STRUCTURES ALGEBRIQUES

ESATIC UP MATHS

2023 - 2024

Table des matières

Notations

Notation	Définition
$\mathbb{N}$	Ensemble des entiers naturels
$\mathbb{Z}$	Ensemble des entiers relatifs
$\mathbb{R}$	Ensemble des nombres réels
Im	Image d'une application
$\ker$	Noyau d'une application linéaire
$\|.\|$	Valeur absolue
$\|\|.\|\|_X$	Application norme sur l'ensemble X
$\oplus$	La somme directe
$\sum$	Symbole de sommation
$\prod$	Symbole du produit
$\circ$	La composition des applications
$\cap$	L'intersection
$\cup$	L'union
$\neq$	La non égalitïé
$\subset$	L'inclusion
$\in$	Appartenance
$\notin$	non Appartenance
$\forall$	Symbole universel "pour tout"
$\exists$	Symbole universel "il existe"
$u^{(k)}$	Dérivée d'ordre k de u définie sur une partie de $\mathbb{R}$
$a\|b$	a divise b
$E(x) = [x]$	partie enti‘ere de x
PGCD	plus grand commun diviseur
$a \wedge b$	$PGCD(a, b)$
PPCM	plus petit commun multiple
$a \vee b$	$PPCM(a, b)$
$a \equiv b[N]$	a est congru à b modulo N
$\overline{a_n...a_0}^b$	écriture en base b
$n!$	factorielle de n : $n! = 1 \times 2 \times \ ... \ \times n$

C_n^k	coefficient binomial : $C_n^k = \frac{n!}{k!(n-k)!}$

Chapitre 1

LOIS DE COMPOSITION INTERNES ET EXTERNES

1.1 Lois de composition internes (LCI)

1.1.1 Définitions et exemples

Définition 1.1.1. *Soit E un ensemble non vide. On appelle loi de composition interne sur E toute application f de $E \times E$ dans E. Le couple constitué par un ensemble et une loi interne sur un ensemble est appelé un magma.*

Notation 1.1.1. *On note de plusieurs manières les lois de composition. Voici quelques notations utilisées fréquemment*

$$(x,y) \mapsto x+y \qquad (x,y) \mapsto x.y \qquad (x,y) \mapsto x*y$$
$$(x,y) \mapsto x \top y \qquad (x,y) \mapsto x \perp y \qquad (x,y) \mapsto x \times y$$

Remarque 1.1.1. *Si la loi est notée $\top$, l'image de l'élément $(x,y) \in E \times E$ est désignée par $x \top y$ et non par $\top(x,y)$.*

Exemples 1.1.1.

1. *Dans $\mathbb{R}$ ($\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$), l'addition $(x,y) \mapsto x+y$ et la multiplication $(x,y) \mapsto x \times y$ sont des lois de composition internes.*
2. *Dans $\mathbb{R}$ (ou $\mathbb{Z}$, $\mathbb{Q}$), la soustration $(x,y) \mapsto x-y$ est une loi de composition interne.*
3. *Soit E un ensemble. Les applications $(X,Y) \mapsto X \cup Y$ et $(X,Y) \mapsto X \cap Y$ sont des lois de composition internes sur l'ensemble des parties de E.*
4. *Dans l'ensemble $\mathcal{A}(E,E)$ des applications de E vers E, la composition $(f,g) \mapsto g \circ f$ est une loi de composition interne.*

1.1.2 Partie stable par une Loi de composition interne, loi induite

Définition 1.1.2. *Soit E un ensemble non vide, muni d'une loi de composition interne $\top$. Soit A une partie non vide de E. On dit que A est stable pour la loi $\top$ si, et seulement si :*

$$\forall (x,y) \in A^2, \quad x \top y \in A.$$

Exemples 1.1.2.

1. *$\mathbb{R}^+$, $\mathbb{N}$, $\mathbb{Z}^+$ et $\mathbb{Q}^+$, sont stables pour l'addition, et pour la multiplication.*
2. *$\mathbb{R}^-$, $\mathbb{Z}^-$ et $\mathbb{Q}^-$, ne sont pas stables pour la multiplication.*

Définition 1.1.3. *Soit E un ensemble non vide, muni d'une loi de composition interne $\top$. Soit A une partie de E stable pour la loi $\top$.*
L'application $T_A : A \times A \to A$ définie par $(x,y) \mapsto x \top y$ est alors une loi interne sur A; elle est appelée loi induite sur A par la loi $\top$ définie sur E. S'il n'y a pas d'ambiguïté, on la note encore $\top$.

Exemple 1.1.1. *L'application $\mathbb{R}^- \times \mathbb{R}^- \to \mathbb{R}^-$ définie par $(x,y) \mapsto x+y$ est la loi induite sur $\mathbb{R}^-$ par la loi $+$ définie sur $\mathbb{R}$.*

1.1.3 Loi associative

Définition 1.1.4. *Soit E un ensemble muni d'une loi de composition interne $\top$. La loi $\top$ est dite associative si et seulement si :*

$$\forall (x,y,z) \in E^3, \qquad x \top (y \top z) = (x \top y) \top z.$$

On dit alors que $(E, \top)$ est un magma associatif appelé semi-groupe.

Exemples 1.1.3.

1. *L'addition et la multiplication des entiers naturels sont des lois de composition associatives sur $\mathbb{N}$.*
2. *L'addition et la multiplication des nombres réels sont des lois de composition associatives sur $\mathbb{R}$;*
3. *Soit E un ensemble. Les lois $\cap$ et $\cup$ sont associatives et commutatives dans $\mathcal{P}(E)$.*

Remarque 1.1.2. *Dans le cas d'une loi associative $\top$, on peut supprimer les parenthèses, et plus généralement associer au $n-$uplet $(x_1, ..., x_n) \in E^n$ l'élément $x_1 \top ... \top x_n$ de E, étant entendu qu'intervient l'ordre dans lequel sont donnés $x_1, ..., x_n$.*

Lorsque $x_1 = ... = x_n = x$, $(n \geq 1)$, l'élément $x_1 \top ... \top x_n$ s'écrit $\overset{n}{\top} x$, et on vérifie par récurrence

$$\forall x \in E, \quad \forall (n,p) \in (\mathbb{N} \backslash \{0\})^2, \quad (\overset{n}{\top} x) \top (\overset{p}{\top} x) = \overset{n+p}{\top} x.$$

En notation additive, on écrit

$$x_1 + ... + x_n = \sum_{i=1}^{n} x_n.$$

Lorsque $x_1 = ... = x_n = x$, $(n \geq 1)$, $x_1 + ... + x_n$ *s'écrit* nx.

En notation multiplicative, on écrit

$$x_1 \times ... \times x_n = \prod_{i=1}^{n} x_n.$$

Lorsque $x_1 = ... = x_n = x$, $(n \geq 1)$, *l'élément* $x_1 \times ... \times x_n$ *s'écrit* x^n. *On dit que* x^n *est la puissance* n^{ime} *de* x.

On vérifie facilement que pour tout entier p tel que $1 \leq p \leq n$, *on a la relation*

$$x_1 \top ... \top x_n = (x_1 \top ... \top x_p) \top (x_{p+1} \top ... \top x_n).$$

on déduit que :
En notation additive, on a

$$\forall x \in E, \quad \forall (n,p) \in (\mathbb{N}\backslash\{0\})^2, \quad nx + px = (n+p)x \quad et \quad n(px) = (np)x.$$

En notation multiplicative, on a

$$\forall x \in E, \quad \forall (n,p) \in (\mathbb{N}\backslash\{0\})^2, \quad x^n \times x^p = x^{n+p} \quad et \quad (x^n)^p = x^{np}.$$

1.1.4 Lois commutatives

Définition 1.1.5. *Soit* $*$ *une loi de composition interne sur* E. *On dit que deux éléments* a *et* b *de* E *sont permutables (ou commutent) pour la loi* $*$ *si*

$$a * b = b * a$$

Définition 1.1.6. *On dit que la loi* $*$ *est commutative si, pour tout* $(x,y) \in E^2$, *on a* $x * y = y * x$ *(en d'autres termes, les éléments de* E *sont permutables 2 à 2).*

Exemples 1.1.4.
— $+$, $\times$ *sont des lois commutatives dans* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
— *Les lois* $\cup$ *et* $\cap$ *sont commutatives dans* $\mathcal{P}(E)$.

Il y a cependant des lois qui ne sont pas commutative. par exemple

Exemple 1.1.2. *La composition des applications* " $\circ$ " *n'est pas commutative.*

Remarque 1.1.3. *Tout élément* $x \in E$ *permute avec lui même. Si* " $*$ " *est associative, tout* x *permute avec* x^n, $(n \in \mathbb{N}^*)$.

Définition 1.1.7. *On dit qu'un élément* x *de* E *est central si tout élément de* E *est permutable avec* x. *On appelle centre de* E *l'ensemble des éléments centraux.*

1.1.5 Elément neutre à gauche, élément neutre à droite, élément neutre

Définition 1.1.8. *Soit E un ensemble muni d'une loi de composition interne $*$.*
On dit que l'élément e de E est un élément :

- *neutre à gauche, si : $\forall x \in E,\ e * x = x$;*
- *neutre à droite, si : $\forall x \in E,\ x * e = x$;*
- *neutre si e est neutre à gauche et à droite : $\forall x \in E,\ e * x = x * e = x$.*

Remarque 1.1.4. **1** *Lorsque la loi est notée additivement, l'élément neutre est noté 0 ;*

2 *Lorsque la loi est notée multiplicativement, l'élément neutre est noté 1.*

Exemple 1.1.3. *a) $(\mathbb{R}, +)$ admet 0 comme élément neutre,*

b) $(\mathbb{R}, \times)$ admet 1 comme élément neutre,

c) $(\mathcal{P}(E), \cap)$ admet E comme élément neutre,

d) $(\mathcal{P}(E), \cup)$ admet $\emptyset$ comme élément neutre,

e) $(\mathcal{A}(E, E), \circ)$ admet Id_E comme élément neutre.

Il y a cependant des lois qui n'ont pas d'élément neutre par exemples

Exemple 1.1.4. **1** *La loi $*$ définie sur $\mathbb{R}$ par $x * y = x.y + 3$ n'a pas d'élément neutre.*

2 *La loi $\top$ définie sur $\mathbb{R}$ par : $x \top y = x^2.y$ n'a pas d'élément neutre.*

3 *La multiplication $\times$ définie sur $[2, +\infty[$ n'a pas d'élément neutre.*

Exemple 1.1.5. *On considère la loi $\perp$ définie sur $\mathbb{R}$ par*

$$\forall x, y \in \mathbb{R}, \qquad x \perp y = \frac{1}{2}x^2 \times y.$$

$\perp$ admet $-\sqrt{2}$ et $\sqrt{2}$ comme éléments neutres à gauche.
$\perp$ n'admet pas d'élément neutre à droite.
$\perp$ n'admet pas d'élément neutre.

Proposition 1.1.1. **1** *Si e' est un élément neutre à gauche de $(E, \top)$ et e'' est un élément neutre à droite de $(E, \top)$, alors $e' = e''$.*

2 *Si e_1 et e_2 sont des éléments neutres de $(E, \top)$, alors $e_1 = e_2$.*

Démonstration. **1** Comme e' est un élément neutre à gauche, on a

$$e' \top e'' = e'' \tag{1.1}$$

Comme e'' est un élément neutre à droite, on a

$$e' \top e'' = e' \tag{1.2}$$

(1.1) et (1.2) nous donne $e' = e''$

2 Ce qui précède permet de conclure

□

Remarque **1.1.5.** *Un magma associatif ou semi-groupe admettant un élément neutre s'appelle* ***monoïde****.*

1.1.6 Elément symétrique à gauche, à droite, élément symétrique

Définition **1.1.9.** *Soit E un ensemble muni d'une loi de composition interne $*$. On suppose que $(E,*)$ possède un élément neutre e.*
On dit que l'élément x de E possède :

- *un symétrique à gauche x_g, si $x_g * x = e$. On dit alors que x est symétrisable à gauche·*
- *un symétrique à droite x_d; si $x * x_d = e$. On dit alors que x est symétrisable à droite.*
- *un symétrique x' si $x' * x = x * x' = e$. On dit alors que x est symétrisable .*

Proposition **1.1.2.** *Soit E un ensemble muni d'une loi de composition interne $*$. On suppose que $(E,*)$ possède un élément neutre e et que la loi $*$ est associative.*

1 *Si un élément x de E possède un symétrique à gauche et un symétrique à droite alors ils sont égaux.*

2 *Si un élément x de E est symétrisable alors il admet un unique symétrique.*

Exemples **1.1.5.**

— *Dans $\mathbb{R}$ muni de $+$, tout élément $x \in \mathbb{R}$ admet $-x$ pour symétrique.*
— *Dans $\mathbb{R}$ muni de $\times$, tout les éléments $x \in \mathbb{R}^*$ admet $\frac{1}{x}$ pour symétrique.*
— *Dans $\mathcal{P}(E)$ muni de la loi Δ*

$$X \Delta Y = (X \cap \overline{Y}) \cup (\overline{X} \cap Y).$$

L'ensemble vide $\emptyset$ est élément neutre et tout élément $X \in \mathcal{P}(A)$ s'admet lui-même pour symétrique.

Notation **1.1.2.** *Si $x \in E$ admet un symétrique, et que ce symétrique est unique, on le note x^{-1} (en notation multiplicative) et $-x$ (en notation additive).*

Proposition **1.1.3.** *Soit E un ensemble muni d'une loi de composition interne $*$. Si x et y sont deux éléments de E de symétrique respectif x^{-1} et y^{-1}, alors $x * y$ admet $y^{-1} * x^{-1}$ pour symétrique*

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Démonstration. Calculer $(x * y) * (y^{-1} * x^{-1})$ puis $(y^{-1} * x^{-1}) * (x * y)$. □

Corollaire **1.1.1.** *Si x admet un symétrique, alors pour tout $n \in \mathbb{N}^*$, x^n admet $(x^{-1})^n$ pour symétrique :*

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

1.1.7 Homomorphismes

Définition **1.1.10.** *Soient E, F, deux ensembles munis respectivement des lois de compositions internes $*$ et $\bullet$. On dit qu'une application $f : E \mapsto F$ est un homomorphisme si*

$$\forall (x, x') \in E^2, \quad \text{on a} \quad f(x * x') = f(x) \bullet f(x').$$

Exemples **1.1.6.**

1 *$id_E : E \to E$ est un homomorphisme*

2 *Si la loi $*$ admet $e \in F$ comme élément neutre, alors l'application constante $h : E \to F$, $x \mapsto e$ est un homomorphisme.*

3 *$\ln : \mathbb{R}^* \to \mathbb{R}$ est un homomorphisme si on considère la multiplication dans R* et l'addition dans $\mathbb{R}$.*

4 *$f : \mathbb{R}^2 \to \mathbb{R}$, $(a, b) \mapsto 2a + b$ est un homomorphisme avec l'addition dans $\mathbb{R}^2$ et l'addition dans $\mathbb{R}$. $\mathbb{R}^2$ muni de la loi cartésienne $(a, b) + (a', b') = (a + a', b + b')$.*

Définition **1.1.11.**

— *Un homomorphisme bijectif est appelé isomorphisme.*

— *Un homomorphisme de $(E, *)$ dans $(E, *)$ est appelé endomorphisme.*

— *Un endomorphisme bijectif est appelé un automorphisme.*

Proposition **1.1.4.** *Soient $f : E \to F$ et $g : F \to G$ deux homomorphismes, alors $g \circ f$ est un homomorphisme.*

Démonstration. On considère $(E, *)$, $(F, \bullet)$, $(G, \top)$. $g \circ f : (E, *) \to (G, \top)$. $\forall z \in E$, on a $(g \circ f)(z) = g(f(z))$.
$\forall x, y \in E$, on a

$$\begin{aligned} (g \circ f)(x * y) &= g(f(x) \bullet f(y)) \\ &= g(f(x)) \top g(f(y)) \\ &= (g \circ f)(x) \top (g \circ f)(y). \end{aligned}$$

□

Proposition **1.1.5.** *Si $f : E \to F$ est un isomorphisme, alors la bijection réciproque f^{-1} est un isomorphisme.*

1.1.8 Distributivité

Définition **1.1.12.** *Soient E un ensemble, $*$ et $\top$ deux lois de composition internes sur E.*

1. *On dit que la loi T est **distributive à gauche** par rapport à la loi $*$ si et seulement si :*
$$\forall (x,y,z) \in E^3, \quad x\top(y*z) = (x\top y)*(x\top z),$$
2. *On dit que la loi T est **distributive à droite** par rapport à la loi $*$ si et seulement si :*
$$\forall (x,y,z) \in E^3, \quad (x*y)\top z = (x\top z)*(y\top z),$$
3. *On dit que la loi $\top$ est **distributive** par rapport à la loi $*$ si et seulement si $\top$ est **distributive à gauche et à droite** par rapport à la loi $*$. C'est-à-dire*
$$\forall (x,y,z) \in E^3, \quad x\top(y*z) = (x\perp y)*(x\top z) \quad et \quad (y*z)\top x = (y\top x)*(z\top x).$$

Remarque **1.1.6.** *Notons que les distributivités à gauche et à droite de $\top$ par rapport à $*$ sont équivalentes dans le cas où $\top$ est commutative.*

Exemple **1.1.6.** *Sur $\mathcal{P}(E)$, les lois $\cup$ et $\cap$ sont distributives l'une par rapport à l'autre.*

1.2 Lois de composition externes (LCE)

1.2.1 Définitions et exemples

Définition **1.2.1.** *Soient E et Ω des ensembles. On appelle loi de composition externe sur E, à ensemble d'opérateurs Ω, toute application de $\Omega \times E$ dans E.*

Exemple **1.2.1.** *Une application $g : \mathbb{N}^* \times E \to E\,;\ (n,e) \mapsto ne$ est le model de lois externes le plus connu.*

Exemple **1.2.2.** *Soit E un ensemble muni d'une loi de composition interne $\top$. En posant $n\perp x = \overset{n}{\top} x$, on définit une loi de composition externe sur E, dont l'ensemble d'opérateurs est, selon les propriétés de $\top$, $\mathbb{N}\backslash\{0\}$, $\mathbb{N}$ ou $\mathbb{Z}$.*

1.2.2 Partie stable par une loi de composition externe, loi induite

Définition **1.2.2.** *Soit E un ensemble muni d'une loi de composition externe $\perp$ à opérateurs dans X. Soit F une partie de E. On dit que F est stable par $\perp$ si :*
$$\forall a \in X, \qquad \forall x \in F, \qquad a\perp x \in F.$$
Si F est une partie stable par $\perp$, alors la restriction de $\perp$ à F est une loi de composition externe sur F dite loi induite par $\perp$ dans F.

1.2.3 Distributivité

Définition **1.2.3.** *Soit E un ensemble muni :*

i) D'une loi de composition interne $*$;

ii) D'une loi de composition externe $\perp$ à opérateurs dans X.

On dit que la loi $\perp$ est distributive par rapport à la loi $*$ si :

$$\forall a \in X, \quad \forall (x, y) \in E^2, \quad a \perp (x * y) = (a \perp x) * (a \perp y).$$

Exemple **1.2.3.** *Sur $\mathcal{P}(E)$, les lois $\cup$ et $\cap$ sont distributives l'une par rapport à l'autre.*

Chapitre 2

STRUCTURES ALGEBRIQUES

2.1 Groupes

2.1.1 Définitions et exemples

Définition 2.1.1. *On appelle groupe tout couple $(G, \top)$ composé d'un ensemble G non vide et d'une loi de composition $\top$ interne sur cet ensemble satisfaisant aux axiomes suivants :*

(G_1) *La loi $\top$ est associative ;*

(G_2) *La loi $\top$ possède un élément neutre ;*

(G_3) *Tout élément de G admet un symétrique pour la loi "$\top$".*

Si de plus la loi $\top$ est commutative, le groupe $(G, \top)$ est appelé ***groupe commutatif*** *ou* ***groupe abélien****.*

Exemples 2.1.1.

1 *$(\mathbb{Z}, +)$ est un groupe abélien. Mais $(\mathbb{Z}, \times)$ n'est pas un groupe.*

2 *$(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes abéliens.*

3 *$(\mathbb{Q}, \times)$, $(\mathbb{R}, \times)$ et $(\mathbb{C}, \times)$ ne sont pas des groupes.*

4 *$(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes abéliens.*

5 *Soient E un ensemble non vide et $\mathcal{A}(E)$ l'ensemble des applications de E dans E. On pose $S(E) = \{f \to \mathbb{A}(E) / \quad f$ bijective$\}$. $S(E)$ est une partie stable par la composition des applications " $\circ$ ".*
" $\circ$ " définit donc une loi de composition interne sur $S(E)$, et muni de cette loi, $S(E)$ est un groupe non abélien. Pour $E = \{1, 2, ..., n\}$, $S(E)$ est noté simplement S_n et est appelé groupe des premutations de n éléments. $Card(S_n) = n!$.

6 *Soit A un ensemble non vide. $\mathcal{P}(A)$ muni de la différence symétrique Δ est un groupe abélien.*

7 *Le produit cartésien de deux groupes $(E, *)$ et $(F, \bullet)$ est un groupe avec la loi cartésienne $\top$:*

$$(e, f)\top(e', f') = (e * e', f \bullet f').$$

En particulier

a *E^2, est un groupe avec la loi cartésienne notée encore $*$*

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

b *Plus généralement E^n est un groupe avec la loi cartésienne $*$*

$$(x_1, ..., x_n) * (y_1, ..., y_n) = (x_1 * y_1, ..., x_n * y_n).$$

c *$(\mathbb{R}^2, +)$ est un groupe abélien, la loi + étant définie par $\forall (a, b), (c, d) \in \mathbb{R}^2$, $(a, b) + (c, d) = (a + c, b + d)$.*

d *$(\mathbb{R}^3, +)$ est un groupe abélien, la loi + étant définie par $\forall (a_1, a_2, a_3), (b_1, b_2, b_3) \in \mathbb{R}^3$, $(a_1, a_2, a_3) + (b_1, b_2, b_3) = (a_1 + b_1, a_2 + b_2, a_3 + b_3)$.*

e *$\mathbb{R}^n$ est un groupe abélien avec la loi cartesienne +.*

2.1.2 Sous-groupes d'un groupe

a) Définitions et Exemples

Définition 2.1.2. *Soient $(G, *)$ un groupe, d'élément neutre e et H une partie de G. On dit que H est un sous-groupe de $(G, *)$ si les 3 propriétés suivantes sont vérifiées :*

i) $e \in H$

ii) $\forall (x, y) \in H^2$, $x * y \in H$.

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

Proposition 2.1.1. *Soient $(G, .)$ un groupe d'élément neutre e et H une partie de G. H est un sous-groupe de G si et seulement si les conditions suivantes sont satisfaites :*

(a) $e \in H$,

(b) $\forall x, y \in H, \quad x.y^{-1} \in H$.

Démonstration. Supposons que H est un sous-groupe de G. Alors $e \in H$ d'après la définition 2.1.2 i). Soient $x, y \in H$. On a $y^{-1} \in H$ d'après la définition 2.1.2 iii) et $xy^{-1} \in H$ d'après la définition 2.1.2 ii), d'où la proposition.

Réciproquement, supposons (a) et (b) vraie. Il est clair que $e \in H$. Soit $x \in H$. D'après (b) on a $ex^{-1} \in H$ donc $x^{-1} \in H$ ce qui prouve iii) de la définition 2.1.2.
Soient $x, y \in H$. Alors $x \in H$ et $y^{-1} \in H$, donc $x(y^{-1})^{-1} \in H$, ainsi $xy \in H$. Ce qui prouve ii) de la définition 2.1.2. Par suite, H est un sous-groupe de G. □

Exemples **2.1.2.** — *G lui même et $\{e\}$ où e est l'élément neutre de $(G,*)$ sont des sous-groupes de $(G,*)$. Ces deux sous groupes sont dits triviaux.*

— *$\mathbb{Z}$ est un sous groupe de $(\mathbb{Q},+)$. $\mathbb{Q}$ est un sous groupe de $(\mathbb{R},+)$. $\mathbb{R}$ est un sous groupe de $(\mathbb{C},+)$*

— *$\mathbb{R}^*$, $\{-1,1\}$ sont des sous-groupes de $(\mathbb{R}^*,\times)$.*

— *$U_n=\{z\in\mathbb{C}:\ z^n=1\}$ est un groupe de n éléments de $(\mathbb{C}^*,\times)$.*

— *Pour tout $a\in\mathbb{Z}$, l'ensemble des multiples de a, noté $a\mathbb{Z}$ est un sous groupe de $(\mathbb{Z},+)$.*

— *Plus généralement, si $(G,*)$ est un groupe et $g\in G$, alors l'ensemble des puissances de a : $\{g^n,\ n\in\mathbb{Z}\}$ est un sous-groupe de $(G,*)$.*

$$a^0=e,\quad a^{-2}=(a^{-1})^2,\quad a^{-3}=(a^{-1})^3$$

Remarque **2.1.1.** **1** *Un sous-groupe H n'est pas vide.*

2 *Si H est un sous-groupe de $(G,*)$ alors H est stable pour la loi $*$, et donc $*$ induit une loi de composition interne sur H. Muni de cette loi, H est un groupe, d'où la terminologie "sous - groupe"*

3 *Très souvent pour montrer qu'un ensemble muni d'une loi de composition interne (LCI) est un groupe, on essaie de voir cet ensemble comme un sous-groupe d'un ensemble plus grands.*

4 *Une partie stable d'un groupe n'est pas nécessairement un sous-groupe. Par exemple $\mathbb{N}$ est une partie stable de $\mathbb{Z}$ pour l'addition, mais ce n'est pas un sous-groupe de $(\mathbb{Z},+)$.*

Théorème **2.1.1** (Caracterisation des sous-groupes de $(\mathbb{Z},+)$)**.** *Soit $H\subset\mathbb{Z}$.*
H un sous-groupe de $(\mathbb{Z},+)$ si et seulement si il existe $a\in\mathbb{N}$ tel que $H=a\mathbb{Z}$.

Démonstration. On montre facilement que pour tous entier n, $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$. Si $H=\{0\}$, alors on peut prendre $n=0$ et c'est le seul entier qui convienne.
Si $H\neq\{0\}$, posons, $n=\min(H\cap\mathbb{N}*)$, (n existe dans $\mathbb{N}$, d'après la propriété fondamentale de $\mathbb{N}$), on a $n\in H$, comme H est un sous-groupe de $(\mathbb{Z},+)$, tout multiple de n est dans$H$, c'est-à-dire $n\mathbb{Z}\subset H$. Soit $k\in H$, effectuons la division euclidienne de k par n, $(n\neq 0)$ $k=nq+r$ avec $0\leq r<n$.
On a donc $r=k-nq\in H\cap\mathbb{N}*$, si $r\neq 0$ alors $r\geq n$, ce qui est absurde, donc $r=0$ ce qui donne $k=nq\in\mathbb{Z}$. Par suite, $H=n\mathbb{Z}$. □

b) Intersection de sous-groupes d'un même groupe

Lemme **2.1.1.** *Soient H_1 et H_2 deux sous-groupes d'un même groupe $(G,*)$; $H_1\cap H_2$ est un sous groupe de $(G,*)$.*

Plus généralement si $\{H_i\}_{i\in I}$ est une famille de sous-groupes d'un même groupe $(G,*)$, alors $\bigcap_{i\in I} H_i$, $I\subset\mathbb{N}$, est un sous groupe de $(G,*)$.

Démonstration. **1** $\forall i\in I,\quad e\in H_i$ donc $e\in\bigcap_{i\in I}H_i$.

2 Soient $x,y\in\bigcap_{i\in I}H_i$. $\forall i\in I$ on a $x\in H_i$ et $y^{-1}\in H_i$, donc $xy^{-1}\in H_i$ car H_i est un sous-groupe de G. Ainsi $xy^{-1}\in\bigcap_{i\in I}H_i$.

□

Par suite, $\bigcap_{i\in I}H_i$ est un sous-groupe de G.

c) Sous-groupe engendré par une partie

Définition 2.1.3. *Soit A une partie de G. On appelle sous groupe engendré par A l'intersection de tous les sous-groupes de G contenant A. Ce sous-groupe est le plus petit (au sens de l'inclusion) sous-groupe de $(G,*)$ contenant A. On le note $<A>$.*

Théorème 2.1.2. *Soient G un groupe d'élément neutre e et A une partie de G. Désignons par H l'ensemble des éléments de G qui peuvent s'écrire*

$$a_1^{\varepsilon_1}a_2^{\varepsilon_2}...a_n^{\varepsilon_n}\qquad avec\quad a_i\in A\quad et\quad \varepsilon_i\in\{-1,+1\},\quad \forall i\in\{1,2,...,n\},$$

en convenant que $H=\{e\}$ si $A=\emptyset$.
Alors H est le sous-groupe de G engendré par A.

Démonstration. — H est non vide, ainsi qu'on le constate en utilisant $A\subset H$ si $A\neq\emptyset$ et $H=\{e\}$ si $A=\emptyset$. D'autre part si

$$x=a_1^{\varepsilon_1}a_2^{\varepsilon_2}...a_n^{\varepsilon_n}\qquad et\qquad y=b_1^{\phi_1}b_2^{\phi_2}...b_n^{\phi_n}.$$

sont deux éléments de H, xy^{-1} s'écrit $a_1^{\varepsilon_1}a_2^{\varepsilon_2}...a_n^{\varepsilon_n}b_1^{-\phi_1}b_2^{-\phi_2}...b_n^{-\phi_n}$; d'où $xy^{-1}\in H$.
Ainsi H est un sous-groupe de G contenant A.

— Inversement soit L un sous-groupe de G contenant A. Pour toute famille finie $(a_1,...,a_n)$ d'éléments de A, $a_1^{-1},...a_n^{-l}$ sont aussi des éléments de L, et il en est de même de tout produit de la forme $a_1^{\varepsilon_1}a_2^{\varepsilon_2}...a_n^{\varepsilon_n}$; on a donc $H\subset L$,
H est ainsi le plus petit sous-groupe de G contenant A.

□

Exemple 2.1.1. *si $A=\emptyset$, $<\emptyset>=\{e\}$; $A=x$, $<x>=\{x^n,\ n\in\mathbb{Z}\}$.*

d) Réunions de sous-groupes

La réunion de deux sous-groupes d'un même groupe G n'est pas un sous-groupe (en général). Par exemple $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous groupe de $\mathbb{Z}$.

2.1.3 Classes d'équivalence suivant un sous-groupe

a) Relation de Lagrange

Soient $(G, *)$ un groupe, d'élément neutre e, et H un sous-groupe de $(G, *)$. H permet de définir sur G la relation binaire $\mathcal{R}_H$ suivant :

$$\forall (x, y) \in G^2, \qquad x\mathcal{R}_H y \quad si \quad x^{-1} * y \in H.$$

On a le théorème suivant :

Théorème 2.1.3 (de Lagrange). *i) $\mathcal{R}_H$ est une relation d'équivalence.*

ii) La classe d'équivalence d'un point $a \in G$ est $\overline{a} = \{a * h, \quad h \in H\}$ qu'on note $a * H$.

iii) Il y a une bijection entre $\overline{e} = H$ et $\overline{a} = aH$.

iv) Si G est un groupe fini, on a

$$Card(G) = Card(H).Card(\frac{G}{\mathcal{R}_H}).$$

Démonstration. i) à faire en exercice

ii) $a^{-1} * (a * h) = h \in H$, donc $(a * h)\mathcal{R}_H a$

iii) $\phi : H \to aH$; $h \mapsto a * h$ est une application bijective.

iv) Comme G est fini, l'ensemble des classes d'équivalence est aussi fini on a

$$G = H \cup (x_1 * H) \cup (x_2 * H) \cup .. \cup (x_k * H).$$

d'où $Card(G) = Card(H) + Card(x_1 * H) + ... + Card(x_k * H)$.
Comme $Card(x_i * H) = Card(H)$, on a $Card(G) = Card(H).Card(\frac{G}{\mathcal{R}_H})$.

□

Remarque 2.1.2. *H permet de définir une autre relation binaire $\mathcal{R}'_H$ sur G par :*

$$x\mathcal{R}'_H y, \quad si \quad x * y^{-1} \in H.$$

$\mathcal{R}'_H$ a toutes les propriétés dans le théorème de lagrange, sauf que la classe d'équivalence de $a \in G$ est $H * a = h * a, \ h \in H$. Très souvent, on a

$$a * H \neq H * a$$

b) Sous-groupes distingés dans un groupe

Définition 2.1.4. *Un sous-groupe H de $(G,*)$ est dit distingué dans G si on a :*

$$\forall x \in G, \quad \text{on a} \quad x * H = H * x.$$

On note $H \lhd G$.

Exemple 2.1.2. **1** *$\{e\}$ et G les deux sous groupes triviaux sont distingués.*

2 *Tout sous-groupe d'un groupe abélien est distingué.*

Proposition 2.1.2. *Soit H un sous-groupe de G. Les assertions suivantes sont équivalentes.*

i) H *est un sous-groupe distingué de* G,

ii) $\forall x \in G,\ xHx^{-1} = H$,

iiii) $\forall x \in G, \forall h \in H,\ xhx^{-1} \in H$,

iv) $\forall x \in G,\ xH \subset Hx$,

v) $\forall x \in G,\ Hx \subset xH$..

Démonstration. A faire en exercice. □

2.1.4 Groupes-quotients

Proposition 2.1.3. *Soit H est un sous-groupe distingué de $(G,*)$,*

a) $\mathcal{R}_H = \mathcal{R}'_H$

b) $\mathcal{R}_H$ *est compatible avec la loi* $*$ *c'est à dire :*
si $a\mathcal{R}_H b$ *et* $x\mathcal{R}_H y$, *alors* $(a*x)\mathcal{R}_H(b*y)$.

Démonstration. a) Il faut montrer que $a\mathcal{R}_H b \Leftrightarrow a\mathcal{R}'_H b$
Soit $(a,b) \in G^2$ tel que $a\mathcal{R}_H b$.
Alors $a^{-1} * b \in H$. Comme H est distingué dans G, $a * (a^{-1} * b) * a^{-1} \in H$. c'est-à-dire $b * a^{-1} \in H$, donc $b\mathcal{R}'_H a$ et $a\mathcal{R}'_H b$ (puisque $\mathcal{R}'_H$ est symétrique).

Réciproquement, si $a\mathcal{R}'_H b$, alors $a * b^{-1} \in H$. H étant distingué dans G, on a $b^{-1}(a * b^{-1}) * b \in H$. Ainsi $b^{-1} * a \in H$ et $a\mathcal{R}_H b$.

b) Soient $(a,b) \in G^2$, $(x,y) \in G^2$ tels que $a\mathcal{R}_H b$ et $x\mathcal{R}_H y$. on a :

$$\begin{aligned}(a*x)^{-1} * (b*y) &= x^{-1} * (a^{-1} * b) * y \\ (a*x)^{-1} * (b*y) &= (x^{-1} * (a^{-1} * b) * x) * (x^{-1} * y) \in H.\end{aligned}$$

□

Notation **2.1.1.** *Si H est distingué, l'ensemble quotient $\frac{G}{\mathcal{R}_H}$ est noté $\frac{G}{H}$*

Proposition **2.1.4.** *La loi $*$ induit une loi de composition interne sur $\frac{G}{H}$ par :*

$$(\overline{a}, \overline{b}) \mapsto \overline{a * b}.$$

$\frac{G}{H}$ muni de cette loi (encore notée $*$) est un groupe, appelé groupe quotient.

Exemple **2.1.3.** *$G = \mathbb{Z}$ avec l'addition +, et $H = 4\mathbb{Z}$. $\frac{\mathbb{Z}}{4\mathbb{Z}}$ est un groupe avec l'addition $\overline{a} + \overline{b} = \overline{a + b}$.*
La table de + de $\frac{\mathbb{Z}}{4\mathbb{Z}}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

2.1.5 Homomorphismes de groupes

Définition **2.1.5.** *Soient $(G, *)$, $(H, \top)$ deux groupes et $f : G \to H$ un homomorphisme. L'homomorphisme f est appelé homomorphisme (ou morphisme) de groupes.*
*On appelle **noyau** de f et on note $\ker(f)$, le sous-ensemble de G défini par*

$$\ker(f) = \{x \in G / f(x) = e_H\}$$

où e_H est l'élément neutre du groupe H.
*L'**image** de f, notée $Im(f)$ ou $f(G)$, est le sous-ensemble de H défini par*

$$Im(f) = \{y \in H / \exists x \in G, y = f(x)\}.$$

Exemple **2.1.4.**

1 *L'application $g : (\mathbb{R}_+^*, \times) \to (\mathbb{R}+)$ définie par $x \mapsto \ln(x)$ est un morphisme de groupes.*

2 *Soit $n \in \mathbb{N}^*$. L'application $f : (\mathbb{C}^*, \times) \to (\mathbb{C}^*, \times)$ définie par $z \mapsto z^n$ est un morphisme de groupes.*

Remarque **2.1.3.** *L'homomorphisme f satisfait la propriété suivante :*

$$\forall x \in G, \qquad f(x^{-1}) = (f(x))-1 \not\in.$$

Théorème **2.1.4.** *Soit $f : (\mathbb{R}, +) \to (\mathbb{R}, +)$ un morphisme de groupes continu en 0, alors :*

$$\forall x \in \mathbb{R}, \qquad f(x) = ax.$$

où $a = f(1)$.

Démonstration. On pose $a = f(1)$, on montre que $\forall n \in \mathbb{N}$, $f(n) = an$ (récurrence), on en déduit que $f(-n) = a(-n)$ car $f(-n) = -f(n)$, d'où : $\forall n \in \mathbb{Z}$, $f(n) = an$. Soit $r = \frac{p}{q}$ un rationnel avec $q \in \mathbb{N}^*$, alors $f(qr) = f(p) = ap = qf(r)$ d'où $f(r) = ar$.
Soit $x \in \mathbb{R}$ et (r_n) une suite de rationnels qui converge vers x, alors $(x - r_n)$ converge vers 0 et donc $f(x - r_n)$ tend vers $f(0) = 0$, or $f(x - rn) = f(x) - f(rn)$ donc $(f(rn))$ converge vers $f(x)$. Or $f(r_n) = ar_n \to ax$, par conséquent $f(x) = ax$. □

Proposition 2.1.5. *Soit $f : G \to H$ un morphisme de groupes. L'image directe par f de tout sous-groupe de G est un sous-groupe de H. En particulier, $Im(f)$ est un sous-groupe de H.*

Démonstration. Soit K un sous-groupe de G. Montrons que $f(K)$ est un sous-groupe de H.

1) Comme $e_G \in K$ alors $f(e_G) \in f(K)$.
2) Soient $a, b \in f(K)$. Alors, il existe $x, y \in K$ tel que $a = f(x)$ et $b = f(y)$. Ainsi

$$ab^{-1} = f(x)f(y^{-1}) = f(xy^{-1}).$$

or $xy^{-1} \in K$ donc $ab^{-1} \in f(K)$. En somme $f(K)$ est un sous-groupe de H. On déduit aussi que $Im(f) = f(G)$ est un sous-groupe de H.

□

Proposition 2.1.6. *Soit $f : G \to H$ un morphisme de groupes. L'image réciproque par f de tout sous-groupe de H est un sous-groupe de G contenant* $\ker f$. *En particulier,* $\ker(f)$ *est un sous-groupe de G.*

Démonstration. A faire en exercice. □

Théorème 2.1.5. *Soit $f : G \to G'$ un morphisme de groupes.*

1 *Si H est un sous-groupe distingué de G, $f(H)$ est un sous-groupe distingué de $f(G)$.*

2 *Si H' est un sous-groupe distingué de G', $f^{-1}(H')$ est un sous-groupe distingué de G.*

Démonstration. **1** Soit $H \lhd G$. Il faut montrer :

$$\forall (a', h') \in f(G) \times f(H) \qquad a'h'(a')^{-1} \in f(H),$$

c'est-à-dire :

$$\forall (a, h) \in G \times H \qquad f(a)f(h)(f(a))^{-1} \in f(H),$$

ce qui résulte de ce que $f(a)f(h)(f(a))^{-1}$ est l'image par f de aha^{-1}, qui est un élément de H (car $(a, h) \in G \times H$).

2 Soit $H' \lhd G'$. Posons $H = f^{-1}(H')$. Il faut montrer : $\forall (a,h) \in G \times H, aha^{-1} \in H$. Cela résulte de ce que $f(aha^{-1})$ qui s'écrit $f(a)f(h)(f(a))^{-1}$, est un élément de H' (car $(f(a), f(h)) \in G' \times H'$).

□

Proposition 2.1.7. *Soit $f : G \to H$ un morphisme de groupes.*

$$f \text{ injective} \Leftrightarrow \ker f = \{e_G\}.$$

Démonstration. ($\Rightarrow$) Supposons f injective. Pour tout $x \in \ker f$ on a $f(x) = f(e_G)$. Le caractère injectif de f implique que $x = e_G$, donc $\ker f = \{e_G\}$.
($\Leftarrow$) Supposons $\ker f = \{e_G\}$. Soient $x, y \in G$ tels que $f(x) = f(y)$. On a $f(x).(f(y))^{-1} = e_H$. Comme $(f(y))^{-1} = f(y^{-1})$ on a $f(x).f(y^{-1}) = e_H$. Ainsi $f(x.y^{-1}) = e_H$, d'où $x.y^{-1} \in \ker f$ et comme $\ker f = \{e_G\}$, on a $x.y^{-1} = e_G$, c'est à dire que $x = y$. Donc f est injective. □

2.2 Anneaux

2.2.1 Définition et exemples

Définition 2.2.1. *On appelle anneau tout triplet $(A, +, .)$, où A est un ensemble dit sous-jacent à l'anneau, où "$+$" et "$.$" sont des lois de composition internes sur A dites addition et multiplication, satisfaisant aux axiomes suivants :*

- (A_1) *$(A, +)$ est un groupe abélien, dit groupe additif de l'anneau ; l'élément neutre est noté 0 et est appelé élément nul ;*
- (A_2) *La multiplication est associative ;*
- (A_3) *La multiplication est distributive par rapport à l'addition.*
  - *On qualifie de commutatif tout anneau dans lequel la multiplication est commutative.*
  - *L'anneau A est dit unitaire si la multiplication admet un élément neutre.*

Notation 2.2.1.
- *L'élément neutre de + dans A est noté 0_A et pour tout $x \in A$, le symétrique de x par rapport à la loi $+$ est noté $-x$. (on dit que $-x$ est l'opposé de x)*
- *Si l'anneau A est unitaire, l'élément neutre de la multiplication " $\cdot$ " dans A est noté 1_A. Un élément $x \in A$ sera dit inversible, s'il admet un symetrique par rapport à la multiplication, dans ce cas le symétrique de x est noté x^{-1}. On note $\mathcal{U}(A)$ l'ensemble de tous les éléments inversibles de A. $\mathcal{U}(A)$ est stable pour la multiplication et $(\mathcal{U}(A), .)$ est un groupe.*

— *Pour tout $a \in A$, et pour tout $n \in \mathbb{N}^*$ on pose :*

$$a^n = \underbrace{a.a \ \cdot \ \cdot \ \cdot \ a}_{n fois} \qquad et \qquad na = \underbrace{a + a + \ \cdot \ \cdot \ \cdot \ + a}_{n fois}.$$

Exemples 2.2.1. **1** *$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, munis de l'addition + et de la multiplication $\times$ sont des anneaux commutatifs et unitaires.*

2 *Soit $(G, +)$ est un groupe abélien. On note $End(G)$ l'ensemble de tous les endomorphisme de G. $(End(G), +, \circ)$ est un anneau en posant :*

$$f, g \in End(G), \quad f + g : x \mapsto f(x) + g(x) \quad et \quad f \circ g : x \mapsto f(g(x)).$$

3 *$(\mathbb{Z}/n\mathbb{Z}, +, .)$ est un anneau commutatif unitaire ayant n éléments.*

4 *Si A et A' sont 2 anneaux, il y a sur $A \times A'$ une structure naturelle d'anneau*

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

En particulier $\mathbb{Z}^2$, $\mathbb{Z}^3$, $\mathbb{Z}^4$, $\mathbb{C}^2$, ... sont des anneaux.

2.2.2 Propriétés remarquables dans l'anneau

i) $0_A.x = 0_A$, $x.0_A = 0_A$ pour tout $x \in A$.

ii) $-(x.y) = (-x).y = x.(-y)$ pour tout $(x, y) \in A^2$

iii) Si A est un anneau unitaire, on a $(-1_A).x = -x$

iv) Si x et y commutent (par rapport à "$\cdot$ ") c'est-à-dire $x.y = y.x$ alors

$$(x.y)^2 = x^2y^2, \quad (x.y)^3 = x^3.y^3 \quad , ..., \quad (x.y)^n = x^n.y^n \quad \forall n \in \mathbb{N}^*,$$

$$(x + y)^2 = x^2 + 2(xy) + y^2.$$

Plus généralement

$$(x + y)^3 = x^3 + 3(x^2y) + 3(xy^2) + y^3$$

$$\begin{aligned} (x + y)^n &= \sum_{k=0}^{n} C_n^k x^k y^{n-k} \\ &= x^n + C_n^1 xy^{n-1} + C_n^2 x^2 y^{n-2} + ... + C_n^k x^k y^{n-k} + ... + C_n^{n-1} xy^{n-1} + y^n. \end{aligned}$$

Exercice 1. *Soit $a \in A$. Calculer $(1_A + a)^5$*

Définition 2.2.2. *Soit A un anneau, on dit que $a \in A$ est un diviseur de zéro dans A si $a \neq 0$ et s'il existe $b \in A$, $b \neq 0$ tel que*

$$ab = 0 \qquad ou \qquad ba = 0.$$

Exemple **2.2.1.** *Dans $\mathbb{Z}/6\mathbb{Z}$, l'élément $\overline{3}$ est un diviseur de $\overline{0}$.*

Exercice 2. *Déterminer tous les diviseurs de $\overline{0}$ de l'anneau $\mathbb{Z}/24\mathbb{Z}$.*

Définition **2.2.3.** *On dit que A est intègre si A est commutatif, non réduit à zéro et dépourvu de diviseur de zéro, c'est à dire que*

$$\forall a, b \in A, \qquad ab = 0 \;\Rightarrow\; a = 0 \quad ou \quad b = 0.$$

Exemple **2.2.2.** **1** *$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sont des anneaux intègres.*

2 *$\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre si et seulement si $n = 0$ ou n est un nombre premier.*

2.2.3 Sous-anneaux, Idéaux

a) Sous-anneaux

Définition **2.2.4.** *Soient A un anneau et B une partie non vide de A. On dit que B est un sous-anneau de A si :*

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

ii) B est stable par le produit $\forall b, b' \in B$, $bb' \in B$.

Exemple **2.2.3.**
- *$\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$*
- *$\mathbb{R}$ est un sous-anneau de $\mathbb{C}$*
- *$\mathbb{Q}$ est un sous-anneau de $\mathbb{R}$*

Remarque **2.2.1.** *L'intersection de sous-anneaux est un sous-anneau. On a alors la notion de sous-anneau engendré par une partie quelconque X d'un anneau A.*
Si 1_A est l'élément unité de l'anneau $(A, +, .)$, tous les sous-anneaux contiennent le sous-anneau

$$\mathbb{Z}.1_A = \{n.1_A;\ n \in \mathbb{Z}\}.$$

Définition **2.2.5.** *Soient A un anneau commutatif unitaire et B une partie non vide de A. On dit que B est un sous-anneau de A si :*

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

ii) B contient 1_A et B est stable par le produit $\forall b, b' \in B$, $bb' \in B$.

b) Idéaux

Définition **2.2.6.** *On dit que B est un idéal de A si*

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

2 *$\forall a \in A$, $\forall b \in B$, on a $ab \in B$.*

Exemple **2.2.4.**
- $\{0_A\}$, A *sont des idéaux de* A *(dits triviaux)*
- aA *l'ensemble des multiples de* a *dans* A *est un idéal (dit principal).*
- *Les idéaux de l'anneau* $\mathbb{Z}$ *sont de la forme* $n\mathbb{Z}$*, où* $n \in \mathbb{N}$

Remarque **2.2.2.**
- *L'intersection d'idéaux d'un anneau est un idéal. On a donc la notion de d'idéal engendré par une partie quelconque* X *d'un anneau* A*.*
- *Le seul idéal qui contient* 1_A *l'élément unité de l'anneau* $(A, +, .)$ *ou tout autre élément inversible est l'idéal* A *lui-meme.*

Définition **2.2.7.**
- *Un idéal* I *est dit propre s'il est différent de l'anneau* A *et de l'idéal* $\{0\}$*.*
- *Parmi les idéaux propres, un idéal* M *est dit maximal s'il n'est contenu strictement dans aucun autre idéal propre.*

Exemple **2.2.5.** *dans l'anneau* $(\mathbb{Z}, +, .)$ *les idéaux* $2\mathbb{Z}, 3\mathbb{Z}, 5\mathbb{Z}$..... *sont maximaux.*

Remarque **2.2.3.** *Notons que la réunion de deux idéaux d'un anneau n'est un idéal.*

2.2.4 Anneaux quotients

Proposition **2.2.1.** *Si* I *est un idéal de* A*, alors les lois " + " et " · " sont compatibles avec la relation d'équivalences (de Lagrange)*

$$a\mathcal{R}b \qquad si \qquad b - a \in I.$$

Proposition **2.2.2.** *L'ensemble quotient* $\dfrac{A}{I}$ *muni des lois de composition internes*

$$\overline{a} + \overline{b} = \overline{a + b} \quad ; \quad \overline{a}.\overline{b} = \overline{a.b}.$$

est un anneau commutatif unitaire.

Exercice 3. **1** *Ecrire les tables de l'addition et de la multiplicattion de l'anneau quotient* $A = \dfrac{\mathbb{Z}}{6Z}$.

2 *Trouver* $\mathcal{U}(A)$.

2.2.5 Morphisme d'anneaux

Définition **2.2.8.** *Soient* A*,* B *deux anneaux, et* $f : A \to B$ *une application. On dit que* f *est un morphisme d'anneaux (ou un homomorphisme) de* A *dans* B *si*

i) $\forall a, b \in A$, $f(a + b) = f(a) + f(b)$,

ii) $\forall a, b \in A$, $f(ab) = f(a)f(b)$.

On définit de façon évidente les notions d'endomorphisme, d'isomorphisme et d'automorphisme d'anneaux.

Définition **2.2.9.** *Soient A, B deux anneaux **unitaires**, et $f : A \to B$ une application. On dit que f est un morphisme d'anneaux (ou un homomorphisme) de A dans B si*

i) $f(1_A) = 1_B$,

ii) $\forall a, b \in A,\ f(a+b) = f(a) + f(b)$,

iii) $\forall a, b \in A,\ f(ab) = f(a)f(b)$.

Exemples **2.2.2.** **1** *L'application $z \mapsto \overline{z}$ est un automorphisme de l'anneau $\mathbb{C}$.*

2 *L'application $(u_n) \mapsto \lim\limits_{n\to+\infty} u_n$ est un morphisme de l'anneau des suites convergentes dans $\mathbb{R}$.*

Théorème **2.2.1.** *Soit $f : A \to B$ un morphisme d'anneaux.*

i) Si A est un sous-anneau de A alors $f(A)$ est un sous-anneau de B,

ii) Si B est un sous-anneau de B alors $f^{-1}(B)$ est un sous-anneau de A,

iii) Si A et B sont commutatifs, et si I' est un idéal de B alors $f^{-1}(I')$ est un idéal de A.
En particulier, $\ker f = \{x \in A / f(x) = 0\}$ est un idéal de A.

Proposition **2.2.3.** *Soit $f : A \to B$ un morphisme d'anneaux. On a l'équivalence*

$$f \text{ injectif} \Leftrightarrow ker f = 0.$$

Démonstration. Le morphisme d'anneaux est un morphisme de groupes . D'après la proposition 2.1.7, on a le résultat. □

Théorème **2.2.2.** *Soient A, B, C trois anneaux.*

1 *Si $f : A \to B$ et $g : B \to C$ sont des morphismes d'anneaux alors $g \circ f : A \to C$ est un morphisme d'anneaux.*

2 *Si $f : A \to B$ est un isomorphisme d'anneaux alors f^{-1} est un isomorphisme de B sur A.*

3 *$(End(A), +, \circ)$ est un anneau, dont le groupe des unités est $(Aut(A), \circ)$.*

Démonstration. A faire en exercice. □

Théorème **2.2.3** (Transport de structure)**.** *Si $(A, +, .)$ est un anneau et f une bijection de A sur un ensemble E, alors on peut définir deux lois sur E, de sorte que f devienne un isomorphisme d'anneaux.*

Démonstration. — A la loi " $+$ ", on associe la loi $\top$ définie par

$$\forall (x', y') \in E^2, \quad x' \top y' = f(f^{-1}(x') + f^{-1}(y')).$$

— A la loi ".", on associe la loi $\perp$ définie par

$$\forall (x', y') \in E^2, \quad x' \perp y' = f(f^{-1}(x').f^{-1}(y')).$$

On montre que $(E, \top, \perp)$ est un anneau. □

2.3 Corps

2.3.1 Définitions-exemples

Définition 2.3.1. *On dit qu'un ensemble $\mathbb{K}$ muni de deux lois "+" et " $\times$ " est un corps si*

i) $(\mathbb{K}, +, \times)$ *est un anneau, et* $1_{\mathbb{K}} \neq 0$,

ii) $\forall x \in \mathbb{K}\backslash\{0\}$, $\exists x' \in \mathbb{K}$, $x'x = 1_{\mathbb{K}} = xx'$.

Si de plus la multiplication est commutative, on dit que $\mathbb{K}$ est un corps commutatif.

Remarque 2.3.1. *Un anneau $\mathbb{K}$ est un corps s'il n'est pas réduit à 0 et si tout élément non nul de $\mathbb{K}$ est inversible.*

Remarque 2.3.2. **1** *Si $\mathbb{K}$ est un corps alors $\mathbb{K}\backslash\{0\}$ est un groupe multiplicatif qui est abélien si et seulement si $\mathbb{K}$ est commutatif.*

2 *Un corps est en particulier un anneau sans diviseurs de zéro.*

3 *Si I est un idéal du corps $\mathbb{K}$ alors $I = \{0\}$ ou $I = \mathbb{K}$.*

Exemples 2.3.1. *1) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps commutatifs pour les lois usuelles.*

2) $\mathbb{Q}[\sqrt{2}] = \{x \in \mathbb{R} / \ \forall a, b \in \mathbb{Q}, \quad x = a + b\sqrt{2}\}$ est un corps commutatif

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

Exemple 2.3.1. *Tout anneau intègre fini A est un corps. En effet :*
On sait que $A \neq \{0\}$. Soit $a \in A\backslash\{0\}$; associons-lui l'endomorphisme $x \to ax$ du groupe $(A, +)$ qui est une injection, puisque, a étant régulier, $ax = 0$ équivaut à $x = 0$; A étant fini, il s'agit même d'une bijection. Il existe donc un, et un seul $a' \in A$ tel que $aa' = 1$; par commutativité $a'a = 1$; a est donc inversible.

2.3.2 Sous-corps

Définition 2.3.2. *Soient $\mathbb{K}$ un corps et K une partie de $\mathbb{K}$. On dit que K est un sous-corps de $\mathbb{K}$ ou que $\mathbb{K}$ est un sur-corps de K si :*

(i) K *est un sous-anneau de* $\mathbb{K}$,

(ii) $\forall x \in K\backslash\{0\}, \qquad x^{-1} \in K\backslash\{0\}$.

Exemple 2.3.2. *(a)* $\mathbb{Q}$ *est un sous-corps de* $\mathbb{Q}[\sqrt{2}]$ *qui est lui-même un sous-corps de* $\mathbb{R}$.

(b) $\mathbb{Z}/p\mathbb{Z}$ *(p premier) n'a pas de sous-corps propres.*

Proposition 2.3.1. *Soient $\mathbb{K}$ un corps et K une partie de $\mathbb{K}$. Alors K est un sous-corps de $\mathbb{K}$ ssi :*

1) $1_{\mathbb{K}} \in K$,

2) $\forall x, y \in K$, $x - y \in K$,

3) $\forall x, y \in K$, $xy \in K$,

4) $\forall x \in K\backslash\{0\}$, $x^{-1} \in K\backslash\{0\}$.

Démonstration. $(\Rightarrow)$ Supposons que K est un sous-corps de $\mathbb{K}$. K est donc un sous-anneau de $\mathbb{K}$ et que l'on a $x^{-1} \in K$ pour tout élément non nul x de K. Par suite, les assertions 1), 2), 3) et 4) sont véréfiés.

$(\Leftarrow)$ Supposons que les assertions 1), 2), 3) et 4) sont véréfiés. Les assertions 1), 2) et 3) expriment que K est un sous-anneau de $\mathbb{K}$. L'assertion 4) exprime que l'inverse de tout élément non-nul de K est dans K. Par suite, K est un sous-corps de $\mathbb{K}$. □

Remarque 2.3.3. *On montre, comme pour les sous-groupes, que toute intersection d'une famille de sous-corps d'un corps $\mathbb{K}$ est un sous-corps de $\mathbb{K}$ et que, pour toute partie $X \subset \mathbb{K}$, il existe un plus petit sous-corps de $\mathbb{K}$ contenant X, on dit qu'il s'agit du sous-corps engendré par X.*

2.4 Espaces vectoriels sur un corps

2.4.1 Définitions-exemples

Définition 2.4.1. *Soit $(\mathbb{K}, +, \times)$ un corps. On appelle espace vectoriel sur le corps $\mathbb{K}$ tout ensemble E muni d'une loi de composition interne " + " (addition)*

$$+ : \left\{ \begin{array}{ccc} E \times E & \to & E \\ (x, y) & \mapsto & x + y \end{array} \right.$$

et d'une loi de composition externe " $\cdot$ "(multiplication par un scalaire)

$$\cdot : \begin{cases} \mathbb{K} \times E & \to & E \\ (\lambda, y) & \mapsto & \lambda y \end{cases}$$

telles que

1 $(E, +)$ *est un groupe commutatif. On note* 0_E *son élément neutre.*

2 *Pour tout* $(\alpha, \beta)\mathbb{K}^2$ *et pour tout* $(x, y) \in E^2$*, on a*

- **a** $(\alpha + \beta).x = \alpha.x + \beta.x$
- **b** $(\alpha \times \beta).x = \alpha.(\beta.x)$
- **c** $\alpha(x + y) = \alpha.x + \alpha.y$
- **d** $1_{\mathbb{K}}.x = x$

On dit alors que $(E, +, .)$ *est un* $\mathbb{K}-$*espace vectoriel. Les éléments de* $\mathbb{K}$ *sont appelés scalaires, ceux de* E*, vecteurs.*
L'élément neutre de $(E, +)$*,* 0_E *est appelé vecteur nul.*

Remarque **2.4.1.** **1** *Si* $\mathbb{K} = \mathbb{R}$*,* E *est appelé espace vectoriel réel.*

2 *Si* $\mathbb{K} = \mathbb{C}$*,* E *est appelé espace vectoriel complexe.*

Exemples **2.4.1.** — *Le corps* $\mathbb{K}$ *est un espace vectoriel sur lui-même.*

— *Si* E_1 *et* E_2 *sont deux espaces vectoriels sur* $\mathbb{K}$ *alors le produit cartésien* $E_1 \times E_2$ *est un espace vectoriel sur* $\mathbb{K}$ *avec les lois cartésiennes.*

— *Ainsi* $\mathbb{R}^2$*,* $\mathbb{R}^3$*,* $\cdots$*,* $\mathbb{R}^n$ *sont des espaces vectoriels sur* $\mathbb{R}$*.* $\mathbb{C}^2$*,* $\mathbb{C}^3$*,* $\cdots$*,* $\mathbb{C}^n$ *sont des espaces vectoriels sur* $\mathbb{C}$*.*

— *Plus généralement,* $\mathbb{K}^n$ *est un espace vectoriel sur* $\mathbb{K}$*.*

Remarque **2.4.2.** *Si* E *est un espace vectoriel sur* $\mathbb{C}$*, alors* E *est un espace vectoriel sur* $\mathbb{R}$*.*

2.4.2 Sous-espaces vectoriels

Définition **2.4.2.** *Soient* E *un espace vectoriel sur* $\mathbb{K}$ *et* V *un sous-ensemble de* E*. On dit que* V *est un sous-espace vectoriel de* E *si*

1 V *est un sous-groupe de* $(E, +)$*.*

2 $\forall x \in V, \forall a \in \mathbb{K}$ *on a* $ax \in V$*.*

Exemples **2.4.2.** $\{0_E\}$ *et* E *sont des sous-espaces vectoriels de* E*, ils sont dits triviaux.*

Proposition **2.4.1.** *Si V_1 et V_2 sont deux sous-espaces vectoriels d'un $\mathbb{K}-$espace vectoriel $(E,+,.)$, alors*

$$V_1 \cap V_2 \qquad et \qquad V_1 + V_2.$$

sont des sous-espaces vectoriels de E.

Démonstration. **1** Montrons que $V_1 \cap V_2$ est un sous-espace vectoriel de E.
Puisque V_1 et V_2 sont deux sous-espaces vectoriels de E, $0_E \in V_1$ et donc $0_E \in V_2$.
Soient $(x,y) \in (V_1 \cap V_2)^2$ et $(\alpha,\beta) \in \mathbb{K}^2$. Montrons que $\alpha.x + \beta.y \in V_1 \cap V_2$.
Soit $i \in \{1,2\}$, comme V_i est un sous-espace vectoriel de E et que $x, y \in V_i$, $\alpha.x + \beta.y \in V_i$. Ce qui montre que $\alpha.x + \beta.y \in V_1 \cap V_2$.

2 Le sous-ensemble $V_1 + V_2$ est bien un sous-espace vectoriel de E. En effet, $V_1 + V_2 \subset E$ car E est stable pour l'addition. De plus, $V_1 + V_2$ est non vide car V_1 et V_2 le sont. Enfin, si $u = x + y \in V_1 + V_2$ et $u' = x' + y' \in V_1 + V_2$ avec $x, x' \in V_1$ et $y, y' \in V_2$ alors, pour $\alpha, \beta \in \mathbb{K}$,

$$\alpha u + \beta u' = \alpha x + \beta x' + \alpha y + \beta y' \in V_1 + V_2,$$

car V_1 et V_2 sont des sous-espaces vectoriels.

□

2.4.3 Applications linéaires ou Homomorphismes d'espaces vectoriels

Définition **2.4.3.** *Soient E et F deux espaces vectoriels sur un corps $\mathbb{K}$. Une application $\phi : E \to F$ est un homomorphisme ou $\mathbb{K}-$linéaire si :*

i) $\phi(ax) = a\phi(x)$.

ii) $\phi(x + x') = \phi(x) + \phi(x') \qquad \forall x, x' \in E \quad et \quad \forall a \in \mathbb{K}.$

Exemples **2.4.3.**

- *id_E est une application linéaire*
- $C : E \to F\,;\, x \mapsto 0_F$
- $p : E \times F \to F\,;\, (x.y) \mapsto y$
- $f : \mathbb{R}^2 \to \mathbb{R}\,;\, (x,y) \mapsto x + y.$

Proposition **2.4.2.** *Soit $f : E \to F$ une application linéaire. Alors $Imf = f(E)$ l'image de f et $\ker f$ le noyau de f sont respectivement sous-espace vectoriel de E et de F.*

Démonstration. Comme $0_E \in E$ et que f est linéaire, $0_F = f(0_E) \in f(E)$ et $f(E)$ est non vide. Soient $a, a' \in \mathbb{K}$ et $y, y' \in f(E)$. Il existe $x, x' \in E$ tels que $y = f(x)$ et $y' = f(x')$. Montrons que $ay + a'y' \in f(E)$. En utilisant la linéarité de f : $ay + a'y' = af(x) + a'f(x)' = f(ax + a'x')$ et donc $ay + a'y' \in f(E)$. $f(E)$ est donc bien un sous-espace vectoriel de F.

De même que précédemment, comme $0_F \in F$ et que f est linéaire, $0_E \in f^{-1}(0_F)$. Soient $a, a' \in \mathbb{K}$ et $x, x' \in f^{-1}(0_F)$. Par la linéarité de f , $f(ax + a'x') = af(x) + a'f(x') = 0_F$. Il vient alors que $ax + a'x' \in f^{-1}(0_F)$. □

Les notions de monomorphisme ; d'épimorphisme, d'endomorphisme et d'isomorphisme sont laissées au lecteur.

2.4.4 Espaces vectoriels quotients

Soient E un espace vectoriel sur $\mathbb{K}$ et V un sous-espace vectoriel de E. Sur le groupe quotient $\dfrac{E}{V}$ on peut définir une loi de composition externe comme suit :

$$\phi : \mathbb{K} \times \frac{E}{V} \to \frac{E}{V}; \qquad (a, \overline{x}) \mapsto \overline{ax}$$

ϕ est bien définie et avec ϕ le groupe quotient $\dfrac{E}{V}$ est un espace vectoriel sur $\mathbb{K}$.

N.B : La structure d'espace vectoriel sera approfondie plus tard.

Chapitre 3

ARITHMÉTIQUE DANS $\mathbb{Z}$

3.1 Relation de divisibilité, division euclidienne dans $\mathbb{Z}$

3.1.1 Diviseurs, multiples

Définition 3.1.1. *Étant donnés deux entiers relatifs a et b, on dit que a est un **diviseur** de b, ou que b est un **multiple** de a, s'il existe $k \in \mathbb{Z}$ tel que $b = ka$.*

Notation 3.1.1.
- *Si d est un diviseur de a on note $d|a$.*
- *L'ensemble des diviseurs de a est noté $\mathcal{D}(a)$.*
- *L'ensemble des multiples de a est noté $\mathcal{M}(a)$ ou $a\mathbb{Z}$.*

Exemple 3.1.1.
- *1 et -1 divisent tous les entiers, mais ne sont divisibles que par 1 et -1.*
- *0 est un multiple de tous les entiers, mais n'est diviseur que de lui-même.*
- $\mathcal{D}(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$.

Remarque 3.1.1.
- *La relation "divise" est réflexive et transitive, mais n'est pas une relation d'ordre dans $\mathbb{Z}$, car elle n'est pas antisymétrique.*
- *En revanche, d'après la proposition suivante, sa restriction à $\mathbb{N}$ est une relation d'ordre. Pour cet ordre, le plus petit élément de $\mathbb{N}$ est 1, et le plus grand 0.*
- *La divisibilité sur $\mathbb{N}^*$ est liée à l'ordre naturel de $\mathbb{N}^*$ par la relation :*

$$a|b \Rightarrow a \leq b.$$

En effet, si $a|b$ alors $b = ka$ avec $k \in \mathbb{Z}$ et, puisque a et b sont strictement positifs, on a $k \in \mathbb{N}^*$ et par suite $b \geq a$.
Ce résultat est faux dans $\mathbb{N}$ puisque, par exemple, $1|0$.

Proposition 3.1.1. *On a :*

$$(a|b \quad et \quad b|a) \quad \Leftrightarrow \quad |a| = |b|.$$

Démonstration. — Supposons $a|b$ et $b|a$. Il existe alors des entiers relatifs k et k' tels que $b = ka$ et $a = k'b$, ce qui donne $a = k'ka$.

- Si $a = 0$, alors $b = k' = 0$ et $|a| = |b| = 0$.
- Si $a \neq 0$, alors $k'k = 1$. Comme k' et k sont des entiers relatifs, on a $|k| = |k'| = 1$, ce qui montre $|a| = |b|$.

— Si $|a| = |b|$, alors $a = b$ ou $a = -b$. Donc $a|b$ et $b|a$.

La proposition suivante est une conséquence évidente de la définition. □

Proposition 3.1.2.

Soient a et b deux entiers relatifs. Soit $d \in \mathbb{Z}^*$.

- Si $(u, v) \in \mathbb{Z}^2$, alors :

$$(d|a \quad et \quad d|b) \Rightarrow d|(au + bv).$$

- Si x est un entier non nul, alors :

$$a|b \Leftrightarrow (ax)|(bx).$$

3.1.2 Critères de divisibilité

♢ Un entier est divisible par 10 si, et seulement s'il se termine par un 0.
♢ Un entier est divisible par 5 si, et seulement s'il se termine par un 0 ou par un 5.
♢ Un entier est divisible par 2 si, et seulement s'il se termine par un 0, un 2, un 4, un 6 ou un 8.
♢ Un entier est divisible par 9 si, et seulement si la somme de ses chiffres l'est.
♢ Un entier est divisible par 3 si, et seulement si la somme de ses chiffres l'est.
♢ Un entier est divisible par 4 si, et seulement si le nombre formé par ses deux derniers chiffres (en base 10) l'est.
♢ Un entier est divisible par 11 si, et seulement si la somme des ses chiffres (en base 10) de rang pair diminuée de la somme de ses chiffres de rang impair est divisible par 11.

Exemples 3.1.1.

- *54 967 est divisible par 11 car (7 + 9 + 5) - (6 + 4) = 11 l'est.*
- *1 576 et 279 834 sont divisibles par 2 car 1576 se termine par 6 et 279834 se termine par 2.*
- *276, 848 et 57 316 sont divisibles par 4 car 76, 48 et 16 le sont*
- *471 et 8 643 sont divisibles par 3 car 4+7+1 = 12 et 8+6+4+3 = 21 et 12 et 21 sont divisibles par 3.*

3.1.3 Division euclidienne sur $\mathbb{Z}$

Théorème 3.1.1. *Soient a un entier relatif et b un entier naturel non nul. Il existe un unique couple d'entiers relatifs (q, r) tel que :*

$$a = bq + r \qquad avec \qquad 0 \leq r < b. \qquad (*)$$

- *q est appelé quotient de la division euclidienne de a par b,*
- *r est appelé reste de la division euclidienne de a par b.*

Démonstration. **Unicité :** Soient (q, r) et (q', r') deux couples vérifiant $(*)$. Montrons que $q = q'$ et $r = r'$. Puisque $0 \leq r < b$ et $0 \leq r' < b$, on a $b|q - q'| = |r' - r| < b$, ce qui entraîne $|q - q'| = 0$ puis $r' - r = 0$.

Existence :

— Si $a \in \mathbb{N}$: l'ensemble $A = \{n \in \mathbb{N} |\ nb \leq a\}$ est une partie de $\mathbb{N}$ non vide puisque $0 \in A$.

De plus A est majorée par a puisque si $n \in A$, alors $n < nb \leq a$ (b est non nul donc supérieur ou égal à 1). Donc A admet un plus grand élément q qui vérifie alors :

- $qb \leq a$ puisque $q \in A$,
- $(q + 1)b > a$ puisque $q + 1 \notin A$. En posant $r = a - bq$, on a alors $a = bq + r$ et $0 \leq r < (q + 1)b - bq = b$.

— Cas général : comme $b \geq 1$, on a $|a|b \leq |a|$, et donc $a + |a|b \in \mathbb{N}$. En appelant q' et r les reste et quotient de la division euclidienne de $a + |a|b$ par b , on obtient :

$$a = bq' + r - |a|b = bq + r$$

avec $q = q' - |a|$.

□

Remarque 3.1.2.

- *Si q est le quotient et r le reste de la division euclidienne de a par $b \neq 0$, on a :*

$$q = E\left(\frac{a}{b}\right) \quad et \quad r \equiv a\ [b]$$

où E désigne la fonction partie entière, puisque l'on a l'équivalence :

$$\forall q \in \mathbb{Z}, \quad q \leq \frac{a}{b} < q + 1 \Leftrightarrow bq \leq a < bq + b).$$

- *Si q est le quotient de la division euclidienne de l'entier naturel a par b, l'ensemble $A = \{n \in \mathbb{N} |\ nb \leq a\}$ est l'intervalle $[[0, q]]$.*
- *Étant donnés $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, notons q et r les quotient et reste de la division euclidienne de a par b.*

  — *Si $r = 0$, alors $a = bq$ et donc $b|a$.*

— *Réciproquement, si* $b|a$*, alors on a* $a = kb + 0$ *avec* $k \in \mathbb{Z}$ *et* $0 \leq 0 < b$*. L'unicité de la division euclidienne nous donne donc* $k = q$ *et* $r = 0$*.*
On a donc l'équivalence $b|a \Leftrightarrow r = 0$*.*

Exemple 3.1.2.
- $a = 271$ *et* $b = 19$*. On a* $271 = 19 \times 14 + 5$ *et* $0 \leq 5 < 19$ *donc* $q = 14$ *et* $r = 5$*.*
- $a = -271$ *et* $b = 19$*. On a* $271 = 19(-14) + (-5)$ *mais* -5 *est négatif* $-271 = 19(-15) + 14$ *avec* $0 \leq 14 < 19$ *donc* $q = 19$ *et* $r = 14$*.*

3.1.4 Décomposition en base b

Théorème 3.1.2 (Décomposition en base b)**.** *Soit* $b > 2$ *un entier. Tout entier* $a > 0$ *s'écrit de fa¸con unique sous la forme :*

$$a = a_0 + a_1 b + a_2 b^2 + ... + a_k b^k$$

où k *est un entier, les* a_i *sont des entiers compris entre 0 et* $b - 1$ *et où* $a_k \neq 0$*. On note parfois* $a = \overline{a_k a_{k-1} ... a_0}^b$*. Cette notation est l'écriture en base* b *de* a*.*

Démonstration. La méthode consiste à effectuer des divisions euclidiennes (par b) successives. On commence par écrire $a = bq_0 + a_0$ avec $a_0 \in \{0, 1, ..., b-1\}$. Si $q_0 = 0$, on a fini. Sinon, on continue nos divisions en écrivant $q_0 = bq_1 + a_1$ avec $a_1 \in \{0, 1, ..., b-1\}$. On a alors :

$$a = a_0 + a_1 b + q_1 b^2$$

De même si $q_1 = 0$, on a fini. Sinon on continue, construisant ainsi a_3, a_4 et ainsi de suite. On obtient successivement des égalités du type :

$$a = a_0 + a_1 b + ... + a_i b^i + q_i b^{i+1}.$$

La suite des q_i est une suite d'entiers positifs strictement décroissante. Elle doit donc s'arrêter, ce qu'ici ne peut être réalisé que si $q_i = 0$. A ce moment, on a bien la décomposition annoncée. Reste à prouver l'unicité. Supposons que l'on puisse écrire :

$$a_0 + a_1 b + ... + a_k b^k = a'_0 + a'_1 b + ... + a'_k b^k$$

pour des entiers a_i et a'_i compris entre 0 et $b - 1$. Alors $a_0 - a'_0$ est un multiple de b et $|a_0 - a'_0| < b$. D'où $a_0 = a'_0$. On simplifie alors par a_0, puis on divise par b. En appliquant le même argument que précédemment, on obtient $a_1 = a'_1$ et ainsi de suite. □

Remarque 3.1.3. *Dans le cas où* $b = 10$*, les* a_i *correspondent exactement aux chiffres usuels de a. On s'aperçoit que 10 ne joue pas un role particulier vis-à-vis de la représentation des nombres : par exemple, on aurait pu noter 143 au lieu de 80 si on avait décidé de compter en base 7.*

Exemple **3.1.3.** *Ecrire 1248 en base 3.*

1 2 4 8	3	4 1 6	3	1 3 8	3	4 6	3	1 5	3	5	3
0 4	4 1 6	1 1	1 3 8	1 8	4 6	1 6	1 5	1 5	5	2	1
1 8		2 6		0		1		0			
0		2									

Ce qui nous donne $1248 = \overline{1201020}^{3}$.

Exemple **3.1.4.** *Ecrire en base 10* $a = \overline{110100100}^{2}$.

$$a = 1\times 2^8 + 1\times 2^7 + 0\times 2^6 + 1\times 5^5 + 0\times 2^4 + 0\times 2^3 + 1\times 2^2 + 0\times 2^1 + 0\times 2^0 = 420$$

3.2 PGCD, Théorèmes d'Euclide et de Bézout

Définition **3.2.1** (PGCD, PPCM). *I) Le PGCD de a et b, noté* $a \wedge b$*, est :*

1) le plus grand des diviseurs communs à a *et* b *lorsque* $(a,b) \neq (0,0)$*,*

2) 0 lorsque $a = b = 0$*.*

II) Le PPCM de a et b, noté $a \vee b$*, est :*

1) le plus petit des multiples strictement positifs communs à a *et* b *lorsque* $ab \neq 0$*,*

2) 0 lorsque $a = 0$ *ou* $b = 0$*.*

Remarque **3.2.1.** — *Étant donnés deux entiers relatifs a et b, on a :*

$$a \wedge b = |a| \wedge |b|.$$

C'est pourquoi l'on supposera souvent par la suite que a et b sont des entiers naturels.

— *Par définition, on a, pour tout* $a \in \mathbb{Z}$ *:* $a \wedge 0 = |a|$.

— *Si* $a = b = 0$*, les diviseurs communs à* a *et* b *sont tous les entiers, et il n'en existe donc pas de plus grand pour la relation d'ordre* $\leq$.

— *Si* $ab = 0$*, seul 0 est un multiple commun à* a *et* b *et il n'existe donc pas de multiple strictement positif commun à* a *et* b.

Exemple **3.2.1.** *Déterminons PGCD(32, 12).*
Les ensembles des diviseurs positifs des entiers 12 et 32 sont $\mathcal{D}^+(12) = \{1,2,3,4,6,12\}$ *et* $\mathcal{D}^+(32) = \{1,2,4,8,16,32\}$*. On a*

$$\mathcal{D}^+(12) \cap \mathcal{D}^+(32) = \{1,2,4\}.$$

Donc, PGCD(32, 12) = 4.

Théorème 3.2.1 (Théorème d'Euclide). *Soient deux entiers $(a,b) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Effectuons la division euclidienne de l'entier a par l'entier b :*

$$\exists (q,r) \in \mathbb{N}^2 : \quad a = bq + r \quad et \quad 0 \leq r < b$$

Alors :

$$a \wedge b = b \wedge r.$$

Démonstration. Comme $r = a - bq$, tout entier divisant à la fois a et b divise aussi r. L'ensemble des diviseurs communs à a et b est égal à l'ensemble des diviseurs communs à b et r . En particulier, ces deux ensembles ont le même plus grand élément, ce qui s'écrit aussi : $a \wedge b = b \wedge r$. □

Remarque 3.2.2. *Le théorème précédent justifie l'algorithme d'Euclide pour trouver le PGCD de deux entiers non nuls $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$. On pose $r_0 = a$, $r_1 = b$ et on définit ensuite $\forall k \geq 1$, les couples (q_k, r_k) en utilisant une division euclidienne :*

$$si\ r_k \neq 0, \quad \exists ! (q_k, r_{k+1}) \in \mathbb{Z}^2 \ tel\ que\ r_{k-1} = q_k r_k + r_{k+1} \quad et \quad 0 \leq r_{k+1} < r_k.$$

Comme la suite d'entiers (r_k) est strictement décroissante, il existe un rang $n \geq 1$ tel que $r_n \neq 0$ et $r_{n+1} = 0$. D'après le théorème d'Euclide, on a $\forall k \in [0, n-1]$, $a \wedge b = rk \wedge r_{k+1}$. Comme r_n divise r_{n-1}, on a $r_n \wedge r_{n-1} = r_n$. Par conséquent, le dernier reste non-nul r_n est le PGCD des entiers (a,b).

Exemple 3.2.2. *Déterminons le pgcd des entiers 366 et 43 en utilisant l'algorithme d'Euclide :*

$$\begin{aligned} 366 &= 43 \times 8 + 22 \\ 43 &= 22 \times 1 + 21 \\ 22 &= 21 \times 1 + 1 \\ 21 &= 21 \times 1 + 0 \end{aligned}$$

donc $366 \wedge 43 = 1$.

Définition 3.2.2 (Nombres premiers entre eux). *On dit que deux nombres a et b sont premiers entre eux si et seulement si leur plus grand diviseur commun est 1, autrement dit si et seulement si*

$$a \wedge b = 1.$$

Théorème 3.2.2 (Coefficients de Bézout). *Soient deux entiers non nuls $(a,b) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Il existe $(u,v) \in \mathbb{Z}^2$ tels que*

$$au + bv = a \wedge b.$$

Un tel couple (u,v) est appelé couple de coefficients de Bézout de a et b.

Démonstration. Quitte à considérer $|a|$ et $|b|$ à la place de a et b, on peut supposer a et b positifs. La preuve se fait par récurrence sur b. Si $b = 0$, alors $a \wedge b = a$ et $1.a + 0.b = a$ donc un couple de coefficient de Bézout est $(1, 0)$. On fixe $b \in \mathbb{N}^*$ et on suppose que la propriété est vraie pour tout $a \in \mathbb{N}$ et tout nombre n de l'intervalle d'entiers $[[0, b-1]]$. Par division euclidienne, il existe $(q, r) \in \mathbb{N}^2$ tels que $a = bq+r$ et $0 \leq r \leq b-1$. D'après le théorème d'Euclide, on sait que $a \wedge b = b \wedge r$. On applique l'hypothèse de récurrence à b et r , il existe $(U, V) \in \mathbb{Z}^2$ tels que $Ub + Vr = b \wedge r$. Donc

$$Ub + V(a - bq) = a \wedge b \quad et \quad Va + (U - Vq)b = a \wedge b.$$

La propriété est alors prouvée par récurrence. □

Autre preuve. On considère l'ensemble $\{am + bn,\ (m, n) \in \mathbb{Z}^2\}$ qu'on note $a\mathbb{Z} + b\mathbb{Z}$. Il est clair que $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$, donc $\exists c \in \mathbb{N}$ tel que

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

Par ailleurs, $a\mathbb{Z} \subset d\mathbb{Z}$ et $b\mathbb{Z} \subset d\mathbb{Z}$ donc

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

En particulier c est un multiple de d et

$$c \geq d \tag{3.1}$$

L'égalité $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$ montre que c divise à la fois a et b, donc

$$c \leq PGCD(a, b) = d\ . \tag{3.2}$$

finalement on a $c = d$ en utilisant (3.1) et (3.2). □

Remarque 3.2.3. **1** *Il n'y a pas unicité du couple de coefficients de Bézout de deux entiers.*

2 *Les coefficients de Bézout s'obtiennent en " remontant " l'algorithme d'Euclide.*

Exemple 3.2.3. *Calculons les coefficients de Bézout pour $a = 600$ et $b = 124$. On a*

$$\begin{aligned} 600 &= 4 \times 124 + 104 \\ 124 &= 1 \times 104 + 20 \\ 104 &= 5 \times 20 + 4 \\ 20 &= 5 \times 4 + 0 \end{aligned}$$

Donc

$$\begin{aligned}
4 &= 104 - 5 \times 20 \\
4 &= 104 - 5 \times (124 - 1 \times 104) \qquad car \qquad 20 = 124 - 1 \times 104 \\
4 &= 6 \times 104 - 5 \times 124 \\
4 &= 6 \times (600 - 4 \times 124) - 5 \times 124 \qquad car \qquad 104 = 600 - 4 \times 124 \\
4 &= 6 \times 600 - 29 \times 124 \\
4 &= 6 \times 600 + (-29) \times 124
\end{aligned}$$

Ainsi pour $u = 6$ *et* $v = -29$*, on a* $600u + 124v = 4 = 600 \wedge 124$.

Théorème 3.2.3 (Théorème de Bézout)**.** *Soient deux entiers non nuls* $(a, b) \in (Z^*)^2$*. On a*

$$a \wedge b = 1 \Leftrightarrow [\exists (u, v) \in \mathbb{Z}^2 : \quad 1 = au + bv].$$

Démonstration. ($\Rightarrow$) C'est une conséquence directe du théorème précédent.
($\Leftarrow$) Supposons qu'il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. Si d est un diviseur commun à a et b alors d est un diviseur de 1. Il est alors clair que $a \wedge b = 1$. □

Théorème 3.2.4 (Théorème de Gauss)**.** *Soient trois entiers non nuls* $(a, b, c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}^*$.

$$[a|bc \qquad et \qquad a \wedge b = 1] \Rightarrow a|c.$$

Démonstration. Si $a \wedge b = 1$ alors, d'après le théorème de Bézout 3.2.3, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. On a donc aussi $auc + bvc = c$. Mais comme a divise bc et que a divise auc, a divise $auc + bvc = c$. □

Proposition 3.2.1 (Caractérisation des diviseurs et des multiples)**.** *Soient deux entiers* $(a, b) \in \mathbb{Z}^2$.

1 *Soit un entier* $d \in \mathbb{Z}$. $\begin{cases} d|a \\ d|b \end{cases} \Leftrightarrow d|(a \wedge b)$.

2 *soit un entier* $m \in \mathbb{Z}$. $\begin{cases} a|m \\ b|m \end{cases} \Leftrightarrow (a \vee b)|m$.

Démonstration.

1 Supposons que que d divise a et b et notons $d = a \wedge b$. D'après le théorème 3.2.2, il existe $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = d$.
Comme $d|a$ et que $d|b$, on sait que $d|d$. La réciproque est facile.

2 Supposons que a et b divisent m et notons $\mu = a \vee b$. Il existe $k, k' \in \mathbb{N}$ tels que $\mu = ka$ et $\mu = k'b$. Il existe aussi $l, l' \in \mathbb{N}$ tels que $m = la$ et $m = l'b$. De plus, par application du théorème 3.1.1, il existe un unique couple $(p, r) \in \mathbb{N}^2$ tel que

$m = p\mu + r$ et $0 \leq r < \mu$. On peut alors écrire $la = pka + r$ et $l'b = pk'b + r$ et donc $a|r$ et $b|r$. Si $r \neq 0$ alors r est un multiple commun à a et b. Par définition de μ, il vient $r \geq \mu$ ce qui est impossible. Donc $r = 0$ et μ divise m. La réciproque est évidente.

□

Proposition 3.2.2. *Soient deux entiers non nuls $(a, b) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Pour un entier $k \in \mathbb{N}^*$,*

$$(ka) \wedge (kb) = k(a \wedge b) \qquad et \qquad (ka) \vee (kb) = k(a \vee b).$$

Démonstration. — Posons $d = a \wedge b$ et $\delta = ka \wedge kb$. Il est clair que $kd|\delta$. Montrons que $\delta|kd$, ce qui prouvera la première égalité. Comme $k|\delta$ il existe $m \in \mathbb{Z}$ tel que $\delta = km$. Mais alors $km|ka$ et $m|a$. De même, $km|kb$ et donc $m|b$. L'entier m est donc un diviseur de d et $\delta = km|kd$.

— Posons maintenant $d = a \vee b$ et $D = ka \vee kb$. L'entier kd est un multiple de ka et kb donc $D|kd$. Si on montre de plus que $kd|D$ alors la seconde égalité sera prouvée. Comme $ka|D$ et que $kb|D$, il existe des entiers m_1 et m_2 tels que $D = kam_1 = kbm_2$. L'entier k est donc un diviseur de D et il existe un entier D' tel que $D = kD'$. Par suite, on a $D' = am_1 = bm_2$ et D' est donc un multiple commun à a et b ce qui amène $d|D'$ ainsi que $kd|D$.

□

Proposition 3.2.3 (Autres propriétés du PGCD)**.** *Soient trois entiers relatifs non nuls a, b et c.*

1 *Soient trois entiers $(d, a', b') \in \mathbb{N}^* \times \mathbb{Z}^2$ tels que $a = da'$, $b = db'$, alors*

$$d = a \wedge b \Leftrightarrow a' \wedge b' = 1.$$

2 $\begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases} \Leftrightarrow a \wedge (bc) = 1.$

3 $\begin{cases} a|c \\ b|c \\ a \wedge b = 1 \end{cases} \Rightarrow ab|c.$

4 *pour tout couple $(p, q) \in \mathbb{Z}^* \times \mathbb{Z}^*$, si $a \wedge b = 1$, alors $ap \wedge bq = 1$;*

5 *pour tout entier $k \in \mathbb{N}*$, $ak \wedge bk = (a \wedge b)k$.*

Démonstration. **1** C'est une conséquence directe de la proposition 3.2.1.

2 ($\Rightarrow$) Si $a \wedge b = 1$ et $a \wedge c = 1$, alors par application du théorème de Bézout 3.2.3, il existe des entiers s, t, u, v tels que $sa + tb = 1$ et $ua + vc = 1$. Si on multiplie membre à membre ces deux égalités, on obtient l'égalité de Bézout :

$(sua + vsc + tub)a + (tvc)b = 1$ et en conclusion $a \wedge (bc) = 1$.

($\Leftarrow$) Réciproquement, si $a \wedge (bc) = 1$ alors il est clair que a est premier à la fois avec b et c.

3 Comme $a|c$, il existe $k \in \mathbb{Z}$ tel que $c = ka$. Mais comme $b|c = ka$ et que $a \wedge b = 1$ alors par le Théorème de Gauss 3.2.4, il vient que $b|k$. En conclusion $ab|c$.

4 Considérons $A, B \in \mathbb{N}^*$ tels que $A \wedge B = 1$ et $m \in \mathbb{N}*$. Si on applique la deuxième règle avec $a = A$, $b = B$ et $c = B$, on obtient : $A \wedge B^2 = 1$. En l'appliquant une nouvelle fois avec $a = A$, $b = B$ et $c = B^2$, il vient que $A \wedge B^3 = 1$. Si on l'applique encore $m - 3$ fois, il vient que : $A \wedge B^m = 1$. En résumé, on a prouvé que si $A \wedge B = 1$ alors $A \wedge B^m = 1$. Considérons $a, b \in \mathbb{N}^*$ tels que $a \wedge b = 1$ et $p, q \in \mathbb{N}^*$. On applique ce résultat à $A = a$, $B = b$ et $m = q$. Il vient $a \wedge bq = 1$. On l'applique alors une nouvelle fois mais à $A = bq$, $B = a$ et $m = p$ et on trouve $ap \wedge bq = 1$.

5 Soit $k \in \mathbb{N}^*$. Posons $d = a \wedge b$. Grâce à la première règle, on a $\frac{a}{d} \wedge \frac{b}{d} = 1$ et grâce à la quatrième a $\left(\frac{a}{d}\right)^k \wedge \left(\frac{b}{d}\right)^k = 1$. En appliquant à nouveau la première règle, il vient que : $a^k \wedge b^k = dk = (a \wedge b)^k$.

□

Théorème 3.2.5 (Relation entre PGCD et PPCM). *Soient deux entiers non nuls* $(a, b) \in \mathbb{Z}^* \times \mathbb{Z}^*$.

1 *Si* $a \wedge b = 1$ *alors* $a \vee b = |ab|$;

2 $(a \wedge b)(a \vee b) = |ab|$.

Démonstration. **1** Supposons que a et b sont positifs et premiers entre eux. Soit d un multiple commun à a et b. Alors il existe $k \in \mathbb{N}$ tels que $d = ka$. Comme $b|d$ et que $a \wedge b = 1$, on en déduit, grâce au théorème de Gauss 3.2.4, que $b|k$ et qu'il existe donc $k' \in \mathbb{N}$ tel que $d = k'ab$. Comme d est le plus petit commun multiple de a et b, il vient forcément que $k' = 1$ et que $d = ab$. Si a et b ne sont pas tous deux positifs, on applique ce résultat à $|a|$ et $|b|$.

2 Notons $d = a \wedge b$ et $a = da'$, $b = db'$ avec $a', b' \in \mathbb{Z}$. Montrons que l'ensemble des multiples communs à a et b est l'ensemble des multiples de $da'b'$. Il est clair que tout multiple de $da'b'$ est un multiple commun à a et b. Réciproquement, si m est un multiple commun à a et b alors il existe $k, k' \in \mathbb{Z}$ tels que $m = ka = k'b$. On a aussi $m = kda' = k'db'$. Comme a' et b' sont premiers entre eux, cette égalité implique, par application du théorème de Gauss 3.2.4 que $b'|k$. Donc m est un multiple de $da'b'$. Il s'ensuit que le ppcm de a et b est le plus petit multiple de

$da'b'$, c'est à dire que $a \vee b = |da'b'|$. Il vient alors $d(a \vee b) = d|da'b'| = |ab|$ d'où l'égalité.

□

Proposition **3.2.4.** *Soient $m, n \in \mathbb{Z}$ et $p \in \mathbb{Z}$.*

$$p = PPCM(m,n) \Leftrightarrow m\mathbb{Z} \cap n\mathbb{Z} = p\mathbb{Z}.$$

Proposition **3.2.5.** *$m, n \in \mathbb{Z}$ et $d \in \mathbb{Z}$.*

$$d = PGCD(m,n) \Leftrightarrow m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}.$$

Exercice 4. *Démontrer que si 2 nombres sont premiers entre eux, il en est de même de leur somme et de leur produit Puis résoudre dans $\mathbb{N}^* \times \mathbb{N}^*$ le système : $x + y = 56$ et $PPCM(x,y) = 105$*

3.3 Congruences

3.3.1 Définition - propriétés

Définition **3.3.1.** *Soit n un entier naturel non nul, a et b deux entiers relatifs . On dit que a est congru à b modulo n si $a - b$ est un multiple de n ; et on écrit*

$$a \equiv b[n] \qquad ou \qquad a \equiv b\ (mod\ n).$$

Si r désigne le reste de la division euclidienne de a par n alors $a \equiv r[n]$.

Exemples **3.3.1.**

$$15 \equiv 1[7], \quad 142 \equiv 2[7], \quad 3 \equiv -11[7], \quad 3 \equiv -4[7], \quad 2013 \equiv 3[10], \quad -13 \equiv 5[6]$$

Proposition **3.3.1.** *Soient a et b deux entiers, et n et m des entiers naturels non nuls.*

1. $a \equiv a[n]$ *(réflexivité).*
2. $a \equiv b[n] \Leftrightarrow b \equiv a[n]$ *(symétrie).*
3. *Si $a \equiv b[n]$ et $b \equiv c[n]$, alors $a \equiv c[n]$ (transitivité).*
4. *Si $a \equiv b[n]$ et si $m|n$, alors $a \equiv b[m]$.*

Démonstration. **1** On a $a - a = 0$. Or $n|0$, d'où $a \equiv a[n]$.

2 $a \equiv b(modn) \Leftrightarrow n|(b-a) \Leftrightarrow n|(a-b) \Leftrightarrow b \equiv a(modn)$.

3 Si $a \equiv b[n]$ et $b \equiv c[n]$, alors $n|(b-a)$ et $n|(c-b)$ donc $n|((b-a)+(c-b))$, c'est-à-dire $n|(c-a)$, d'où $a \equiv c[n]$.

4 Si $m|n$, alors il existe un entier k tel que $n = km$, et si $a \equiv b[n]$, alors il existe un entier k' tel que $b - a = k'n$. On a donc $b - a = k'km$, c'est-à-dire $m|(b - a)$, d'où $a \equiv b[m]$.

□

Proposition 3.3.2. *Soit n un entier naturel non nul et a, a', b, b' quatre entiers relatifs.*

1 *Si $a \equiv a'[n]$ et $b \equiv b'[n]$ alors $a + b \equiv a' + b'[n]$.*

2 *Si $a \equiv a'[n]$ et $b \equiv b'[n]$ alors $a \times b \equiv a' \times b'[n]$.*

3 *si $a \equiv b[n]$ alors $a^k \equiv b^k[n]$ $\quad k \in \mathbb{N}$.*

Démonstration. **1** Si $a \equiv b[n]$ et $c \equiv d[n]$, alors il existe deux entiers α et β tels que $b-a = \alpha n$ et $d-c = \beta n$. On a donc $(b+d)-(a+c) = (b-a)+(d-c) = (\alpha+\beta)n$, d'où $a + c \equiv b + d[n]$.

2 Si $a \equiv b[n]$ et $c \equiv d[n]$, alors il existe deux entiers α et β tels que $b - a = \alpha n$ et $d - c = \beta n$. On a donc $bd - ac = (a + \alpha n)(c + \beta n) - ac = (\alpha c + \beta a + a\beta n)n$, d'où $ac \equiv bd[n]$.

3 On utilise le 2. pour la preuve.

□

Exemple 3.3.1. *Montrons que $\forall x \in \mathbb{Z}$, $(5x + 8)^2 \equiv 4[5]$.*
On a $8 \equiv 3[5]$ et $3^2 \equiv 4[5]$. On a aussi $5 \equiv 0[5]$ donc $5x \equiv 0x[5]$. Par suite $5x + 8 \equiv 3[5]$ et $(5x + 8)^2 \equiv 3^2[5]$, ce qui donne $(5x + 8)^2 \equiv 4[5]$.

Théorème 3.3.1. *Soit n un entier naturel non nul, a et a' deux entiers relatifs, r et r' les restes respectifs des divisions euclidiennes de a et a' par n.*

$$a \equiv a'[n] \Leftrightarrow r = r'$$

Démonstration. $(\Rightarrow)$ Supposons $a \equiv a'[n]$. Il existe un entier k tel que $a' - a = kn$. Il existe deux entiers q et r tels que $a = nq+r$ avec $0 \leq r < n$. On a donc $a' = n(q+k)+r$, toujours avec $0 \leq r < n$, ce qui montre que $r = r'$.

$(\Leftarrow)$ Supposons que $r = r'$. Il existe des entiers q et q' tels que $a = nq + r$ et $a' = nq' + r$. Par suite $a' - a = n(q' - q)$, c'est-à-dire $a \equiv a'[n]$. □

Théorème 3.3.2. *Soit $N > 1$ un entier et c un entier premier avec N. Alors il existe un entier c' tel que $cc' \equiv 1[n]$. Un tel entier c' est appelé un* ***inverse de*** *c* ***modulo*** *N.*

Démonstration. Il s'agit d'une simple application du théorème de Bézout. Comme N et c sont premiers entre eux, on peut écrire une égalité du type $uN + vc = 1$. On voit directement que l'entier $c' = v$ convient pour le théorème. On remarque également que l'algorithme d'Euclide étendu donne un moyen effectif pour calculer l'inverse de c modulo N. □

Exercice 5. *1) Démontrer que* $2 \times 35^{2002} - 3 \times 84^{2003} \equiv 5[17]$.

2) Quel est le reste de la division de 5^n *par 13.*

3) Déterminer suivant les valeurs de n le reste de la division de 3^n *par 7 et déterminer le reste de la division par 7 du nombre* $A = 2243^{325} + 1179^{154}$

4) Montrer que 11 divise 2123 + 3121 .

3.3.2 Équations diophantiennes

a) Définition - exemples

Définition 3.3.2. *On appelle équation diophantienne toute équation dont on cherche les solutions en nombres entiers.*

Exemples 3.3.2. **1** *Résoudre dans* $\mathbb{Z}^2$, $ax + by = d$ *avec* $(a, b, c) \in \mathbb{R}^3$.

2 *Résoudre dans* $\mathbb{Z}^3$, $x^2 + y^2 = z^2$ *avec* $(a, b, c) \in \mathbb{R}^3$.

3 *Résoudre dans* $\mathbb{Z}$, $x^2 = 4k + 3$.

b) L'équation $ax + by = c$

Proposition 3.3.3.

Considérons l'équation

$$ax + by = c \tag{3.3}$$

où $a, b, c \in \mathbb{Z}$. Soit $d = PGCD(a, b)$

1 L'équation (3.3) possède des solutions $(x, y) \in \mathbb{Z}^2$ si et seulement si $d|c$.

2 Si $d|c$ alors il existe même une infinité de solutions entières et elles sont exactement les

$$(x, y) = (x_0 + ak, y_0 + bk)$$

avec $x_0, y_0, a, b \in \mathbb{Z}$ fixés et k parcourant $\mathbb{Z}$.

Démonstration. **1** $(\Rightarrow)$ Supposons que $d|c$. Soit (u, v) le couple de coefficients de Bézout de a et b. On a alors $d|cu$ et $d|cv$ c'est-à-dire $cu = \alpha d$ et $cv = \beta d$ avec $\alpha, \beta \in \mathbb{Z}$. En posant $x_0 = \alpha$ et $y_0 = \beta$ on a

$$ax_0 + by_0 = \frac{acu}{d} + \frac{bcv}{d} = \frac{c}{d}(au + bv) = \frac{c}{d}d = c.$$

Donc (x_0, y_0) est solution de (3.3).
$(\Leftarrow)$ Supposons que possède au moins une solution $(x_0, y_0) \in \mathbb{Z}^2$.

a Si $c = 0$, alors $(x_0, y_0) = (0, 0)$ est solution de (3.3).

b Si $c \neq 0$. D'après le Théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = d$. Comme $d|a$ et $d|b$, on obtient que $d|(ax_0 + by_0)$, d'où $d|c$.

2 Posons $a = a'd$, $b = b'd$ et $c = c'd$. Un couple d'entier (x, y) est une solution de $ax + by = c$ si et seulement si c'est une solution de $a'x + b'y = c'$. Une solution est donc donnée par $(c'x_0, c'y_0)$. Soit (x_1, y_1) une autre solution. Alors :

$$a'x_1 - a'c'x_0 = b'c'y_0 - b'y_1.$$

Soit encore :

$$a'(x_1 - c'x_0) = b'(c'y_0 - y_1).$$

Donc a' divise $b'(c'y_0 - y_1)$. Comme $a' \wedge b' = 1$, $a' divise c'y_0 - y_1$. Il existe donc $k \in \mathbb{Z}$ tel que $y_1 = c'y_0 - ka0$. Mais alors $(x_1 - c'x_0) = kb'$. Finalement, $x_1 = c'x_0 + kb'$ et $y_1 = c'y_0 - ka'$. Réciproquement, le couple $(x_1, y_1) = (c'x_0 + kb', c'y_0 - ka')$ avec k entier est bien une solution de (3.3).

□

Exemple **3.3.2.** *Trouver les solutions entières de*

$$161x + 368y = 115 \tag{3.4}$$

• ***Première étape.*** Y a-t-il des solutions ? *L'algorithme d'Euclide. On effectue l'algorithme d'Euclide pour calculer le PGCDde* $a = 161$ *et* $b = 368$.

$$\begin{aligned} 368 &= 161 \times 2 + 46 \\ 161 &= 46 \times 3 + 23 \\ 46 &= 23 \times 2 + 0 \end{aligned}$$

Donc $368 \wedge 161 = 23$. *Comme* $115 = 5 \times 23$ *alors* $(368 \wedge 161)|115$. *Par le Théorème de Bézout, l'équation (3.4) admet des solutions entières.*

• ***Deuxième étape.*** Trouver une solution particulière *: la remontée de l'algorithme d'Euclide. On effectue la remontée de l'algorithme d'Euclide pour calculer les coefficients de Bézout.*

$$\begin{aligned} 23 &= 161 - 3 \times 46 \\ 23 &= 161 - 3 \times (368 - 161 \times 2) \qquad car \qquad 46 = 368 - 161 \times 2 \\ 23 &= 161 \times 7 - 368 \times 3 \end{aligned}$$

On trouve donc $161 \times 7 + 368 \times (-3) = 23$. *Comme* $115 = 5 \times 23$ *en multipliant par* 5 *on obtient :* $161 \times 35 + 368 \times (-15) = 115$.

Ainsi $(x_0, y_0) = (35, -15)$ *est une solution particulière de (3.4).*

• ***Troisième étape.*** Recherche de toutes les solutions. *Soit* $(x, y) \in \mathbb{Z}^2$ *une solution de (3.4). Nous savons que* (x_0, y_0) *est aussi solution. Ainsi :*

$$161x + 368y = 115 \qquad et \qquad 161x_0 + 368y_0 = 115.$$

La différence de ces deux égalités conduit à

$$\begin{aligned} 161 \times (x - x_0) + 368 \times (y - y_0) = 0 \quad &\Rightarrow \quad 23 \times 7 \times (x - x_0) + 23 \times 16 \times (y - y_0) = 0 \\ &\Rightarrow \quad 7(x - x_0) = -16(y - y_0). \end{aligned} \tag{3.5}$$

Nous avons simplifié par 23 qui est le pgcd de 161 et 368. (Attention, n'oubliez surtout pas cette simplification, sinon la suite du raisonnement serait fausse.) Ainsi $7|16(y - y_0)$, *or* $PGCD(7, 16) = 1$ *donc par le Théorème de Gauss 3.2.4* $7|y - y_0$. *Il existe donc* $k \in \mathbb{Z}$ *tel que* $y - y_0 = 7 \times k$. *Repartant de l'équation (3.5) :* $7(x - x_0) = -16(y - y_0)$. *On obtient maintenant* $7(x - x_0) = -16 \times 7 \times k$. *D'où* $x - x_0 = -16k$. *(C'est le même* k *pour* x *et pour* y.*) Nous avons donc* $(x, y) = (x_0 - 16k, y_0 + 7k)$. *Il n'est pas dur de voir que tout couple de cette forme est solution de l'équation (3.4). Il reste donc juste à substituer* (x_0, y_0) *par sa valeur et nous obtenons : Les solutions entières de* $161x + 368y = 115$ *sont les* $(x, y) = (35 - 16k, -15 + 7k)$, k *parcourant* $\mathbb{Z}$.

Exercice 6. *Soit* (E) *l'équation* $6x + 7y = 57$.

1. *Déterminer un couple d'entiers relatifs* $(u\,;v)$ *tel que* $6u + 7v = 1$*puis en déduire une solution particulière de* (E).
2. *Résoudre* (E).

c) Résolution de certaines formes d' équations diophantiennes

Quelques réflexes

Les propriétés des entiers et les notions de divisibilité sont essentielles dans la résolution des équations diophantiennes. Rappelons tout de suite quelques propriétés qu'il est bon d'avoir constamment en tête :

Quelques idées à tester systématiquement

- ♣ Si le produit ab est une puissance d'un nombre premier p, alors a et b sont également des puissances de ce nombre premier. Si le produit ab est une puissance d'un entier n, il peut être intéressant de décomposer n en facteurs premiers.
- ♣ Si le produit ab est un carré et que a et b sont premiers entre eux, alors a et b sont des carrés. Plus généralement si $d = pgcd(a, b)$, a s'écrit dx^2 et b s'écrit dy^2 pour des entiers x et y. Rappelons à ce niveau que le PGCD de deux entiers dont

la différence est n est un diviseur de n. En particulier, cette propriété est forte utile pour les situations faisant intervenir des produits $a(a+n)$ ou plus souvent $(a-n)(a+n) = a^2 - n^2$.

- ♣ Un entier strictement positif est supérieur ou égal à 1. De même, si n est entier et $n \leq x$, alors $n \leq [x]$ où $[x]$ est la partie entière de x. Un bon reflexe à avoir à ce niveau est de ne jamais (ou du moins le plus rarement possible) conserver des inégalités strictes entre nombres entiers : elles peuvent toujours être améliorées.
- ♣ On dispose de la factorisation :

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + ... + b^{n-1}).$$

et si n est impair, de la factorisation analogue :

$$a^n + b^n = (a+b)(a^{n-1} + a^{n-2}b + ... + b^{n-1}).$$

Ces factorisations s'avèrent très utiles lorsque l'on a besoin de modifier l'aspect d'une équation diophantienne, le plus souvent en faisant des manipulations algébriques. Signalons également que toute expression de la forme $\alpha x + \beta y + \gamma xy + \delta$ peut en général se factoriser sous la forme :

$$(ax+b)(cx+d) + e$$

pour certains rationnels (pas forcément entiers même si α, β, γ et δ le sont) a, b, c, d et e.

Quelques exemples

Exemple 3.3.3. *Résoudre dans $\mathbb{Z}$,*

$$2^n + 1 = x^2.$$

Solution. On fait passer le 1 de l'autre côté de l'égalité et on factorise :

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

et donc d'après une des propriétés rappelées précédemment, à la fois $x+1$ et $x-1$ doivent être des puissances de 2. Or, des puissances de 2 dont la diffèrence est égale à 2, il n'y a que 2 et 4. Donc $x = 3$ est la seule solution, et fournit $n = 3$. □

Cet exemple illustre de façon parfaite le fait mentionné précédemment stipulant qu'il peut parfois être intéressant de faire des manipulations algébriques simples sur l'équation pour lui donner un aspect plus propice à sa résolution. Souvent savoir factoriser un

membre de l'égalité s'avère déterminant.

Lorsque seulement deux valeurs interviennent, un premier pas éclairant consiste souvent à comparer les ordres de grandeur de ces valeurs.

Exemple **3.3.4.** *Résoudre dans $\mathbb{Z}^2$, l'équation :*

$$x^2 = 2 + 6y^2 + y^4.$$

Solution. Sans trop réfléchir, on voit que si cette équation admet une solution, x doit être de l'ordre de y^2 et même plus précisément l'écriture suivante :

$$x^2 = (y^2 + 3)^2 - 7$$

nous dit que x ne doit pas être loin de $y^2 + 3$. Précisément en fait, on a $x < y^2 + 3$. On a également :

$$x^2 = (y^2 + 2)^2 + 2y^2 - 2$$

et donc dès que $2y^2 - 2 > 0$, on doit avoir $x > y^2 + 2$. Comme il n'y a pas d'entiers entre $y^2 + 2$ et $y^2 + 3$ l'équation n'admet pas de solution. Les seules solutions éventuelles seraient alors obtenues pour les y tels que $2y^2 - 1 > 0$, c'est-à-dire $y = -1$, $y = 0$ et $y = 1$. On vérifie ensuite au cas par cas. □

La morale est que lorsque l'équation a un petit nombre d'inconnues, des techniques d'inégalité, peuvent permettre de restreindre l'étude à un nombre fini de cas. Lorsque l'exercice est bien fait, ce nombre est petit, et on peut donc traiter ces cas un par un.

Exemple **3.3.5.** *Trouver tous les entiers positifs n tel que $3n + 7$ divise $5n + 13$.*

Solution. Le quotient $\dfrac{5n + 13}{3n + 7}$ est toujours compris strictement entre 0 et 2 et donc, comme il est entier, il ne peut en fait valoir que 1. Il ne reste alors plus qu'à résoudre l'équation $5n + 13 = 3n + 7$ qui admet pour solution $n = -3$. Ce nombre n'est pas positif, donc il n'existe aucun n répondant à notre question. □

Remarquons que l'utilisation d'inégalités peut s'avérer efficace même si le nombre d'inconnues est plus important. Pour exemple, nous donnons l'exercice suivant :

Exemple **3.3.6.** *Trouver tous les entiers strictement positifs x, y et z tels que :*

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1.$$

Solution. Comme les inconnues jouent un role symétrique, on peut supposer $0 < x \leq y \leq z$. Dans ces conditions, on a :

$$1 = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} \leq \frac{3}{x}$$

et donc $x \leq 3$. Il ne peut valoir 1, il vaut donc 2 ou 3. On traite les deux cas séparemment en utilisant à nouveau la même méthode. Si $x = 2$, l'équation devient :

$$\frac{1}{y} + \frac{1}{z} = \frac{1}{2}$$

puis par le même argument $x = 2 \leq y \leq 4$. On teste alors les cas un par un trouve que les seules solutions sont $y = 3$, $z = 6$ et $y = 4$, $z = 4$. Pour $x = 3$, on obtient :

$$\frac{1}{y} + \frac{1}{z} = \frac{2}{3}$$

puis $x = 3 \leq y \leq 3$. La seule solution est, dans ce cas, $x = y = 3$.
Finalement, les solutions sont les triplets (2, 3, 6), (2, 4, 4), (3, 3, 3) et toutes leurs permutations. □

Confrontés à une équation, on peut également se demander s'il n'y a pas une manipulation simple qui permet de transformer une solution en une autre. Par exemple, il est possible qu'en multipliant tous les entiers d'une solution par une même valeur d, on obtienne une nouvelle solution. On dit souvent alors que l'équation est homogène. Ce cas se produit par exemple lorsque l'équation proposée est une somme de monomes, tous de même degré. Souvent la solution obtenue ainsi est « plus grande ». Cependant cela peut-être encore plus intéressant si elle se trouve " plus petite".

Ces manipulations permettent par exemple de faire des hypothèses supplémentaires sur une solution recherchée. Par exemple, dans le cas « homogène » présenté précédemment, on peut supposer que les inconnues sont premières entre elles dans leur ensemble. Ces solutions sont souvent appelées fondamentales. Les autres solutions (différentes de (0, 0, . . . , 0) qui convient toujours dans ce cas) s'obtiennent alors par multiplication à partir d'une solution fondamentale. Ainsi, si on trouve toutes les solutions fondamentales, on aura trouvé toutes les solutions.

Cette dernière remarque est par exemple appliquée dans la preuve usuelle de l'irrationnalité de $\sqrt{2}$. On se ramène directement à montrer que l'équation diophantienne :

$$a^2 = 2b^2$$

n'a pas de solution non nulle. On remarque que l'équation est homogène et il suffit donc de chercher les solutions avec $PGCD(a, b) = 1$. On remarque ensuite que a^2 est pair,

donc a doit être pair. Ceci implique que a^2 est un multiple de 4, et donc b^2 est pair. Ainsi b est pair, et il n'y a pas de solution avec a et b premiers entre eux.

La remarque sur l'homogénéité implique alors qu'il n'y a aucune solution hormis la solution triviale $a = b = 0$. Cela démontre l'irrationnalité de $\sqrt{2}$.

Noter que parfois, la manière dont on transforme une solution en une autre est moins évidente. Par exemple, pour l'équation suivante :

$$x^3 + y^5 = z^2$$

il faut remarquer que si (x, y, z) est solution et si α est un entier quelconque, alors le triplet $(\alpha^{10}x, \alpha^6 y, \alpha^{15}z)$ est aussi solution. Si l'on demande ensuite simplement de prouver que cette équation admet une infinité de solutions, on conclut en remarquant que (2, 1, 3) est solution. On a ainsi prouvé que pour tout entier a, le triplet $(2\alpha^{10}, \alpha^6, 3\alpha^{15})$ est solution, ce qui en fait bien une infinité.

De façon plus générale, lorsque l'on souhaite prouver que telle équation admet une infinité de solutions, il s'agit souvent de trouver une formule. L'exemple de l'équation :

$$x^3 + y^3 + z^3 + t^3 = 3$$

est frappant. Pour conclure, il suffit de sortir de son chapeau l'identité :

$$(4 + 24n^3)^3 + (4 - 24n^3)^3 + (-24n^2)^3 + (-5)^3 = 3.$$

On pourrait objecter qu'on ne voit pas trop comment on peut arriver à une telle formule. En réalité, si l'on sait ce que l'on cherche, à force de patience et avec un peu de pratique, on arrive assez bien à bricoler des coefficients qui conviennent.

3.3.3 Théorème chinois

Le théorème chinois s'énonce comme suit :

Théorème **3.3.3** (Théorème chinois)**.** *Soient $N_1,\ N_2,\ \ldots\ ,\ N_k$ des entiers strictement positifs deux à deux premiers entre eux, et $a_1,\ a_2,\ \ldots\ ,\ a_k$ des entiers quelconques. Alors il existe un entier a tel que le système de congruences :*

$$\begin{cases} x & \equiv & a_1[N_1] \\ x & \equiv & a_2[N_2] \\ & . & \\ & . & \\ & . & \\ x & \equiv & a_k[N_k] \end{cases}$$

soit équivalent à la simple congruence $x \equiv a[N_1 N_2 ... N_k]$.
En particulier, le système précédent possède au moins une solution.

Démonstration. On remarque dans un premier temps qu'il suffit de prouver le théorème lorsque $k = 2$. Une récurrence directe permettra ensuite de l'avoir dans toute sa généralité. On cherche à résoudre le système $\begin{cases} x & \equiv & a_1[N_1] \\ x & \equiv & a_2[N_2] \end{cases}$.
La première condition assure l'existence d'un entier q tel que $x = a_1 + qN_1$ et la seconde congruence s'écrit alors :

$$a_1 + N_1 q \equiv a_2[N_2]$$

ce qui fournit :

$$q \equiv (a_2 - a_1)N_1'[N_2]$$

où N_1' désigne un inverse de N_1 modulo N_2 qui existe bien car N_1 et N_2 sont supposés premiers entre eux. Ainsi si l'on pose

$$a = a_1 + (a_2 - a_1)N_1'N_1, \tag{3.6}$$

on obtient $x \equiv a[N_1N_2]$. La réciproque est immédiate. □

Exemple **3.3.7.** *Résolvons dans $\mathbb{Z}$ le système :*

$$\begin{cases} x & \equiv & 2[10] \\ x & \equiv & 5[13] \end{cases}. \tag{3.7}$$

Déterminons $10 \wedge 13$

$$\begin{aligned} 13 &= 1 \times 10 + 3 \\ 10 &= 3 \times 3 + 1 \\ 3 &= 3 \times 1 + 0 \end{aligned}$$

donc $10 \wedge 13 = 1$. *D'après le Théorème chinois 3.3.3,*

$$(3.7) \Leftrightarrow x \equiv a[130]$$

avec $a = 2+10(5-2)N_1'$ *et* $10N_1' \equiv 1[13]$. *On peut déterminer N_1' à partir des coefficients de Bézout de 10 et 13. On a*

$$\begin{aligned} 1 &= 10 - 3 \times 3 \\ 1 &= 10 - 3 \times (13 - 1 \times 10) \qquad car \qquad 3 = 13 - 1 \times 10 \\ 1 &= 4 \times 10 - 3 \times 13 \end{aligned}$$

On peut donc prendre $N_1' = 4$, *ce qui nous donne* $a = 122$. *Par suite,*

$$(3.7) \Leftrightarrow x = 122 + 130k \quad avec \quad k \in \mathbb{Z}.$$

Autre méthode :

Déterminons une solution particulière : $x = 2 + 10k = 5 + 13k'$ *avec* $k, k' \in \mathbb{Z}$. $10k - 13k' = 3$. *Cherchons* $u, v \in \mathbb{Z}$ *tel que* $10u + 13v = 1$. $u = 4$ *et* $v = -3$ *conviennent. Prenons* $k = 12$, $k' = 9$ *ce qui donne* $x = 122$.

Soit x une autre solution. On a $\begin{cases} x \equiv 122[10] \\ x \equiv 122[13] \end{cases}$ *donc* $10|x - 122$ *et* $13|x - 122$, *ce qui donne* $130|x - 122$ *et par suite* $x = 122 + 130k$ *avec* $k \in \mathbb{Z}$.

Inversement si $x = 122 + 130k$ *avec* $k \in \mathbb{Z}$, *on a*
$122 \equiv 2[10]$ *et* $130 \equiv 0[10]$ *donc* $x \equiv 2[10]$. $122 \equiv 5[13]$ *et* $130 \equiv 0[13]$ *donc* $x \equiv 2[13]$.
Par suite, $\begin{cases} x \equiv 2[10] \\ x \equiv 5[13] \end{cases}$

3.4 Nombres premiers

3.4.1 Nombres premiers

Définition 3.4.1 (Nombre premier, nombre composé)**.** *Un entier* $n \in \mathbb{N}$ *est dit premier si* $n \geq 2$ *et si ses seuls diviseurs dans* $\mathbb{N}$, *sont 1 ou lui-même :*

$$\forall k \in \mathbb{N}^*, \quad k|n \ \Rightarrow \ k \in \{1, n\}.$$

On note $\mathbb{P}$ *l'ensemble des nombres premiers.*
Si un entier $n \in \mathbb{N}$ *n'est pas premier, on dit qu'il est composé.*

Proposition 3.4.1. *Soit* $n > 1$ *un entier. Son plus petit diviseur* $d > 1$ *est un nombre premier. Si de plus* n *est composé, alors* $d \leq \sqrt{n}$.

Démonstration. Supposons que d ne soit pas premier. Alors par définition, il existe un diviseur $d' \in \{2, ..., d-1\}$ de d. Donc d' divise n, $d' > 1$ et $d' < d$, ce qui contredit la minimalité de d.
Comme d divise n, on peut écrire $n = dd'$. On a $d > 1$ et comme n n'est pas premier, $d < n$. Ainsi d' est un diviseur de n strictement supérieur à 1. Par minimalité de d, on obtient $d' \geq d$ et donc $n \geq d^2$ puis finalement $d \leq \sqrt{n}$. □

Remarque 3.4.1. *On déduit de la propriété précédente que pour tester si un entier* $n > 1$ *est premier, il suffit de regarder s'il est divisible ou non par un des entiers compris entre 2 et vn. Par exemple, pour vérifier que 37 est premier, il suffit de voir q'il n'est divisible ni par 2, ni par 3, ni par 4, ni par 5, ni par 6. On aurait également pu éviter les divisions par 4 et 6 si on savait par avance que ces nombres étaient composés.*

La remarque précédente nous amène à la méthode suivante, appelée crible d'Ératosthène pour lister tous les nombres premiers entre 1 et n : on écrit à la suite les uns des autres tous les entiers compris entre 2 et n. On entoure le premier 2 et on barre tous ses multiples (i.e. tous les nombres pairs). On entoure ensuite le prochain nombre non barré (en l'occurrence 3) et on barre tous ses multiples. Ainsi de suite jusqu'à vn. On entoure finalement les nombres non barrés. Les nombres entourés sont alors exactement les nombres premiers compris entre 1 et n.

Exemples 3.4.1. *1) Les nombres premiers inférieurs à 100 classés dans l'ordre croissant sont, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 et 97.*

2) Le entiers : 9, 12, 25, 123, 405, 2001 sont composés.

3) Le nombre 103 est-il premier ?
Comme $\sqrt{103} \approx 10,149$, il nous suffit de vérifier que 103 n'est divisible par aucun des nombres 2, 3, 5 et 7 . Les caractères de divisibilité montrent que 103 n'est pas divisible par 2 ou par 3 ou par 5. Pour 7 on effectue les divisions euclidiennes : $103 = 14 \times 7 + 5$, le reste de la division de 103 par 7 est 5. 103 n'est donc pas divisible par 7.
On en conclut que 103 est un nombre premier.

Remarque 3.4.2. *Un entier positif est premier si et seulement si le cardinal de l'ensemble de ses diviseurs est égal à 2.*

Proposition 3.4.2 (Propriétés des nombres premiers)**.** **1** *Soit un entier $p \in \mathbb{N}$ premier, et $a \in \mathbb{Z}$ un entier. Alors, $p|a$ ou bien $p \wedge a = 1$.*

2 *Si n et m sont deux nombres premiers distincts, ils sont premiers entre eux : $n \neq m \Rightarrow n \wedge m = 1$.*

3 *Si n est un nombre premier et si $(a_1, \ldots, a_k) \in \mathbb{Z}^k$,*

$$n|a_1 ... a_k \Rightarrow [\ \forall i \in [[1, n]] : \quad n|a_i\ ]$$

Démonstration. **1** Si n et a ne sont pas premiers entre eux alors $d = n \wedge a > 1$. Mais comme $d|n$ et que n est premier, $d = 1$ ce qui n'est pas possible ou $d = n$. En conclusion, $n|a$.

2 n est premier et peut diviser m donc d'après le point précédent $n \wedge m = 1$.

3 D'après le théorème de Gauss et une petite récurrence.

□

Proposition 3.4.3. *Tout entier supérieur à 2 admet un diviseur premier.*

Démonstration. Effectuons une récurrence forte. Si $p = 2$ alors p possède un diviseur premier : lui même. Supposons la propriété vérifiée pour tout entier $p \in [[2, n]]$ et montrons la pour $p = n + 1$. Soit A l'ensemble des diviseurs de $n + 1$. On a $|A| \geq 2$. Si $|A| = 2$ alors $n + 1$ est premier et cela démontre la propriété sinon A contient un entier $q \in [[2, n]]$ qui divise $n + 1$. On applique l'hypothèse de récurrence à q : q possède un diviseur premier. Ce diviseur premier divise nécessairement aussi $n + 1$ et donc $n + 1$ possède un diviseur premier. La propriété est donc démontrée par récurrence. □

Proposition 3.4.4. *L'ensemble $\mathbb{P}$ des nombres premiers est infini.*

Démonstration. Supposons que ce ne soit pas le cas. $\mathbb{P}$ forme alors une partie finie de $\mathbb{N}$. $\mathbb{P}$ possède donc un plus grand élément n. Considérons le nombre entier $N = n! + 1$. On a : $N > n$. D'après la proposition précédente, N possède un diviseur premier p différent de 1. Ce dernier est nécessairement élément de l'ensemble $[[2, n]]$. p divise donc aussi $n!$. Mais alors p divise 1 ce qui est impossible. L'ensemble $\mathbb{P}$ des nombres premiers est donc infini. □

3.4.2 Décomposition en facteurs premiers

Lemme 3.4.1. *Soit $m \in \mathbb{N}*$. On considère m nombre premiers $p_1, ..., p_m \in \mathbb{P}$ distincts deux à deux et des entiers naturels non nuls $a_1, ..., a_m$. On forme le nombre entier $n = p_1^{a_1}...p_m^{a_m}$. Alors tout diviseur premier de n est l'un des p_i où $i \in [[1, m]]$.*

Démonstration. Considérons l'ensemble A des entiers de la forme $n = p_1^{a_1}...p_m^{a_m}$ avec $m \in \mathbb{N}^*$, $p_1, ..., p_m \in \mathbb{P}$ distincts deux à deux et $a_1, ..., a_m \in \mathbb{N}^*$ qui admettent un diviseur premier différent de chacun des p_i. La propriété sera prouvée si on montre que A est vide. Supposons que ce n'est pas le cas. Alors comme A est une partie de N, A admet un plus petit élément $n_0 = p_1^{a_1}...p_m^{a_m}$ et d'après la proposition 3.4.3, n_0 admet un diviseur premier p qui n'est, par définition de A , aucun des p_i. L'entier p divise donc le produit $p_1 p_1^{a_1-1}...p_m^{a_m}$. Les entiers p et p_1 sont premiers entre eux car premiers. On en déduit, par application du lemme de Gauss, que $p|p_1^{a_1-1}...p_m^{a_m}$. Mais comme n est le plus petit élément de A, l'entier $p_1^{a_1-1}...p_m^{a_m}$ n'est pas élément de A et p est l'un des p_i pour $i \in [[1, m]]$ ce qui rentre en contradiction avec l'hypothèse faite sur p. Le lemme est alors prouvé par l'absurde. □

Théorème 3.4.1 (Décomposition en facteurs premiers)**.** *Soit un entier $n \in \mathbb{N}\backslash\{0, 1\}$. Cet entier n s'écrit de façon unique de la manière suivante :*

$$n = p_1^{a_1}. \ . \ .p_m^{a_m},$$

où $m \in \mathbb{N}^*$, $p_1 < \ . \ . \ . \ < p_m$ sont m nombres premiers et où $a_1, . \ . \ ., a_m \in \mathbb{N}^*$. Ce résultat se formule aussi sous la forme suivante : n s'écrit de manière unique, à l'ordre

des facteurs près, comme

$$n = \prod_{p \in \mathbb{P}} p^{V_p(n)}$$

où $V_p(n) \in \mathbb{N}$ est appelé la $p-$valuation de l'entier n.

Démonstration. **Existence** La preuve se fait par récurrence sur n. Si $n = 2$ alors comme $2 \in \mathbb{P}$, la proposition est vraie. Soit $n \in \mathbb{N}\backslash\{0,1\}$. Supposons que tout entier $< n$ se décompose comme indiqué dans le théorème. Si n est premier alors le théorème est vrai pour n. Sinon n admet un diviseur premier $p \in \mathbb{P}$ et il existe $0 < m < n$ tel que $n = pm$. Mais par application de l'hypothèse de récurrence, m se décompose comme indiqué dans le théorème et il en est alors de même de n. L'existence de la décomposition est alors prouvée par récurrence.
Unicité La preuve se fait à nouveau par récurrence. Supposons que $2 = p_1^{a_1}...p_m^{a_m}$ avec pour tout $i \in [[1,m]]$, $p_i \in \mathbb{P}$, $a_i \in \mathbb{N}^*$ et $p_1 < ... < p_m$. Comme 2 est le plus petit des nombres premiers, il vient : $2 = p_1^{a_1}...p_m^{a_m} \geq 2^{a_1}...2^{a_m}$ ce qui n'est possible que si $m = 1$, $p_1 = 2$, $a_1 = 1$. L'unicité de la décomposition de 2 en facteurs premiers est alors prouvée. Soit $n \in \mathbb{N}$. Supposons que tout entier $< n$ admet une unique décomposition en facteurs premiers et supposons que que ce ne soit pas le cas pour n, c'est à dire que n admet au moins deux décompositions en facteurs premiers :

$$n = p_1^{a_1}...p_m^{a_m} = p_1'^{a_1'}...p_{m'}'^{a_{m'}'}.$$

Par application du lemme précédent, il vient $p_1 = p_i'$ pour un certain $i \in [[1,m']]$ et $p_1' = p_j$ pour un certain $j \in [[1,m]]$. Mais $p_1 \leq p_j = p_1' \leq p_i' = p_1$ et forcement $p_1 = p_1'$. On peut alors écrire :

$$\frac{n}{p_1} = p_1^{a_1-1}...p_m^{a_m} = p_1'^{a_1'-1}...p_{m'}'^{a_{m'}'}$$

L'hypothèse de récurrence nous permet d'affirmer que la décomposition de n/p_1 en facteurs premiers est unique donc : $m = m'$, $p1 = p_1'$, $p_2 = p_2'$,..., $p_m = p_m'$, $a_1 = a_1'$,...,$a_m = a_m'$. Les deux décompositions de n en facteurs premiers sont donc égales. L'unicité est ainsi prouvée par récurrence. □

Pour obtenir la décomposition d'un entier naturel en produit de facteurs premiers on pourra utiliser l'une des deux méthodes suivantes appliquées à 300.

Méthode **3.4.1.** *On écrit 300 sous la forme d'un produit, puis on recommence avec chacun des facteurs obtenus tant que c'est possible.*

$$300 = 30 \times 10 = 5 \times 6 \times 2 \times 5 = 2 \times 5 \times 5 \times 3 \times 2 = 2^2 \times 3 \times 5^2.$$

Méthode **3.4.2.** *On effectue des divisions successives par les nombres premiers (2, 3, 5, 7, 11,...) tant que c'est possible. Les résultats sont placés dans un tableau.*

300	*2*
150	*2*
75	*3*
25	*5*
5	*5*
1	

300 est divisible par 2, le quotient est 150. 150 est divisible par 2, le quotient est 75. 75 n'est pas divisible par 2, mais 75 est divisible par 3, le quotient est 25. 25 est divisible par 5, le quotient est 5. 5 est divisible par 5, le quotient est 17 est n'est pas divisible par 5, mais 7 est divisible par 7, le quotient est 1, ce qui termine le tableau.
Le résultat dans la 2^{me} colonne du tableau donne : $300 = 2\times 2\times 3\times 5\times 5 = 2^2\times 3\times 5^2$.

Théorème 3.4.2 (Expression du PGCD et du PPCM à l'aide des facteurs premiers)**.** *Soient deux entiers non-nuls $(a,b)\in\mathbb{N}^*\times\mathbb{N}^*$. Leur décomposition en facteurs premiers s'écrit :*

$$a=\prod_{p\in\mathbb{P}} p^{V_p(a)} \qquad b=\prod_{p\in\mathbb{P}} p^{V_p(b)}$$

Alors la décomposition de $a\wedge b$ et de $a\vee b$ en facteurs premiers s'écrit :

$$a\wedge b=\prod_{p\in\mathbb{P}} p^{\min\{V_p(a),V_p(b)\}} \qquad a\vee b=\prod_{p\in\mathbb{P}} p^{\max\{V_p(a),V_p(b)\}}.$$

Démonstration. Posons $d=\prod_{p\in\mathbb{P}} p^{\min\{V_p(a),V_p(b)\}}$ et montrons que $d=a\wedge b$. Considérons $a',b'\in\mathbb{N}$ tels que $a=da'$ et $b=db'$. D'après la proposition 3.2.3, on aura montré que $d=a\wedge b$ si et seulement si $a'\wedge b'=1$. Supposons que ce ne soit pas le cas alors il existe un diviseur $d\neq 1$ commun à a et b qu'on peut supposer premier. On a donc :

$$d\Big|\frac{a}{d}=\prod_{p\in\mathbb{P}} p^{V_p(a)-\min\{V_p(a),V_p(b)\}} \quad et \quad d\Big|\frac{b}{d}=\prod_{p\in\mathbb{P}} p^{V_p(b)-\min\{V_p(a),V_p(b)\}}.$$

Il vient alors que d est un facteur de chacun des deux produits ci dessus et que $V_p(a)-\min\{V_p(a),V_p(b)\}\geq 1$ ainsi que $V_p(a)-\min\{V_p(a),V_p(b)\}\geq 1$ ce qui constitue une contradiction et prouve par l'absurde que $a'\wedge b'=1$. La formule pour le PGCD est ainsi démontrée. On procède de même pour le PPCM. □

Exemple 3.4.1. *Soit $a=60$ et $b=16$. On a :*

60	*2*		*16*	*2*
30	*2*		*8*	*2*
15	*3*	*et*	*4*	*2*
5	*5*		*2*	*2*
1			*1*	

Par suite, $a=2^2\times 3\times 5$ et $b=2^4$ donc $a\wedge b=2^2\times 3^0\times 5^0=4$ et $a\vee b=2^4\times 3\times 5=240$.

Chapitre 4

POLYNÔMES

Dans tout ce chapitre $\mathbb{K}$ désigne un corps commutatif (pour nous ce sera $\mathbb{R}$ ou $\mathbb{C}$).

4.1 Définitions et exemple

Définition 4.1.1. *Un polynôme à une indéterminée, à coefficients dans $\mathbb{K}$, est une suite de valeurs a_i de $\mathbb{K}$, nulle à partir d'un certain rang n. Un tel polynôme se note P ou $P(X)$:*

$$P(X) = a_0 + a_1X + ... + a_nX^n,$$

avec $a_i \in A$, $\forall i \in \{0, ..., n\}$

- *Les nombres a_i sont les **coefficients** du polynôme P.*
- *a_0 est appelé **terme constant** du polynôme.*
- *X est appelé l'**indéterminée**.*
- *a_n est le **coefficient dominant** de P.*
- *On appelle **terme dominant** de P le monôme a_nX^n.*
- *Lorsque $a_n = 1$, le polynôme est dit **unitaire**, ou **normalisé**.*
- *Si tous les coefficients a_i sont nuls, P est appelé le **polynôme nul**, il est noté 0.*
- *Un polynôme de la forme $P = a_0$ avec $a_0 \in A$ est appelé un **polynôme constant**.*

Notation 4.1.1. *On note $\mathbb{K}[X]$ l'ensemble de tous les polynômes en X à coefficients dans $(\mathbb{K}, +, \times)$.*

4.2 Opérations sur les polynômes

•**Égalité.** Soient $P = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ et $Q = b_nX^n + b_{n-1}X^{n-1} + ... + b_1X + b_0$ deux polynômes à coefficients dans $\mathbb{K}$.

$$P = Q \Leftrightarrow \forall i \in \{1, 2, ..., n\},\ a_i = b_i.$$

•**Addition.** Soient $P = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ et $Q = b_nX^n + b_{n-1}X^{n-1} + ... + b_1X + b_0$ deux polynômes à coefficients dans $\mathbb{K}$. On définit :

$$P + Q = (a_n + b_n)X^n + (a_{n-1} + b_{n-1})X^{n-1} + ... + (a + b)X + (a_0 + b_0).$$

•**Multiplication.** Soient $P = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ et $Q = b_mX^m + b_{m-1}X^{m-1} + ... + b_1X + b_0$ deux polynômes à coefficients dans $\mathbb{K}$. On définit :

$$P \times Q = c_rX^r + c_{r-1}X^{r-1} + ... + c_1X + c_0.$$

$$avec \quad r = m + n \quad et \quad c_k = \sum_{i=0}^{k} a_i b_{k-i} \quad pour \quad k \in \{0, ..., r\}.$$

•**Multiplication par un scalaire.** Si $\lambda \in \mathbb{K}$ alors $\lambda.P$ est le polynôme dont le i-ème coefficient est λa_i.

Exemples **4.2.1.** **1** *Soient $P = aX^3 + bX^2 + cX + d$ et $Q = \alpha X^2 + \beta X + \gamma$. Alors*
$P + Q = aX^3 + (b + \alpha)X^2 + (c + \beta)X + (d + \gamma)$,
$P \times Q = (a\alpha)X^5 + (a\beta + b\alpha)X^4 + (a\gamma + b\beta + c\alpha)X^3 + (b\gamma + c\beta + d\alpha)X^2 + (c\gamma + d\beta)X + d\gamma$.
Enfin $P = Q$ si et seulement si $a = 0$, $b = \alpha$, $c = \beta$ et $d = \gamma$.

2 *La multiplication par un scalaire $\lambda.P$ équivaut à multiplier le polynôme constant λ par le polynôme P.*

Proposition **4.2.1.** *$(\mathbb{K}[X], +, \times)$ est un anneau commutatif unitaire, d'élément nul le polynôme nul et d'élément unité le polynôme constant égal à 1.*

Proposition **4.2.2.** *Pour $P,\ Q,\ R \in \mathbb{K}[X]$, on a*
- $0 + P = P$,
- $P + Q = Q + P$,
- $(P + Q) + R = P + (Q + R)$;
- $1.P = P$,
- $P \times Q = Q \times P$,
- $(P \times Q) \times R = P \times (Q \times R)$;
- $P \times (Q + R) = P \times Q + P \times R$.

4.3 Degré d'un polynôme

Définition **4.3.1** (Degré d'un polynôme, terme dominant)**.** *Soit un polynôme $P = a_0 + ... + a_pX^p \in \mathbb{K}[X]$ avec $a_p \neq 0$.*
- *On appelle degré de P et on note $deg(P)$ l'entier p.*
- *Par convention, le degré du polynôme nul est $-\infty$.*
- *a_iX^i avec $i \in \{0, ..., p\}$, est appelé monôme de degré i et de coefficient a_i.*

Remarque **4.3.1.** *Si P est un polynôme constant non nul, alors son degré est 0.*

Notation 4.3.1. *On note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n.*

Théorème 4.3.1 (Degré d'un produit, degré d'une somme)**.** *On a : Pour tout $P, Q \in \mathbb{K}[X]$,*

1 $deg(P+Q) = \max\{deg(P), deg(Q)\}$.

2 $deg(P \times Q) = deg(p) + deg(Q)$.

Démonstration. **1** **a** Si $P = Q = 0$ alors $degP = degQ = -\infty$ et $deg(P+Q) = -\infty$ et la formule est prouvée dans ce cas.

b Si P ou Q est non nul alors, supposant, quitte à interchanger P et Q, que $P \neq 0$, on a : $P = \sum_{k=0}^{n} a_k X^k$, $Q = \sum_{k=0}^{n} b_k X^k$ où $n = \max\{degP, degQ\}$ et où les a_k pour $k \in \{1, ..., n\}$ ne sont pas tous nuls. Les b_k peuvent être tous nuls. On a donc :

$$P + Q = (a_n + b_n)X^n + (a_{n-1} + b_{n-1})X^{n-1} + ... + (a+b)X + (a_0 + b_0).$$

Si $a_n + b_n \neq 0$ alors $deg(P+Q) = \max\{degP, degQ\}$ et sinon $deg(P+Q) \leq \max\{degP, degQ\}$.

2 **a** Si $P = 0$ ou $Q = 0$ alors $PQ = 0$ et $deg(PQ) = -\infty = degP + degQ$ d'après les lois d'addition dans $\mathbb{R}$.

b Si P ou Q est non nul alors, on suppose que $P = \sum_{k=0}^{n} a_k X^k$, $Q = \sum_{k=0}^{m} b_k X^k$ où $a_n \neq 0$ et $b_m \neq 0$. Par conséquent, $degP = n$ et $degQ = m$. Quitte à échanger le rôle de P et de Q, on peut supposer que $n \geq m$. Soit $l \in \mathbb{N}$. Notons c_l le coefficient d'indice l dans PQ. On a $c_l = \sum_{i=0}^{l} a_i b_{l-i}$ pour $l \in \{0, ..., m+n\}$ et $c_l = 0$ pour $l \in \mathbb{N}\backslash\{0, ..., m+n\}$. Nécessairement, $deg(PQ) \leq m+n$. Le coefficient d'indice $m+n$ dans PQ est $a_n b_m \neq 0$ donc $deg(P \times Q) = deg(P) + deg(Q)$.

□

Remarque 4.3.2. *Si $deg(P) \neq deg(Q)$ alors $deg(P+Q) = \max\{deg(P), deg(Q)\}$.*

Proposition 4.3.1 (Intégrité de l'anneau des polynômes $\mathbb{K}[X]$)**.** *Soient $P, Q \in \mathbb{K}[X]$.*

$$P \times Q = 0 \Rightarrow P = 0 \quad ou \quad Q = 0.$$

Démonstration. Si $P \times Q = 0$ alors $deg(P \times Q) = -\infty = degP + degQ$ ce qui n'est possible que si $degP = -\infty$ ou $degQ = -\infty$ et donc que si $P = 0$ ou $Q = 0$. □

Proposition **4.3.2** (Éléments inversibles de l'anneau $\mathbb{K}[X]$)**.** *Les seuls éléments inversibles de l'anneau $\mathbb{K}[X]$ sont les polynômes de degré 0, c'est à dire les polynômes constants non nuls.*
Autrement dit, si $P, Q \in \mathbb{K}[X]$ et si $P \times Q = 1$ alors il existe $a \in \mathbb{K}^*$ tel que $P = a$ et $Q = a^{-1}$.

Démonstration. Soit $P \in \mathbb{K}[X]$ un polynôme inversible. Il existe alors un polynôme $Q \in \mathbb{K}[X]$ tel que : $P \times Q = 1$. On a donc : $degP + degQ = 0$. Cette égalité n'est possible que si $degP = degQ = 0$ et donc que si P est un polynôme constant non nul. Réciproquement, si P est un polynôme constant non nul alors il est clair que P est inversible. □

4.4 Valuation d'un polynôme

Définition **4.4.1** (Valuation d'un polynôme)**.** *Soit un polynôme $P = a_0 + ... + a_pX^p \in \mathbb{K}[X]$ non nul. On appelle valuation de P le plus petit entier k tel que $a_k \neq 0$. On le note $val(P)$.*
La valuation du polynôme nul est $val(0) = +\infty$

Théorème **4.4.1** (Valuation d'un produit, valuation d'une somme)**.** *Soient $P, Q \in \mathbb{K}[X]$, on a : On a : pour tout $P, Q \in \mathbb{K}[X]$,*

1. $val(P + Q) \geq \min\{val(P), val(Q)\}$.
2. $val(P \times Q) = val(P) + val(Q)$.

4.5 Composition de polynômes

Définition **4.5.1** (Composition de deux polynômes)**.** *Soient deux polynômes $P, Q \in \mathbb{K}[X]$. On suppose que $P = a_0 + a_1X + ... + a_nX^n$. On définit le polynôme composé de Q par P, noté $P \circ Q$, par :*

$$P \circ Q = \sum_{k=0}^{n} a_k Q^k.$$

Proposition **4.5.1.** *Soient deux polynômes non nuls $P, Q \in \mathbb{K}[X]$. Alors :*

$$deg(P \circ Q) = deg(P) \times deg(Q).$$

.

Démonstration. Supposons que $P = a_0 + a_1X + ... + a_nX^n$. Comme $P \neq 0$, on a $a_n \neq 0$. Alors $P \circ Q = \sum_{k=0}^{n} a_k Q^k$ et $deg(P \circ Q) = degQ^n = ndegQ = degP \times degQ$ car $Q \neq 0$. □

Exemple 4.5.1. **1** $(X^2+4)\circ(X-3) = (X-3)^2+4 = X^2-6X+13$;

2 $(X-3)\circ(X^2+4) = (X^2+4)-3 = X^2+1$;

3 *en général,* $P\circ(X+a)$ *est noté* $P(X+a)$.

4.6 Division euclidienne

Définition 4.6.1 (Divisibilité)**.** *Soient deux polynômes* $A, B \in \mathbb{K}[X]$. *On dit que* A *divise* B *si et seulement si il existe* $Q \in \mathbb{K}[X]$ *tel que* $B = QA$. *On le note* $A|B$. *Le polynôme* A *s'appelle diviseur de B et* B *s'appelle multiple de* A.
On dit que A *et* B *sont des polynômes associés lorsque* $A = \lambda B$, *avec* $\lambda \in \mathbb{K}^*$.

Exemple 4.6.1. *textbullet* $(X-1)$ *divise* X^2-2X+1. *En effet* $X^2-2X+1 = (X-1)^2$.
textbullet $(X-1)$ *divise* X^2-1. *En effet :* $X^2-1 = (X-1)(X+1)$.
textbullet $(1-X)$ *divise* $1-X^{n+1}$. *En effet* $1-X^{n+1} = (1+X+X^2+...+X^n)(1-X)$.

Proposition 4.6.1. *Polynômes associés Soient* $A, B \in \mathbb{K}[X]$ *deux polynômes non nuls. On a équivalence entre :*

1 $A|B$ *et* $B|A$.

2 $\exists\lambda \in \mathbb{K}^*$ *tel que* $B = \lambda A$.

Démonstration. $(\Rightarrow)$ Supposons que $A|B$ et $B|A$. Alors il existe des polynômes $Q_1, Q_2 \in \mathbb{K}[X]$ tels que : $A = Q_1B$ et $B = Q_2A$. On a alors : $A = (Q_1Q_2)A$ ou encore : $A(1-Q_1Q_2) = 0$. Par intégrité de $\mathbb{K}[X]$, comme $A \neq 0$, ceci n'est possible que si $1-Q_1Q_2 = 0$ c'est à dire si $Q_1Q_2 = 1$. Par conséquent, Q_1 et Q_2 sont des polynômes inversibles inverses l'un de l'autre. appliquant la proposition 4.3.2, il existe $a \in \mathbb{K}^*$ tel que $Q_1 = a$ et $Q_2 = a^{-1}$. On a alors $B = aA$. A et B sont donc bien associés.
$(\Leftarrow)$ La réciproque est triviale. □

Théorème 4.6.1 (Division euclidienne)**.** *Soient* $A, B \in \mathbb{K}[X]$ *deux polynômes. On suppose que* $B \neq 0$. *Alors il existe un unique couple* (Q, R) *de polynômes de* $\mathbb{K}[X]$ *vérifiant :*

1 $A = BQ + R$

2 *deg (R) < deg(B).*

On dit que Q *est le quotient, et* R *le reste, dans la division euclidienne de* A *par* B.

Démonstration.
— Unicité. Si $A = BQ + R$ et $A = BQ' + R'$, alors $B(Q-Q') = R'-R$. Or $deg(R'-R) < degB$. Donc $Q-Q' = 0$. Ainsi $Q = Q'$, d'où aussi $R = R'$.
— Existence. On montre l'existence par récurrence sur le degré de A.

- Si $degA = 0$ et $degB > 0$, alors A est une constante, on pose $Q = 0$ et $R = A$.
  Si $degA = 0$ et $degB = 0$, on pose $Q = A/B$ et $R = 0$.
- On suppose l'existence vraie lorsque $degA \leq n-1$. Soit $A = a_nX^n + ... + a_0$ un polynôme de degré n avec $a_n \neq 0$. Soit $B = b_mX^m + ... + b_0$ avec $b_m \neq 0$.
  Si $n < m$ on pose $Q = 0$ et $R = A$.
  Si $n > m$ on écrit $A = B \times \frac{a_n}{b_n}X^{n-m} + A_1$ avec $degA_1 \leq n-1$. On applique l'hypothèse de récurrence à A_1 : il existe $Q_1, R_1 \in \mathbb{K}[X]$ tels que $A_1 = BQ_1 + R_1$ et deg $R_1 < degB$. Il vient :

$$A = B\Big(\frac{a_n}{b_m}X^{n-m} + Q_1\Big) + R_1.$$

  Donc $Q = \frac{a_n}{b_m}X^{n-m} + Q_1$ et $R = R_1$ conviennent.

□

Exemple 4.6.2.

$$\begin{array}{rrrrrrr|l}
X^3 & + & & & X & + & 3 & X+1 \\
\cline{8-8}
-(X^3 & + & X^2) & & & & & X^2-X+2 \\
\cline{1-3}
 & & -X^2 & + & X & & & \\
 & & -(-X^2 & - & X) & & & \\
\cline{3-5}
 & & & & 2X & + & 3 & \\
 & & & & -(2X & + & 2) & \\
\cline{5-7}
 & & & & & & 1 &
\end{array}$$

On a donc : $X^3 + X + 3 = (X+1)(X^2 - X + 2) + 1$ *et* $deg(1) = 0 < deg(X+1) = 1$.

Exercice 7. *Soit* $A = X^7 - 2X + 1$ *et* $B = X^2 + 1$ *deux polynomes à coefficients réels. Effectuer la division euclidienne de A par B.*

Exercice 8. *Déterminer le reste de la division euclidienne de* $A = X^{2000} - X^3 + X$ *par* $B = X^2 + 1$, *puis par* $C = X^2 + X + 1$.

4.7 Division selon les puissances croissantes

Théorème 4.7.1 (Division selon les puissances croissantes)**.** *Soient* A *et* B *deux polynômes à coefficients dans* $\mathbb{K}$. *On suppose que le terme constant de* B *n'est pas nul et on note p un entier supérieur ou égal au degré de* B. *Il existe un unique couple de polynômes* (Q, R) *tels que* $A = BQ + X^{p+1}R$ *et deg* $Q \leq p$.

Exemple **4.7.1.**

$$\begin{array}{rcrcrcrcrcr|l}
1 & + & 3X & + & 2X^2 & - & 7X^3 & & & & & 1+X-2X^2 \\
\cline{12-12}
-(1 & + & X & - & 2X^2) & & & & & & & 1+2X+2X^2-5X^3 \\
\cline{1-6}
 & + & 2X & + & 4X^2 & - & 7X^3 & & & & & \\
 & - & (2X & + & 2X^2 & - & 4X^3) & & & & & \\
\cline{3-8}
 & & & + & 2X^2 & - & 3X^3 & & & & & \\
 & & & - & (2X^2 & + & 2X^3 & - & 4X^4) & & & \\
\cline{4-9}
 & & & & & - & 5X^3 & + & 4X^4 & & & \\
 & & & & & - & (-5X^3 & - & 5X^4 & + & 10X^5) & \\
\cline{6-11}
 & & & & & & & + & 9X^4 & - & 10X^5 &
\end{array}$$

Ce qui s'écrit :

$$\underbrace{1+3X+2X^2-7X^3}_{A} = \underbrace{(1+X-2X^2)}_{B}\underbrace{(1+2X+2X^2-5X^3)}_{Q} + X^4\underbrace{(9-10X)}_{R}.$$

4.8 Fonctions polynomiales

Définition **4.8.1.** *Soit $P = a_0 + a_1X + ... + a_nX^n \in \mathbb{K}[X]$. Soit $x \in \mathbb{K}$. Le scalaire $P = a_0 + a_1x + ... + a_nx^n \in \mathbb{K}$ est appelé valeur de P en x, on le note $P(x)$.*

Définition **4.8.2.** *$P = \sum_{i=0}^{n} a_iX^i$ étant un polynôme de $\mathbb{K}[X]$, la fonction polynomiale associée à P est l'application $\widetilde{P}$, de $\mathbb{K}$ dans $\mathbb{K}$, définie par :*

$$x \mapsto \widetilde{P}(x) = \sum_{i=0}^{n} a_ix^i.$$

Remarque **4.8.1.** *Si $\mathbb{K}$ est infini, vous pouvez confondre sans risque P et $\widetilde{P}$. Ce n'est pas le cas si $\mathbb{K}$ est fini. En effet, lorsque le corps est fini, si l'on note $a_i, a_2, ..., a_n$ ses éléments, le polynôme*

$$\prod_{i=1}^{n}(X - a_i)$$

est non nul puisque de degré n, alors que sa fonction polynômiale associée est nulle.

Proposition **4.8.1.** *On a*

i) $\forall P, Q \in \mathbb{K}[X]$, $\widetilde{(P+Q)} = \widetilde{P} + \widetilde{Q}$,
ii) $\forall \lambda \in \mathbb{K}, \forall P \in \mathbb{K}[X]$, $\widetilde{(\lambda P)} = \lambda\widetilde{P}$,
iii) $\forall P, Q \in \mathbb{K}[X]$, $\widetilde{(PQ)} = \widetilde{P}\widetilde{Q}$,
iv) $\forall P, Q \in \mathbb{K}[X]$, $\widetilde{(P \circ Q)} = \widetilde{P} \circ \widetilde{Q}$.

Démonstration. A faire en exercice. □

4.9 Racines d'un polynôme

Définition 4.9.1 (Racine d'un polynôme)**.** *Soit $P \in \mathbb{K}[X]$ un polynôme. Soit $a \in \mathbb{K}$. On dit que a est une racine de P si et seulement si $\widetilde{P}(a) = 0$.*

Théorème 4.9.1. *Soient $P \in \mathbb{K}[X]$ un polynôme et $a \in \mathbb{K}$ un scalaire. On a une équivalence entre :*

1. *a est une racine de P.*
2. *On peut factoriser P par $X - a$, c'est à dire : $(X - a)|P$.*

Démonstration. $(\Rightarrow)$ Soit a une racine de P. Alors $\widetilde{P}(a) = 0$. Par division euclidienne, il existe $(Q, R) \in (\mathbb{K}[X])^2$ tels que :

$$P = (X - a)Q + R \qquad deg(R) < deg(X - a) = 1$$

On a alors deux possibilités, soit $degR = 0$, soit $degR = -\infty$, c'est à dire $R = 0$. Montrons que la première n'est pas possible : si on avait $degR = 0$ alors il existerait $\gamma \in \mathbb{K}^*$ tel que $R = \gamma$ et on aurait : $p = (X - a)Q + \gamma$. On a alors : $P = (X - a)Q + \gamma$ et $0 = \widetilde{P}(a) = \widetilde{R}(a) = \gamma \neq 0$ ce qui est une contradiction. On a donc bien $R = 0$ et $P = (X - a)Q$.
$(\Leftarrow)$ Supposons que $(X - a)|P$. Alors il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - a)Q$. Par conséquent : $P = (X - a)Q$ et $\widetilde{P}(a) = 0$ ce qui prouve que a est une racine de P. □

Corollaire 4.9.1. *Si $a_1, ..., a_p$ sont p racines distinctes d'un polynôme $P \in \mathbb{K}[X]$ alors le polynôme*

$$(X - a_1)...(X - a_p) = \prod_{k=1}^{p}(X - a_k)$$

divise P.

Démonstration. La démonstration se fait par récurrence sur le nombre p de racines distinctes de P considérées.

1. La propriété vient d'être prouvée au rang 1 dans le théorème précédent.
2. Soit p > 1.
3. On suppose que la propriété est vraie au rang $p - 1$ et prouvons-la au rang p. Soient $a_1, ..., a_p$ p racines de P. Par application de l'hypothèse de récurrence, il existe $B \in \mathbb{K}[X]$ tel que : $P = (X - a_1)...(X - a_{p-1})B$. Comme a_p est une racine de P, on a :
$$0 = \widetilde{P}(a) = (a_p - a_1)...(a_p - a_{p-1})\widetilde{B}(a).$$
Comme : $\forall i \in \{1, ..., p-1\}$, $a_i \in a_p$, le nombre $(a_p - a_1)...(a_p - a_{p-1})$ est non nul et donc nécessairement $\widetilde{B}(a) = 0$, c'est-à-dire a_p est une racine de B. appliquant le théorème précédent, il existe $C \in \mathbb{K}[X]$ tel que : $B = (X - a_p)C$ et donc $P = (X - a_1)...(X - a_p)C$. On a alors prouvé que $(X - a_1)...(X - a_p)$ divise P.

4 Le théorème est alors prouvé par application du principe de récurrence.

□

Théorème 4.9.2 (Un polynôme **non nul** de degré $\leq n$ admet au plus n racines.)**.** *Soit $P \in \mathbb{K}[X]$ un polynôme non nul de degré $\leq n$. Si P admet au moins $n+1$ racines distinctes alors P est nul.*

Démonstration. Supposons qu'il existe $a_1, ..., a_{n+1}$, $n+1$ racines distinctes du polynôme P non nul de degré $\geq n$. appliquant le théorème précédent, le polynôme de degré $n+1$: $(X-a_1)...(X-a_{n+1})$ divise P. Il existe donc $B \in \mathbb{K}[X]$ tel que : $P = B(X-a_1)...(X-a_{n+1})$. On a alors $n = degP = degB + n + 1$. Comme $degP \geq 0$, cette égalité n'est pas possible et donc notre hypothèse de départ est absurde. □

On en déduit :

Théorème 4.9.3. *Tout polynôme qui admet une infinité de racines est le polynôme nul.*

Définition 4.9.2. *Soit $k \in \mathbb{N}^*$. On dit que α est une racine de multiplicité k de P si $(X-\alpha)^k$ divise P alors que $(X-\alpha)^{k+1}$ ne divise pas P. Lorsque $k=1$ on parle d'une racine simple, lorsque $k=2$ d'une racine double, etc.*

Remarque 4.9.1.
- *Lorsque α est une racine de multiplicité k de P, on dit aussi que α est une racine d'ordre k.*
- *Pour déterminer la multiplicité d'une racine, on peutc faire a priori un certain nombre de divisions euclidiennes.*

Exemple 4.9.1. *$X^4 - X^2$ admet 0 comme racine double, et 1 et -1 comme racines simples.*

4.10 Polynômes dérivés

Supposons que $\mathbb{K}$ est infini.

4.10.1 Définitions et propriétés de base

Définition 4.10.1 (Polynôme dérivé)**.** *Soit $P = a_0 + a_1X + ... + a_nX^n \in \mathbb{K}[X]$ un polynôme. On définit le polynôme dérivé de P par :*

$$P' = a_1 + 2a_2X + ... + na_nX^{n-1} = \sum_{k=1}^{n} ka_kX^{k-1}.$$

Remarque 4.10.1.
- *Cette définition est purement algébrique.*

— *Elle coïncide avec la dérivée des fonctions polynomiales sur le corps* $\mathbb{K}$·

Proposition **4.10.1.** *Soit* $P \in \mathbb{K}[X]$ *un polynôme. On a :*

1 *Si* $deg(P) > 0$ *alors* $deg(P') = deg(P) - 1$.

2 P *est constant si et seulement si* $P' = 0$.

Démonstration. **1** Si $deg(P) = p > 0$ alors $P = \sum_{k=0}^{p} a_k X^k$ avec $a_p \neq 0$ et $P' = \sum_{k=1}^{p} k a_k X^{k-1}$. Le coefficient de terme dominant de P' est pap qui est non nul. Par conséquent $degP' = p - 1$.

2 Si P est constant, il est clair que $P' = 0$. Réciproquement, si P n'est pas constant, alors $degP > 0$ et $degP' \geq 0$ ce qui prouve que P' est non nul.

□

Proposition **4.10.2** (Linéarité de la dérivation)**.** *Soient* $P, Q \in \mathbb{K}[X]$ *deux polynômes et* $a, b \in \mathbb{K}$ *deux scalaires. On a :*

$$(aP + bQ)' = aP' + bQ'.$$

Démonstration. Laissée en exercice. □

Proposition **4.10.3** (Dérivée d'un produit)**.** *Soient* $P, Q \in \mathbb{K}[X]$ *deux polynômes. On a :*

$$(PQ)' = P'Q + PQ'$$

Démonstration. Supposons que $P = \sum_{k\in\mathbb{N}} a_k X^k$ et $Q = \sum_{k\in\mathbb{N}} b_k X^k$. On a donc : $PQ = \sum_{i+j=0}^{+\infty} a_i b_j X^{i+j}$ et :

$$\begin{aligned}
(PQ)' &= \sum_{i+j=0}^{+\infty} (i+j) a_i b_j X^{i+j-1} \qquad \texttt{par linéarité de la dérivation} \\
&= \sum_{i+j=0}^{+\infty} i a_i b_j X^{i-1} X^j + \sum_{i+j=0}^{+\infty} j a_i b_j X^i X^{j-1} \\
&= P'Q + PQ'
\end{aligned}$$

□

4.10.2 Dérivées successives

Définition **4.10.2** (Polynôme dérivé d'ordre r)**.** *Pour* $r \in \mathbb{N}$*, on définit, par récurrence, le polynôme dérivé d'ordre* r *:*

$$p^{(0)} = P \qquad et \qquad P^{r+1} = (P^r)'$$

Remarque **4.10.2.** *Pour $r \in \mathbb{N}$, l'application $P \mapsto P'$ est linéaire puisque c'est l'itérée r-ième de la dérivation.*

Remarque **4.10.3.** *Pour $n \in \mathbb{N}$ et $p \in \{0, ..., n\}$, on a :*

$$\begin{cases} (X^n)^{(p)} = n(n-1)...(n-p+1)X^{n-p} = p!C_n^p X^{n\,p} & si \quad p \leq n \\ 0 \quad si \quad p > n \end{cases}$$

Proposition **4.10.4** (Formule de Leibniz)**.** *Si A et B sont deux polynômes. Pour $r \in \mathbb{N}$, on a :*

$$(AB)^r = \sum_{k=0}^{r} C_r^k A^k B^{r-k}.$$

Démonstration. Cette formule se démontre par récurrence de la même façon que pour les fonctions dérivables, en utilisant le résultat :

$$(A^k B^{r-k}) = A^{k+1}B^{r-k} + A^k B^{r-k+1}.$$

□

Proposition **4.10.5.** *(Formule de Taylor) Étant donnés $P \in \mathbb{K}[X]$ un polynôme de degré inférieur ou égal à n et $a \in \mathbb{K}$, on a :*

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

ce qui peut encore s'écrire

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

:

Démonstration. Raisonnons par recurrence forte sur n :

- si $n = 0$, $P(X) = \frac{P(0)(a)}{0!}(X.a)0$;

- soit $n \in \mathbb{N}^*$. tel que la formule soit vraie pour tout polynôme de degré inferieur ou égal a $n-1$, et soit P un polynome de degre n. Effectuons la division euclidienne de P par $(X-a)^n$:

$$P(X) = (X-a)^n Q + R \quad avec \quad degQ = 0 \quad et \quad degR \leq n-1.$$

Posons $Q = \lambda$. On peut appliquer l'hypothese de recurrence au polynôme R :

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

En derivant successivement cette relation, on obtient :

$$\forall p \in \{0, ..., n-1\}, \quad P^{(p)}(X) = \frac{\lambda n!}{(n-p)!}(X-a)^{n-p} + \sum_{k=p}^{n-1} \frac{R^{(k)}(a)}{k!} \frac{k!}{(k-p)!}(X-a)^{k-p}$$

et : $P^{(n)}(X) = \lambda n!$.
D'où $\forall p \in \{0, ..., n-1\}, \quad P^{(p)}(a) = R^{(p)}(a)$ et $P^{(n)}(a) = \lambda n!$.
En definitive :

$$P(X) = \frac{P^{(n)}(a)}{n!}(X-a)^n + \sum_{k=0}^{n-1} \frac{P^{(k)}(a)}{k!}(X-a)^k.$$

La seconde formule se deduit de la premiere en remplacant X par $X + a$. □

Lemme **4.10.1.** *Soient $r \in \mathbb{N}^*$ et $P \in \mathbb{K}[X]$. Soit $a \in \mathbb{K}$. Si a est une racine d'ordre r de P alors a est une racine d'ordre $r-1$ de P'.*

Démonstration. Comme a est une racine d'ordre r de P, il existe $Q \in \mathbb{K}[X]$ tel que : $P = (X-a)^r Q$ et $Q(a) \neq 0$. Par conséquent :

$$P'(X) = r(X-a)^{r-1}Q(X) + (X-a)^r Q'(X) = (X-a)^{r-1}\Big(rQ(X) + (X-a)Q'(X)\Big).$$

Posons $B(X) = rQ(X) + (X-a)Q'(X)$. On a clairement $B(a) \neq 0$, ce qui prouve le lemme. □

Proposition **4.10.6** (Caractérisation des racines multiples)**.** *Soient un polynôme $P \in \mathbb{K}[X]$, un scalaire $a \in \mathbb{K}$ et un entier $r > 0$. On a équivalence entre :*

1. *a est une racine d'ordre r de P.*
2. *$P(a) = P'(a) = ... = P^{(r-1)}(a) = 0 \quad et \quad P^{(r)}(a) \neq 0$.*

Démonstration. ($\Rightarrow$) Par application du lemme 4.10.1, si a est une racine d'ordre r de P alors a est une racine d'ordre 1 de $P^{(r-1)}$ et d'ordre 0 de $P^{(r)}$ donc $P(a) = P'(a) = ... = P^{(r-1)}(a) = 0$ et $P^{(r)}(a) \neq 0$.
($\Leftarrow$) Si $P(a) = P'(a) = ... = P^{(r-1)}(a) = 0$ alors, par application de la formule de Talor :

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

avec $B \in \mathbb{K}[X]$ tel que $B(a) \neq 0$. □

Corollaire **4.10.1.** *Soit A un polynôme. Un scalaire a est racine multiple de A si, et seulement si, $A(a) = A'(a) = 0$.*

4.11 Polynômes scindés

4.11.1 Définition

Définition 4.11.1 (Polynôme scindé sur $\mathbb{K}$)**.** *Soit $P \in \mathbb{K}[X]$ de degré p. On dit que P est scindé sur $\mathbb{K}$ si et seulement si il s'écrit :*

$$P = \alpha_p(X - a_1)...(X - a_p) = \alpha_p \prod_{k=0}^{p}(X - ak)$$

où les scalaires $a_k \in \mathbb{K}$ sont les racines de P comptées avec leur multiplicité et α_p est le coefficient du terme dominant de P.

4.11.2 Factorisation dans $\mathbb{C}[X]$

Théorème 4.11.1 (Théorème de d'Alembert-Gauss)**.** *Soit P un polynôme de $\mathbb{C}[X]$ de degré ≥ 1 (c'est à dire non constant) alors P possède au moins une racine dans $\mathbb{C}$.*

Remarque 4.11.1. *Attention ce théorème est faux dans $\mathbb{R}$. Par exemple $P = X^2 + 1$ est non constant mais ne possède aucune racine dans $\mathbb{R}$.*

Corollaire 4.11.1 (Factorisation dans $\mathbb{C}[X]$)**.** *Tout polynôme de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$, c'est à dire tout polynôme $P \in \mathbb{C}[X]$ s'écrit sous la forme*

$$P(X) = \alpha_p(X - a_1)...(X - a_p)$$

où les scalaires a_k sont les racines de P comptées avec leur multiplicité et α_p est le coefficient du terme dominant de P.

Démonstration. Supposons que P est non constant, sinon la propriété est évidente. Soient $a_1, ..., a_p \in \mathbb{C}$ la liste des racines de P. Par application du théorème de d'Alembert-Gauss cette liste est non vide. Il existe $Q \in \mathbb{C}[X]$ tel que : $P = \prod_{i=1}^{p}(X - a_i)Q$. Si Q est non constant alors il possède une racine a et a est nécessairement aussi une racine de P. Donc la liste $a_1, ..., a_p$ n'était pas celle de toutes les racines de P, ce qui constitue une contradiction. Par conséquent, Q est un polynôme constant et la proposition est démontrée. □

Une formulation équivalente du théorème de d'Alembert-Gauss est la suivante :

Théorème 4.11.2. *Un polynôme $P \in \mathbb{C}[X]$ de degré n possède n racines (comptées avec leur multiplicité) dans $\mathbb{C}$.*

Démonstration. C'est un corollaire immédiat de la proposition précédente. □

4.11.3 Factorisation dans $\mathbb{R}[X]$

Proposition **4.11.1** (Factorisation dans $\mathbb{R}[X]$)**.** *Soit $P \in \mathbb{R}[X]$ un polynôme non nul. Alors, il existe $a_1, ..., a_r \in \mathbb{R}$ non nécessairement deux à deux distincts, $(b_1, c_1), ..., (b_s, c_s) \in \mathbb{R}^2$ non nécessairement deux à deux distincts tels que $\Delta_l = b^2 - 4c_l < 0$ pour tout $l \in \{1, ..., s\}$, et $\lambda \in \mathbb{R}^*$ tels que*

$$P = \lambda \prod_{k=1}^{r} (X - a_k)^{k_r} \prod_{l=1}^{s} (X^2 + b_l X + c_l).$$

4.11.4 Polynômes irréductibles

Définition **4.11.2** (Polynôme irréductible)**.** *Soit $P \in \mathbb{K}[X]$ un polynôme non constant . On dit que P est irréductible si et seulement si :*

$$P = QH \Rightarrow Q \in \mathbb{K} \quad ou \quad H \in \mathbb{K}$$

Autrement dit : un polynôme P non constant est irréductible si et seulement si ses seuls diviseurs sont les polynômes constants et les polynômes proportionnels à P.

Proposition **4.11.2** (Les polynômes de degré 1 sont irréductibles)**.** *Quel que soit le corps $\mathbb{K}$, pour tout $a \in \mathbb{K}$, le polynôme $P = (X - a)$ est iréeductible dans $\mathbb{K}[X]$.*

Démonstration. Soit P un polynôme de degré 1. P est clairement non constant et si $Q \in \mathbb{K}[X]$ est un diviseurs de P alors il existe $H \in \mathbb{K}[X]$ tel que : $P = QH$. Par conséquent : $1 = degP = degQ + degH$. Une des deux possibilités suivantes est alors vraie :

- $degQ = 1$ et $degH = 0$ donc Q est un polynôme proportionnel à P
- $degQ = 0$ (et $degH = 1$) et Q est un polynôme constant. Par conséquent P est irréductible.

□

Théorème **4.11.3** (Polynômes irréductibles de $\mathbb{C}[X]$)**.** *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*

Démonstration. On vient de prouver que les polynômes de degré 1 sont irréductibles dans $\mathbb{C}[X]$.
Réciproquement, si $P \in \mathbb{C}[X]$ est un polynôme irréducible de $\mathbb{C}[X]$, montrons qu'il est de degré 1. Si ce n'était pas le cas, alors comme P est non nul :

- soit $degP > 1$ et par application du théorème 4.11.1, P possède au moins une racine a dans $\mathbb{C}$. Par conséquent le polynôme $X - a$ divise P et donc P n'est pas irréductible.
- soit $degP = 0$ et dans ce cas P est un polynôme constant non nul et ne peut être irréductible.

Dans les deux cas, on aboutit à une contradiction et la proposition est alors prouvée par l'absurde. □

Théorème 4.11.4 (Polynômes irréductibles de $\mathbb{R}[X]$)**.** *Les polynômes irréductibles de $\mathbb{R}[X]$ sont :*

- *les polynômes de degré 1.*
- *les polynômes de degré 2 dont le disciminant est négatif.*

Démonstration.
- Les polynômes de degré 1 sont irréductibles dans $\mathbb{R}[X]$.
- Soit $P \in \mathbb{R}[X]$ un polynôme de degré 2. Il est irréducible si et seulement si il n'est pas divisible par un polynôme de degré 1, c'est à dire si et seulement si il n'a pas de racine réelle, ce qui est équivalent à dire que son discriminant est strictement négatif.
- Tout polynôme de degré ≥ 3 se décompose, d'après le théorème de factorisation dans $\mathbb{R}[X]$ 4.11.1, comme le produit de polynômes de degré 1 et de degré 2. Un tel polynôme ne peut être irréductible.

□

Exemples 4.11.1.
- *Tous les polynômes de degré 1 sont irréductibles. Par conséquent il y a une infinité de polynômes irréductibles.*
- $X^2 - 1 = (X-1)(X+1) \in \mathbb{R}[X]$ *est réductible.*
- $X^2 + 1 = (X-i)(X+i)$ *est réductible dans* $\mathbb{C}[X]$ *mais est irréductible dans* $\mathbb{R}[X]$.
- $X^2 - 2 = (X-\sqrt{2})(X+\sqrt{2})$ *est réductible dans* $\mathbb{R}[X]$ *mais est irréductible dans* $\mathbb{Q}[X]$.

Exemples 4.11.2. *Soit* $P(X) = X^4 + 1$.
- *Sur* $\mathbb{C}$. *On peut d'abord décomposer* $P(X) = (X^2+i)(X^2-i)$. *Les racines de* P *sont donc les racines carrées complexes de* i *et* $-i$. *Ainsi* P *se factorise dans* $\mathbb{C}[X]$ *:*

$$P(X) = \big(X - \tfrac{\sqrt{2}}{2}(1+i)\big)\big(X + \tfrac{\sqrt{2}}{2}(1+i)\big)\big(X - \tfrac{\sqrt{2}}{2}(1-i)\big)\big(X + \tfrac{\sqrt{2}}{2}(1-i)\big).$$

- *Sur* $\mathbb{R}$. *Pour un polynôme à coefficient réels, si* α *est une racine alors* $\bar{\alpha}$ *aussi. Dans la décomposition ci-dessus on regroupe les facteurs ayant des racines conjuguées, cela doit conduire à un polynôme réel :*

$$\begin{aligned} P(X) &= \Big[\big(X - \tfrac{\sqrt{2}}{2}(1+i)\big)\big(X - \tfrac{\sqrt{2}}{2}(1-i)\big)\Big]\Big[\big(X + \tfrac{\sqrt{2}}{2}(1+i)\big)\big(X + \tfrac{\sqrt{2}}{2}(1-i)\big)\Big] \\ &= \big[X^2 + \sqrt{2}X + 1\big]\big[X^2 - \sqrt{2}X + 1\big], \end{aligned}$$

qui est la factorisation dans $\mathbb{R}[X]$.

4.11.5 Relations coefficients-racines

Définition 4.11.3 (Polynômes symétriques élémentaires)**.** *Soit $a_1, ..., a_p \in \mathbb{K}$. On définit les polynômes symétriques élémentaires en les variables $a_1, ..., a_p$ par :*

$$\begin{aligned} s_1 &= a_1 + ... + a_p \\ s_2 &= \sum_{i_1<i_2} a_{i_1} a_{i_2} \\ &\vdots \\ s_p &= a_1 ... a_p \end{aligned}$$

Plus précisément, $\forall\ k \in \{1, ...p\}$

$$s_k = \sum_{i_1<...<i_k} a_{i_1} ... a_{i_k}$$

Théorème 4.11.5 (Relations entre les coefficients et les racines d'un polynôme)**.** *Soit $P = a_0 + a_1 X + ... + a_p X^n \in \mathbb{K}[X]$ un polynôme scindé de degré n. Soient $a_1, ..., a_n \in \mathbb{K}$ les n racines de P. On a :*

$$\forall k \in \{1, ..., n\}, \quad s_k = (-1)^k \frac{a_{n-k}}{a_n}$$

Démonstration. On démontre ces égalités en identifiant les coefficients des monômes de même degré dans l'égalité :

$$P = a_n(X - \alpha_1)...(X - \alpha_n) = a_n\Big(X^n - s_1 X^{n-1} + s_2 X^{n-2} + ... + (-1)^n s_n\Big)$$

□

Remarque 4.11.2. *En particulier,*

— *si $p = 2$, on a :*

$$P = a_2(X - \alpha_2)(X - \alpha_1) = a_2(X^2 - (\alpha_1 + \alpha_2)X + \alpha_1\alpha_2)$$

et donc :

$$s_1 = \alpha_1 + \alpha_2 = -\frac{a_1}{a_2} \quad et \quad s_2 = \alpha_1\alpha_2 = \frac{a_0}{a_2}.$$

— *Si p = 3,*

$$\begin{aligned} P &= a_3(X - \alpha_1)(X - \alpha_2)(X - \alpha_3) \\ &= a_3\Big(X^3 - (\alpha_1 + \alpha_2 + \alpha_3)X^2 + (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3)X - \alpha_1\alpha_2\alpha_3\Big) \end{aligned}$$

et :

$$s_1 = \alpha_1+\alpha_2+\alpha_3 = -\frac{a_2}{a_3}, \quad s_2 = \alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_1\alpha_3 = \frac{a_1}{a_3} \quad et \quad s_3 = \alpha_1\alpha_2\alpha_3 = -\frac{a_0}{a_3}.$$

4.12 Arithmétique dans $\mathbb{K}[X]$

4.12.1 Diviseurs communs

Proposition 4.12.1 (Propriétés de la divisibilité). — *La relation "divise" est transitive :*

$$(P,Q,R) \in \mathbb{K}[X]^3, \qquad \Big[P|Q \quad et \quad Q|R\Big] \Rightarrow P|R.$$

— *Soit $P,Q,R \in \mathbb{K}[X]$ et $U,V \in \mathbb{K}[X]$. Alors :*

$$[P|Q \quad et \quad P|R] \Rightarrow P|(UQ+VR).$$

On note pour la suite $\mathcal{D}(P,Q) = \mathcal{D}(P)\mathcal{D} \cap (Q)$ l'ensemble des diviseurs communs à P et à Q. Remarque : Si $D \in \mathcal{D}(P,Q)$, alors tout polynôme associé à D est aussi dans $\mathcal{D}(P,Q)$.

Proposition 4.12.2. *Soit P un polynôme non nul. $\mathcal{D}(P,0) = \mathcal{D}(P)$.*

Proposition 4.12.3. *Si $P = BQ + R$ alors $\mathcal{D}(P,Q) = \mathcal{D}(Q,R)$.*

Démonstration. En effet, si $D \in \mathcal{D}(P,Q)$, alors $D|Q$ et $D|P - BQ$ donc $D|Q$ et $D|R$ donc $D \in \mathcal{D}(Q,R)$ et $\mathcal{D}(P,Q) \subset \mathcal{D}(Q,R)$.
Inversement, si $D \in \mathcal{D}(Q,R)$, alors $D|Q$ et $D|BQ+R$ donc $D|Q$ et $D|P$ donc $D \in \mathcal{D}(P,Q)$ et $\mathcal{D}(Q,R) \subset \mathcal{D}(P,Q)$. □

Théorème 4.12.1. *Soient $P,Q \in \mathbb{K}[X]$,non tous les deux nuls, il existe un unique polynôme $D \in \mathbb{K}[X]$ unitaire, tel que $\mathcal{D}(P,Q) = \mathcal{D}(D)$.*

Démonstration. Unicité : Si D_1 et D_2 sont solutions alors $\mathcal{D}(D_1) = \mathcal{D}(D_2)$ donc $D_1|D_2$ et $D_2|D_1$ donc ils sont associés. Ils sont unitaires et associés donc égaux.

Existence : Quitte à échanger P et Q on peut supposer $Q \neq 0$. Posons $P_0 = P$ et $P_1 = Q$. On réalise ensuite les divisions euclidiennes suivantes tant que les restes obtenus sont non nuls (c'est l'algorithme d'Euclide) :

$$\begin{aligned}
P_0 &= P_1B_1 + P_2 \qquad avec \quad degP_2 < degP_1,\\
&\dots\\
P_{m-2} &= P_{m-1}B_{m-1} + P_m \quad avec \quad degP_m < degP_{m-1},\\
P_{m-1} &= P_mB_m + 0.
\end{aligned}$$

Ce processus s'arrête puisqu'on a une suite strictement décroissante d'entiers naturels $degP1 > degP2 > ....$ On a alors $\mathcal{D}(P,Q) = \mathcal{D}(P_0,P_1) = ... = \mathcal{D}(P_m,0) = \mathcal{D}(P_m)$ Le polynôme D unitaire associé à P_m convient. □

4.12.2 PGCD, théorèmes d'Euclide et de Bezout

Définition 4.12.1 (PGCD). *Soient P et Q deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls. L'ensemble des diviseurs communs à admet un polynôme unitaire de plus grand degré Δ noté $\Delta = P \wedge Q$. C'est le plus grand commun diviseur des polynômes P et Q.*

Démonstration. On choisit Δ unitaire pour que $\mathcal{D}(P,Q) = \mathcal{D}(\Delta)$ avec les notations du paragraphe précédent. C'est dire que tout diviseur commun à P et à Q divise Δ. Donc son degré est inférieur ou égal à celui de D. Par ailleurs l'algorithme d'euclide fournit un moyen de calculer le PGCD : on normalise le dernier reste non nul. □

Proposition 4.12.4. *$P \wedge Q = Q \wedge P$. Si un polynôme divise deux polynômes, alors il divise leur PGCD.*

Théorème 4.12.2 (Bezout). *Soient P et Q deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls, soit $\Delta = P \wedge Q$. Il existe deux polynômes U et V tels que $PU + QV = \Delta$.*

Démonstration. Par récurrence sur $n = \min\{degP, degQ\}$.
Si $n = -\infty$ ou $n = 0$ la propriété est claire. Pour fixer les idées $degP \geq degQ = n + 1$. On écrit la division euclidienne de P par Q, $P = BQ + R$ avec $degR \leq n$. En utilisant la propriété de récurrence, il existe deux polynômes U_1 et $V1$ de $\mathbb{K}[X]$ tels que $\Delta = U_1Q + V_1R$ avec $\Delta = Q \wedge R$. Or $\Delta = P \wedge Q$ d'une part, et d'autre part $\Delta = U_1Q + V_1(P - BQ) = V_1P + (U_1 - BV_1)Q$. D'où le résultat en penant $U = V_1$ et $V = U_1 - BV_1$. □

Proposition 4.12.5. *Si C est unitaire alors $AC \wedge BC = C(A \wedge B)$.*

Démonstration. Posons $\Delta = AC \wedge BC$ et $D = A \wedge B$. On a $DC|AC$ et $DC|BC$ donc $DC|\Delta$. Dans l'autre sens $D = AU + BV$ donc $DC = ACU + BCV$ d'où $\Delta|DC$. □

Exercice 9. *Déterminer le pgcd des polynomes $A = X^3 + X^2 + 2$ et $B = X^2 + 1$. Trouver ensuite un couple (U, V) tel que $AU + BV = d$.*

Exercice 10. *On considère deux entiers non nuls $(a, b) \in \mathbb{N}^2$. On note $d = a \wedge b$ leur PGCD. Montrer, en utilisant l'algorithme d'Euclide que*

$$(X^a - 1) \wedge (X^b - 1) = X^d - 1.$$

4.12.3 Polynômes premiers entre eux

Définition 4.12.2 (Polynômes premiers entre eux). *Soient P et Q deux polynômes de $\mathbb{K}[X]$. On dit que P et Q sont **premiers entre eux** si leur PGCD est égal à 1.*

Proposition 4.12.6 (Bezout). *Soient P et Q deux polynômes de $\mathbb{K}[X]$. P et Q sont premiers entre eux si et seulement s'il existe deux polynômes U et V de $\mathbb{K}[X]$ tels que*

$$PU + QV = 1.$$

Démonstration. Dans un sens c'est le théorème de Bezout déjà vu. Dans l'autre sens, comme $PU + QV = 1$ on en déduit que $P \wedge Q$ divise 1. Il n'y a qu'un seul polynôme unitaire qui divise 1, c'est 1 lui-même. □

Proposition 4.12.7 (Lemme de Gauss). *Si P, Q et R sont trois polynômes vérifiant*

1. $P|QR$
2. $P \wedge Q = 1$.

alors $P|R$.

Démonstration. La condition $P \wedge Q = 1$ permet d'écrire une relation de Bezout : $PU + QV = 1$ qui multipliée par R donne $PUR + QRV = R$. Mainteant la condition $P|QR$ assure l'existence d'un polynôme A tel que $AP = QR$ et donc $PUR + APV = P(UR + AV) = R$ et donc P divise R. □

Proposition 4.12.8. *Soient P et Q deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls et soit $D = P \wedge Q$. $\frac{P}{D}$ et $\frac{Q}{D}$ sont des polynômes et ils sont premiers entre eux.*

Démonstration. On écrit $P = P_1 D$ et $Q = Q_1 D$. On a $\frac{P}{D} = P_1$ et $\frac{Q}{D} = Q_1$. De plus

$$D = P \wedge Q = P_1 D \wedge Q_1 D = D(P_1 \wedge Q_1)$$

puisque D est unitaire. Ceci établit le résultat $(\mathbb{K}[X] estintgre)$. □

Proposition 4.12.9. *Si un polynôme P est premier avec Q_1 et avec Q_2 alors il est premier avec $Q_1 Q_2$.*

Démonstration. On écrit une relation de Bezout pour (P, Q_1) : $PU_1 + Q_1 V_1 = 1$ puis une autre pour (P, Q_2) : $PU_2 + Q_2 V_2 = 1$. On effectue le produit de ces deux égalités : $P^2 U_1 U_2 + PU_1 Q_2 V_2 + PU_2 Q_1 V_1 + Q_1 Q_2 U_1 U_2 = 1$ soit $P(PU_1 U_2 + U_1 Q_2 V_2 + U_2 Q_1 V_1) + Q_1 Q_2 (U_1 U_2) = 1$, ce qui donne le résultat.

Autre preuve : Soit D un diviseur commun à P et à $Q_1 Q_2$. D est premier avec Q_1, En effet, soit d un diviseur commun à Q_1 et D. Comme $d|D$ et $D|P$, on a $d|P$ et donc d diviseur commun à P et Q donc $degd = 0$. Maintenant d'après le lemme de Gauss, $D|Q_1 Q_2$ et $D \wedge Q_1 = 1$ donc $D|Q_2$, donc $D|P \wedge Q_2$, ce qu'il fallait démontrer. □

Proposition 4.12.10. *Si un polynôme P est premier avec Q_1, Q_2, ..., Q_m alors il est premier avec leur produit.*

Démonstration. Par une récurrence sans malice. □

Corollaire 4.12.1. *Soient P et Q deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls et premiers entre eux. Alors*

- *Pour tout entier m, P est premier avec Q^m.*
- *Pour tous entiers m et n, P_n est premier avec Q^m.*

4.12.4 PPCM

Proposition 4.12.11. *Soient P et Q deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls et soit $D = P \wedge Q$. à P et à Q. $\frac{PQ}{D}$ est un polynôme, multiple commun*

Démonstration. On écrit $P = P_1 D$ et $Q = Q_1 D$. On a $\frac{PQ}{D} = P_1 Q = P Q_1$ ce qui établit le résultat. □

Proposition 4.12.12. *Soient P et Q deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls et soit $D = P \wedge Q$. Tout multiple commun à P et à Q est multiple de $\frac{PQ}{D}$.*

Démonstration. Soit M un multiple commun à P et à Q. On écrit $M = AP = AP_1D = BQ = BQ_1D$. Après simplification par D on a $AP_1 = BQ_1$ avec P_1 et Q_1 premiers entre eux. Maintenant P_1 divise $BQ_1 et P_1 \wedge Q_1$. Donc d'après le lemme de Gauss, $P_1|B$.

Autrement dit, on peut écrire $B = B_1 P_1$. Donc $M = BQ_1D = B_1P_1Q_1D = B_1\frac{PQ}{D}$. Ce qu'il fallait démontrer. □

Définition 4.12.3 (PPCM)**.** *Soient P et Q deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls.*
L'ensemble des polynômes de $\mathbb{K}[X]$ multiples communs de P et Q admet un polynôme unitaire de plus petit degré μ noté : $\mu = P \vee Q$. C'est le plus petit commun multiple des polynômes P et Q.

Proposition 4.12.13. *Soient P et Q deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls. $(P \wedge Q) \times (P \vee Q)$ est associé à PQ.*

4.12.5 Polynômes irréductibles

Proposition 4.12.14. *Soient P et Q deux polynômes irréductibles de $\mathbb{K}[X]$. P et Q sont soit associés, soit premiers enre eux.*

Démonstration. Soit $D = P \wedge Q$. Comme $D|P$ et que P est irréductible, alors $D = 1$ ou D est associé à P. Dans le deuxième cas, comme $D|Q$ et que Q est irréductible, alors $D = 1$ (impossible) ou D est associé à Q. Donc P est associé à Q. □

Théorème **4.12.3** (Décomposition en produit de facteurs irréductibles.)**.** *Soit P un polynômes de $\mathbb{K}[X]$ non nul. Il existe $\alpha \in \mathbb{K}^*$, il existe $m \in \mathbb{N}$, m polynômes $P_1, \ \ldots \ , \ P_m$ unitaires et irréductibles tels que*

$$P = \alpha \prod_{k=1}^{m} P_k.$$

α, m sont uniques et les P_k sont uniques à l'ordre près.

Chapitre 5

EXERCICES

Exercice 11. *Vrai ou faux ?*

a) 0 est élément neutre de la soustraction dans $\mathbb{Z}$.

b) Tout élément regulier d'un monoïde est symétrisable.

c) Tous les éléments d'un groupe sont réguliers.

d) $\mathbb{N}$ *est un sous-groupe de* $(\mathbb{Z}, +)$

e) Le noyau d'un morphisme de groupe est un singleton.

f) Tous les éléments non nuls d'un anneau sont réguliers pour les deux opérations.

g) L'ensemble des éléments inversibles d'un anneau est un groupe pour l'addition.

h) Un diviseur de zéro d'un anneau n'est jamais inversible.

i) Tout corps commutatif est un anneau intègre.

Exercice 12. *Sur l'ensemble* $\mathbb{Z}$*, on considère la loi "*$\bigstar$*" définie par :*

$$p \bigstar q = p + q + pq.$$

1 *Montrer que "*$\bigstar$*" est une loi de composition interne commutative et associative.*

2 *Montrer que la loi* $\bigstar$ *possède un élément neutre à gauche* e_1.

3 *La loi "*$\bigstar$*" possède elle un élément neutre à droite ?*

4 *La loi "*$\bigstar$*" possède elle un élément neutre ?*

5 *Quels sont les éléments symétrisables à gauche ? symétrisables à droite ? symétrisables ?*

6 *Est-ce que* $(\mathbb{Z}, \bigstar)$ *est un groupe ?*

7 *L'ensemble* $\mathbb{R}\backslash\{-1\}$ *muni de la loi "*$\bigstar$*" définie par*

$$\forall a, b \in \mathbb{R}, \quad a \bigstar b = a + b + ab$$

est-il un groupe ?

8 *Sur $\mathbb{R}$ déjà muni de la multiplication et de l'addition, on définit la loi "$\bigstar$" La loi "$\bigstar$" est-elle distributive par rapport à la multiplication ? Est-elle distributive par rapport à l'addition ?*

Exercice 13. *Soit $A = \{e,\ \alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon\}$ muni de la loi $*$ un groupe. Compléter sa table. On ne demande pas de justification. e est l'élément neutre de $*$.*

$*$	e	α	β	γ	δ	ε
e						
α			δ			γ
β		ε		δ	γ	
γ		δ				
δ			α		ε	e
ε		β		α		

Exercice 14. *Soient les quatre applications de $\mathbb{C}^*$ dans $\mathbb{C}^*$:*

$$f_1(z) = z, \qquad f_2(z) = \frac{1}{z}, \qquad f_3(z) = -z, \qquad f_4(z) = -\frac{1}{z}.$$

Montrer que $G = \{f_1, f_2, f_3, f_4\}$ est un groupe pour la loi " $\circ$ ".

Exercice 15. *a) Soient $(G, .)$ un groupe, E un ensemble, $f : E \to G$ une application bijective. On note $*$ la loi interne dans E définie par :*

$$\forall x, y \in E, \quad x * y = f^{-1}(f(x)f(y)),$$

où f^{-1} désigne la bijection réciproque de f.
Démontrer que $(E, *)$ est un groupe et que f est un isomorphisme de groupes de $(E, *)$ dans (G, Δ). On dit qu'il y a transfert de la structure de groupe, du groupe (G, Δ) sur $(E, *)$.

b) Exemple : On note $*$ la loi interne dans $\mathbb{R}$ définie par :

$$\forall (x, y) \in \mathbb{R}^2, \quad x * y = \sqrt[3]{x^3 + y^3}.$$

Montrer que (R,) est un groupe, isomorphe à (R,+).*

Exercice 16. *Soit x un élément d'un anneau intègre A . Démontrez que si x est inversible à droite, alors x est inversible à gauche.*

Exercice 17. *Soit $(A, +, .)$ un anneau commutatif. On dit qu'un élément x est nilpotent s'il existe $n \in \mathbb{N}$ tel que $x^n = 0$.*

1 *Montrez que, si x est nilpotent, alors $1 - x$ est inversible.*

2 *Montrez que, si x et y sont nilpotents, alors xy et $x + y$ le sont aussi.*

Exercice 18. *Soit $(A, +, .)$ un anneau. On suppose : $\forall x \in A$, $x^2 = x$.*

a) Montrer : $\forall x \in A$, $2x = 0$.

b) Établir que A est commutatif.

Exercice 19. *Montrez que le corps des rationnels $\mathbb{Q}$ n'admet pas d'autre sous-corps que lui-même.*

Exercice 20. *On note A l'ensemble de réels suivant :*

$$A = \{m + n\sqrt{6},\ m, n \in \mathbb{Z}\}.$$

1 *Montrer que $(A, +, .)$ (ensemble A muni de l'addition et de la multiplication des réels), est un sous-anneau de $(\mathbb{R}, +, .)$.*

2 *On considère l'application f, de A dans lui-même, qui à $m + n\sqrt{6}$ associe : $f(m + n\sqrt{6}) = m - n\sqrt{6}$. Montrer que f est un automorphisme de l'anneau $(A, +, .)$.*

3 *Pour tout $x \in A$, on pose $N(x) = xf(x)$. Montrer que N est une application de A dans $\mathbb{Z}$, qui est un morphisme pour la multiplication.*

4 *Démontrer que x est un élément inversible de A si et seulement si $N(x) = \pm 1$.*

5 *Vérifier que $5 + 2\sqrt{6}$ est inversible dans A et calculer son inverse.*

Exercice 21. *Sur $\mathbb{Z}^2$, on définit deux lois " $+$ " et " $*$ " par : $\forall (a, b), (c, d) \in \mathbb{Z}^2$,*

$$(a, b) + (c, d) = (a + c, b + d) \qquad et \qquad (a, b) * (c, d) = (ac, ad + bc).$$

(a) Montrer que $(\mathbb{Z}^2, +, *)$ est un anneau commutatif.

(b) Montrer que $A = \{(a, 0), a \in \mathbb{Z}\}$ est un sous-anneau de $(\mathbb{Z}^2, +, *)$.

Exercice 22. *Montrer que $\mathbb{Z}$ n'est pas un corps pour les lois usuelles.*

Exercice 23. *Vrai ou faux ?*

a) Étant donnés cinq nombres entiers consécutifs, on trouve toujours parmi eux au moins deux multiples de 2.

b) 60 a moins de diviseurs positifs que 90.

c) Si un nombre est divisible par 10 et par 12, alors il est divisible par 15.

d) Si un nombre divise le produit de deux entiers, alors il divise au moins un de ces deux entiers.

e) L'entier d est un multiple de $PGCD(a, b)$ si et seulement si il existe un couple d'entiers (u, v), tel que $au + bv = d$.

f) Si un entier est congru à 4 modulo 6 alors toutes ses puissances sont aussi congrues à 4 modulo 6.

g) La puissance quatrième d'un entier quelconque est toujours congrue à 1 modulo 5.

h) Aucun entier n'est tel que son carré soit congru à 2 modulo 5.

i) Si $PGCD(a,b)$ divise d, alors il existe un couple d'entiers (u,v) unique, tel que $au+bv=d$.

Exercice 24. **1** *Trouver le nombre d'entiers relatifs qui, dans la division euclidienne par 23, ont un quotient égal au reste.*

2 *Trouver deux entiers positifs a et b sachant que $a<4000$ et que la division euclidienne de a par b donne un quotient de 82 et un reste de 47.*

3 *Démontrez que 143 et 100 sont premiers entre eux.*

4 *Dans une division euclidienne entre entiers naturels quels peuvent être le diviseur et le quotient lorsque le dividende est 320 et le reste 39 ?*

5 *Écrire 13 en base 2, en base 3, puis en base 7*

6 *Soit a et b deux entiers relatifs et d leur P.G.C.D. Déterminer le P.G.C.D. de A = 15a+4b et B = 11a+3b.*

Exercice 25. *On considère les couples d'entiers (a,b) suivants.*

$a)$ $a=60,$	$b=84$	$b)$ $a=360,$	$b=240$	$c)$ $a=160,$	$b=171$
$d)$ $a=360,$	$b=345$	$e)$ $a=325,$	$b=520$	$f)$ $a=720,$	$b=252$
$g)$ $a=955,$	$b=183$	$h)$ $a=1665,$	$b=1035$	$i)$ $a=18480,$	$b=9828$

Pour chacun de ces couples :

1 *Calculer $PGCD(a,b)$ par l'algorithme d'Euclide.*

2 *En déduire une identité de Bézout.*

3 *Calculer $PPMC(a,b)$.*

4 *Déterminer l'ensemble des couples (a,b) d'entiers relatifs tels que : $au+bv=PGCD(a,b)$*

5 *Donner la décomposition en facteurs premiers de a et b.*

6 *En déduire la décomposition en facteurs premiers de $PGCD(a,b)$ et $PPMC(a,b)$, et retrouver les résultats des questions 1 et 3.*

Exercice 26. **1** *On considère dans $\mathbb{Z}^2$ l'équation :*

$$(E_1)\ :\qquad 11x+8y=79$$

a *Montrer que si* (x, y) *est solution de* (E_1) *alors* $y \equiv 3[11]$

b *Résoudre alors l'équation* (E_1)

2 *Soit dans* $\mathbb{Z}^2$ *l'équation :*

$$(E_2): \qquad 3y + 11z = 372.$$

a *Montrer que si* (y, z) *est solution de* (E_2) *alorsz* $z \equiv 0[3]$

b *Résoudre alors l'équation* (E_2)

3 *Résoudre dans* $\mathbb{Z}^2$*, l'équation :* $(E_3): 3x - 8z = -249$.

4 *Le prix total de 41 pièces détachées, réparties en trois lots, est de 480 f cfa. Le prix d'une pièce du premier lot est de 48 dinars. Le prix d'une pièce du deuxième lot est de 36 f cfa. Le prix d'une pièce du troisième lot est de 4 f cfa.*
Déterminer le nombre de pièces de chaque lot.

Exercice 27. **1** *Résoudre dans* $\mathbb{Z}^2$ *l'équation* $3u - 8v = 6$.

2 *En déduire l'ensemble des solutions dans* $\mathbb{Z}$ *du système* $\begin{cases} x \equiv 1[3] \\ x \equiv 7[8] \end{cases}$

Exercice 28. *Vrai ou faux ?*

a) Le degré de la somme de deux polynômes est le plus grand des deux degrés.

b) Le degré du produit de deux polynômes est la somme des deux degrés.

c) Les polynômes A et B sont premiers entre eux si et seulement si aucun des deux ne divise l'autre.

d) S'il existe des polynômes U et V tels que $AU + BV = D$*, alors le polynôme D est le P.G.C.D. des polynômes A et B.*

e) Si un polynôme est divisible par deux polynômes, il est divisible par leur produit.

f) Si un polynôme est premier avec deux polynômes, il est premier avec leur produit.

g) Tout polynôme non constant qui n'a pas de racines est irréductible.

h) Tout polynôme de degré n de $\mathbb{C}[X]$ *possède n racines distinctes.*

i) Le produit des racines d'un polynôme scindé unitaire de degré n est $(-1)^n P(0)$.

Exercice 29. **1** *Montrer qu'il existe une unique suite de polynomes* $(P_n)_{n\in\mathbb{N}}$ *telle que :*

$$P_0 = 1, \quad P_1 = X \quad et \quad \forall n \in \mathbb{N}, \quad P_{n+2} = 2XP_{n+1} - P_n.$$

2 *Calculer les polynomes* (P_n) *jusqu'a* $n = 10$.

3 *Montrer que* $\forall n \in \mathbb{N}$, $\exists x \in \mathbb{R}$ *tel que* $\cos nx = P_n(cosx)$.

4 *En deduire les racines du polynome* P_n.

Exercice 30. *Décomposer en produit de polynômes irréductibles dans* $\mathbb{C}[X]$ *puis dans* $\mathbb{R}[X]$ *les polynômes suivants :*

1 $P_l = X^4 - l$

2 $P_2 = X^S - l$

3 $P_3 = X^4 + X^2 + l$

4 $P_4 = X^6 + l$

5 $P_S = (X^2 - X + l)^2 + l$

6 $P_6 = X^6 - X^S + X^4 - X^3 + X^2 - X + l$

7 $P_7 = (X^2 + l)^2 + (X^2 - X - l)^2$

8 $P_8 = X^8 + X^4 + l$

Exercice 31. *Décomposer les polynômes suivants :*

1 $X^4 + X^2 + l$

2 $X^8 + X^4 + l$

3 $X^6 + l$

en produits de polynômes irréductibles sur $\mathbb{R}[X]$.

Exercice 32. *Soient* x_1, x_2 *et* x_3 *les trois racines complexes du polynôme* $X^3 + pX + q$.

1 *Trouver le polynôme normalisé du troisième degré dont les racines sont* $x_1 + x_2$, $x_2 + x_3$ *et* $x_1 + x_3$.

2 *Trouver le polynôme normalisé du troisième degré dont les racines sont* x_1x_2, x_2x_3 *et* x_1x_3.

Exercice 33. *Effectuer la division euclidienne de* A *par* B *dans les cas suivants :*

1 $A = X^3 + X^2 - 2X + 3$ *et* $B = X^2 + 2X - 1$

2 $A = X^4 + 2X^2 - 3X^3 - 2X + 4$ *et* $B = X^2 + 1$

3 $A = X^2 + IX + 3$ *et* $B = X + 2i$

4 $A = X$ *et* $B = X^2 + 1$

5 $A = 2X^2 + 4X - 1$ *et* $B = X^2 + 3X - 1$

6 $A = X^2 - 1$ *et* $B = X^3 + 2X - 1$

7 $A = X^8 - 1$ *par* $B = X^3 - 1$.

Exercice 34. *Soit* $P = X^5 + X^4 + 2X^3 + 2X^2 + X + 1$

1 *Calculer le PGCD de* P *et* P'.

2 *Quelles sont les racines communes à P et P' ?*

3 *Quelles sont les racines multiples de P dans $\mathbb{C}$?*

4 *Montrer que $(X^2+1)^2$ divise P.*

5 *Factoriser P dans $\mathbb{R}[X]$.*

Exercice 35. *Soit $P = X^4 - 5X^3 + 9X^2 - 15X + 18$ un polynôme de $\mathbb{C}[X]$. On note α, β, γ et δ ses racines.*

1 *Trouver les racines dans $\mathbb{C}$ du polynôme P sachant qu'il possède deux racines dont le produit est 6.*

2 *En déduire la factorisation de P dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$.*

Exercice 36.

Soit $*$ la loi définie sur $\mathbb{R}$ par

$$\forall (x,y) \in \mathbb{R}^2 \qquad x * y = x \times y + (x^2-1) \times (y^2-1)$$

où $x^2 = x \times x$ et $y^2 = y \times y$ avec $+$ et $\times$ les opérations usuelles sur $\mathbb{R}$.

1 *La loi $*$ est-elle associative sur $\mathbb{R}$? Commutative sur $\mathbb{R}$?*

2 *Vérifier que $\mathbb{R}$ possède un élément neutre pour la loi $*$.*

3 *La loi $*$ confère-t-elle à $\mathbb{R}$ une structure de groupe ?*

4 *Calculer le(s) symétrique(s) du réel 2 pour la loi $*$.*

5 *Résoudre les équations suivantes : $2 * x = 2$, $2 * x = 5$.*

Exercice 37.

On définit sur $\mathbb{R}$ les lois $*$ et $\top$ par

$$x * y = ax + by - 1 \quad (a \in \mathbb{R}, b \in \mathbb{R}), \qquad x \top y = x + y - x \times y$$

avec $+$ et $\times$ les opérations usuelles sur $\mathbb{R}$

1 **a** *Déterminer des conditions sur a et b pour que $*$ soit commutative dans $\mathbb{R}$.*

b *Déterminer des conditions sur a et b pour que $*$ soit associative dans $\mathbb{R}$.*

2 *On pose $a = b = 1$.*

a *Montrer que $(\mathbb{R}, *)$ est un groupe commutatif.*

b *Montrer que la loi $\top$ est distributive par rappport à la loi $*$.*

c *$(\mathbb{R}, *, \top)$ est il un corps commutatif ?*

Exercice 38.

1 *Résoudre dans* $\mathbb{Z}^2$ *l'équation* $3x - 8y = 6$.

2 *En déduire l'ensemble des solutions dans* $\mathbb{Z}$ *du système* $\begin{cases} x \equiv 1 \ [3] \\ x \equiv 7 \ [8] \end{cases}$

Exercice 39.

1 *Soit* $P = a_o + a_1 X + \cdots + a_n X^n$ *un polynôme à coefficients entiers. Montrer que si P admet une racine rationnelle* $\frac{p}{q}$ *avec* p *et* q *entiers et* $pgcd(p, q) = 1$, *alors* p *divise* a_0 *et* q *divise* a_n.

2 *On considère les polynômes* $A = X^4 + X^3 + X + 1$ *et* $B = X^3 + X^2 + X + 1$ *de* $\mathbb{R}[X]$.

a *Calculer* $D = pgcd(A, B)$.

b *Trouver des polynômes* U *et* V *de* $\mathbb{R}[X]$ *tels que* $UA + VB = D$.

c *Décomposer* A *et* B *en produit de facteurs irréductibles dans* $\mathbb{R}[X]$ *et dans* $\mathbb{C}[X]$.

Bibliographie

[1] **A. Bodin** : *Algèbre*. Exo 7 (2016).

[2] **A. Soyeur, F. Capaces, E. Vieillard-Baron** : *Cours de Mathématiques Sup MPSI PCSI PTSI TSI* . sesamath.net (2011).

[3] **C. Deschamps, A. Warusfel, F. Moulin, J. François Ruaud, A. AAiquel, J-C Sifre** : *Mathématiques TOUT-EN-UN • I^e année : cours exercices corrigés MPSI-PCSI*. Dunod, Paris, (2003).

[4] **D. Fredon** : *Mathématiques Résumé du cours en fiches MPSI - MP*. Dunod, Paris, (2010).

[5] **E. Ramis, C. Deschamps, J. Odoux** : *Cours de Mathématiques Spéciales Algèbre*. Masson (1993).

[6] **J. Dixmler** : *Cours de Mathématiques du premier cycle* 1^e *année*, Gauthier-villars, (1976).

[7] **M. Allano Chevalier, X. Oudot** : *Maths MPSI*. Hachette, (2008).

[8] **N. Bourbaki** : *Éléments de Mathématique : Algèbre*. Springer (1970).

[9] **P. Bornsztein, X. Caruso, P. Nolin, M. Tibouchi** : *Cours d'arithmétique*. (2004).