - 2$ sont associés et donc $\ker \mathrm{eval}_\alpha = (X^3 - 2)$. Aussi, le raisonnement que l'on vient de faire montre que l'idéal $(X^3 - 2)$ est maximal dans $\mathbb{Q}[X]$. En effet si $I \subset \mathbb{Q}[X]$ est un idéal qui contient $(X^3 - 2)$, alors, comme $\mathbb{Q}[X]$ est principal il existe $Q_0 \in \mathbb{Q}[X]$ tel que $I = (Q_0) \supseteq (X^3 - 2)$, et l'on a vu qu'alors soit $I = A$ (i.e. Q_0 est constant, distinct de 0), soit on peut déduire $(Q_0) = (X^3 - 2)$.
Finalement l'application eval_α induit donc un isomorphisme d'anneaux :

$$\mathbb{Q}[X]/(X^3 - 2) \simeq \mathbb{Q}[\alpha]\,;$$

et donc, comme $\mathbb{Q}[X]/(X^3 - 2)$ est un corps, $\mathbb{Q}[\alpha]$ est également un corps.

Chapitre 8

Polynômes et fractions rationnelles

Dans toute la suite, A désigne un anneau commutatif et K désigne un corps.
On a traité d'exemples, notamment dans les deux chapitres précédents, où des polynômes apparaissaient. On a alors utilisé notre connaissance "intuitive" de ce qu'est un polynôme, une somme de polynômes, et un produit de polynômes. On décrit dans ce chapitre plus rigoureusement la structure et les opérations propres aux polynômes. Dans un second temps on étudie les "quotients de polynômes" : les *fractions rationnelles*.

1 Définitions et premières propriétés

Définition 1
Un polynôme à coefficients dans A est une suite $(a_n)_{n\in\mathbb{N}}$ nulle à partir d'un certain rang, c'est-à-dire telle qu'il existe $N \in \mathbb{N}$ avec la propriété que a_n est nul pour tout $n > N$. On convient de noter $A[X]$ l'ensemble des polynômes à coefficients dans A.

Informellement, un polynôme est donc une suite

$$(a_0, a_1, a_2, a_3, \ldots, a_N, 0, 0, 0 \ldots) .$$

Avec cette définition il est immédiat de définir la somme de deux polynômes :

Définition 2
si $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ sont deux polynômes, leur somme est le polynôme $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$.

Il faut vérifier que la somme $P + Q$ que l'on vient de définir est bien un *polynôme*, c'est-à-dire qu'elle est nulle à partir d'un certain rang. Or il existe $N_1 \in \mathbb{N}$ tel que a_n est nul pour tout $n > N_1$ et $N_2 \in \mathbb{N}$ tel que b_n est nul pour tout $n > N_2$, donc $a_n + b_n$ est nul pour tout $n > N := \max(N_1, N_2)$.

On peut également, de façon un peu moins immédiate, définir le produit de deux polynômes :

Définition 3
Le produit de deux polynômes $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ est le polynôme $PQ = (c_n)_{n\in\mathbb{N}}$ où c_n est défini par la formule

$$c_n = a_0b_n + a_1b_{n-1} + a_2b_{n-2} + \ldots + a_{n-1}b_1 + a_nb_0 = \sum_{k=0}^{n} a_kb_{n-k}.$$

Remarque. Là encore, il faut s'assurer que c_n est nul pour n "assez grand", ce qui est clair : $a_n = 0$ pour tout $n > N_1$ et $b_n = 0$ pour tout $n > N_2$, alors $c_n = \sum_{k=0}^{n} a_kb_{n-k}$ est nul dès que $n > N_1 + N_2$.

Proposition 1
Muni des deux lois précédentes, l'ensemble $A[X]$ est un anneau, d'élément neutre additif le polynôme nul $(0, 0, \ldots)$ et d'élément neutre multiplicatif le polynôme $(1, 0, 0, \ldots)$.

Preuve. C'est immédiat. □

Après ce préambule un peu formel, on peut revenir à une notation plus familière en posant

$$X := (0, 1, 0, 0, 0, \ldots).$$

Le symbole X ainsi défini est une *indéterminée*. On vérifie alors sans difficulté (récurrence) que

$$\begin{aligned} X^2 &= (0, 0, 1, 0, \ldots), \\ X^3 &= (0, 0, 0, 1, 0, \ldots), \\ &\vdots \\ X^n &= (0, 0, \ldots, 0, 1, 0, 0, \ldots), \\ \text{et également } X^0 &= (1, 0, 0, 0, \ldots). \end{aligned}$$

Avec ces notations, on voit qu'un polynôme $P = (a_0, a_1, \ldots, a_N, 0, 0, \ldots)$ peut s'écrire

$$P = a_0 + a_1X + \ldots + a_nX^n.$$

On appelle *monôme* un élément de $A[X]$ dont exactement un coefficient est non-nul. D'après ce qui précède, un monôme peut toujours s'écrire a_iX^i pour un certain $i \in \mathbb{N}$ et un certain $a_i \in A \setminus \{0\}$.

Définition 4
Le degré d'un polynôme P non nul, noté $\deg P$*, est le plus grand entier n tel que le coefficient a_n de X^n dans P soit non nul. Le coefficient a_n est alors appelé* coefficient dominant *de P.*
Par convention, le degré du polynôme nul, est égal à $-\infty$. On convient également que :

- *$n + -\infty = -\infty$ pour tout $n \in \mathbb{N}$,*
- *$n > -\infty$ pour tout $n \in \mathbb{N}$.*

Proposition 2
Soient P et Q deux polynômes à coefficients dans un anneau A.

1) $\deg(P+Q) \leq \max(\deg P, \deg Q)$ *et on a égalité si* $\deg P \neq \deg Q$.

2) *Si A est* **intègre**, $\deg(PQ) = \deg P + \deg Q$. *En particulier, si A est intègre, $A[X]$ est également intègre.*

Une conséquence immédiate de la formule $\deg(PQ) = \deg P + \deg Q$ est le

Corollaire 1
Soient P et Q deux polynômes non nuls à coefficients dans un anneau A **intègre**. *Si P divise Q, alors* $\deg P \leq \deg Q$.

2 Division euclidienne

Donnons un théorème généralisant le fait, vu dans le chapitre précédent, que $K[X]$ est un anneau euclidien.

Théorème 1
Soient F et G deux polynômes à coefficients dans un anneau intègre A. ***Si le coefficient dominant de G est inversible dans*** *A, alors il existe un unique couple (Q, R) de polynômes qui vérifie*

$$\begin{cases} F = GQ + R \\ \deg R < \deg G \end{cases}$$

Preuve.

- Existence. Posons

  $$G = g_0 + g_1 X + \ldots + g_d X^d, \text{ avec } g_d \in A^\times \text{ (en particulier, } \deg G = d)$$

  et

  $$F = f_0 + f_1 X + \ldots + f_n X^n.$$

  - Si $n < d$, alors le couple $(Q, R) = (0, F)$ convient.
  - Sinon, le polynôme $F_1 := F - f_n g_d^{-1} X^{n-d} G$ est de degré strictement inférieur à n. On reprend alors le processus avec le couple (F_1, G).

- Unicité. Si $F = GQ_1 + R_1 = GQ_2 + R_2$ avec $\deg R_1 < \deg G$ et $\deg R_2 < \deg G$, alors

  $$G(Q_1 - Q_2) = R_2 - R_1$$

  d'où

  $$\deg(G(Q_1 - Q_2)) = \deg G + \deg(Q_1 - Q_2) = \deg(R_2 - R_1) < \deg G$$

  ce qui n'est possible que si $Q_1 - Q_2 = 0$, auquel cas on a également $R_2 - R_1 = 0$.

□

On notera que la preuve de l'existence, dans le résultat ci-dessus n'utilise pas l'hypothèse "A intègre". De ce fait la proposition 3 ci-dessous vaut pour les polynômes à coefficients dans un anneau commutatif non nécessairement intègre.

3 Racines et multiplicités

À un polynôme $P = a_0 + a_1X + \cdots + a_nX^n \in A[X]$, on associe une *fonction polynomiale*

$$\begin{array}{rccc} \widetilde{P}: & A & \longrightarrow & A \\ & \alpha & \longmapsto & \widetilde{P}(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n. \end{array}$$


Il faut prendre garde de ne pas identifier un polynôme à la fonction polynomiale qui lui est associée, à cause du gag suivant : le polynôme $P(X) = X^2 + X \in \mathbb{Z}/2\mathbb{Z}[X]$ est non nul, mais sa fonction polynomiale associée $\widetilde{P}$ l'est, puisque $\widetilde{P}(0) = \widetilde{P}(1) = 0$. Cependant, ce problème ne se pose pas si l'on considère des polynômes à coefficients dans un corps K infini, car alors l'application $P \mapsto \widetilde{P}$ est injective (exercice).

Ceci étant, on commet le plus souvent l'abus de notation consistant à noter "$P(\alpha)$" l'image de α par la fonction $\widetilde{P}$ (plutôt que "$\widetilde{P}(\alpha)$").

Définition 5
Avec les notations ci-dessus, on dit que $\alpha \in A$ est racine *de $P \in A[X]$ si $\widetilde{P}(\alpha) = 0$ dans A.*

Proposition 3
Les propriétés suivantes sont équivalentes :

1) *α est racine de P.*

2) *$(X - \alpha)$ divise P.*

Preuve. On effectue la division euclidienne de P par $X - \alpha$:

$$P = (X - \alpha)Q + R \text{ avec } \deg R < 1. \tag{8.1}$$

Autrement dit, R est un polynôme constant, éventuellement nul (auquel cas $\deg R = -\infty$). Supposons que α soit racine de P. Alors, en évaluant le polynôme P en α et en utilisant l'équation (8.1) on obtient que

$$0 = P(\alpha) = R(\alpha),$$

ce qui signifie que $R = 0$ puisque R est un polynôme constant. Donc $X - \alpha$ divise P. Inversement, si $X - \alpha$ divise P, alors il existe $Q \in A[X]$ tel que $P = (X - \alpha)Q$ auquel cas $P(\alpha) = 0$. □

Donnons une généralisation du corollaire 1 du chapitre précédent.

Théorème 2
Soient $\alpha_1, \alpha_2, \ldots, \alpha_k$ des racines deux à deux distinctes d'un polynôme $P \in A[X]$, où A ***est un anneau intègre****. Alors le produit $(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_k)$ divise P. En particulier, le nombre de racines deux à deux distinctes d'un polynôme P non nul à coefficients dans un anneau intègre est au plus égal à* $\deg P$.

Preuve. La proposition précédente montre que $X-\alpha_1$ divise P ; il existe donc $Q_1 \in A[X]$ tel que

$$P = (X-\alpha_1)Q_1.$$

Comme α_2 est racine, on a

$$0 = P(\alpha_2) = (\alpha_2-\alpha_1)Q_1(\alpha_2)$$

et donc $Q_1(\alpha_2) = 0$ puisque $\alpha_2 - \alpha_1 \neq 0$ **et que** A **est intègre**. En vertu de la proposition 3, on peut donc affirmer que $X-\alpha_2$ divise Q_1, c'est-à-dire qu'il existe $Q_2 \in A[X]$ tel que

$$Q_1 = (X-\alpha_2)Q_2$$

et par conséquent

$$P = (X-\alpha_1)(X-\alpha_2)Q_2.$$

En poursuivant ce raisonnement, on montre que $(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_k)$ divise P. □


Le résultat est faux si l'anneau A n'est pas intègre. Par exemple, si $A = \mathbb{Z}/6\mathbb{Z}$ le polynôme $X^2 - X \in A[X]$ a quatre racines dans A !

Définition 6
Soit P un polynôme à coefficients dans A et $\alpha \in A$ une racine de P. On appelle multiplicité de la racine α le plus grand entier naturel n tel que $(X-\alpha)^n$ divise P.

Remarque : Dans le cas où A est intègre, la multiplicité d'une racine est majorée par le degré du polynôme.

On obtient alors le raffinement suivant du théorème 2 :

Théorème 3
Soient P un polynôme à coefficients dans un anneau intègre A et $\alpha_1, \alpha_2, \ldots, \alpha_k$ ses racines deux à deux distinctes dans A, de multiplicités respectives $n_1, n_2, \ldots, n_k$. Alors il existe un polynôme $Q \in A[X]$, sans racine dans A, tel que

$$P = (X-\alpha_1)^{n_1}(X-\alpha_2)^{n_2}\cdots(X-\alpha_k)^{n_k}Q.$$

En particulier, le nombre de racines d'un polynôme non nul $P \in A[X]$, comptées avec multiplicité, est majoré par le degré de P.

Preuve. Exercice (copier la preuve du théorème 2). □

4 Polynômes irréductibles

On a vu que l'anneau $K[X]$ était euclidien. En particulier, tout polynôme P de $K[X]$ s'écrit de façon essentiellement unique comme produit de polynômes irréductibles (*cf.* Théorème 2 du chapitre précédent).

Exemples.

1) Les éléments inversibles de $K[X]$ sont les polynômes de degré 0. Leur ensemble s'identifie à $K^\times$.

2) Pour tout $a \in K$, le polynôme $X - a$ est irréductible dans $K[X]$.

3) Le polynôme $X^2 + 2$ est irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$.

4) Le polynôme $X^2 - 2$ est irréductible dans $\mathbb{Q}[X]$ mais pas dans $\mathbb{R}[X]$.

5)

$$\begin{aligned} X^4 + 1 &= (X - e^{i\pi/4})(X - e^{-i\pi/4})(X - e^{3i\pi/4})(X - e^{-3i\pi/4}) \text{ dans } \mathbb{C}[X] \\ &= (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1) \text{ dans } \mathbb{R}[X] \\ &\text{et il est irréductible dans } \mathbb{Q}[X]. \end{aligned}$$

5 Fractions rationnelles

Pour tout anneau intègre A, il existe un "plus petit corps" le contenant. Il s'agit du *corps des fractions* de A. Dans le cas $A = \mathbb{Z}$, ce corps est $\mathbb{Q}$. On donne dans un premier temps la construction générale du corps des fractions d'un anneau intègre, puis l'on se concentre dans un second temps sur le cas $A = K[X]$.

5.1 Corps des fractions d'un anneau intègre

Définition 7
Soit A un anneau intègre et $\mathcal{C} = A \times (A \setminus \{0\})$.
Sur $\mathcal{C}$ on introduit deux opérations $+$ et $\times$ définies comme suit : pour tous (a, b) et (c, d) de $\mathcal{C}$, on pose

$$(a, b) \times (c, d) = (ac, bd)$$

et

$$(a, b) + (c, d) = (ad + cb, bd).$$

Définition 8
Sur $\mathcal{C}$ on définit la relation $\mathcal{R}$ suivante

$$(a, b)\mathcal{R}(c, d) \;\; si \;\; ad = cb.$$

Théorème 4
La relation $\mathcal{R}$ est une relation d'équivalence compatible avec les opérations $+$ et $\times$ définies précédemment. Celles-ci induisent une structure d'anneau sur le quotient $\mathcal{C}/\mathcal{R}$, et cet anneau est un corps.

Preuve. On vérifie facilement que $\mathcal{R}$ est une relation d'équivalence (l'intégrité de A est cruciale pour établir la transitivité).
La compatibilité des opérations avec $\mathcal{R}$ est un calcul facile. Par exemple, si $(a,b)\mathcal{R}(a',b')$ et $(c,d)\mathcal{R}(c',d')$, alors

$$\begin{aligned}(ad+bc)b'd' - (a'd'+b'c')bd &= (ab')dd' + (cd')bb' - (a'b)dd' - (c'd)bb' \\ &= (a'b)dd' + (c'd)bb' - (a'b)dd' - (c'd)bb' \\ &= 0\end{aligned}$$

donc $(a,b)+(c,d)\mathcal{R}(a',b')+(c',d')$.
Si on note (provisoirement) $[a,b]$ la classe modulo $\mathcal{R}$ d'un élément (a,b) de $\mathcal{C}$, on peut donc munir le quotient $\mathcal{C}/\mathcal{R}$ de deux lois $+$ et $\times$

$$[a,b]+[c,d] = [ad+cb,bd] \text{ et } [a,b]\times[c,d] = [ac,bd]$$

dont on vérifie facilement qu'elles définissent sur $\mathcal{C}/\mathcal{R}$ une structure d'anneau. En particulier, le neutre additif est égal à $[0,1]$ et le neutre multiplicatif à $[1,1]$.
Si $[a,b]$ est un élément de $\mathcal{C}/\mathcal{R}$ son opposé est $[-a,b]$, car $[-a,b]+[a,b] = [a,b]+[-a,b] = [0,b^2] = [0,1]$.
Vérifions enfin que $\mathcal{C}/\mathcal{R}$ est un corps : si $[a,b] \neq [0,1]$, c'est-à-dire si $a \neq 0$, alors $(b,a) \in \mathcal{C}$ et $[a,b]\times[b,a] = [ab,ab] = [1,1]$. □

Définition 9
L'anneau $\mathcal{C}/\mathcal{R}$ s'appelle le corps des fractions de A. On le note Frac$A$.

On convient de noter désormais $\frac{a}{b}$ la classe d'un élément (a,b) dans Frac$A$.

Proposition 4
Si A est un anneau principal, tout élément de Frac$A$ *admet un réprésentant* irréductible*, c'est-à-dire de la forme $\frac{a}{b}$ avec a et b premiers entre eux.*

Proposition 5
L'application

$$\begin{array}{rccc} i: & A & \longrightarrow & \text{Frac}A \\ & a & \longmapsto & \dfrac{a}{1} \end{array}$$

est un morphisme d'anneaux injectif.

Par conséquent, on peut identifier A à un sous-anneau de son corps des fractions Frac$A$, en identifiant l'élément $a \in A$ avec son image $\frac{a}{1}$ dans Frac$A$.

5.2 Le corps des fractions rationnelles $K(X)$

Définition 10
Soit K un corps et X une indéterminée sur K. Le corps des fractions de l'anneau intègre $A = K[X]$ s'appelle le corps des fractions rationnelles en une indéterminée X sur K. *On note $K(X)$ ce corps.*

Théorème 5 (Décomposition en éléments simples)
Soit $F \in K(X)$ une fraction rationnelle non nulle. Soit $F = \dfrac{N}{D}$ un représentant irréductible de F, c'est-à-dire avec N et D premiers entre eux, et soit

$$D = {P_1}^{\alpha_1} \dots {P_r}^{\alpha_r}$$

la décomposition de D en facteurs irréductibles de $K[X]$. Alors on peut écrire F de manière unique sous la forme

$$F = E + \sum_{i=1}^{r} \left(\sum_{j=1}^{\alpha_i} \frac{A_{i,j}}{P_i^j} \right) \tag{8.2}$$

où E et les $A_{i,j}$ sont des polynômes et $\deg(A_{i,j}) < deg(P_i)$ pour tout i et tout j. Le polynôme E s'appelle la partie entière *de F.*
L'écriture (8.2) *de F s'appelle la* décomposition en éléments simples *de F. Les termes E et $A_{i,j}/P_i^j$ du membre de droite sont appelés* éléments simples.

Preuve.

- **Existence.** La démonstration se découpe en les étapes suivantes :

  1) Si $F = \dfrac{N}{D}$, il existe un unique couple (E, R) de polynômes tels que

  $$F = E + \frac{R}{D} \qquad \text{et} \qquad \deg R < \deg D$$

  obtenu en faisant la division euclidienne de N par D

  2) On suppose désormais que $F = \dfrac{N}{D}$, avec N et D premiers entre eux et $\deg N < \deg D$.

  (a) Si $D = Q_1 Q_2$ avec $Q_1 \wedge Q_2 = 1$, il existe un unique couple (U_1, U_2) de polynômes tels que

  $$F = \frac{U_1}{Q_1} + \frac{U_2}{Q_2} \quad , \quad \deg U_1 < \deg Q_1 \quad \text{et} \quad \deg U_2 < \deg Q_2.$$

  Preuve. Puisque $Q_1 \wedge Q_2 = 1$, d'après le théorème de Bézout, il existe $V_1, V_2 \in \mathbb{K}[X]$ tels que $Q_1 V_1 + Q_2 V_2 = 1$ et par conséquent, $Q_1(NV_1) + Q_2(NV_2) = N$. Effectuons maintenant la division euclidienne de NV_1

par Q_2 : il existe $S, T \in \mathbb{K}[X]$, avec $\deg T < \deg Q_2$, tels que $NV_1 = Q_2S + T$, d'où $Q_1T + Q_2(NV_2 + Q_1S) = N$. Comme $\deg Q_1T < \deg Q_1 + \deg Q_2$ et comme $\deg N < \deg Q_1 + \deg Q_2$, on a $\deg(NV_2 + Q_1S) < \deg Q_1$. Il suffit donc de prendre $U_1 = NV_2 + Q_1S$ et $U_2 = T$.
Montrons maintenant l'unicité de (U_1, U_2). Si $N = Q_1U_2 + Q_2U_1 = Q_1V_2 + Q_2V_1$ (avec (V_1, V_2) qui vérifie aussi les conclusions du lemme) alors $Q_1(U_2 - V_2) = Q_2(V_1 - U_1)$. Comme $Q_1 \wedge Q_2 = 1$, d'après le théorème de Gauss, Q_1 divise $V_1 - U_1$ ce qui est impossible vu que $\deg(V_1 - U_1) < \deg U_1$, sauf si $U_1 = V_1$. Par conséquent, on a aussi $U_2 = V_2$. □

(b) Si $D = Q_1Q_2 \dots Q_k$ et $Q_i \wedge Q_j = 1$ si $i \neq j$, il existe un unique k-uplet $(U_1, U_2, \dots, U_k)$ de polynômes tel que

$$F = \frac{U_1}{Q_1} + \frac{U_2}{Q_2} + \cdots + \frac{U_k}{Q_k} \quad , \quad \text{et } \deg U_i < \deg Q_i \quad \text{pour tout } k.$$

Preuve. Nous faisons une récurrence sur k. D'après le lemme précédent, le résultat est vrai pour $k = 2$. Supposons que le lemme est vrai pour k facteurs et montrons-le pour $k+1$ facteurs. Comme $Q_i \wedge Q_{k+1} = 1$ pour tout $i \leq k$, on a $\text{pgcd}(Q_1Q_2 \dots Q_k, Q_{k+1}) = 1$ d'après la proposition 2, 4) du chapitre 7. Par conséquent, d'après (a), il existe $U, U_{k+1} \in (\mathbb{K}[X])^2$ vérifiant $\deg U < \deg Q_1 + \deg Q_2 + \cdots + \deg Q_k$, $\deg U_{k+1} < \deg Q_{k+1}$ et tels que $F = U/(Q_1Q_2 \dots Q_k) + U_{k+1}/Q_{k+1}$. On peut alors appliquer l'hypothèse de récurrence à la première fraction. □

(c) Si $F = \dfrac{A}{Q^\alpha}$ avec $\deg A < \alpha \deg Q$, il existe un unique α-uplet $(A_1, \dots, A_\alpha)$ de polynômes tel que

$$F = \frac{A_1}{Q} + \frac{A_2}{Q^2} + \cdots \frac{A_\alpha}{Q^\alpha} \quad \text{et} \quad \deg A_j < \deg Q \text{ pour tout } j.$$

Preuve. On procède par récurrence sur α. Pour $\alpha = 1$, c'est évident. Supposons le résultat vrai pour $\alpha \geq 1$. La relation $A = Q(A_{\alpha-1} + \cdots + A_2Q^{\alpha-3} + A_1Q^{\alpha-2}) + A_\alpha$ avec $\deg A_\alpha < \deg Q$ montre que A_α est nécessairement le reste de la division euclidienne de A par Q.
Effectuons donc la division euclidienne de A par Q : $A = QS + A_\alpha$ avec $\deg A_\alpha < \deg Q$. De plus, on a $\deg S \leq \deg A - \deg Q < (\alpha - 1) \deg Q$, ce qui permet d'appliquer l'hypothèse de récurrence.

□

- **Unicité :** résulte de l'unicité à chaque étape.

□

Quelques exemples de calcul :

1) Soit K un corps commutatif et Q un polynôme à coefficients dans K, scindé sur K, et n'ayant que des racines simples, c'est-à-dire $Q(X) = \prod_{i=1}^{n}(X - x_i)$, avec $x_i \neq x_j$ si $i \neq j$. Alors, pour tout $P \in K[X]$ de degré $< n$,

$$\frac{P}{Q} = \sum_{i=1}^{n} \frac{P(x_i)}{Q'(x_i)(X - x_i)}.$$

Application : déterminer la décomposition en éléments simples de la fraction rationnelle $\dfrac{1}{X^n - 1}$ dans $\mathbb{R}(X)$, où n désigne un entier naturel non nul.

2) (*Exercice*) Déterminer la décomposition en éléments simples de

$$F(X) = \frac{X^2 + 1}{(1 + X)^2(1 + X + X^2)^2}$$

dans $\mathbb{R}(X)$.