Mathématiques 2013-2014

Cours d'Algèbre 3

Olivier Guibé,

Bureau n^{o} M.2.17

olivier.guibe@univ-rouen.fr

Université de Rouen

Laboratoire de Mathématiques Raphaël Salem,

Avenue de l'Université, BP.12,

F76801 Saint-Étienne-du-Rouvray.

Rédigé avec LaTeX

par Hicham AMARIR

le 11 mai 2026

Table des matières

Chapitre 1

Arithmétique de base

Sites : mathématiques.net, mathématec??, pages web

1.1 Division euclidienne dans $\mathbb{N}$

Remarque :

On suppose connue la construction de $\mathbb{N}$ avec les 5 axiomes de Peano :

1. L'élément appelé zéro et noté 0 est un entier naturel.
2. Tout entier naturel n a un unique successeur, noté s(n) ou Sn qui est un entier naturel.
3. Aucun entier naturel n'a 0 pour successeur.
4. Deux entiers naturels ayant le même successeur sont égaux.
5. Si un ensemble d'entiers naturels contient 0 et contient le successeur de chacun de ses éléments, alors cet ensemble est $\mathbb{N}$.

Théorème 1.1 : (*Théorème fondamental de* $\mathbb{N}$)

Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Corollaire 1.2 : (*Corollaire*)

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

Théorème 1.3 : (*Division euclidienne dans* $\mathbb{N}$)

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

$$a = bq + r \quad \text{et} \quad 0 \leqslant r < b,$$

où q est le quotient et r le reste.

Preuve :

Posons $A = \{q \in \mathbb{N} \mid a < b(q+1)\}$.

Pour appliquer le th. fondamental de $\mathbb{N}$, il faut d'abord montrer que $A \neq \emptyset$.

— Si $a = 0$, c'est évident $(\forall q \in \mathbb{N},\ 0 < b(q+1))$.

— Si $a \neq 0$, $b \neq 0$, on a $b \geqslant 1$ donc $a \in A$.

Donc $A \neq \emptyset$. D'après le th. fondamental, soit q le plus petit élément de A.

Posons $r = a - bq$. Comme q est le plus petit élément de A, $q-1 \notin A$, donc

$$a \geqslant b(q-1+1) = bq \implies a - bq \geqslant 0 \implies r \geqslant 0.$$

Comme $a < b(q+1)$, on a $a - bq < b$, donc $r < b$.

On a donc montré l'existence de (q,r).

Unicité. Soit (q',r') un autre couple vérifiant $a = bq' + r'$, $0 \leqslant r' < b$. Alors $bq + r = bq' + r'$, soit $b(q-q') = r' - r$. Comme $0 \leqslant r' < b$ et $0 \leqslant r < b$, on a $|r' - r| < b$, donc $b|q-q'| < b$, soit $|q-q'| < 1$. Si $q \neq q'$, on obtient $b|q-q'| \geqslant b$, contradiction.

Donc $q = q'$ et $r = r'$.

1.2 Arithmétique dans $\mathbb{Z}$

Définition 1.4 : (*Valeur absolue*)

Pour tout $a \in \mathbb{Z}$, on pose $|a| = \max(a, -a)$.

Théorème 1.5 : (*Division euclidienne dans* $\mathbb{Z}$)

Pour tout $(a, b) \in \mathbb{Z}^2$ avec $b \neq 0$, il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ tel que

$$a = bq + r \quad \text{et} \quad 0 \leqslant r < |b|.$$

Preuve :

— *Unicité :* identique au cas dans $\mathbb{N}$.

— *Existence :* On pose $A = \{a - bk \mid k \in \mathbb{Z}\} \cap \mathbb{N}$. On montre $A \neq \emptyset$, puis on pose r le plus petit élément de A et $a = bq + r$ (voir polycopié).

Définition 1.6 : (*Divisibilité*)

Soient $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}$.

On dit que a ***divise*** b s'il existe un entier $q \in \mathbb{Z}$ tel que :

$$b = a \cdot q.$$

On note cette relation :

$$\boxed{a \mid b}$$

Exemple :

i) $3 \mid 12$ car $12 = 3 \times 4$.

ii) $5 \nmid 13$ car il n'existe pas d'entier q tel que $13 = 5 \times q$.

iii) Pour tout $n \in \mathbb{Z}$, on a $1 \mid n$ et $n \mid 0$.

Définition 1.7 : (*Nombre premier*)

Un ***nombre premier*** est un entier naturel $p \geqslant 2$ tel que l'ensemble de ses diviseurs naturels soit $\{1; p\}$:

$$\{d \in \mathbb{N} \mid d \mid p\} = \{1; p\}.$$

Autrement dit, p n'admet aucun diviseur autre que 1 et lui-même.

Exemple :

i) Les premiers nombres premiers sont :

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ \ldots$$

ii) 4 n'est pas premier car $4 = 2 \times 2$ (divisible par 2).

iii) 1 n'est **pas** un nombre premier par convention (il n'a qu'un seul diviseur).

Théorème 1.8 : (*Décomposition en produit de facteurs premiers*)

Tout entier $n \geqslant 2$ peut s'écrire comme un produit de nombres premiers :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k}$$

où les p_i sont des nombres premiers distincts et les $\alpha_i \in \mathbb{N}^*$.

Cette décomposition est ***unique*** à l'ordre des facteurs près.

Exemple :

i) $12 = 2^2 \times 3$

ii) $60 = 2^2 \times 3 \times 5$

iii) $100 = 2^2 \times 5^2$

Théorème 1.9 : (*Infinité des nombres premiers*)

L'ensemble des nombres premiers est ***infini***.

Preuve :

Preuve par l'absurde (*faite par Euclide*) :

Supposons que l'ensemble des nombres premiers soit fini. Notons-les $p_1, p_2, \ldots, p_m$.

Considérons l'entier :

$$N = 1 + p_1 \times p_2 \times \cdots \times p_m.$$

— $N > 1$, donc N admet au moins un diviseur premier q (tout entier > 1 possède un diviseur premier).

— Par hypothèse, la liste $p_1, \ldots, p_m$ contient **tous** les nombres premiers, donc $q = p_i$ pour un certain $i \in \{1, \ldots, m\}$.

— Or, pour tout $i \in \{1; \ldots; m\}$, la division de N par p_i donne un reste de 1 :

$$N = p_i \times (p_1 \cdots p_{i-1} \times p_{i+1} \cdots p_m) + 1.$$

Donc $p_i \nmid N$.

— Ainsi, aucun des $p_1, \ldots, p_m$ ne divise N, et en particulier $q \nmid N$.

Ceci est une **contradiction**, car q est à la fois un diviseur de N et un élément de la liste $p_1, \ldots, p_m$ qui ne divise pas N.

Donc l'ensemble des nombres premiers est infini.

Propriété 1.10 : (*Propriétés de la divisibilité*)

Soient $a, b, c \in \mathbb{Z}$.

i) Si $a \mid b$ et $b \mid c$, alors $a \mid c$ (transitivité).

ii) Si $a \mid b$ et $a \mid c$, alors $a \mid (b + c)$ et $a \mid (b - c)$.

iii) Si $a \mid b$ et $b \mid a$, alors $a = b$ ou $a = -b$.

iv) Si $a \mid b$ et $b \neq 0$, alors $|a| \leqslant |b|$.

Lemme 1.11 : (*Lemme d'Euclide*)

Soient a et $b \neq 0$ deux entiers relatifs.

Si p est un nombre premier divisant ab alors p divise a ou p divise b.

Preuve :

Supposons que p ne divise pas a et montrons que p divise b.

Posons $A = \{n \geqslant 1 \mid p \text{ divise } an\}$.

A est non vide car b et $-b$ sont éléments de A.

Supposons $b > 0$ dans la suite.

D'après le th. fondamental de $\mathbb{N}$, soit m le plus petit élément de A.

Comme on a supposé que p ne divise pas a, donc $1 \notin A$ et donc $m \geqslant 2$.

Soit $n \in A$ et montrons que m divise n.

Pour cela, on effectue la division euclidienne de n par m :

soit (q, r) avec $n = mq + r$, et $0 \leqslant r < m$.

$$p \text{ divise } an, \qquad p \text{ divise } am, \qquad p \text{ divise } amq, \qquad p \text{ divise } an - amq = ra.$$

Comme $0 \leqslant r < m$, le caractère minimal de m entraîne $r = 0$, donc $n = mq$, donc m divise n.

(Remarque : A est de la forme mk, $k \in \mathbb{Z}$.)

L'entier $p \in A \implies m \mid p$. Donc comme p premier et comme $m \geqslant 2$, $m = p$. Comme $b \in A$, on a $p \mid b$.

Corollaire 1.12 : (*Généralisation*)

Si p, nombre premier, divise un produit d'entiers, alors il divise au moins un de ces entiers.

En particulier, si p premier divise un produit de nombres premiers, alors il est égal à l'un d'eux.

Théorème 1.13 : (*Décomposition en facteurs premiers*)

Tout entier $\geqslant 2$ s'écrit de façon unique

$$n = p_1^{\alpha_1} \times \cdots \times p_q^{\alpha_q}$$

où $\alpha_i \geqslant 1$ pour tout $1 \leqslant i \leqslant q$ et où $p_1, \ldots, p_q$ sont des nombres premiers vérifiant $p_i < p_{i+1}$ pour tout $1 \leqslant i \leqslant q-1$.

1.3 PGCD

Définition 1.14 : (*Plus grand commun diviseur*)

Soient a et b deux entiers non nuls.

Considérons l'ensemble des diviseurs non nuls positifs communs à a et b :

$$\{d > 0 \mid d \text{ divise } a \text{ et } d \text{ divise } b\}$$

Cet ensemble admet un plus grand élément appelé ***PGCD de a et b***, noté $\text{pgcd}(a,b) = (a \wedge b)$.

Remarque :

L'ensemble des diviseurs communs est nécessairement non vide : 1 divise a, 1 divise b.

De plus, il est nécessairement borné :

d divise $a \quad \Rightarrow \quad d \leqslant |a| \quad \Rightarrow \quad -a \leqslant d \leqslant a$

d divise $b \quad \Rightarrow \quad d \leqslant |b| \quad \Rightarrow \quad -b \leqslant d \leqslant b$

d'où l'existence du plus grand élément et du plus petit élément.

Définition 1.15 : (*Nombres premiers entre eux*)

Deux entiers $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}^*$ sont dits ***premiers entre eux*** si leurs seuls diviseurs communs sont -1 et 1.

Autrement dit :

$$\text{PGCD}(a,b) = 1.$$

Exemple :

i) 8 et 15 sont premiers entre eux :

$$\text{Diviseurs de } 8 : \{1;2;4;8\}, \quad \text{Diviseurs de } 15 : \{1;3;5;15\}.$$

Le seul diviseur commun est 1.

ii) 12 et 18 ne sont **pas** premiers entre eux :

$$\text{PGCD}(12,18) = 6 \neq 1.$$

iii) Deux nombres premiers distincts sont toujours premiers entre eux.

Théorème 1.16 : (*Identité de Bézout*)

Soient a et b deux entiers non nuls.

Alors $\exists (u,v) \in \mathbb{Z} \times \mathbb{Z}$ tels que

$$au + bv = \text{pgcd}(a,b).$$

De plus, tout diviseur commun à a et b divise $\text{pgcd}(a,b)$.

Preuve :

Posons $H = \{an + bm \mid n,m \in \mathbb{Z}\}$.

Alors il existe un unique entier naturel d tel que $H = d\mathbb{Z} = \{dn \mid n \in \mathbb{Z}\}$ et on montre que $d = \text{pgcd}(a,b)$.

Soit $H^+ = H \setminus \{0\}$.

— $H^+ \neq \emptyset$ car $a^2 + b^2 \geqslant 1$ et $a \times a + b \times b \in H^+$.

D'après le th. fondamental de $\mathbb{N}$, soit d le plus petit élément de $H^+ \setminus \{0\}$.

Montrons que $H = d\mathbb{Z}$.

($\subseteq$) : Si $d \in H$, alors d s'écrit $d = am + bn$. Pour tout $k \in \mathbb{Z}$, $dk = (am+bn)k = a(nk) + b(mk) \in H$. Donc $d\mathbb{Z} \subseteq H$.

($\supseteq$) : Soit $h \in H$ et montrons que d divise h. Division euclidienne de h par d :

$$h = dq + r, \quad 0 \leqslant r < d.$$

$r = h - dq$. $h \in H$, $h = an + bm$. $dq \in H$, $dq = an_1 + bm_1$.

$$r = a(n - n_1) + b(m - m_1) \in H.$$

$r \in H$, $0 \leqslant r < d$. Le caractère minimal de d dans $H^+ \setminus \{0\}$ entraîne $r = 0$.

Donc $h = dq$, d divise h, $H \subseteq d\mathbb{Z}$, d'où $H = d\mathbb{Z}$.

Montrons que d divise a et b : $a \in H$ car $a = 1 \times a + 0 \implies a \in d\mathbb{Z} \implies a = dk$, $k \in \mathbb{Z}$, d divise a.

Idem pour $b \in H = d\mathbb{Z}$.

Par la définition première de H, il existe u et v tels que $au + bv = d$.

Soit t un diviseur commun à a et b : $t \mid a \implies t \mid au$, $t \mid b \implies t \mid bv$, donc $t \mid au + bv = d$.

Tout diviseur commun à a et b divise d.

Si $t > 1$ et t divise d, alors $t \leqslant d$, donc d est le plus grand des diviseurs positifs communs à a et b, soit $d = \text{pgcd}(a, b)$.

Corollaire 1.17 : (*Théorème de Bézout*)

Deux entiers a et b sont premiers entre eux si et seulement si $\exists (u, v) \in \mathbb{Z} \times \mathbb{Z}$ tels que $au + bv = 1$.

Preuve :

Si a et b sont premiers entre eux, leur p.g.c.d. est 1. La loi de Bézout s'écrit $au + bv = 1$.

Réciproquement, soient u et v tels que $au + bv = 1$. Soit t un diviseur commun à a et b : $t \mid a \implies t \mid au$, $t \mid b \implies t \mid bv$,

donc $t \mid au + bv = 1$, soit $t = \pm 1$. Donc a et b sont premiers entre eux.

Théorème 1.18 : (*Théorème de Gauss*)

Soient a, b, c trois entiers non nuls. Si a divise bc et si a et b sont premiers entre eux, alors a divise c.

Preuve :

$\text{pgcd}(a, b) = 1$. D'après Bézout, $\exists u, v \in \mathbb{Z} \times \mathbb{Z}$, $au + bv = 1$. Donc $c = auc + bvc$. a divise $bc \implies a$ divise bvc. a divise auc.

Donc a divise $auc + bvc = c$.

1.4 PPCM

Définition 1.19 : (*PPCM*)

Soient a et b deux entiers non nuls. On définit le **PPCM** de a et b le plus petit élément de l'ensemble des multiples communs strictement positifs de a et de b. On note

$$\text{ppcm}(a,b) = a \vee b.$$

Théorème 1.20 : (*Propriétés du PPCM*)

Soient a et $b \neq 0$. Alors tout multiple commun à a et b est divisible par $(a \vee b)$, et

$$\text{ppcm}(a,b) \times \text{pgcd}(a,b) = |ab|.$$

Preuve :

$A = \{m > 0 \mid \text{multiples communs à } a \text{ et } b\}$.

— $A \neq \emptyset$ car $|ab| > 0$ et $|ab| \in A$.

— $A \subseteq \mathbb{N}$.

Soit $\text{ppcm}(a,b)$ le plus petit élément de A.

Soit $t \in A$ et montrons que $\text{ppcm}(a,b)$ divise t. Division euclidienne :

$$t = q \times \text{ppcm}(a,b) + r, \quad 0 \leqslant r < \text{ppcm}(a,b).$$

t multiple commun de a et b, $\text{ppcm}(a,b)$ multiple commun de a et b, donc $t - q \times \text{ppcm}(a,b)$ est multiple commun. Le caractère minimal du ppcm entraîne $r = 0$.

Donc $\text{ppcm}(a,b)$ divise t.

Posons $d = \text{pgcd}(a,b)$. On écrit $a = dk$, $b = dk'$, k et k' premiers entre eux (sinon d n'est plus le plus grand commun diviseur).

Montrons que $d|kk'|$ est multiple commun à a et b : $d|kk'| = |a|k'$, $d|kk'| = |b|k$.

Donc $\text{ppcm}(a,b)$ divise $d|kk'|$. On a $\text{ppcm}(a,b) = aq = bq'$ pour $q, q' \in \mathbb{Z}$. $aq = bq'$, donc $dkq = dk'q'$, $kq = k'q'$. Comme $\text{pgcd}(k,k') = 1$, on obtient k divise q', $|q'| \geqslant k$, donc $\text{ppcm}(a,b) = |bq'| \geqslant |b|k = d|kk'|$.

Le caractère minimal du ppcm et le fait que $d|kk'|$ soit multiple commun entraînent $\text{ppcm}(a,b) = d|kk'|$.

Donc $\text{ppcm}(a,b) \times \text{pgcd}(a,b) = d|kk'| \times d = |dk||dk'| = |a||b| = |ab|$.

1.5 Algorithme d'Euclide

Etant donné deux nombres $a, b \in \mathbb{Z}^*$, on cherche comment calculer u et v ainsi que le pgcd(a,b) de l'identité de Bézout 1.16.

On commence déjà par chercher le pgcd(a,b).

Les divisions successives « donnent » le pgcd(a,b).

Pour $a \geqslant 1$ et $b \geqslant 1$ tels que $a \geqslant b$, on peut toujours écrire :

$$a = bq_1 + r_2, \quad 0 \leqslant r_2 < b.$$

Propriété clé :

— Si d divise a et b, alors d divise a et bq_1,

donc d divise $a - bq_1 = r_2$,

donc d divise b et r_2.

— Si d divise b et r_2, alors d divise b, bq_1 et r_2,

donc d divise $bq_1 + r_2 = a$ et b.

Donc {diviseurs communs à a et b} = {diviseurs communs à b et r_2}.

Algorithme d'Euclide :

$r_0 = a$, $r_1 = b$.

$$a = bq_1 + r_2, \quad 0 \leqslant r_2 < b.$$

Si $r_2 = 0$, STOP : $b \mid a \implies \text{pgcd}(a,b) = b$.

Si $r_2 \neq 0$, on continue la division euclidienne de b par r_2 :

$$b = r_1 = r_2 q_2 + r_3, \quad 0 \leqslant r_3 < r_2.$$

Tant que r_n est différent de 0, on continue le procédé.

La suite (r_n) ainsi définie est strictement décroissante (car $r_{n+1} < r_n$) et elle est positive.

Théorème 1.21 : (*Algorithme d'Euclide et PGCD*)

Soit $m \in \mathbb{N}$ tel que $r_m \neq 0$ et $r_{m+1} = 0$.

Alors le PGCD(a,b) est égal au dernier reste non nul :

$$\text{PGCD}(a,b) = r_m$$

Preuve :

pgcd$(a,b) = \text{pgcd}(r_0, r_1) = \text{pgcd}(r_1, r_2) = \cdots = \text{pgcd}(r_{m-1}, r_m)$.

Comme $r_{m+1} = 0$,

$$r_{m-1} = q_m r_m + r_{m+1} \implies r_{m-1} = q_m r_m$$
$$\implies \text{pgcd}(r_{m-1}, r_m) = r_m$$

Algorithme d'Euclide étendu :

Pour trouver u et v, on fait « remonter » l'algorithme d'Euclide :

on fait la version étendue qui calcule en plus à chaque étape u_i et v_i tels que $r_i = au_i + bv_i$.

Exemple :

$a = 1071$, $b = 1029$:

$$1071 = 1 \times 1029 + 42$$
$$1029 = 24 \times 42 + \boxed{21} \quad \textit{(dernier reste non nul)}$$
$$42 = 2 \times 21 + 0$$
$$\Longrightarrow \text{pgcd}(1071, 1029) = 21$$

Pour trouver u et v on repart de la ligne avec le derniere reste non nul

(attention : on ne fait que remplacer, dévlopper et factoriser. Pas de calcul d'opération!) :

$$1029 = 24 \times 42 + \boxed{21}$$
$$\Longleftrightarrow \boxed{21} = 1029 - 24 \times 42$$
$$= 1029 - 24(1071 - 1029) \quad \textit{(car } 1071 = 1 \times 1029 + 42\textit{)}$$
$$= 25 \times 1029 - 24 \times 1071$$

1.6 Congruences

Définition 1.22 : (*Congruence*)

On dit que deux entiers sont ***congrus modulo*** n ($n \in \mathbb{N}$, $n \geqslant 2$), noté $a \equiv b\ [n]$ ou $a \equiv b \pmod{n}$, si n divise $(a-b)$, autrement dit $a = b + kn$ ($k \in \mathbb{Z}$).

On démontre que $\equiv [n]$ est une relation d'équivalence (réflexivité R, symétrie S, transitivité T).

Propriété 1.23 : (*Compatibilité de la congruence avec les opérations usuelles*)

Soient $n \geqslant 2$ et a_1, a_2, b_1, b_2 tels que $a_1 \equiv b_1\ [n]$ et $a_2 \equiv b_2\ [n]$. Alors :

$$a_1 + a_2 \equiv b_1 + b_2\ [n]$$
$$a_1 a_2 \equiv b_1 b_2\ [n]$$
$$a_1^q \equiv b_1^q\ [n],\ \forall q \geqslant 1$$

Preuve :

Soient $n \geqslant 2$ et a_1, a_2, b_1, b_2 tels que $a_1 \equiv b_1\ [n]$ et $a_2 \equiv b_2\ [n]$. Donc :

$$\exists k_1 \in \mathbb{Z}, \quad a_1 = b_1 + k_1 n$$
$$\exists k_2 \in \mathbb{Z}, \quad a_2 = b_2 + k_2 n$$

En additionnant chaque membre de ces équations, on obtient :

$$a_1 + a_2 = (b_1 + b_2) + (k_1 + k_2)n$$
$$\Longrightarrow a_1 + a_2 \equiv b_1 + b_2\ [n]$$

En multipliant chaque membre des deux premères équations, on obtient :

$$a_1 a_2 = (b_1 + k_1 n)(b_2 + k_2 n)$$
$$\Longrightarrow a_1 a_2 = b_1 b_2 + n(k_1 b_2 + k_1 k_2 n + b_1 k_2)$$

$$\Longrightarrow a_1 a_2 \equiv b_1 b_2 [n]$$

$a_1^q \equiv b_1^q [n]$ par récurrence avec $\times$ (à faire).

Chapitre 2

Groupes, Anneaux, Corps

2.1 Loi de composition interne

Définition 2.1 : (*Loi de composition interne (l.c.i.)*)

Soit E un ensemble non vide.

Une ***loi de composition interne*** *(abrégée l.c.i.)* dans E est une application $*$ de $E \times E$ dans E :

$$\begin{array}{rccc} *: & E \times E & \longrightarrow & E \\ & (a,b) & \longmapsto & *(a,b) = a * b \end{array}$$

$a * b$ est appelé ***composé*** de a et de b.

Définition 2.2 : (*Magma*)

On appelle ***magma*** un ensemble E **muni** d'une loi de composition interne $*$. On le note $(E, *)$.

Exemple :

- $\mathbb{N}$ muni de l'addition : $(\mathbb{N}, +)$,
- $\mathcal{M}_n(\mathbb{K})$ muni du produit matriciel : $(\mathcal{M}_n(\mathbb{K}), \cdot)$,
- $\mathbb{C}$ muni de la multiplication : $(\mathbb{C}, \cdot)$,
- $\mathcal{P}(E)$ muni de l'union : $(\mathcal{P}(E), \cup)$.
- $\mathcal{C}_c^\infty(\mathbb{R})$ muni de la convolution $(f * g)(x) = \int_0^x f(x-t)g(t)\,dt$
- La division dans $\mathbb{Q}$ n'est pas une l.c.i. sur $\mathbb{N}$.

Définition 2.3 : (*Associativité*)

Soit $(E, *)$ un magma.

La loi $*$ est dite ***associative*** si

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

On dit que $(E, *)$ est un magma associatif.

Définition 2.4 : (*Commutativité*)

Soit $(E, *)$ un magma.

La loi $*$ est dite ***commutative*** si

$$\forall a, b \in E, \quad a * b = b * a$$

Exemple :

Le produit matriciel est associatif et **n'est pas** commutatif.

Définition 2.5 : (*Élément neutre*)

Soit $(E, *)$ un magma.

Un ***élément neutre de*** E ***pour*** $*$ est un élément e tel que :

$$\forall a \in E, \quad a * e = e * a = a$$

Pour une loi notée « + » dans E, le neutre est noté 0_E (ou simplement 0).

Pour une loi notée « × » dans E, le neutre est noté 1_E (ou simplement 1).

On peut définir neutre à gauche et neutre à droite.

Propriété 2.6 : (*Unicité du neutre*)

L'élément neutre, s'il existe, est unique.

Preuve :

En effet, soient e et e' deux neutres de $(E, *)$:

$$e * e' = e \quad (\text{car } e' \text{ neutre})$$

et

$$e * e' = e' \quad (\text{car } e \text{ neutre})$$

donc

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

donc

$$e = e'$$

Donc s'il y a un neutre, il est unique.

Définition 2.7 : (*Magma unifère*)

Soit $(E, *)$ magma.

$(E, *)$ est dit ***unifère*** s'il existe un élément neutre.

Définition 2.8 : (*Elément symétrisable*)

Soit $(E, *)$ un magma unifère.

Un élément a est dit ***symétrisable*** s'il existe $a' \in E$ tel que $a * a' = a' * a = e$.

L'élément a' est dit ***élément symétrique*** de a.

On peut aussi définire ***symétrisable à droite*** et ***symétrisable à gauche*** d'un élément a en demandant que $a * a' = e$ ou $a'' * a = e$ respectivement. A noter que a' et a'' ne sont pas nécessairement égaux.

Exemple :

$(\mathbb{N}, +)$ est un magma unifère.

0 est symétrisable et son élément symétrique est 0 car $0 + 0 = 0$.

C'est le seul élément symétrisable car il n'y a pas d'autre solution à l'équation $a + b = 0$ pour $a \in \mathbb{N}$ et $b \in \mathbb{N}$.

Propriété 2.9 : (*Unicité du symétrique dans un magma associatif unifère*)

Soit $(E, *)$ un magma unifère et associatif.

Tout élément possède **au plus** un symétrique *(donc soit il n'en a pas soit il en a exactement un).*

Preuve :

Soient a_1 et a_2 deux symétriques de a :

$$(a_2 * a) * a_1 = e * a_1 = a_1 \quad \text{(la loi } * \text{ est associative)}$$

$$a_2 * (a * a_1) = a_2 * e = a_2$$

Comme $(a_2 * a) * a_1 = a_2 * (a * a_1)$, on a $a_1 = a_2$.

Propriété 2.10 : (*Symétrique d'un composé*)

Soit $(E, *)$ un magma unifère et associatif.

Si a et b sont deux éléments symétrisables, alors le composé $a * b$ est symétrisable et son symétrique est :

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

Preuve :

Soient a' et b' les symétriques respectifs de a et b :

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

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

Définition 2.11 : (*Élément simplifiable (ou régulier)*)

Un élément a est dit ***simplifiable*** ou ***régulier*** si :

$$\forall b \in E, c \in E, \quad a * b = a * c \iff b = c$$

$$\text{et} \quad b * a = c * a \iff b = c$$

Exemple :

Tout élément de $(\mathbb{N}, +)$ est régulier.

0 n'est pas régulier dans $(\mathbb{R}, \times)$.

Propriété 2.12 : (*Symétrisable implique régulier*)

Soit $(E, *)$ un magma unifère et associatif.

Si a est symétrisable, alors a est régulier. *(La réciproque est fausse)*

Preuve :

Soient $b, c \in E$. Notons a' le symétrique de a.

$a * b = a * c \implies a' * (a * b) = a' * (a * c) \implies (a' * a) * b = (a' * a) * c \implies e * b = e * c \implies b = c.$

De la même façon, $b * a = c * a \implies b * a * a' = c * a * a' \implies b = c.$

Remarque :

Dans $(\mathbb{N}^*, \times)$, 2 est régulier mais n'est pas symétrisable.

Définition 2.13 : (*Partie stable, loi induite*)

$(E, *)$ un magma et F une partie non vide de E.

F est dite ***stable pour*** $*$ si

$$\forall a \in F, \forall b \in F, \quad a * b \in F$$

Dans ce cas, la restriction de $*$ à $F \times F$ est une l.c.i. dans F.

On dit alors que F est muni de la ***loi induite*** par celle de E.

La commutativité et l'associativité sont conservées aux structures induites.

Définition 2.14 : (*Morphisme (homomorphisme)*)

Soient $(E, *)$ et (F, T) deux magmas.

Une application f de $E \to F$ est appelée ***homomorphisme*** (ou ***morphisme***) de $(E, *)$ dans (F, T) si $\forall a, b \in E$,

$$f(a * b) = f(a)\ T\ f(b).$$

Exemple :

— $(\mathcal{M}_n(\mathbb{C}), \cdot) \to (\mathbb{R}, \cdot)$, $A \mapsto \det(A)$.

— $(\mathbb{R}_+^*, \cdot) \to (\mathbb{R}, +)$, $x \mapsto \ln x$.

— $(\mathbb{C}, \cdot) \to (\mathbb{R}, \cdot)$, $z \mapsto \bar{z}$.

Définition 2.15 : (*Isomorphisme, automorphisme*)

Soient $(E, *)$ et (F, T) deux magmas.

— Un **morphisme bijectif** est un **isomorphisme**.

— Un isomorphisme de $(E, *)$ dans $(E, *)$ est un **automorphisme**.

— $(E, *)$ et (F, T) sont dits **isomorphes** s'il existe un isomorphisme de $(E, *)$ dans (F, T).

Théorème 2.16 : (*Composition de morphismes*)

Soient $(E, *)$, (F, T) et (G, Δ) trois magmas.

Si $f : (E, *) \to (F, T)$ et $g : (F, T) \to (G, \Delta)$ sont deux morphismes, alors $g \circ f : (E, *) \to (G, \Delta)$ est un morphisme.

Preuve :

$g \circ f$ est bien définie de E dans G. Pour $a, b \in E$:

$$g \circ f(a * b) = g(f(a * b)) = g(f(a)\ T\ f(b)) = g(f(a))\ \Delta\ g(f(b)) = (g \circ f)(a)\ \Delta\ (g \circ f)(b).$$

Théorème 2.17 : (*Inverse d'un isomorphisme*)

Soient $(E, *)$ et (F, T) deux magmas.

Si f est un isomorphisme de $(E, *)$ dans (F, T), alors f^{-1} est un isomorphisme de (F, T) dans $(E, *)$.

Preuve :

Comme f est bijective, f^{-1} est bien définie de F dans E et est bijective.

Pour $y_1, y_2 \in F$, f étant bijective, soient $x_1, x_2 \in E$ (uniques) tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$.

$$y_1 \ T \ y_2 = f(x_1) \ T \ f(x_2) = f(x_1 * x_2).$$

Comme f est bijective,

$$f^{-1}(y_1 \ T \ y_2) = (f^{-1} \circ f)(x_1 * x_2) = x_1 * x_2 = f^{-1}(y_1) * f^{-1}(y_2)$$

2.2 Groupes

2.2.1 Définition

Définition 2.18 : (*Groupe*)

Soit $(G, *)$ un magma.

$(G, *)$ est un ***groupe*** si :

- $*$ est associative,
- $(G, *)$ possède un élément neutre,
- tout élément est symétrisable.

Remarque :

— L'élément neutre est unique, noté e.

— Le symétrique est unique, noté a^{-1}.

— Tout élément est régulier.

— $(x * y)^{-1} = y^{-1} * x^{-1}$.

— $x * y = e \implies y = x^{-1}$.

— $x_1 * x_2 * \cdots * x_n$ est bien défini (car $*$ associative).

Si la loi est commutative, $(G, *)$ est dit **groupe abélien** (ou commutatif).

2.2.2 Sous-groupes

Définition 2.19 : (*Sous-groupe*)

Soit $(G,*)$ un groupe et H une partie non vide de G, stable par la loi $*$.

Si H muni de la loi induite par celle de $(G,*)$ possède une structure de groupe, on dit que H est un **sous-groupe** de $(G,*)$.

Propriété 2.20 : (*Propriété du sous-groupe*)

$e \in H$. Si e_1 est le neutre de H, alors $\forall x_1 \in H$, $e_1 * x_1 = x_1 * e_1 = x_1$. Pour tout $x \in G$, $e * x = x * e = x$, donc $x = x_1$ et $e_1 * x_1 = e * x_1$. Comme x_1 est régulier, $e_1 = e$.

De même, $a^{-1} \in H$ (le symétrique dans H est le symétrique dans G).

Théorème 2.21 : (*Caractérisation des sous-groupes*)

Soit $(G,*)$ un groupe et $H \subseteq G$, $H \neq \emptyset$. $(H,*)$ est un sous-groupe de $(G,*)$ si et seulement si :

1. $\forall a,b \in H$, $a * b \in H$ (stabilité),
2. $\forall a \in H$, $a^{-1} \in H$ (le symétrique de a dans G).

Preuve :

($\Longrightarrow$) : 1) vrai par def du ss-groupe. 2) Soit $a \in H$ et a^{-1} le symétrique de a dans $(G,*)$ et a_1 le symétrique de a dans $(H,*)$. Comme $a * a^{-1} = e$ dans G et $a * a_1 = e$ dans H, et comme a est régulier dans G, $a^{-1} = a_1 \in H$.

($\Longleftarrow$) : H est stable pour $*$ et $*$ associative. H est non vide, soit $a \in H$. Par 2), $a^{-1} \in H$. H stable pour $*$, donc $a^{-1} * a \in H$, d'où $e \in H$. $(H,*)$ possède un élément neutre e. Par 2), tout élément est symétrisable.

Théorème 2.22 : (*Autre version (critère condensé)*)

Soit $(G,*)$ un groupe, $H \subseteq G$, $H \neq \emptyset$. $(H,*)$ est un sous-groupe de $(G,*)$ si et seulement si

$$\forall a,b \in G, \quad a^{-1} * b \in H.$$

Preuve :

($\Longrightarrow$) : d'après le théorème précédent, $a^{-1} \in H$. Par la stabilité de H, $a^{-1} * b \in H$.

($\Longleftarrow$) : H étant non vide, soit $a \in H$. D'après la propriété, $a^{-1} * a \in H$, d'où $e \in H$. Comme $e \in H$, $\forall a \in H$, $a^{-1} * e \in H$, d'où $a^{-1} \in H$. Il reste la stabilité : si $a,b \in H$, alors $a^{-1} \in H$, $(a^{-1})^{-1} * b = a * b \in H$.

Exemple :

— $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ sous-groupe de $(\mathbb{Z},+)$.

— $\{e^{2ik\pi/n} \mid 0 \leqslant k \leqslant n-1\}$ sous-groupe de $(U,\cdot)$ où $U = \{z \in \mathbb{C} \mid |z| = 1\}$.

— $\{M \in \mathcal{M}_n(\mathbb{R}) \mid \det M = 2^k,\ k \in \mathbb{Z}\}$ sous-groupe de $(\mathrm{GL}_n(\mathbb{R}),\cdot)$.

Propriété 2.23 : (*Intersection de sous-groupes*)

L'intersection d'une famille non vide de sous-groupes de $(G,*)$ est un sous-groupe de $(G,*)$.

Preuve :

Soit $(H_i)_{i\in I}$, $I \neq \emptyset$, une famille de ss-groupes de $(G,*)$. Soit $a,b \in \bigcap_{i\in I} H_i$ ($\neq \emptyset$ car $e \in H_i$ pour tout $i \in I$). D'après le th. précédent, $\forall I$, $a \in H_i$ et $b \in H_i$, donc $a^{-1} * b \in H_i$. D'où $a^{-1} * b \in \bigcap_{i\in I} H_i$. Par la caractérisation des ss-groupes, $\bigcap_{i\in I} H_i$ est un ss-groupe de $(G,*)$.

Remarque :

On ne peut rien dire de l'union de deux ss-groupes ou plus. Ex. : $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un ss-groupe de $(\mathbb{Z},+)$. Si $2\mathbb{Z} \cup 3\mathbb{Z}$ était un ss-groupe, on aurait $2+3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, ce qui est faux.

Propriété 2.24 : (*Sous-groupe engendré*)

Soit A une partie de G. Il existe un plus petit ss-groupe au sens de l'inclusion contenant A. Ce ss-groupe est appelé **sous-groupe de** $(G,*)$ **engendré par** A.

Preuve :

D'après le théorème précédent, $\bigcap_{H\supseteq A,\ H \text{ ss-gpe de } (G,*)} H = H_A$ est un ss-groupe. Par déf. de H_A, $A \subseteq H_A$. De la même façon, si S est un ss-groupe de $(G,*)$ contenant A, on a aussi $\bigcap_{H\supseteq A} H \subseteq S$.

Définition 2.25 : (*Sous-groupe monogène*)

H un ss-groupe de $(G,*)$ est dit **monogène** s'il existe $a \in G$ tel que $H = G_r(\{a\})$ = le sous-groupe engendré par $\{a\}$.

Exemple :

[Exercice]

Soit $(G,\cdot)$ groupe noté multiplicativement et $A \subseteq G$, $A \neq \emptyset$. Alors

$$G_r(A) = \{a_1, a_2, \ldots, a_n \mid n \in \mathbb{N}^* \text{ et } a_i \in A \text{ ou } a_i^{-1} \in A,\ \forall i \in \{1,\ldots,n\}\}.$$

(Sous-groupe engendré par A.)

2.2.3 Groupe produit

Définition 2.26 : (*Groupe produit*)

Soient (G_1,T_1) et (G_2,T_2) deux groupes. Alors le produit cartésien $G_1 \times G_2$ muni de la loi de composition interne définie par

$$\forall (a_1,b_1) \in G_1 \times G_2,\ \forall (a_2,b_2) \in G_1 \times G_2, \quad (a_1,b_1) * (a_2,b_2) = (a_1 T_1 a_2,\ b_1 T_2 b_2)$$

est un groupe appelé **groupe produit**.

On démontre :

1. l.c.i.
2. associativité
3. le neutre est (e_1,e_2)
4. chaque élément a un symétrique : $(a,b)^{-1} = (a^{-1},b^{-1})$ (dans G_1 et G_2 respectivement).

Plus généralement, si $(G_i,T_i)_{1\leqslant i\leqslant n}$ sont n groupes, on définit $G_1 \times G_2 \times \cdots \times G_n$ muni de la loi

$$(a_1,a_2,\ldots,a_n) * (b_1,b_2,\ldots,b_n) = (a_1 T_1 b_1,\ a_2 T_2 b_2,\ \ldots,\ a_n T_n b_n),$$

qui est un groupe produit cartésien.

2.2.4 Morphismes de groupes

Définition 2.27 : (*Morphisme de groupe*)

Soient $(G,*)$ et (G',T) deux groupes et f une application de $G \to G'$. f est un **homomorphisme** (ou morphisme) de groupes de $(G,*)$ dans (G',T) si

$$\forall a,b \in G, \quad f(a*b) = f(a)\,T\,f(b).$$

Si f bijective : isomorphisme de groupe.

Si $G = G'$ et que $* = T$, alors f est un endomorphisme et si f est bijectif, alors f est un automorphisme.

Théorème 2.28 : (*Propriétés des morphismes de groupes*)

Soient $(G,*)$ et (G',T) deux groupes, e neutre de G, e' neutre de G', f un morphisme de $(G,*)$ dans (G',T).

1. $f(e) = e'$.
2. $f(a^{-1}) = \big(f(a)\big)^{-1}$.
3. $f(G)$ muni de la loi induite par celle de (G',T) est un ss-groupe de (G',T), appelé **groupe image** de G par f : $f(G) = \operatorname{Im} f$.
4. $f^{-1}\{e'\}$ muni de la loi induite par celle de $(G,*)$ est un ss-groupe de $(G,*)$ appelé **noyau** de f et noté $\ker f$. $\ker f = f^{-1}\{e'\}$.

Remarque :

Attention : $f(G) = \{f(a),\ a \in G\}$, $f(G) \subseteq G'$. $f^{-1}\{e'\} = \{a \in G \mid f(a) = e'\}$, $\ker f \subseteq G$.

Preuve :

1) $x \in G \implies x*e = e*x = x$, donc $f(x*e) = f(e*x) = f(x)$.

Morphisme : $f(x)\,T\,f(e) = f(e)\,T\,f(x) = f(x)$.

Régularité de G' : $f(e) = e'$.

2) Soit $a \in G$, $a * a^{-1} = e$.

D'après 1) et f morphisme : $f(a)\,T\,f(a^{-1}) = f(a*a^{-1}) = f(e) = e'$.

La déf du symétrique : $\big(f(a)\big)^{-1} = f(a^{-1})$.

3) $f(G) \neq \emptyset$, $e' = f(e) \in f(G)$.

Soient $x', y' \in f(G)$. Par déf de $f(G)$, $\exists x \in G$ et $\exists y \in G$ tel que $x' = f(x)$ et $y' = f(y)$.

$(x')^{-1}\,T\,y' = f(x)^{-1}\,T\,f(y) = f(x^{-1})\,T\,f(y) = f(x^{-1} * y)$.

Comme $x^{-1} * y \in G$, $(x')^{-1}\,T\,y' \in f(G)$.

Par le théorème de caractérisation des sous-groupes, $f(G)$ est un ss-groupe de (G',T).

4) $\ker f = \{x \in G \mid f(x) = e'\}$. D'après 1), $f(e) = e'$, donc $e \in \ker f \neq \emptyset$. Soient a et $b \in \ker f$. $f(a^{-1} * b) = f(a^{-1})\,T\,f(b) = \big(f(a)\big)^{-1}\,T\,f(b) = (e')^{-1}\,T\,e' = e'$. Donc $a^{-1} * b \in \ker f$.

Donc $(\ker f, *)$ est un ss-groupe de $(G,*)$.

Théorème 2.29 : (*Injectivité et noyau*)

Soient $(G,*)$ et (G',T) deux groupes et f un morphisme de groupes de $(G,*)$ dans (G',T).

$$f \text{ injective} \iff \ker f = \{e\}.$$

Preuve :

$\boxed{\Longrightarrow}$: Soit f injective. Alors $f(e) = e'$, on a donc :

$$\begin{aligned} x \in \ker f &\iff f(x) = e' \\ &\iff f(x) = f(e) \\ &\iff x = e \quad (\text{car } f \text{ est injective}) \end{aligned}$$

D'où

$$\ker f = \{e\}$$

$\boxed{\Longleftarrow}$: Si $\ker f = \{e\}$. Soient $a, b \in G$ tels que $f(a) = f(b)$. Alors :

$$\begin{aligned} e' &= \left(f(a)\right)^{-1} T f(a) \\ &= \left(f(a)\right)^{-1} T f(b) && \text{car } f(a) = f(b) \\ &= f\left(a^{-1}\right) T f(b) \\ &= f\left(a^{-1} * b\right) && \text{car } f \text{ morphisme de } (G,*) \text{ dans } (G',T) \end{aligned}$$

Donc $a^{-1} * b \in \ker f = \{e\}$.

Donc $a^{-1} * b = e$, $a * a^{-1} * b = a * e$, $b = a$.

Donc f injective.

2.2.5 Groupes finis

Définition 2.30 : (*Ordre d'un groupe, ordre d'un élément*)

Soit $(G,*)$ un groupe.

Si G contient un nombre fini d'éléments, on appelle ***ordre de*** G le cardinal de G. Sinon G est dit d'ordre infini.

Soit $a \in G$. On définit l'***ordre de*** a par l'ordre du sous-groupe engendré par $\{a\}$: $G_r(\{a\})$.

Un groupe ou un sous-groupe est dit ***cyclique*** s'il est fini et monogène.

Exemple :

$\{e^{i\frac{2k\pi}{n}} \mid 0 \leqslant k \leqslant n-1\}$ groupe cyclique des racines n-ièmes de l'unité. $G_r = |\{e^{i\frac{2\pi}{n}}\}|$ dans $(U,\times)$.

Si θ et π ne sont pas liés par deux rationnels, $G_r(e^{i\theta})$ est monogène d'ordre infini.

Théorème 2.31 : (*Théorème de Lagrange*)

Soit H un sous-groupe de G, G d'ordre fini. Alors l'ordre de H divise l'ordre de G.

Preuve :

Voir polycopié.

2.2.6 Groupe quotient

Définition 2.32 : (*Groupe quotient*)

Soit $(G,*)$ un groupe. Soit $\mathscr{R}$ une relation d'équivalence sur $(G,*)$. $\mathscr{R}$ est dite **compatible avec la loi** $*$ si

$$x\mathscr{R}y \text{ et } z\mathscr{R}w \implies x*z\mathscr{R}y*w.$$

Théorème 2.33 : (*Groupe quotient*)

Soit $\mathscr{R}$ une relation d'équivalence sur $(G,*)$ compatible avec $*$. Alors l'ensemble quotient $G/\mathscr{R}$ muni de la l.c.i. $\overline{*}$ définie par

$$\bar{x}\overline{*}\bar{y} = \overline{x*y}$$

est un groupe.

Preuve :

1. $\overline{*}$ est-elle une l.c.i. ? Indépendance par rapport au choix du représentant de la classe d'équivalence : $\bar{x}=\bar{x}' \iff x\mathscr{R}x'$, $\bar{y}=\bar{y}' \iff y\mathscr{R}y'$. Comme $\mathscr{R}$ est compatible avec $*$: $x*y\mathscr{R}x'*y'$, donc $\overline{x*y}=\overline{x'*y'}$.
2. $\overline{*}$ associative : $(\bar{x}\overline{*}\bar{y})\overline{*}\bar{z} = \overline{(x*y)*z} = \overline{x*(y*z)} = \bar{x}\overline{*}(\bar{y}\overline{*}\bar{z})$.
3. Neutre : $\bar{x}\overline{*}\bar{e} = \overline{x*e} = \bar{x}$ (e neutre de G). De même $\bar{e}\overline{*}\bar{x} = \bar{x}$.
4. Symétrique : pour $\bar{x}\in G/\mathscr{R}$, $\bar{x}\overline{*}\overline{x^{-1}} = \overline{x*x^{-1}} = \bar{e}$. De même $\overline{x^{-1}}\overline{*}\bar{x} = \bar{e}$. Donc $\overline{x}^{-1} = \overline{x^{-1}}$.

Application : Cas $(G,*)$ groupe abélien et H un sous-groupe de $(G,*)$.

Définition 2.34 : (*Relation modulo H*)

La **relation modulo** H définie par $x\mathscr{R}y$ ssi $x*y^{-1}\in H$ est une relation d'équivalence compatible avec la loi $*$.

L'ensemble quotient $G/\mathscr{R}$ noté G/H, $(G/H,\overline{*})$ est le **groupe quotient**.

Preuve :

$\mathscr{R}$ relation d'équivalence : $x\in G \implies x*x^{-1}=e\in H \implies x\mathscr{R}x$ réflexive. $x\mathscr{R}y \implies x*y^{-1}\in H \implies (x*y^{-1})^{-1}\in H$ (car H ss-groupe) $\implies y*x^{-1}\in H \implies y\mathscr{R}x$ symétrique.

Si $x\mathscr{R}y$ et $y\mathscr{R}z$, alors $x*y^{-1}\in H$ et $y*z^{-1}\in H$. Comme H stable : $x*y^{-1}*y*z^{-1} = x*z^{-1}\in H$, donc $x\mathscr{R}z$ transitivité.

$\mathscr{R}$ compatible avec $*$: Soient x,y,z,w tel que $x\mathscr{R}y$ et $z\mathscr{R}w$. $x*y^{-1}\in H$, $z*w^{-1}\in H$. Comme G est abélien : $x*z*(y*w)^{-1} = x*z*w^{-1}*y^{-1}\in H$. Donc $x*z\mathscr{R}y*w$ (compatibilité avec $*$).

D'après le th. précédent, $G/\mathscr{R} = G/H$ muni de la loi $\overline{*}$: $\bar{x}\overline{*}\bar{y} = \overline{x*y}$ est un groupe abélien.

Quelles sont les classes d'équivalence ?

$\bar{x} = x*H = \{x*y \mid y\in H\}$.

Preuve :

Si $z = x*y$ avec $y\in H$, alors $x*z^{-1} = x*(x*y)^{-1} = x*y^{-1}*x^{-1} = y^{-1}\in H$ (car H ss-groupe). Donc $z\mathscr{R}x$, d'où $x*H\subseteq\bar{x}$.

Réciproquement, si $z\in\bar{x}$, par déf : $x*z^{-1}\in H$. H ss-groupe $\implies z*x^{-1}\in H$ (commutativité). $\implies x^{-1}*z\in H$ commutativité.

Donc $z = x*(x^{-1}*z)\in x*H$, d'où $\bar{x}\subseteq x*H$. Donc $\bar{x} = xH$.

Exemple :

$(\mathbb{Z},+)$ groupe commutatif, $2\mathbb{Z}$ ss-groupe. $x\mathscr{R}y$ ssi $x-y\in 2\mathbb{Z} \iff x\equiv y[2]$.

2 classes d'équivalence $\bar{0}$ et $\bar{1}$:

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

2.2.7 $\mathbb{Z}/n\mathbb{Z}$: groupes cycliques

Théorème 2.35 : (*Sous-groupes de* $(\mathbb{Z},+)$)

Soit H un sous-groupe de $(\mathbb{Z},+)$. Alors il existe $a\in\mathbb{N}$ tel que $H=a\mathbb{Z}$.

Preuve :

$H\neq\emptyset$. Si $H=\{0\}$, c'est fini, $H=0\times\mathbb{Z}$.

Sinon $H\neq\{0\}$. Posons $H^+\setminus\{0\}=\{n\in H,\ n>0\}\neq\emptyset$.

Propriété fondamentale de $\mathbb{N}$: $H^+\setminus\{0\}$ partie non vide de $\mathbb{N}$, possède un plus petit élément, noté a.

$a\in H \implies -a\in H$ par récurrence $na\in H$ pour tout $m\in\mathbb{N}$, $-na\in H$ pour tout $n\in\mathbb{N}$. Donc $a\mathbb{Z}\subseteq H$.

Soit $x\in H$. Il existe q et r tels que $x\in H,\ qa\in H,\ \implies r\in H$. On ne peut avoir $r\neq 0$ car a est le plus petit élément de $H^+\setminus\{0\}$.

Donc $r=0$ et $x=aq$, soit $x\in a\mathbb{Z}$, donc $H\subseteq a\mathbb{Z}$.

(1) et (2) $\implies H=a\mathbb{Z}$.

Soit $n\geqslant 0$. $n\mathbb{Z}$ sous-groupe de $(\mathbb{Z},+)$ et définit $\mathbb{Z}/n\mathbb{Z}$.

Si $n\geqslant 1$, on démontre que $\mathbb{Z}/n\mathbb{Z}$ est d'ordre n et que ses éléments sont $\bar{0},\bar{1},\ldots,\overline{n-1}$.

Preuve :

Soit $0\leqslant i<j\leqslant n-1$. Si $i\equiv j[n]$, alors $i-j=kn$, $k\in\mathbb{Z}$. Comme $0<j-i\leqslant n-1$, on a $k=0$, soit $i=j$, contradiction. Donc $i\not\equiv j[n] \implies \bar{i}\neq\bar{j}$.

$\mathbb{Z}/n\mathbb{Z}$ possède au moins n éléments $\bar{0},\bar{1},\ldots,\overline{n-1}$.

Soit $k\in\mathbb{Z}$, division euclidienne de k par n : $k=qn+r$, $0\leqslant r\leqslant n-1$. Donc $k\equiv r[n]$. Comme $0\leqslant r\leqslant n-1$, $\bar{k}=\bar{r}$ avec $0\leqslant r\leqslant n-1$.

Conclusion : les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont $\bar{0},\bar{1},\bar{2},\ldots,\overline{n-1}$.

$(\mathbb{Z}/n\mathbb{Z},+)$ monogène (engendré par $\bar{1}$) cyclique d'ordre n.

Si $1\leqslant i\leqslant n-1$, $\bar{i}=\underbrace{\bar{1}+\bar{1}+\cdots+\bar{1}}_{i \text{ termes}}$, donc $\bar{1}$ engendre $(\mathbb{Z}/n\mathbb{Z},+)$.

D'où la conclusion : $(\mathbb{Z}/n\mathbb{Z},+)$ cyclique d'ordre n.

Théorème 2.36 : (*Classification des groupes monogènes*)

Soit $(G,*)$ un groupe monogène. Alors :

1. Si G n'est pas d'ordre fini, alors $(G,*)$ est isomorphe à $(\mathbb{Z},+)$.
2. Si G est d'ordre n ($n\geqslant 1$), alors $(G,*)$ est cyclique et isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$.

Preuve :

G monogène, soit $a \in G$ tel que $G = G_r(\{a\})$.

Définissons $f : (\mathbb{Z}, +) \to (G, *)$ par $k \mapsto a^k = \underbrace{a * a * \cdots * a}_{k \text{ fois}}$.

1. Si G n'est pas d'ordre fini, alors f est un morphisme surjectif de $(\mathbb{Z}, +)$ dans $(G, *)$. Pour le voir, il suffit de voir que $G_r(\{a\}) = \{a^n,\ n \in \mathbb{N}\} \cup \{a^{-n},\ n \in \mathbb{N}\}$.
2. Si G est d'ordre n ($n \geqslant 1$). Définissons $\varphi : (\mathbb{Z}/n\mathbb{Z}, +) \to (G, *)$ par $\bar{k} \mapsto \overline{a^k} = a^k$.

   φ est bien définie : $\bar{k} = \bar{q} \iff k - q \in n\mathbb{Z} \iff k = q + nk' \implies a^k = a^q \cdot (a^n)^{k'} = a^q$ (car $a^n = e$, exercice).

   φ morphisme : $\varphi(\bar{k}) * \varphi(\bar{q}) = a^k * a^q = a^{k+q} = \varphi(\overline{k+q}) = \varphi(\bar{k} + \bar{q})$.

   φ bijectif : G d'ordre $n \implies a^k \neq e$ pour $1 \leqslant k \leqslant n-1$ et $\forall k \in \mathbb{N}$, $k = nq + r$, $0 \leqslant r < n$, $a^k = a^r$. Donc φ surjective. Si $a^k = a^q$, alors $a^{k-q} = e$, n divise $k - q$, $\bar{k} = \bar{q}$, φ injective.

   Donc φ bijective et conclusion $(G, *)$ isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

[Remarque : il faut montrer (voir exercice) que $a^n = e$.]

2.2.8 Groupe symétrique

Définition 2.37 : (*Groupe symétrique*)

Soit $n \geqslant 1$. On note $\mathscr{S}_n$ l'ensemble des permutations de $\{1, \ldots, n\}$ (bijections de $\{1, \ldots, n\}$ sur lui-même), muni de la composition des applications. C'est le **groupe symétrique** $(\mathscr{S}_n, \circ)$.

$\text{Card}(\mathscr{S}_n) = n!$

Remarque :

— Id (identité) $\in \mathscr{S}_n$, neutre.

— La composée de 2 bijections est une bijection, donc $\circ$ l.c.i. sur $\mathscr{S}_n$.

— $\sigma \circ \text{Id} = \text{Id} \circ \sigma = \sigma$, Id neutre.

— $(\sigma_1 \circ \sigma_2) \circ \sigma_3 = \sigma_1 \circ (\sigma_2 \circ \sigma_3)$, associativité.

— $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \text{Id}$, $\sigma^{-1} \in \mathscr{S}_n$.

Si $n \geqslant 3$, $\mathscr{S}_n$ n'est pas abélien.

Notation : Une permutation σ se note $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$.

Définition 2.38 : (*Points fixes, support*)

Soit $\sigma \in \mathscr{S}_n$.

— i est dit **point fixe** si $\sigma(i) = i$.

— $\text{supp}(\sigma) = \{i \in \{1, \ldots, n\} \mid \sigma(i) \neq i\}$ (complémentaire de l'ensemble des pts fixes).

Propriété 2.39 : (*Support de la composée*)

Soient σ et $\tau \in \mathcal{S}_n$.

$$\mathrm{supp}(\sigma \circ \tau) \subseteq \mathrm{supp}(\sigma) \cup \mathrm{supp}(\tau).$$

Si σ et τ ont des supports disjoints ($\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \emptyset$), alors

$$\mathrm{supp}(\sigma \circ \tau) = \mathrm{supp}(\sigma) \cup \mathrm{supp}(\tau), \quad \sigma \circ \tau = \tau \circ \sigma, \quad \sigma \circ \tau = \mathrm{Id} \implies \sigma = \mathrm{Id} \text{ et } \tau = \mathrm{Id}.$$

Définition 2.40 : (*Cycle, transposition*)

Soit p un entier $\geqslant 2$ et soit $i_1, \ldots, i_p$ des entiers dans $\{1, \ldots, n\}$ deux à deux distincts. On note $(i_1, \ldots, i_p)$ l'élément $\gamma \in \mathcal{S}_n$ défini par

$$\gamma_i = \begin{cases} i & \text{si } i \notin \{i_1, \ldots, i_p\} \\ i_{k+1} & \text{si } i = i_k,\ 1 \leqslant k \leqslant p-1 \\ i_1 & \text{si } i = i_p. \end{cases}$$

Une telle permutation γ est appelée **cycle** (ou permutation circulaire) $= (i_1, \ldots, i_p)$ de longueur p (ou d'ordre p).

Une **transposition** est tout cycle de longueur 2, autrement dit $t = (i, j)$, $i \neq j$ avec $t(i) = j$, $t(j) = i$, $t(k) = k$ si $k \notin \{i, j\}$.

Théorème 2.41 : (*Décomposition en cycles à supports disjoints*)

Soit $\sigma \in \mathcal{S}_n$. Alors σ se décompose en $\sigma = \gamma_1 \circ \cdots \circ \gamma_m$, où $m \in \mathbb{N}$ et $\gamma_1, \ldots, \gamma_m$ sont des cycles à supports disjoints. Cette décomposition est unique à l'ordre près.

Propriété 2.42 : (*Le groupe symétrique est engendré par les transpositions*)

Le groupe symétrique est engendré par les transpositions : $\forall \sigma \in \mathcal{S}_n, \exists t_1, \ldots, t_p$ transpositions tel que $\sigma = t_1 \circ t_2 \circ \cdots \circ t_p$.

Preuve :

D'après le th. précédent, il suffit de montrer que les transpositions engendrent les cycles. Pour $l \geqslant 2$:

$$(1, 2, 3, \ldots, l) = (1,2)(2,3)\cdots(l-1, l), \quad (i_1, i_2, \ldots, i_m) = (i_1 i_2)(i_2 i_3)\cdots(i_{e-1}, i_e).$$

Définition 2.43 : (*Signature d'une permutation*)

Soit $n \geqslant 1$, $\sigma \in \mathcal{S}_n$. On appelle **signature** de σ et on note $\varepsilon(\sigma)$:

$$\varepsilon(\sigma) = (-1)^{\mathrm{inv}(\sigma)},$$

où $\mathrm{inv}(\sigma) = \mathrm{Card}\{(i, j) \in \{1, 2, \ldots, n\}^2 \mid i < j \text{ et } \sigma(i) > \sigma(j)\}$ est le nombre d'inversions.

Propriété 2.44 : (*Signature et produit*)

$$\varepsilon(\sigma \circ \tau) = \varepsilon(\sigma)\,\varepsilon(\tau), \quad \varepsilon : (\mathcal{S}_n, \circ) \to (\{-1, +1\}, \times) \text{ morphisme de groupe.}$$

Propriété 2.45 : (*Signature d'un produit de transpositions*)

Si σ est un produit de m transpositions, alors $\varepsilon(\sigma) = (-1)^m$.

Il suffit de montrer que la signature d'une transposition vaut (-1).

Corollaire 2.46 : (*Invariance de la parité*)

La parité du nombre de transpositions dans une décomposition de σ en produit de transpositions est invariante.

Propriété 2.47 : (*Signature d'un cycle*)

Si c est un cycle de longueur l, alors $\varepsilon(c) = (-1)^{l+1}$.

Preuve :

$(i_1, i_2, i_3, \ldots, i_l) = (i_1, i_2)\cdot(i_2, i_3)\circ\cdots\circ(i_{l-1}, i_l)$ ($l-1$ transpositions, chacune de signature -1). $\varepsilon((i_1\, i_2 \cdots i_l)) = \varepsilon(i_1\, i_2)\cdot\varepsilon(i_2\, i_3)\cdots\varepsilon(i_{l-1}\, i_l) = (-1)^{l-1} = (-1)^{l+1}$.

Définition 2.48 : (*Groupe alterné*)

On définit le **groupe alterné** $\mathscr{A}_n$ comme le sous-groupe des éléments de $\mathscr{S}_n$ de signature égale à 1 :

$$\mathscr{A}_n = \varepsilon^{-1}(\{1\}) \text{ ss-groupe de } \mathscr{S}_n.$$

Permutation paire : $\varepsilon(\sigma) = 1$. **Permutation impaire** : $\varepsilon(\sigma) = -1$.

Chapitre 3

Anneaux

3.1 Définition et propriétés

Définition 3.1 : (*Anneau*)

Un **anneau** $(A,+,\times)$ est un ensemble non vide muni de 2 lois de composition interne telles que :

- $(A,+)$ groupe commutatif,
- $\times$ est associative,
- la $\times$ est distributive à droite et à gauche par rapport à l'addition : $a(b+c)=ab+ac$ et $(b+c)a=ba+ca$.

L'anneau est dit **commutatif** si $\times$ est commutative. L'anneau est dit **unitaire** si $\times$ admet un neutre.

On note $-a$ le symétrique de a par rapport à la loi $+$, appelé **opposé** de a.

Règles de calcul : 0_A neutre pour $+$.

$$\forall a\in A,\quad a\times 0_A=0_A\times a=0_A.$$

$$\forall a,b\in A,\quad (-a)b=a(-b)=-(ab),\quad (-a)(-b)=ab.$$

$$(a+(-a))b=0_A\cdot b=0_A \implies ab+(-a)b=0_A \implies (-a)b=-(ab).$$

Si A unitaire, 1_A neutre pour $\times$. $(-1_A)x=-x=x(-1_A)$.

Si A unitaire non réduit à $\{0_A\}$, alors $0_A\neq 1_A$.

Exemple :

— $(\mathcal{M}_n(\mathbb{C}),+,\times)$ anneau non commutatif unitaire.

— $(\mathbb{R},+,\times)$ anneau commutatif unitaire.

— $(2\mathbb{Z},+,\times)$ anneau non unitaire.

— $(\mathbb{Z}/n\mathbb{Z},+,\times)$ unitaire et commutatif.

Formule du binôme : Si A est commutatif :

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

Définition 3.2 : (*Morphisme d'anneaux*)

Un **morphisme d'anneaux** $f:(A,+,\times)\to(B,+,\times)$ vérifie :

$$f(x+y)=f(x)+f(y)\quad\text{et}\quad f(xy)=f(x)f(y).$$

Si A et B sont unitaires, f est dit **unitaire** si de plus $f(1_A)=1_B$. f isomorphisme si de plus f bijective.

Exemple :
$(\mathbb{Z},+,\times) \to (\mathbb{Z}/n\mathbb{Z},+,\times)$, $x \mapsto \bar{x}$ morphisme d'anneaux unitaire.

Définition 3.3 : (*Sous-anneau*)
Soit $(A,+,\times)$ un anneau. Une partie C de A est appelée **sous-anneau** de A si $C \neq \emptyset$, si C est stable pour $+$ et pour $\times$, et si C est un anneau pour les lois induites. De façon équivalente :

— $(C,+)$ ss-groupe de $(A,+)$,

— $\forall a,b \in C$, $ab \in C$ (stabilité de $\times$).

Si A est unitaire, le ss-anneau C est dit unitaire si $1_A \in C$.

Propriété 3.4 : (*Image et préimage d'un morphisme*)
Soit $f : (A,+,\times) \to (B,+,\times)$ morphisme d'anneaux. Si C ss-anneau de A, alors $f(C)$ ss-anneau de B. Si C' ss-anneau de B, alors $f^{-1}(C')$ ss-anneau de A.

3.2 Diviseurs de zéro — Anneau intègre

À partir de maintenant les anneaux sont commutatifs unitaires.

Définition 3.5 : (*Diviseur de zéro*)
Soit $(A,+,\times)$ un anneau commutatif unitaire. Un élément a de A est dit **diviseur de zéro** s'il existe $b \in A$, $b \neq 0_A$, tel que $ab = 0_A$.

Propriété 3.6 : (*Régularité et diviseurs de zéro*)
a est régulier pour la loi $\times$ si et seulement si a n'est pas diviseur de 0.

Définition 3.7 : (*Anneau intègre*)
Un anneau est dit **intègre** s'il est unitaire, commutatif, non réduit à $\{0_A\}$, et s'il ne possède pas de diviseurs de 0.

Conséquence : Dans un anneau intègre, tout élément est régulier. Si $a \neq 0_A$ et $ax = ay$, alors $x = y$.

3.3 Corps, éléments inversibles

Définition 3.8 : (*Élément inversible*)

On rappelle que $a \in A$ est dit **inversible** dans $(A,+,\times)$ (commutatif unitaire) si a admet un symétrique pour la loi $\times$.

Définition 3.9 : (*Corps*)

Soit K un anneau commutatif unitaire. On dit que K est un **corps** si $K \neq \{0_K\}$ et tout élément non nul est inversible.

Exemple :

$(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des corps.

Conséquence : Dans un corps, il n'existe pas de diviseurs de 0.

Définition 3.10 : (*Sous-corps*)

L sous-corps de $(K,+,\times)$ si L ss-anneau de $(K,+,\times)$ dont tous les éléments sont inversibles et $L \neq \{0_K\}$. De façon équivalente :

- $L \neq \{0_K\}$,
- $(L,+)$ ss-groupe,
- $\forall a,b \in L$, $ab \in L$, et si $a \neq 0$, $a^{-1} \in L$ (inv de a dans K).

3.4 Idéaux — Anneau quotient

Définition 3.11 : (*Idéal*)

$(A,+,\times)$ commutatif unitaire. Un **idéal** I de A est une partie non vide de A telle que :

- $(I,+)$ est un ss-groupe de $(A,+)$,
- $\forall x \in I$, $\forall a \in A$, $ax \in I$.

Exemple :

$(\mathbb{Z},+,\times)$, $2\mathbb{Z}$ idéal de $\mathbb{Z}$. $\{0_A\}$ idéaux triviaux.

Propriété 3.12 : (*Préimage d'un idéal*)

Soit $f : (A,+,\times) \to (B,+,\times)$ morphisme d'anneaux unitaires. Soit J un idéal de B. Alors $f^{-1}(J)$ est un idéal de A. En particulier $\ker f \subseteq f^{-1}(J)$ et $\ker f$ est un idéal de A.

Propriété 3.13 : (*Intersection d'idéaux*)

L'intersection d'une famille d'idéaux de A est un idéal de A (A commutatif unitaire).

Définition 3.14 : (*Idéal engendré*)

Soit S une partie de A (non vide). On appelle **idéal engendré par** S l'intersection des idéaux contenant S. D'après la proposition précédente, on a bien un idéal.

Définition 3.15 : (*Anneau quotient*)

Soit $(A,+,\times)$ un anneau commutatif unitaire et I un idéal de A. On note $a \equiv b \pmod{I}$ si $a-b \in I$.

Propriété 3.16 : (*Compatibilité*)

$a \equiv b \pmod{I}$ est une relation d'équivalence sur A compatible avec l'addition et la multiplication (les 2 l.c.i. sur A).

Théorème 3.17 : (*Anneau quotient*)

L'ensemble quotient A/I est un anneau commutatif unitaire pour les lois définies par $\bar{a}+\bar{b} = \overline{a+b}$ et $\bar{a}\times\bar{b} = \overline{ab}$.

Remarque :

Si $\pi : A \to A/I$, $x \mapsto \bar{x}$ est la surjection canonique de A sur A/I, alors π est un morphisme surjectif de $(A,+,\times)$ sur $(A/I,+,\times)$.

Exemple : $n\mathbb{Z}$ idéal de $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ anneau quotient.

$\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Chapitre 4

Divisibilité — Anneau principal — $\mathbb{Z}$

Définition 4.1 : (*Divisibilité dans un anneau intègre*)

Soit $(A,+,\times)$ un anneau intègre et soient $a,b\in A$ $(\neq 0_A)$. On dit que a divise b dans A s'il existe $x\in A$ tel que $b=ax$. On écrit $a\mid b$.

Propriété 4.2 : (*Idéal principal engendré par a*)

Si l'idéal engendré par $\{a\}$ est noté (a), alors

$$(a)=aA=\{ax\mid x\in A\}.$$

Propriété 4.3 : (*Divisibilité et idéaux*)

$a\mid b \iff (b)\subseteq(a)$.

Définition 4.4 : (*Associés*)

Si $a\mid b$ et $b\mid a \iff (a)=(b)$, a et b sont dits **associés**. De plus, il existe u inversible tel que $a=ub$.

Exemples : dans $\mathbb{Z}$, n et $-n$ sont associés. $\forall n\in\mathbb{Z}$, les seuls éléments associés à n sont n et $-n$. Dans $\mathbb{R}[X]$, $X-1$ et $\lambda X-\lambda$ sont associés pour tout $\lambda\in\mathbb{R}^*$.

Définition 4.5 : (*Anneau principal*)

Un idéal I de A est dit **principal** s'il existe $a\in A$ tel que $I=aA=(a)$.

Un anneau est dit **principal** si c'est un anneau intègre dans lequel tout idéal est principal. $(\mathbb{Z},+,\times)$ est principal.

Exemple : $(\mathbb{R}[X,Y],+,\times)$ polynômes à 2 indéterminées est un anneau non principal.

Dans un anneau principal, $\forall a,\forall b\in A$, un PGCD et un PPCM (a,b) existent.

Définition 4.6 : (*PGCD dans un anneau principal*)

Soient a et $b\in A$. $d\in A$ est un **PGCD** de a et b si

$$\mathrm{Div}(a)\cap\mathrm{Div}(b)=\mathrm{Div}(d),$$

ce qui veut dire : $d\mid a$ et $d\mid b$, et tout diviseur commun à a et b est un diviseur de d.

Le PGCD existe, est unique à une association près, et il existe $u,v\in A$ tels que $d=au+bv$ (Bézout).

Définition 4.7 : (*PPCM dans un anneau principal*)

Soient a et $b\in A$, $m\in A$ est un **PPCM** de a et b si $(a)\cap(b)=(m)$. m existe, est unique à une association près.

Définition 4.8 : (*Éléments premiers entre eux, irréductibles*)

Les éléments a et b sont **premiers entre eux** si 1_A est un PGCD.

a est **irréductible** si :

1. $a\neq 0_A$,
2. a n'est pas inversible,
3. tout diviseur de a est soit inversible soit associé à a.

On peut alors refaire les lemmes de Gauss et d'Euclide :

Lemme 4.9 : (*Lemme de Gauss*)

Soient $a, b, c \in A$ (anneau principal). Si $a \mid bc$ et si a et b sont premiers entre eux, alors $a \mid c$.

Lemme 4.10 : (*Lemme d'Euclide*)

Soient $p, b, c \in A$. Supposons p irréductible et $p \mid bc$. Alors $p \mid b$ ou $p \mid c$.

Preuve :

Si p ne divise pas b, comme p irréductible, p et b sont premiers entre eux. Donc le th. de Gauss permet de conclure que $p \mid c$.

Remarque :

Pour définir le pgcd, il faut ajouter un critère pour le choix du représentant :

- $(\mathbb{Z}, +, \times)$: le pgcd sera choisi positif.
- $(\mathbb{R}[X], +, \times)$: le pgcd sera choisi unitaire.

Pour les calculs, il faut une division euclidienne.

Chapitre 5

Les polynômes à 1 indéterminée

Dans la suite $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$ ou un sous-corps de $\mathbb{C}$.

5.1 Définitions

Définition 5.1 : (*Polynôme formel*)

On appelle **polynôme formel à coefficients dans** $\mathbb{K}$ (ou polynôme à 1 indéterminée) toute suite infinie d'éléments de $\mathbb{K}$, notée $(a_0, a_1, a_2, \ldots, a_n, \ldots)$, $\forall i \in \mathbb{N}$, $a_i \in \mathbb{K}$, où à partir d'un certain rang tous les éléments de la suite sont nuls.

On notera $P = (a_0, a_1, \ldots, a_n, \ldots)$. a_0 est le **terme constant**. Les a_i sont les **coefficients** de P.

On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$.

Définition 5.2 : (*Degré et valuation*)

Soit $P = (a_0, a_1, \ldots, a_n, \ldots) \in \mathbb{K}[X]$ non nul.

Le **degré** de P est le plus grand indice $n \in \mathbb{N}$ tel que $a_n \neq 0$ et $\forall k > n$, $a_k = 0$. On note $\deg P$ cet indice.

La **valuation** de P est le plus petit indice i tel que $a_i \neq 0$ et $\nexists k \in \mathbb{N}$ avec $k < i$ et $a_k \neq 0$. On note $\operatorname{val} P$.

Propriétés : $\forall k > \deg P$, $a_k = 0$.

Si $\operatorname{val} P \geqslant 1$, alors $\forall 0 \leqslant k < \operatorname{val} P$, $a_k = 0$.

$\operatorname{val} P \leqslant \deg P$.

Si $\operatorname{val} P = \deg P$, P est un **monôme**.

Convention pour le polynôme nul : $\operatorname{val}(0_{\mathbb{K}[X]}) = +\infty$, $\deg(0_{\mathbb{K}[X]}) = -\infty$.

5.2 Structure de $\mathbb{K}[X]$

Pour $P=(a_0,a_1,\dots,a_n,\dots)$ et $Q=(b_0,b_1,\dots,b_n,\dots)$:

Somme : $P+Q=(a_0+b_0,a_1+b_1,\dots,a_n+b_n,\dots)$.

Élément neutre $_{\mathbb{K}[X]}$. Commutatif, associatif.

Opposé : $-P=(-a_0,-a_1,\dots,-a_n,\dots)$.

$(\mathbb{K}[X],+)$ groupe abélien.

Produit : $P\times Q=(c_0,c_1,\dots,c_m,\dots)$ où $\forall k\in\mathbb{N}$, $c_k=\sum_{i=0}^{k}a_ib_{k-i}$.

$$PQ=QP,\quad (PQ)R=P(QR),\quad \forall P\in\mathbb{K}[X],\ (1,0,0,\dots,0,\dots)P=P.$$

$(\mathbb{K}[X],+,\times)$ anneau commutatif unitaire.

Propriété 5.3 : (*Degré du produit*)

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

Donc $(\mathbb{K}[X],+,\times)$ anneau commutatif intègre.

Notation définitive : Posons $X=(0,1,0,\dots,0,\dots)$. Alors $X^2=(0,0,1,\dots,0,\dots)$ et identifions $\alpha\in\mathbb{K}$ avec le polynôme $(\alpha,0,0,\dots,0,\dots)$.

Alors $P=(a_0,a_1,\dots,a_n,\dots)$ s'écrit si $n=\deg P$:

$$P=a_0+a_1X+a_2X^2+\cdots+a_nX^n=\sum_{k=0}^{n}a_kX^k.$$

Les polynômes de degré 0 s'appellent les **constantes**. Soit $P=a_nX^n+\cdots+a_0$ de degré n ($a_n\neq 0$). Alors a_n s'appelle le **coefficient dominant** et a_nX^n le **monôme de plus haut degré**. Si $a_n=1$, P est dit **unitaire**.

5.3 Les deux divisions de polynômes dans $\mathbb{K}[X]$

5.3.1 Divisibilité dans $\mathbb{K}[X]$

B divise A ($B\mid A$) avec A et B non nuls si $\exists Q\in(\mathbb{K}[X])^*$ tel que $A=BQ$.

5.3.2 Division euclidienne

Théorème 5.4 : (*Division euclidienne dans* $\mathbb{K}[X]$)

Soient A et B deux polynômes $\neq 0$ de $\mathbb{K}[X]$. Il existe un unique couple (Q,R) de polynômes de $\mathbb{K}[X]$ tel que

$$A=BQ+R,\quad \deg R<\deg B.$$

Déterminer (Q,R) c'est effectuer la **division euclidienne** de A par B.

Exemple :

$A=3x^5+4x^2+1$, $B=x^2+2x+3$.

$3x^5+4x^2+1$	x^2+2x+3
$\cdots$	$3x^3-6x^2+3x+16$

$Q=3x^3-6x^2+3x+16$, $R=-41x-47$.

5.3.3 Division suivant les puissances croissantes

Théorème 5.5 : (*Division selon les puissances croissantes*)

Soient 2 polynômes A et B non nuls tels que $\text{val}(B) = 0$. Soit $k \in \mathbb{N}$, il existe un unique couple d'éléments de $\mathbb{K}[X]$ tel que (Q, R) :

$$A = BQ + X^{k+1}R, \quad \text{avec } Q = 0 \text{ ou } \deg Q \leqslant k.$$

5.4 $\mathbb{K}[X]$ anneau principal — PGCD — PPCM — Irréductible

Théorème 5.6 : ($\mathbb{K}[X]$ *est un anneau principal*)

$\mathbb{K}[X]$ est un anneau principal : de plus $\forall I$ idéal, il existe un unique polynôme unitaire D tel que $I = D\mathbb{K}[X]$ (on choisit un représentant particulier : polynôme unitaire).

Conséquence : Comme $\mathbb{K}[X]$ anneau principal, soient $A, B \in \mathbb{K}[X]$ non nuls. Alors $\text{pgcd}(A, B)$ existe et est unique à une association près (on choisit l'unitaire comme représentant), et il existe U_0 et V_0 tel que $AU_0 + BV_0 = \text{pgcd}(A, B)$. $A\mathbb{K}[X] + B\mathbb{K}[X] = \text{pgcd}(A, B)\mathbb{K}[X]$.

$\text{ppcm}(A, B)$ existe (unique si on choisit le représentant unitaire). $A\mathbb{K}[X] \cap B\mathbb{K}[X] = \text{ppcm}(A, B)\mathbb{K}[X]$.

On peut refaire le lemme de Gauss, le lemme d'Euclide, le th. de Bézout.

Exemple :

[Exercice] Montrer que si $a \neq b$, $X - a$ et $X - b$ sont premiers entre eux.

Algorithme d'Euclide pour les polynômes. Soient A et B deux poly avec $\deg A \geqslant \deg B$. Division euclidienne de A par B : $A = BQ_1 + R_1$, $\deg R_1 < \deg B$. Comme pour les entiers, $\text{pgcd}(A, B) = \text{pgcd}(B, R_1)$. Si $R_1 \neq 0$, on fait la div. eucl. de B par R_1 : $B = R_1 \times Q_2 + R_2$, $\deg R_2 < \deg R_1$, $\text{pgcd}(B, R_1) = \text{pgcd}(R_1, R_2)$.

Si $R_2 = 0$, on arrête. Sinon on continue. On construit ainsi la suite $R_{k-1} = Q_{k+1}R_k + R_{k+1}$, avec $\deg R_{k+1} < \deg R_k$. La suite $(\deg R_k)$ est une suite d'entiers strictement décroissante, au bout d'un nombre fini de div. euclid. on aura $R_{k+1} = 0$ ou $R_{k+1} = \lambda$, $\lambda \in \mathbb{R}^*$.

(a) Si $R_{k+1} =_{\mathbb{K}[X]}$, $\text{pgcd}(A, B) = \cdots = \text{pgcd}(R_k, R_{k-1}) = R_k$.

(b) Si $R_{k+1} = \lambda$, $\lambda \in \mathbb{R}^*$, $\text{pgcd}(A, B) = \cdots = \text{pgcd}(R_k, R_{k-1}) = 1$.

Exemple :

$A = 2x^5 + 2x^4 + 4x^3 + 1$, $B = 3x^4 + x^3 - 3x - 1$. $\text{pgcd}(A, B) = x^2 + x + 1$.

Théorème 5.7 : (*Décomposition en facteurs irréductibles*)

Soit P non irréductible unitaire tel que $\deg P \geqslant 1$. Alors P s'écrit de manière unique à l'ordre près comme produit de polynômes irréductibles unitaires.

Remarque :

On peut dans chaque décomposition regrouper les facteurs premiers et obtenir

$$P = a_n S_1^{\alpha_1} \cdots S_k^{\alpha_k}, \quad \alpha_i \in \mathbb{N}^*, \quad S_i \text{ unitaire irréductible, } S_1, \ldots, S_k \text{ distincts.}$$

Les polynômes de degré 1 sont irréductibles.

5.5 Racines

5.5.1 Fonction polynôme

Définition 5.8 : (*Racine (zéro) d'un polynôme*)

Soit $P = a_n X^n + \cdots + a_0$ avec $\deg P = n$. On associe à P la **fonction polynôme** notée $f_P : \mathbb{K} \to \mathbb{K}$, $x \mapsto a_n x^n + \cdots + a_0$.

Soit P un polynôme non nul de $\mathbb{K}[X]$ et $a \in \mathbb{K}$. a est **racine** de P (ou zéro de P) si $P(a) = 0$ ($f_P(a) = 0$).

Théorème 5.9 : (*Critère de racine*)

a est racine de P si et seulement si $(X - a)$ divise P.

Preuve :

On fait la division euclidienne de P par $(X - a)$:

$$P = (X - a)Q + R, \quad \deg R < 1, \quad \deg R < 1 \implies R = \alpha \neq 0 \in \mathbb{K}^* \text{ ou } R \equiv 0.$$

On utilise la fonction polynôme en a :

$$0 = P(a) = (a - a)Q(a) + R(a) = R(a).$$

Donc $R(a) = 0$. Comme R est de degré < 1, c'est une constante, on en déduit $R \equiv 0$. Donc $(X - a) \mid P$.

Définition 5.10 : (*Racine multiple — ordre*)

On dit que a est racine multiple de P d'ordre k ($k \in \mathbb{N}^*$) si $P = (X - a)^k Q$ avec $k \geqslant 1$, $Q(a) \neq 0$.

$k = 1$: ordre simple (ou racine simple). $k = 2$: racine double, ordre 2.

Théorème 5.11 : (*Racines distinctes et multiplicités*)

Soit $P \in \mathbb{K}[X]$ non nul et $a_1, \ldots, a_k$ des racines distinctes de multiplicités respectives $m_1, \ldots, m_k$ ($k \in \mathbb{N}^*$). Alors

$$P = (X - a_1)^{m_1} (X - a_2)^{m_2} \cdots (X - a_k)^{m_k} T$$

avec $T \in \mathbb{K}[X]$, $T(a_i) \neq 0$ pour tout $1 \leqslant i \leqslant k$.

Corollaire 5.12 : (*Nombre de racines*)

Un polynôme de degré n ($n \in \mathbb{N}^*$) admet au plus n racines.

5.6 Polynôme dérivé — lien avec les racines multiples

5.6.1 Polynôme dérivé

Définition 5.13 : (*Polynôme dérivé*)

Soit $P \in \mathbb{K}[X]$, $\deg P \geqslant 1$,

$$P = \sum_{k=0}^{n} a_k X^k, \quad n = \deg P \geqslant 1,\ a_n \neq 0.$$

On appelle **polynôme dérivé** de P, noté P', le polynôme $P' = \sum_{k=1}^{n} k a_k X^{k-1}$.

Si $\deg P = 0$ ou $P = 0$, alors $P' = 0$.

Propriété 5.14 : (*Propriétés du dérivé*)

$(P+Q)' = P' + Q'$, $(\lambda P)' = \lambda P'$, $(PQ)' = P'Q + PQ'$.

Dérivées successives : On note $D : \mathbb{K}[X] \to \mathbb{K}[X]$, $P \mapsto P'$, et $D^2, D^3, \ldots, D^k$ les opérateurs composés. On démontre que

$$D^k(X^n) = \begin{cases} \dfrac{n!}{(n-k)!} X^{n-k} & \text{si } 1 \leqslant k \leqslant n \\ 0 & \text{si } k \geqslant n+1. \end{cases}$$

Notation : $k = 0$, $D^k P = P$, $P^{(k)} = D^k P$.

Formule de Leibniz : $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$.

5.6.2 Formule de Taylor pour un polynôme

Théorème 5.15 : (*Formule de Taylor*)

Soit $P \in \mathbb{K}[X]$, $\deg P = n$. Alors $\forall a \in \mathbb{K}$:

$$P = \sum_{k=0}^{n} P^{(k)}(a) \frac{(X-a)^k}{k!}.$$

5.6.3 Lien entre zéros multiples et dérivées

Théorème 5.16 : (*Zéro multiple et dérivées*)

Soit $P \in \mathbb{K}[X]$ non nul. P admet α comme racine d'ordre k ($k \geqslant 1$) si et seulement si $P, P', \ldots, P^{(k-1)}$ admettent α comme racine et $P^{(k)}(\alpha) \neq 0$ (α n'est pas racine de $P^{(k)}$).

5.7 Cas complexe

Théorème 5.17 : (*Théorème de d'Alembert–Gauss (théorème capital)*)

Tout polynôme de $\mathbb{C}[X]$ admet au moins une racine dans $\mathbb{C}$.

Corollaire 5.18 : (*Irréductibles de $\mathbb{C}[X]$*)

Les seuls polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Conséquence : $\forall P \in \mathbb{C}[X]$, $\deg P \geqslant 1$, alors il existe $\lambda \in \mathbb{C}^*$, $a_1, \dots, a_m \in \mathbb{C}$ tels que

$$P = \lambda(X - a_1)\cdots(X - a_m).$$

5.8 Cas réel

Propriété 5.19 : (*Conjugaison*)

Soit $P \in \mathbb{R}[X]$. $\forall z \in \mathbb{C}$, $P(\bar{z}) = \overline{P(z)}$.

Corollaire 5.20 : (*Racines conjuguées*)

Si α est racine de P ($P \in \mathbb{R}[X]$ plongé dans $\mathbb{C}[X]$), alors $\bar{\alpha}$ est racine de P.

Théorème 5.21 : (*Irréductibles de $\mathbb{R}[X]$*)

Dans $\mathbb{R}[X]$, les polynômes unitaires et irréductibles sont :

— les polynômes de degré 1 (autrement dit $(X - a)$, $a \in \mathbb{R}$),

— les polynômes de degré 2 du type $X^2 + \alpha X + \beta$ avec $\alpha, \beta \in \mathbb{R}$ et $\alpha^2 - 4\beta < 0$.

5.9 Fractions rationnelles

Définition 5.22 : (*Fraction rationnelle*)

Une **fraction rationnelle** est une expression $\dfrac{P}{Q}$ où P et Q sont deux éléments de $\mathbb{K}[X]$ avec $Q \neq 0$. On note cet ensemble $F_{\mathbb{K}}[X]$.

$\dfrac{a}{b} \equiv \dfrac{c}{d} \iff ad = bc$. $F_{\mathbb{K}}[X] = \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\}) / \equiv$.

On choisit comme représentant privilégié de $\left[\dfrac{a}{b}\right]$ l'élément $\dfrac{a_1}{b_1}$ tel que $\operatorname{pgcd}(a_1, b_1) = 1$ (fraction irréductible).

Définition 5.23 : (*Pôles et zéros*)

Soit $\dfrac{P}{Q}$ une fraction rationnelle avec $\operatorname{pgcd}(P, Q) = 1$.

— Les zéros de Q sont appelés les **pôles** de la fraction rationnelle.

— Les zéros de P sont appelés les **zéros** de la fraction rationnelle.

— $\dfrac{P(t)}{Q(t)}$, $t \in \mathbb{K}$, t n'étant pas un zéro de Q (c.à.d. un pôle), est la fonction rationnelle associée.

5.9.1 Décomposition en éléments simples

Théorème 5.24 : (*Premier théorème de décomposition*)

Soient P, Q avec $\deg P < \deg Q$ et $\text{pgcd}(P,Q) = 1$. Supposons $Q = Q_1 Q_2 \cdots Q_m$, $m \geqslant 2$, Q_i polynômes non nuls de $\mathbb{K}[X]$ et $Q_1, \ldots, Q_m$ premiers entre eux ($\forall i \neq j$, $\text{pgcd}(Q_i, Q_j) = 1$).

Alors il existe n polynômes l_i uniques tel que $\forall i \in \{1, \ldots, n\}$: $\deg l_i < \deg Q_i$ et $\text{pgcd}(l_i, Q_i) = 1$ et

$$\frac{P}{Q} = \frac{l_1}{Q_1} + \frac{l_2}{Q_2} + \cdots + \frac{l_m}{Q_m}.$$

Théorème 5.25 : (*Deuxième théorème de décomposition*)

$\text{pgcd}(P,Q) = 1$, $\deg P < \deg Q$. $Q = \lambda Q_1^{\alpha_1} \cdots Q_r^{\alpha_r}$, Q_i premiers entre eux.

D'après ce qui précède, $\dfrac{P}{Q} = \dfrac{l_1}{Q_1^{\alpha_1}} + \cdots + \dfrac{l_r}{Q_r^{\alpha_r}}$.

$\forall 1 \leqslant i \leqslant r$, $\dfrac{l_i}{Q_i^{\alpha_i}}$ peut se décomposer de façon unique en :

$$\frac{l_i}{Q_i^{\alpha_i}} = \frac{e_{\alpha_i}}{Q_i^{\alpha_i}} + \frac{e_{\alpha_i - 1}}{Q_i^{\alpha_i - 1}} + \cdots + \frac{e_1}{Q_i}, \quad \forall j \in \{1, \ldots, \alpha_i\},\ \deg e_j < \deg Q_i,\ e_{\alpha_i} \neq 0_{\mathbb{K}[X]}.$$

Éléments simples :

Dans $\mathbb{C}[X]$, tous les irréductibles unitaires sont $(X-a)$, $a \in \mathbb{C}$. Éléments simples : $\dfrac{\beta}{(X-a)^n}$, $\beta \in \mathbb{C}$, $n \in \mathbb{N}^*$.

Dans $\mathbb{R}[X]$: irréductibles unitaires $\{(X-a),\ a \in \mathbb{R}\}$ et $\{X^2 + \alpha X + \beta,\ \alpha^2 - 4\beta < 0\}$. Éléments simples de 1ière espèce : $\dfrac{\beta}{(X-a)^n}$, $\beta \in \mathbb{R}$, $a \in \mathbb{R}$, $n \in \mathbb{N}^*$. Éléments simples de 2ième espèce : $\dfrac{\lambda X + \mu}{((X-h)^2 + q^2)^n}$, $q \neq 0$, $\lambda, \mu \in \mathbb{R}$, $h, q \in \mathbb{R}$, $n \in \mathbb{N}^*$.

Exemple :

$$\frac{X^3 + 3X^2 + 2}{(X-1)^4} = \frac{\lambda_4}{(X-1)^4} + \frac{\lambda_3}{(X-1)^3} + \frac{\lambda_2}{(X-1)^2} + \frac{\lambda_1}{(X-1)}.$$

Pour λ_4, on multiplie par $(X-1)^4$ et on fait $X = 1$:

$$\lambda_4 = X^3 + 3X^2 + 2\big|_{X=1} = 1 + 3 + 2 = 6.$$

Puis $\dfrac{X^3 + 3X^2 + 2 - 6}{(X-1)^4} = \dfrac{X^3 + 3X^2 - 4}{(X-1)^4} = \dfrac{(X-1)(X^2 + 4X + 4)}{(X-1)^4} = \dfrac{(X+2)^2}{(X-1)^3}$.

Examen : mardi 14/01/2014 de 9h à 12h.