ALGEBRE ALGORITHMIQUE
Licence L3 Mathématiques
Chapitres IV, V et VI
Année Universitaire 2022-2023

Table des matières

IV Arithmétique Modulaire, Fonction Indicatrice d'Euler et Théorème des restes Chinois **3**

IV.1 Les ensembles $\mathbb{Z}/n\mathbb{Z}$ 3

IV.2 Les anneaux $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ 5

IV.3 La fonction indicatrice d'Euler 9

IV.4 Le théorème des restes chinois 10

IV.5 Ordre d'un élément dans les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{Z}/n\mathbb{Z}^{\times}, \times)$ 14

Exercices sur le chapitre IV **19**

V Polynômes **21**

V.1 Notations, premières propriétés et exemples 21

V.2 Division euclidienne 24

V.3 Polynômes irréductibles 25

Exercices sur le chapitre V **29**

VI Le théorème fondamental de l'algèbre et ses conséquences **32**

VI.1 Racines d'un polynôme 32

VI.2 Les nombres complexes 33

VI.3 Le théorème fondamental de l'algèbre et ses conséquences 33

VI.4 Cas des polynômes à coefficients réels 34

Exercices sur le chapitre VI **36**

Chapitre IV

Arithmétique Modulaire, Fonction Indicatrice d'Euler et Théorème des restes Chinois

IV.1 Les ensembles $\mathbb{Z}/n\mathbb{Z}$

Nous supposons connus les axiomes de $\mathbb{Z}$, en particulier, toute partie finie non vide majorée de $\mathbb{Z}$ admet un plus grand élément.

Théorème IV.1.1 (Division euclidienne dans $\mathbb{Z}$)**.** *Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$. Alors, il existe un unique couple $(q, r) \in \mathbb{Z}$ tel que*

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

Démonstration. Unicité : Si $a = bq + r = bq' + r$ avec $0 \leqslant r, r' < |b|$, alors $b(q - q') = r' - r$. Ceci entraîne $|b||q' - q| = |r' - r|$. Or $0 \leqslant r' < |b|$ implique $-|b| < -r' \leqslant 0$, de sorte que $-|b| < r' - r < |b|$. Ainsi $|r' - r| < |b|$; si $r' - r \neq 0$, on aurait $|b||q' - q| = |r' - r| < |b|$ et aussi $|b||q' - q| \geqslant |b|$, ce qui est impossible. D'où $|r' - r| = 0$, i.e. $r = r'$; on en déduit que $q = q'$.
Existence : Supposons $b > 0$. Soit $A = \{n \in \mathbb{Z} \mid nb \leqslant a\}$. Alors A n'est pas vide (en effet, si $a \geqslant 0$, alors $0 \in A$ et si $a < 0$, alors $a \in A$), et majoré par $\max(0, a)$ (car $n \leqslant \frac{1}{b}\max(0, a) \leqslant \max(0, a)$). Donc A admet un plus grand élément que l'on note q_A. Soit $r = a - q_A b$. On a $q_A \in A$, ce qui implique que $q_A b \leqslant a$, d'où $r \geqslant 0$ et $q_A + 1$ n'appartient pas à A. On en déduit que $(q_A + 1)b > a$, ce qui implique que $q_A b + b > a$ ou $b > a - q_A b$, donc $r < b = |b|$. On a donc montré que $0 \leqslant r < |b|$ et on a bien $a = q_A b + r$.
Si $b < 0$, alors $-b > 0$ et par le résultat ci-dessus, il existe $q, r \in \mathbb{Z}$ tels que $a = (-b)q + r$ avec $0 \leqslant r < |b|$. D'où $a = b(-q) + r$ et le couple $(-q, r)$ convient. □

Notations. Les entiers q et r du Théorème IV.1.1 sont respectivement appelés le quotient, noté $a \operatorname{div} b$ et le reste, note $a \mod b$, de la division euclidienne de a par b

Exemples IV.1.2. (1) On a $-9 = (-7)(2) + 5$, donc $(-9)\operatorname{div}(-7) = 2$ et $(-9) \mod (-7) = 5$.

Notation. Pour $n \in \mathbb{N}$, nous notons par $n\,\mathbb{Z}$ l'ensemble des multiples de n dans $\mathbb{Z}$:

$$n\,\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\} = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}.$$

Exemples IV.1.3. (1) On a $0\,\mathbb{Z} = \{0\}$,
(2) $1\,\mathbb{Z} = \mathbb{Z}$,
(3) $2\,\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$.

Définition IV.1.4 (Congruence)**.** Soit $n \geqslant 1$ un entier. La relation de *congruence modulo* n est définie pour tout $b \in \mathbb{Z}$ par

$$a \equiv b \pmod{n} \iff a - b \in n\,\mathbb{Z},$$

ce qui équivaut aux deux propriétés suivantes :
(1) $\Big(\exists k \in \mathbb{Z}\Big)\ \Big[a - b = kn\Big]$,
(2) a et b ont même reste par la division euclidienne par n.

Il nous faut montrer que les deux équations (1) et (2) ci-dessus sont équivalentes à celle de la définition de $\equiv$. La première équation est équivalente à la définition de $\equiv$ d'après la définition de $n\,\mathbb{Z}$. Supposons que a et b ont le même reste par la division euclidienne par n : $a = nq + r$ et $b = nu + r$ avec $0 \leqslant r < n$. Alors $a - b = n(q - u) \in n\,\mathbb{Z}$, donc $a \equiv b \pmod{n}$. Réciproquement, supposons que $a \equiv b \pmod{n}$. Alors, il existe $k \in \mathbb{N}$ tel que $a = b + kn$. En effectuant la division euclidienne de b par n, nous avons $b = nq + r$ avec $0 \leqslant r < n$. Alors $a = n(q + k) + r$. Par l'unicité du quotient et du reste, r est aussi le reste de a par la division euclidienne par n. Donc a et b ont même reste par la division euclidienne par n.

Exemples IV.1.5. (1) Pour $n = 1$, tout entier relatif a est congru à tout entier relatif b modulo 1, car $a - b \in 1\,\mathbb{Z} = \mathbb{Z}$. En fait, tout entier relatif est divisible par 1, donc son reste est nul.
(2) Pour $n = 2$, tout entier pair est congru à 0 modulo 2 et tout entier impair est congru à 1 modulo 2.
(3) On a $4 \equiv 14 \pmod{5}$: $4 \bmod 5 = 4 = (14 \bmod 5)$. On a aussi $14 - 4 = 10 = 2 \cdot 5 \in 5\,\mathbb{Z}$.

Théorème IV.1.6. *Soit $n \geqslant 1$ un entier. La relation de congruence modulo n est une relation d'équivalence.*

Démonstration. Refléxivité ; On a $a - a = 0 \in n\,\mathbb{Z}$ donc $a \equiv a \pmod{n}$.
Symétrie : Supposons que $a \equiv b \pmod{n}$: il existe $k \in \mathbb{Z}$ tel que $a - b = kn$. Alors $b - a = (-k)n$, avec $-k \in \mathbb{Z}$, donc on a aussi $b \equiv a \pmod{n}$.
Transitivité : Supposons que $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$: il existe $k, l \in \mathbb{Z}$ tels que $a - b = kn$ et $b - c = ln$. Alors $a - c = (a - b) + (b - c) = kn + ln = (k + l)n$ avec $k + l \in \mathbb{Z}$, donc $a \equiv c \pmod{n}$. □

Définition IV.1.7 (Classes)**.** Soit $n \in \mathbb{N}^*$. (1) Pour $a \in \mathbb{Z}$, la classe d'équivalence de a pour la relation de congruence modulo n (ou simplement la classe de a) est

$$\begin{aligned}\overline{a} &= \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\} \\ &= \{a + kn \mid k \in \mathbb{Z}\} \\ &= \{a, a \pm n, a \pm 2n, a \pm 3n, \ldots\} \subset \mathbb{Z},\end{aligned}$$

(2) L'ensemble-quotient de $\mathbb{Z}$ par la relation de congruence modulo n est

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{a} \mid a \in \mathbb{Z}\}.$$

C'est l'ensemble des classes des éléments de $\mathbb{Z}$.

Notation. L'ensemble $\{a + kn \mid k \in \mathbb{Z}\}$ est noté par $a + n\mathbb{Z}$. Donc $\overline{a} = a + n\mathbb{Z}$.
La proposition suivante permet de trouver plus facilement la classe d'un élément de $\mathbb{Z}$ et l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$:

Proposition IV.1.8. *Soit $n \geqslant 1$ un entier.*
(1) *Pour $a \in \mathbb{Z}$, on a $\overline{a} = \overline{a \mod n}$.*
(2) *On a $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \ldots, \overline{n-1}\}$.*

Démonstration. (1) Puisque $a = (a \operatorname{div} n)n + a \bmod n$, on a $a - a \bmod n = (a \operatorname{div} n)n \in n\mathbb{Z}$, donc $a \equiv a \bmod n \pmod{n}$. Ainsi, a et $a \bmod n$ ont même classe.
(2) Les restes modulo n des éléments de $\mathbb{Z}$ sont 0, …, $n-1$. Donc les classes de ces éléments donnent les éléments de $\mathbb{Z}/n\mathbb{Z}$. □

Exemples IV.1.9. (1) On a $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\} = \{\mathbb{Z}\}$.
(2) On a $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$, avec $\overline{0} = 2\mathbb{Z}, \overline{1} = 1 + 2\mathbb{Z}$.
(3) On a $\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$, avec $\overline{r} = r + 6\mathbb{Z}$ pour $r = 0, \ldots, 5$.

IV.2 Les anneaux $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Dans cette section, n désigne un entier $\geqslant 2$ (les cas $\mathbb{Z}/0\mathbb{Z} = \{0\}$ et $\mathbb{Z}/1\mathbb{Z} = \{\mathbb{Z}\}$ correspondant à $n = 0$ et $n = 1$ ne sont pas intéressants).
Dans $\mathbb{Z}/n\mathbb{Z}$, on définit l'*addition* et la *multiplication modulo* $n$par

$$\overline{a} + \overline{b} = \overline{(a+b)} \quad \text{et} \quad \overline{a}\overline{b} = \overline{ab}$$

pour tout $a, b \in \mathbb{Z}$. Notons que ces opérations sont bien définies car $a + b$ et $ab \in \mathbb{Z}$, donc les classes correspondantes sont bien définies.

Théorème IV.2.1. *Soit $n \geqslant 1$ un entier. Alors $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.*

Démonstration. Il nous faut démontrer que
(I) $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif,

(II) La muitiplication est

- associative,
- distributive par rapport à l'addition,
- commutative
- il existe un élément neutre pour la multiplication.

(I) $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif :

• Associativite de $+$: on a, pour $a, b, c \in \mathbb{Z}$,

$$\begin{aligned}
\bar{a} + (\bar{b} + \bar{c}) &= \bar{a} + \overline{b+c} \\
&= \overline{a + (b+c)} \quad \text{(définition de l'addition des classes } \bar{a} \text{ et } \overline{b+c}\text{)} \\
&= \overline{(a+b)+c} \quad \text{(associativité de l'addition dans } \mathbb{Z}\text{)} \\
&= \overline{a+b} + \bar{c} \quad \text{(définition de la classe de la somme } (a+b)+c\text{)} \\
&= (\bar{a} + \bar{b}) + \bar{c} \quad \text{(définition de la classe de la some } a+b\text{)}
\end{aligned}$$

d'où l'associativité.

• Commutativité de $+$: on a, pour $a, \in \mathbb{Z}$:

$$\begin{aligned}
\bar{a} + \bar{b} &= \overline{a+b} \quad \text{(définition de la somme de classes)} \\
&= \overline{b+a} \quad \text{(commutativité de l'addition dans } \mathbb{Z}\text{)} \\
&= \bar{a} + \bar{b} \quad \text{(définition de la classe de la somme)}
\end{aligned}$$

d'où la commutativité.

• 0 est neutre : on a, pour $a \in \mathbb{Z}, \bar{0} + \bar{a} = \overline{0+a} = \bar{a}$.

• Si $a \in \mathbb{Z}$, alors l'opposé de $\bar{a}$ est $\overline{n-a}$. En effet

$$\overline{n-a} + \bar{a} = \overline{(n-a)+a} = \overline{n} = \bar{0}.$$

Pour le groupe de propriétés (II), les démonstrations s'effectuent de façon analogue ; l'élément neutre pour la multiplication est $\bar{1}$.

Théorème IV.2.2 (Eléments inversibles dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$)**.** *Un élément $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si l'entier a est premier avec n.*

Démonstration. $(\Longrightarrow)$: Supposons que $\bar{a}$ est inversible dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$. Alors il existe $\bar{b} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\bar{a}\bar{b} = \bar{1}$, i.e. $ab \equiv 1 \pmod{n}$. Il existe donc $k \in \mathbb{Z}$ tel que $ab - kn = 1 = ab + n(-k)$. D'après l'identité de Bézout, a et n sont premiers entre eux.
$(\Longleftarrow)$: Supposons que $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ avec a et n premiers entre eux : il existe $u, v \in \mathbb{Z}$ tels

que $au + nv = 1$. Alors

$$\begin{aligned}\overline{(au+nv)} &= \bar{1}\\ \overline{au} + \overline{nv} &= \bar{1}\\ \bar{a}\bar{u} + \bar{n}\bar{v} &= \bar{1}\\ \bar{a}\bar{u} + \bar{0}\bar{v} &= \bar{1}\\ \bar{a}\bar{u} + \bar{0} &= \bar{1}\\ \bar{a}\bar{u} &= \bar{1}\end{aligned}$$

donc $\bar{a}$, est inversible, d'inverse $\bar{u} \in \mathbb{Z}/n\mathbb{Z}$. □

Notation.(1) L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est noté par $\mathbb{Z}/n\mathbb{Z}^\times$. On a donc

$$\mathbb{Z}/n\mathbb{Z}^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid a \text{ et } n \text{ premiers entre eux}\}. \tag{IV.1}$$

(1) Pour $\bar{a} \in \mathbb{Z}/n\mathbb{Z}^\times$, l'inverse de $\bar{a}$ est noté $\frac{1}{\bar{a}}$ ou $\bar{a}^{-1}$.

Corollaire IV.2.3 (Nombre des éléments inversibles)**.** *Soit $n \geqslant 2$ un entier. Alors, le nombre des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est*

$$\operatorname{card}\{k \in \mathbb{N} \mid 1 \leqslant k < n \text{ et } k \text{ premier avec } n\}.$$

Démonstration. L'ensemble des éléments inversibles est $\mathbb{Z}/n\mathbb{Z}^\times$et on a, par (IV.1)

$$\begin{aligned}\mathbb{Z}/n\mathbb{Z}^\times &= \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid a \text{ et } n \text{ premiers entre eux}\}\\ &= \{\bar{k} \in \{1,\dots,n-1\} \mid k \text{ et } n \text{ premiers entre eux}\},\end{aligned}$$

d'où le nombre des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$:

$$\operatorname{card}(\mathbb{Z}/n\mathbb{Z}^\times) = \operatorname{card}\{\bar{k} \in \{1,\dots,n-1\} \mid k \text{ et } n \text{ premiers entre eux}\};$$

qui est le même que celui énoncé dans la Proposition IV.2.3. □

Exemples IV.2.4. (1) On a $\mathbb{Z}/2\mathbb{Z}^\times = \{\bar{1}\}$. Le seul nombre entre 1 et 1, premier avec 1 est 1, et on a $\operatorname{card}(\mathbb{Z}/2\mathbb{Z}^\times) = 1$.
(2) $\mathbb{Z}/3\mathbb{Z}^\times = \{\bar{1}, \bar{2}\}$. Il y a, entre 1 et 2, deux nombres premiers avec 3, à savoir 1 et 2 et on a $\operatorname{card}(\mathbb{Z}/5\mathbb{Z}) = 2$. On a $\bar{2}\cdot\bar{2} = \overline{4} = \bar{1}$, donc $\frac{1}{\bar{2}} = \bar{2}$.
(3) $\mathbb{Z}/4\mathbb{Z}^\times = \{\bar{1}, \bar{3}\}$. Il y a entre 1 et 4, deux nombres premiers avec 3 à savoir 1 et 2 et $\operatorname{card}(\mathbb{Z}/4\mathbb{Z}) = 2$. On a $\bar{5}\cdot\bar{3} = \overline{9} = \bar{1}$, donc $\frac{1}{\bar{3}} = \bar{3}$.
(4) $\mathbb{Z}/8\mathbb{Z}^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$. Il y a entre 1 et 7 quatre nombres premiers avec 8, à savoir 1,3,5 et 7 et on a $\operatorname{card}(\mathbb{Z}/8\mathbb{Z}) = 4$.
On a, $\bar{3}\cdot\bar{3} = \bar{9} = \bar{1}$. Donc l'inverse de $\bar{3}$ est lui-même : $\frac{1}{\bar{3}} = \bar{3}$; de même, $\bar{5}\cdot\bar{5} = \overline{25} = \bar{1}$, donc $\frac{1}{\bar{5}} = \bar{5}$ et $\bar{7}\cdot\bar{7} = \overline{49} = \bar{1}$, donc $\frac{1}{\bar{7}} = \bar{7}$.

Corollaire IV.2.5 (Les corps $(\mathbb{Z}/p\mathbb{Z},+,\times)$)**.** *Soit $p \geqslant 2$ un entier premier. Alors $(\mathbb{Z}/p\mathbb{Z},+,\times)$ est un corps commutatif.*

Démonstration. Si p est premier, alors tout entier k tel que $1 \leqslant k < p$ est premier avec p. Il en résulte que les classes $\bar{k}$ correspondantes sont inversibles dans l'anneau $(\mathbb{Z}/p\mathbb{Z},+,\times)$. D'où

$$\mathbb{Z}/n\mathbb{Z}^\times = \{\bar{1},\dots,\overline{p-1}\} = \mathbb{Z}/n\mathbb{Z}\setminus\{0\} = \mathbb{Z}/n\mathbb{Z}^*.$$

Ainsi, tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible. Donc $(\mathbb{Z}/p\mathbb{Z},+,\times)$ est un corps (commutatif). □

Si n n'est pas premier, $(\mathbb{Z}/n\mathbb{Z},+,\times)$ n'est jamais un corps.

Exemples IV.2.6. (1) Les anneaux $(\mathbb{Z}/4\mathbb{Z},+,\times)$ et $(\mathbb{Z}/8\mathbb{Z},+,\times)$ ne sont pas des corps.
(2) Les anneaux $(\mathbb{Z}/2\mathbb{Z},+,\times), \mathbb{Z}/3\mathbb{Z},+,\times), (\mathbb{Z}/47\mathbb{Z},+,\times)$ sont des corps commutatifs.

Nous avons alors le corrollaire suivnt :

Proposition IV.2.7. *Pour $n \geqslant 1$, le couple $(\mathbb{Z}/n\mathbb{Z}^\times,\times)$ est un groupe commutatif.*

Démonstration. On a $\mathbb{Z}/n\mathbb{Z}^\times \neq \emptyset$ car $\bar{1} \in \mathbb{Z}/n\mathbb{Z}^\times$.
La multiplication est interne dans $\mathbb{Z}/n\mathbb{Z}^\times$: si $\bar{a},\bar{b} \in \mathbb{Z}/n\mathbb{Z}^\times$, alors il existe $\bar{u},\bar{v} \in \mathbb{Z}/n\mathbb{Z}$ tels que $\bar{a}\bar{u} = \bar{1}$ et $\bar{b}\bar{v} = \bar{1}$. Alors

$$(\bar{a}\bar{b})(\bar{v}\bar{u}) = \bar{a}(\bar{b}\bar{v})\bar{u} = \bar{a}(\bar{1})\bar{u} = \bar{a}\bar{u} = \bar{1},$$

donc $\bar{a}\bar{b}$ est inversible, d'inverse $\bar{v}\bar{u}$, i.e. $\bar{a}\bar{b} \in \mathbb{Z}/n\mathbb{Z}^\times$.
La multiplication $\mathbb{Z}/n\mathbb{Z}^\times$ est associative et commutative : c'est vrai car elle hérite de ces propriétés de qui sont vraies dans $\mathbb{Z}/n\mathbb{Z}$.
Elément est neutre : $\bar{1}$ est neutre dans $\mathbb{Z}/n\mathbb{Z}$ et $\bar{1} \in \mathbb{Z}/n\mathbb{Z}^\times$; c'est donc neutre pour la multiplication dans $\mathbb{Z}/n\mathbb{Z}^\times$.
Tout élément de $\mathbb{Z}/n\mathbb{Z}^\times$ possède un inverse : c'est évident par construction de $\mathbb{Z}/n\mathbb{Z}^\times$.
□

Exemple IV.2.8. Le couple $(\mathbb{Z}/8\mathbb{Z}^\times,\times)$ est donc un groupe commutatif, avec $\mathbb{Z}/8\mathbb{Z}^\times = \{\bar{1},\bar{3},\bar{5},\bar{7}\}$. Voici la table de multiplication :

$\times$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

IV.3 La fonction indicatrice d'Euler

Définition IV.3.1 (Fonction indicatrice d'Euler)**.** La fonction indicatrice d'Euler est la fonction définie par

$$\begin{aligned}\varphi : \mathbb{N}^* &\longrightarrow \mathbb{N} \\ n &\longmapsto \begin{cases} 1 \text{ si } n = 1, \\ \operatorname{card}\{k \in \mathbb{N} \mid 1 \leqslant k \leqslant n-1 \text{ et } k \text{ premier avec } n\}. \end{cases}\end{aligned}$$

C'est le nombre d'entiers non nuls plus petits que n et premier avec n.

Exemples IV.3.2. (1) On a $\varphi(2) = \operatorname{card}\{1\} = 1; \varphi(3) = \operatorname{card}\{1,2\} = 2$,
(2) $\varphi(4) = \operatorname{card}\{1,3\} = 2; \varphi(5) = \operatorname{card}\{1,2,3,4\} = 4$,
(3) $\varphi(8) = \operatorname{card}\{1,3,5,7\} = 4$.

D'après le Corollaire IV.2.3, nous avons le théorème important suivant :

Théorème IV.3.3 (Caractérisation de $\varphi(n)$)**.** *Soit $n \geqslant 2$ un entier. Alors*

$$(\forall n \in \mathbb{N}^*) \quad \varphi(n) = \operatorname{card} \mathbb{Z}/n\mathbb{Z}^{\times}.$$

Théorème IV.3.4 (Euler)**.** *Pour tout entier $n \geqslant 1$ et tout entier a premier avec n, on a*

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Démonstration. Par définition, on a

$$\varphi(n) = \operatorname{card}\{a \in \mathbb{N}^* \mid 1 \leqslant a \leqslant n-1 \text{ et } a \text{ premier avec } n\},$$

ce qui montre qu'on peut écrire

$$\{a \mid 0 \leqslant a < n, \operatorname{pgcd}(a,n) = 1\} = \{a_1, a_2, \cdots, a_{\varphi(n)} \text{ où } a_1 < a_2 < \cdots < a_{\varphi(n)} < n \text{ et } a_i \text{ premier avec } n\}.$$

Soit a un entier tel que $\operatorname{pgcd}(a,n) = 1$. On considère maintenant l'ensemble de produits modulo n

$$\{a \cdot a_1, a \cdot a_2, \cdots, a \cdot a_{\varphi(n)}\},$$

Si $a \cdot a_i = a \cdot a_j$, alors

$$a \cdot (a_i - a_j) \equiv 0 \mod n,$$

donc $a_i = a_j$ puisque $\operatorname{pgcd}(a,n) = 1$ et $|a_i - a_j| < n$. Ainsi, on a encore

$$\{a_1, a_2, \cdots, a_{\varphi(n)}\} = \{a \cdot a_1, a \cdot a_2, \cdots, a \cdot a_{\varphi(n)}\}.$$

En formant les produits des éléments de ces deux ensembles, on obtient :

$$\prod_{i=1}^{\varphi(n)} a_i = \prod_{i=1}^{\varphi(n)} a \cdot a_i \equiv a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} a_i \mod n.$$

De plus, pour chaque i, on a $\mathrm{pgcd}(a_i, n) = 1$. Donc a_i et le produit $\prod_{i=1}^{\varphi(n)} a_i$ sont inversibles modulo n, ce qui donne, par simplification :

$$a^{\varphi(n)} \equiv 1 \mod n.$$

□

Théorème IV.3.5 (Calcul de $\varphi(p^n)$)**.** *La fonction φ possède les propriétés suivantes :*
(1) *Si p est un entier premier, alors $\varphi(p) = p - 1$.*
(2) *Si p est un entier premier, alors pour tout $n \in \mathbb{N}^*$, on a*

$$\varphi(p^n) = (p-1)p^{n-1}. \tag{IV.2}$$

Démonstration. (1) Puisque p est premier, tout entier naturel k tel que $1 \leqslant k \leqslant p-1$ est premier avec p, on a $\varphi(p) = p - 1$.
(3) Par définition, on a

$$\varphi(p^n) = \mathrm{card}\{k \in \mathbb{N}^* \,|1 \leqslant k \leqslant p^n - 1 \text{ et } \mathrm{pgcd}(k, p^n) = 1\}.$$

Nous allons plutôt compter les nombres inférieurs à $p^n - 1$ et qui ne sont pas premiers avec p^n : si $m \in \mathbb{N}^*$ est tel que $1 \leqslant m \leqslant p^n - 1$ et $\mathrm{pgcd}(m, p^n) \neq 1$, alors p est facteur de m. Donc a $m = hp$ avec $h \in \mathbb{N}^*$, $hp \leqslant p^n$, ce qui implique que m appartient à l'ensemble

$$M_p = \{hp \in \mathbb{N}^* \,|1 \leqslant h \leqslant p^{n-1}\} = \{p, 2p, 3p, \cdots, p^{n-1}p\}$$

Par suite, on a $\mathrm{card}M_p = p^{n-1}$. Par conséquent, $\varphi(p^n) = p^n - \mathrm{card}M_p$. Ainsi, $\varphi(p^n) = p^n - p^{n-1} = (p-1)p^{n-1}$. □

IV.4 Le théorème des restes chinois

Notations. Soit $n \geqslant 2$ un entier. Pour simplifier les écritures, nous écrivons

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$$

(nous supprimons les barres). Quand nous disons "un élément $a \in \mathbb{Z}/n\mathbb{Z}$" (sans barres) , cela signife que nous adoptons cette notation, donc $a \in \{0, 1, \ldots, n-1\}$. Quand nous écrivons "un élément $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$" (avec barres), cela signifie que a peut être un élément quelconque de $\mathbb{Z}$, mais il existe $b \in \{0, \ldots, n-1\}$ tel que $a \equiv b \mod n$; donc $\bar{a} = \bar{b}$.

Exemple IV.4.1. On a $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ et $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$. Dans $\mathbb{Z}/2\mathbb{Z}$, on a $\bar{7} = \bar{1}$; dans $\mathbb{Z}/4\mathbb{Z}$, on a $\bar{7} = \bar{3}$.

Les formules de la proposition suivante sont utiles pour effectuer les calculs dans $\mathbb{Z}/n\mathbb{Z}$:

Proposition IV.4.2 (Reste modulo n d'une somme et d'un produit)**.** *Soit $n \geqslant 2$ un entier. Pour $a, b \in \mathbb{Z}$, on a*

$$(a+b) \bmod n = (a \bmod n + b \bmod n) \bmod n.$$

et

$$(ab) \bmod n = ((a \bmod n)(b \bmod n)) \bmod n.$$

Démonstration. (1) Soit $a = q_1 n + r$, où $q_1 \in \mathbb{Z}$, $0 \leqslant r < n$, la division euclidienne de a par n et $b = q_2 n + s$, où $q_2 \in \mathbb{Z}$, $0 \leqslant s < n$, celle de b. Donc,

$$a + b = (q_1 + q_2)n + r + s. \tag{IV.3}$$

Il se peut que $r + s \geqslant n$. Effectuons alors la division euclidienne de $r + s$ par n. On a $r + s = q_3 n + t$, où $q_3 \in \mathbb{Z}$, $0 \leqslant t < n$. Nous avons alors

$$a + b = (q_1 + q_2 + q_3)n + t, \quad 0 \leqslant t < n.$$

Par unicité du reste, on a

$$\begin{aligned}(a + b) \bmod n = t &= (r + s) \bmod n \\ &= (a \bmod n + b \bmod n) \bmod n.\end{aligned}$$

(2) Soit $a = q_1 n + r$, où $q_1 \in \mathbb{Z}$, $0 \leqslant r < n$, la division euclidienne de a par n et $b = q_2 n + s$, où $q_2 \in \mathbb{Z}$, $0 \leqslant s < n$, celle de b. Donc,

$$ab = (q_1 q_2 n + q_2 r + s q_1)n + rs. \tag{IV.4}$$

Il se peut que $rs \geqslant n$. Effectuons la division euclidienne de rs par n. On a $rs = q_3 n + t$, où $q_3 \in \mathbb{Z}$, $0 \leqslant t < n$. En d'autres termes, $t = (rs) \bmod n$. Nous avons :

$$ab = (q_1 q_2 n + q_2 r + s q_1 + q_3)n + t, \quad 0 \leqslant t < n.$$

Par unicité du reste, on a

$$\begin{aligned}(ab) \bmod n = t &= (rs) \bmod n \\ &= [(a \bmod n)(b \bmod n)] \bmod n. \quad \square\end{aligned}$$

Soient $m, n \geqslant 2$ des entiers. Nous adoptons la notation précédente (sans barres) pour les éléments de $\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/mn\mathbb{Z}$:

$$\begin{aligned}\mathbb{Z}/m\mathbb{Z} &= \{0, 1, \ldots, m-1\} \\ \mathbb{Z}/n\mathbb{Z} &= \{0, 1, \ldots, n-1\} \\ \mathbb{Z}/mn\mathbb{Z} &= \{0, 1, \ldots, mn-1\}.\end{aligned}$$

Théorème IV.4.3 (Théorème des restes chinois)**.** *Soit $m, n \geqslant 1$ deux entiers tels que $\operatorname{pgcd}(m, n) = 1$. Alors, l'application*

$$\begin{aligned}f : \mathbb{Z}/mn\mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x &\longmapsto (x \bmod m,\ x \bmod n)\end{aligned}$$

est un isomorphisme d'anneaux.

Démonstration. On sait que $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont des anneaux. L'addition dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est définie par $(u,v)+(w,t) = (u+w, v+t)$ et la multiplication par $(u,v)\cdot(w,t) = (uw, vt)$ pour $(u,v),(w,t) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Les éléments unités sont respectivement 1 et $(1,1)$.

• L'image de l'élément neutre 1 de $\mathbb{Z}/mn\mathbb{Z}$ est $f(1) = (1 \bmod m, 1 \bmod n) = (1,1)$, qui est l'élément neutre de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Pour $x, y \in \mathbb{Z}/mn\mathbb{Z}$,

• Calculons $f(xy)$:

$$\begin{aligned} f(xy) &= ((xy) \bmod m, (xy) \bmod n) \\ &= (((x \bmod m)(y \bmod m)) \bmod m, ((x \bmod n)(y \bmod n)) \bmod n) \\ &\quad \text{(reste modulo } m \text{ et } n \text{ du produit, d'après la proposition IV.4.2)}; \end{aligned}$$

et calculons $f(x)f(y)$:

$$\begin{aligned} f(x)f(y) &= (x \bmod m, x \bmod n)(y \bmod m, y \bmod n) \\ &= (((x \bmod m)(y \bmod m)) \bmod m, ((x \bmod n)(y \bmod n)) \bmod n) \\ &\quad \text{(multiplication dans } \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \text{)} \\ &\quad \text{(et reste modulo } m \text{ et } n \text{ du produit, d'après la Proposition IV.4.2)} \\ &= f(xy). \end{aligned}$$

• Calculons $f(x+y)$:

$$\begin{aligned} f(x+y) &= ((x+y) \bmod m, (x+y) \bmod n) \\ &= ((x \bmod m + y \bmod m) \bmod m, (x \bmod n + y \bmod n) \bmod n) \\ &\quad \text{(reste modulo } m \text{ et } n \text{ d'une somme, d'après la Proposition IV.4.2)} \\ &= (x \bmod m, x \bmod n) + (y \bmod m, y \bmod n) \quad \text{(somme dans } \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \\ &= f(x) + f(y). \end{aligned}$$

D'après ces trois points, f est un morphisme d'anneaux.

Puisque $\mathrm{card}(\mathbb{Z}/mn\mathbb{Z})$ et $\mathrm{card}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$ sont finis et égaux à mn, pour montrer que f est un isomorphisme, il suffit de montrer que . Or $f(x) = (0,0)$ implique $x \equiv 0 \pmod m$ et $x \equiv 0 \pmod n$; i.e

$$x = km \text{ et } x = ln \quad \text{avec } k, l \in \mathbb{Z}\,. \tag{IV.5}$$

Donc $km = ln$, i.e $m|ln$. Or $\mathrm{pgcd}(m,n) = 1$ par hypothèse, et d'après le lemme de Gauß, on a $m|l$, i.e il existe $h \in \mathbb{N}$ tel que $l = hm$. Par (IV.5), on a $x = hmn$. Donc $mn|x$, i.e $x \equiv 0 \pmod{mn}$, ce qui implique l'injectivité de f. D'où, l'isomorphisme $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. □

Corollaire IV.4.4 (Equations aux congruences)**.** *Soit m, n deux entiers tels que* $\mathrm{pgcd}(m,n) =$

1. *Alors, pour tout couple d'entiers* (a, b)*, le système de congruence*

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases} \tag{IV.6}$$

admet une unique solution dans $\mathbb{Z}/mn\mathbb{Z}$*.*

Démonstration. C'est une conséquence du Théorème IV.4.3.

Corollaire IV.4.5 (Cas de plusieurs entiers)**.** *Soit* $N = m_1 \cdots m_k$ *où les* m_i *sont deux à deux premiers entre eux. Alors, pour tout k-uplet* $(a_1, ..., a_k)$*, le système de congruence*

$$x \equiv a_i (\mathrm{mod}\ m_i), 1 \leqslant i \leqslant k,$$

admet une unique solution dans $\mathbb{Z}/N\mathbb{Z}$*.*

Démonstration. Il suffit de prendre un k-uplet, où $k \geqslant 3$ au lieu d'un couple dans le Théorème IV.4.4.

Exemples IV.4.6. Résoudre le système de congruence

$$\begin{cases} x \equiv 2 \mod 37 \\ x \equiv 9 \mod 19 \end{cases} \tag{IV.7}$$

Existence : On a $\mathrm{pgcd}(37, 19) = 1$. D'après le Corollaire IV.4.4, ce système admet une unique solution dans $\mathbb{Z}/(37 \times 19)\mathbb{Z} = \mathbb{Z}/703\mathbb{Z}$.
Calcul : On a

$$\begin{aligned} x = 2 + 37r &= 9 + 19s \\ 2 + 37r &= 9 \mod 19 \\ 37r &= 7 \mod 19 \end{aligned}$$

Or

$$\begin{aligned} 37 &\equiv -1 \mod 19 \\ \text{et } 18 &\equiv -1 \mod 19. \end{aligned}$$

Donc $18 \times 37 \equiv 1 \mod 19$. Alors

$$\begin{aligned} 18 \times 37r = r &= 18 \times 7 \mod 19 \\ r &= 126 \mod 19 = 12. \end{aligned}$$

Ainsi, $x = (2 + 37 \times 12) \mod 703 = 446$.

Une autre application est le théorème suivant :

Théorème IV.4.7 (Calcul de φ avec pour les entiers décomposés en facteurs premiers)**.** *On a*
(1) *Si* $a, b \geqslant 1$ *sont deux entiers tels que* $\mathrm{pgcd}(a, b) = 1$*, alors*

$$\varphi(ab) = \varphi(a)\,\varphi(b). \tag{IV.8}$$

(2) *Soit* $n = \prod_{k=1}^{s} p_k^{\alpha_k}$ *la factorisation de* n *en un produit de puissances de nombres premiers avec* $\alpha_k \geqslant 1$*. Alors*

$$\varphi(n) = \prod_{k=1}^{s} (p_k - 1) p_k^{\alpha_k - 1}. \tag{IV.9}$$

(1) D'après le Théorème des restes chinois, puisque $\operatorname{pgcd}(a, b) = 1$, on a $\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Dans cet isomorphisme, les éléments inversibles s'envoient sur les éléments inversibles (c'est vrai dans tout isomorphisme d'anneaux). D'où l'isomorphisme de groupes multiplicatifs $(\mathbb{Z}/ab\mathbb{Z})^\times \cong (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$. En prenant le cardinal de chaque membre, on a $\varphi(ab) = \varphi(a)\varphi(b)$.
(2) On a

$$\begin{aligned}
\varphi(n) &= \varphi\Big(\prod_{k=1}^{s} p_k^{\alpha_k}\Big) \\
&= \prod_{k=1}^{s} \varphi(p_k^{\alpha_k}) \quad \text{car les } p_i^{\alpha_i} \text{ étant premiers entre eux)} \\
&= \prod_{k=1}^{s} p_k^{\alpha_k - 1}(p_k - 1) \quad \text{(D'après (IV.9))}. \quad \square
\end{aligned}$$

IV.5 Ordre d'un élément dans les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{Z}/n\mathbb{Z}^\times, \times)$

Soit $n \geqslant 2$ un entier. Pour $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ et $m \in \mathbb{Z}$, on pose

$$m \cdot \bar{a} = \begin{cases} 0 & \text{si } m = 0, \\ \underbrace{\bar{a} + \bar{a} + \cdots + \bar{a}}_{\text{somme } m \text{ fois dans } \mathbb{Z}/n\mathbb{Z}} & \text{si } m > 0, \\ \underbrace{\overline{(-a)} + \overline{(-a)} + \cdots + \overline{(-a)}}_{\text{somme } -m \text{ fois dans } \mathbb{Z}/n\mathbb{Z}} & \text{si } m < 0. \end{cases}$$

Pour $\bar{g} \in \mathbb{Z}/n\mathbb{Z}^\times$ et $m \in \mathbb{N}$, on pose

$$\bar{g}^m = \begin{cases} 1 & \text{si } m = 0, \\ \underbrace{\bar{g} \times \bar{g} \times \cdots \times \bar{g}}_{\text{produit } m \text{ fois dans } \mathbb{Z}/p\mathbb{Z}} & \text{si } m > 0, \\ \underbrace{\overline{g^{-1}} \times \overline{g^{-1}} \times \cdots \times \overline{g^{-1}}}_{\text{produit } -m \text{ fois dans } \mathbb{Z}/p\mathbb{Z}} & \text{si } m < 0. \end{cases}$$

Proposition IV.5.1. *Soit* $n \geqslant 2$ *un entier et* $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$*. On a, pour* $m, n \in \mathbb{Z}$ *:*
(1) $(m + n) \cdot \bar{a} = m \cdot \bar{a}$
(2) $m(n \cdot \bar{a}) = (mn) \cdot \bar{a}$*.*

Démonstration. Exercice, voir TD. $\square$

Proposition IV.5.2 ($n\bar{a} = 0$)**.** *Soit* $n \geqslant 2$ *un entier. L'entier* n *est le plus petit des entiers* > 0 *tels que pour tout* $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$*, on a* $k \cdot \bar{a} = \bar{0}$*.*

Démonstration. Il existe $r \in \{0, 1, \ldots, n-1\}$ tel que $a \equiv r \pmod{n}$. En tant que produit de deux éléments de $\mathbb{Z}$, on a $nr \in \mathbb{Z}$ et

$$nr = \underbrace{r + r + \cdots + r}_{\text{somme } n \text{ fois dans } \mathbb{Z}} . \tag{IV.10}$$

En prenant les classes modulo n, on a

$$\begin{aligned} \bar{0} = \overline{nr} &= \overline{\underbrace{r + r + \cdots + r}_{\text{somme } n \text{ fois dans } \mathbb{Z}}} \\ &= \bar{r} + \bar{r} \cdots + \bar{r} \quad \text{(somme } n \text{ fois dans } \mathbb{Z}/n\mathbb{Z}) \\ &= n \cdot \bar{r} \quad \text{(selon la définition ci-dessus)} \\ &= n \cdot \bar{a} \quad \text{(car } \bar{r} = \bar{a}). \end{aligned}$$

Ainsi, $n \cdot \bar{a} = \bar{0}$ pour tout $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. Soit k un autre entier > 0 tel que $k \cdot \bar{a} = \bar{0}$ pour tout $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. En particulier, on a $k \cdot \bar{1} = \overline{k \cdot 1} = \bar{k} = \bar{0}$ (calcul analogue à ce que l'on a fait pour $n \cdot \bar{a}$ précédent). Il existe donc $l \in \mathbb{Z}$ tel que $k = ln$. Donc $k \geqslant n$. Ainsi, n est bien le plus petit entier qui vérifie $k \cdot \bar{a} = \bar{0}$ pour tout $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. □

Définition IV.5.3 (Caractéristique de $\mathbb{Z}/n\mathbb{Z}$)**.** L'entier n est appelé la *caractéristique* de $\mathbb{Z}/n\mathbb{Z}$.

Exemples IV.5.4. (1) L'anneau $(\mathbb{Z}/2\mathbb{Z}, +, \times)$ est de caractérisque 2.
(2) L 'anneau $(\mathbb{Z}/3\mathbb{Z}, +, \times)$ est de caractéristique 3.
(3) L 'anneau $(\mathbb{Z}/2022\mathbb{Z}, +, \times)$ est de caractéristique 2022.

Proposition IV.5.5. *Soit $n \geqslant 2$ un entier et $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. Alors*
(1) *Il existe un plus petit entier $m > 0$ tel que $m \cdot \bar{a} = 0$.*
(2) *Soit $\bar{g} \in \mathbb{Z}/n\mathbb{Z}^\times$. Alors, il existe un plus petit entier $m > 0$ tel que $\bar{g}^m = 1$.*

Démonstration. (1) On a $n \cdot \bar{a} = 0$ d'après la Proposition IV.5.2 . Ainsi, l'ensemble des entiers $k \geqslant 1$ tels que $k \cdot \bar{a} = \bar{0}$ est non vide car contient n. Cet ensemble possède alors un plus petit élément m, qui vérifie donc $m \cdot \bar{a} = \bar{0}$.
(2) Nous savons que $\bar{g}^{\varphi(n)} = \bar{1}$ dans $\mathbb{Z}/n\mathbb{Z}^\times$, d'après le théorème de Fermat. Donc l'ensemble des entiers $k \geqslant 1$ vérifiant $\bar{g}^k = \bar{1}$ nest pas vide ; il admet donc un plus petit élément m qui vérifie donc $\bar{g}^m = \bar{1}$. □

Définition IV.5.6 (Ordre d'un élément de $(\mathbb{Z}/n\mathbb{Z}, +)$ et de $(\mathbb{Z}/n\mathbb{Z}^\times, \times)$)**.** (1) Soient $n \geqslant 2$ un entier et $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. L'*ordre* de $\bar{a}$ dans le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est le plus petit entier $m > 0$ tel que $m \cdot \bar{a} = \bar{0}$.
(2) Soit $\bar{g} \in \mathbb{Z}/n\mathbb{Z}^\times$. L'*ordre* de $\bar{g}$ dans le groupe $(\mathbb{Z}/n\mathbb{Z}^\times, \times)$ est le plus petit entier $m > 0$ tel que $\bar{g}^m = \bar{1}$.

Notations. L'ordre de $\bar{a}$ (resp. de g) dans $(\mathbb{Z}/n\mathbb{Z}, +)$ (resp. dans $(\mathbb{Z}/n\mathbb{Z}^\times, \times)$ est note $o(a)$ (resp. $o(g)$).

Exemples IV.5.7. (1) Dans $(\mathbb{Z}/2\mathbb{Z},+)$, on a $1\cdot\bar{1}=\bar{1}, \quad 2\cdot\bar{1}=\bar{2}=\bar{0}$, donc $o(2)=2$.
(2) Dans $(\mathbb{Z}/4\mathbb{Z},+)$, on a $1\cdot\bar{3}=\bar{3}, \quad 2\cdot\bar{3}=\bar{6}=\bar{2}, \quad 3\cdot\bar{3}=\bar{9}=\bar{1}, 4\cdot\bar{3}=\overline{12}=\bar{0}$, donc $o(\bar{3})=4$.
(3) Dans $(\mathbb{Z}/3\mathbb{Z}^*,\times)$, on a $\bar{2}^1=\bar{2}, \quad \bar{2}^2=\bar{4}=\bar{1}$, donc $o(\bar{2})=2$.
(4) Dans $(\mathbb{Z}/5\mathbb{Z}^*,\times)$, on a $\bar{4}^1=\bar{4}, \bar{4}^2=\overline{16}=\bar{1}$, donc $o(\bar{4})=\bar{2}$.

Définition IV.5.8 (Sous-groupe engendré par un élément de $(\mathbb{Z}/n\mathbb{Z},+)$ et de $(\mathbb{Z}/n\mathbb{Z}^\times,\times)$)**.**
(1) Soient $n\geqslant 2$ un entier et $\bar{a}\in\mathbb{Z}/n\mathbb{Z}$. Le *sous-groupe* engendré par $\bar{a}$ est

$$\langle\bar{a}\rangle=\{k\cdot\bar{a}\mid k\in\mathbb{Z}\}.$$

(2) Soit $\bar{g}\in\mathbb{Z}/n\mathbb{Z}^\times$. Le *sous-groupe* engendré par $\bar{g}$ est

$$\langle\bar{g}\rangle=\{\bar{a}^k\mid k\in\mathbb{Z}\}.$$

On vérifie que, selon les notations de la Définition IV.5.8, $\langle\bar{a}\rangle$ et $\langle\bar{g}\rangle$ sont bien des sous-groupes (voir TD).

Proposition IV.5.9 (Ordre du sous-groupe engendré par un élément)**.** *Les notations sont les même que celles de la Définition IV.5.8. On a*

$$\mathrm{card}\langle\bar{a}\rangle=o(a) \quad \textit{et} \quad \mathrm{card}\langle\bar{g}\rangle=o(g).$$

Démonstration. Soit $k\in\mathbb{Z}$; effectuons la division euclidienne de k par $o(\bar{a})$; il existe $q,r\in\mathbb{Z}$ tels que $k=o(\bar{a})q+r$ avec $0\leqslant r<o(a)$. Alors

$$\begin{aligned}
k\bar{a} &= (o(a)q+r)\cdot\bar{a}\\
&= (o(a)q)\cdot\bar{a}+r\cdot\bar{a}\\
&= (qo(a))\cdot\bar{a}+r\cdot\bar{a}\\
&= q(o(a)\cdot\bar{a})+r\cdot\bar{a} \quad \text{(par la Proposition IV.5.1)}\\
&= q\cdot\bar{0}+r\cdot\bar{a}\\
&= r\cdot\bar{a}.
\end{aligned}$$

Ainsi, $\langle\bar{a}\rangle=\{k\cdot\bar{a}\mid k\in\mathbb{Z}\}=\{r\cdot\bar{a}\mid r=0,\dots,o(a)-1\}=\{\bar{0},\bar{a},\dots,\bar{k}\cdot a,\dots,(o(a)-1)\cdot\bar{a}\}$
Pour $\mathrm{card}\langle\bar{g}\rangle$, on effectue des calculs semblables : pour $k\in\mathbb{Z}$, on effectue la division euclidienne de k par $o(g)$; et on calcule $\bar{g}^k$. (voir TD) □

D'après la démonstration du Théorème IV.5.9, nous avons des écritures simples pour les sous-groupes mentionnés :

Corollaire IV.5.10. *Avec les notations du Théorème IV.5.9, on a*

$$\begin{aligned}
\langle\bar{a}\rangle &= \{r\cdot\bar{a}\mid r=0,1,\dots,o(a)-1\}\\
\langle\bar{g}\rangle &= \{\bar{g}^r\mid r=0,1,\dots,o(g)-1\}.
\end{aligned}$$

Le corollaire suivant est immédiat :

Corollaire IV.5.11. *Avec les notations du Théorème IV.5.9, on a*

(1) $o(\bar{a}) = n \iff \langle \bar{a} \rangle = \mathbb{Z}/n\mathbb{Z}$.

(2) $o(\bar{g}) = p - 1 \iff \langle \bar{g} \rangle = \mathbb{Z}/n\mathbb{Z}^{\times}$.

Définition IV.5.12 (Générateurs)**.** Avec les notations du Théorème IV.5.9 :

(1) Un *générateur de du groupe* $(\mathbb{Z}/n\mathbb{Z}, +)$ est un élément $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\langle \bar{a} \rangle = \mathbb{Z}/n\mathbb{Z}$.

(2) Un *générateur de du groupe* $(\mathbb{Z}/n\mathbb{Z}^*, \times)$ est un élément $\bar{g} \in \mathbb{Z}/n\mathbb{Z}^{\times}$ tel que $\langle \bar{g} \rangle = \mathbb{Z}/n\mathbb{Z}^{\times}$.

Exemple IV.5.13. Soit $n \geqslant 1$ un entier. Alors, $\bar{1}$ est générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$.

Démonstration. Exercice (voir TD). □

Exemples IV.5.14. D'après l'Exemple IV.5.7, on a

(1) Dans $(\mathbb{Z}/2\mathbb{Z}, +), \langle \bar{2} \rangle = \{\bar{0}, \bar{1}\}$, donc $\bar{2}$ est un générateur de $(\mathbb{Z}/2\mathbb{Z}, +)$.

(2) Dans $(\mathbb{Z}/4\mathbb{Z}, +)$, on a $\langle \bar{3} \rangle = \mathbb{Z}/4\mathbb{Z}$, donc $\bar{3}$ est générateur de $(\mathbb{Z}/4\mathbb{Z}, +)$,

(3) Dans $(\mathbb{Z}/3\mathbb{Z}^*, \times)$, on a $o(2) = 2 = \mathrm{card}(\mathbb{Z}/3\mathbb{Z}^*)$, donc $\langle \bar{2} \rangle = \mathbb{Z}/3\mathbb{Z}^{\times}$ et $\bar{4}$ est générateur de $(\mathbb{Z}/3\mathbb{Z}, \times)$.

(4) Dans $(\mathbb{Z}/5\mathbb{Z}^*, \times)$, on a $o(\bar{4}) = 2$ et $\langle \bar{4} \rangle = \{\bar{1}, \bar{4}\}$. Donc $\bar{4}$ n'est pas générateur de $(\mathbb{Z}/5\mathbb{Z}^*, \times)$.

Théorème IV.5.15 (Générateus de $(\mathbb{Z}/n\mathbb{Z}, +)$)**.** *Soit $n \geqslant 1$ un entier. Alors, un élément $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ avec $1 \leqslant a < n$ est générateur si et eulement si a est premier avec n.*

Démonstration. ($\Longrightarrow$) : Supposons que $\bar{a}$ est générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$ (nécessairement $\bar{a} \neq 0$. Alors $o(\bar{a}) = n$. Soit $d = \mathrm{pgcd}(a, n)$. Il existe $k, l \in \mathbb{N}$ tels que $a = kd$ et $n = ld$; on a $l > 0$. Supposons que $d > 1$; alors $l < n$ et

$$\begin{aligned} l \cdot \bar{a} &= l \cdot (\overline{kd}) \\ &= \overline{lkd} \\ &= \overline{kld} \\ &= \overline{kn} \\ &= \bar{0}, \end{aligned}$$

ce qui implique que $o(a) \leqslant l < n$, qui est absurde. Donc forcément $d = 1$ et a est premier avec n.

($\Longleftarrow$) : Supposons a premier avec n ; supposons que $k = o(\bar{a}) < n$; on a $k \cdot \bar{a} = \bar{0}$: il existe $h \in \mathbb{N}$ tel que $ka = hn$ Ainsi, $a|hn$ et comme a est premier avec n, on a $a|h$. Il existe alors $u \in \mathbb{N}$ tel que $h = au$, ce qui entraîne $ka = aun$; donc $k = un$ et $k \geqslant n$, ce qui est absurde car $k < n$. Donc $k = o(a) = n$ et dans ce cas, $\bar{a}$ engendre $\mathbb{Z}/n\mathbb{Z}$. □

Puisque $(\mathbb{Z}/n_zed, +)$ peut être engendré par un seul élément, il est *cyclique*, d'où le corollaire suivant :

Corollaire IV.5.16. *Le groupe* $(\mathbb{Z}/n\mathbb{Z}, +)$ *est cyclique.*

En utilisant la fonction d'Euler, le corollaire suivant est immédiat :

Corollaire IV.5.17. *Soit* $n \geqslant 2$ *un entier. Alors le groupe* $(\mathbb{Z}/n\mathbb{Z}, +)$ *possède* $\varphi(n)$ *générateurs.*

Exemples IV.5.18. (1) Le groupe $(\mathbb{Z}/4\mathbb{Z}, +)$ possède $\varphi(4) = 2$ générateurs ; ce sont $\bar{1}$ et $\bar{2}$.
(2) Le groupe $(\mathbb{Z}/8\mathbb{Z}, +)$ possède $\varphi(8) = 4$ générateurs ; ce sont $\bar{1}, \bar{3}, \bar{5}$ et $\bar{7}$.

Exercices sur le Chapitre IV

Exercice 1. (1) Ecrire les tables des opérations de

(a) $(\mathbb{Z}/4\mathbb{Z}, +)$ et $(\mathbb{Z}4\mathbb{Z}, \times)$

(b) $(\mathbb{Z}/6\mathbb{Z}, +, \times)$ et $(\mathbb{Z}/6\mathbb{Z}, +)$

(2) Expliquer pourquoi ces anneaux ne sont pas de corps.

(3) Quelles sont les caractéristiques de ces anneaux ?

(4) Trouver $\mathbb{Z}/4\mathbb{Z}^\times$ et $\mathbb{Z}/6\mathbb{Z}^\times$ et écrire la table de multiplication dans ces ensembles.

(5) Pour chacun des groupes $(\mathbb{Z}/4\mathbb{Z}, +)$ et de $(\mathbb{Z}/6\mathbb{Z}, +)$:

(a) Trouver l'ordre de chacun de ses éléments :

(b) Quels éléments sont générateurs et quels éléments ne sont pas générateurs ? (expliquer vos réponses).

(c) Combien y-a-t-il de générateurs dans chacun de ces ensembles ?

Exercice 2. Soit $n \geqslant 2$ un entier. On fixe un élément $a \in \mathbb{Z}/n\mathbb{Z}^\times$ quelconque.

(1) Montrer que l'application

$$f : \mathbb{Z}/n\mathbb{Z}^\times \longrightarrow \mathbb{Z}/n\mathbb{Z}^\times$$
$$x \longmapsto ax$$

est bijective.

(2) Montrer que dans $\mathbb{Z}/n\mathbb{Z}^\times$, on a $\prod_{x \in \mathbb{Z}/n\mathbb{Z}^\times} x = \prod_{x \in \mathbb{Z}/n\mathbb{Z}^\times} ax$.

(3) En déduire le théorème d'Euler $a^{\varphi(n)} = 1 \pmod{n}$.

(4) Montrer que $13^{24} = 1 \mod 35$.

(5) Calculer 13^{74} dans $\mathbb{Z}/35\mathbb{Z}$.

Exercice 3. (1) Montrer que le système d'équations

$$\begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

admet une solution unique dans $\mathbb{Z}/35\mathbb{Z}$.

(2) Donner cette solution unique de $\mathbb{Z}/35\mathbb{Z}$.

(3) Trouver une autre solution dans $\mathbb{Z}$ (donc qui n'est pas dans $\mathbb{Z}/35\mathbb{Z}$).

Exercice 4. (1) Combien $(\mathbb{Z}/12\mathbb{Z}, +)$ possède-t-il de générateurs ?

(2) Donner un générateur de $(\mathbb{Z}/12\mathbb{Z}, +)$

(3) Trouver $\mathbb{Z}/12\mathbb{Z}^{\times}$

(4) Ecrire la table de $(\mathbb{Z}/12\mathbb{Z}^{*}, \times)$.

Exercice 5. (1) On considère le groupe $(\mathbb{Z}/5\mathbb{Z}^{*}, \times)$

(a) Trouver l'ordre de chacun de ses éléments.

(b) Trouver un générateur de ce groupe.

(2) Mêmes questions pour le groupe $(\mathbb{Z}/7\mathbb{Z}^{*}, \times)$.

Exercice 6. Résoudre dans $\mathbb{Z}$ le système

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod 3. \end{cases}$$

Exercice 7. (1) Soient $a, b, k \in \mathbb{N}^{*}$. Montrer que $\operatorname{pgcd}(ka, kb) = k \operatorname{pgcd}(a, b)$.

(2) Soit $n \geqslant 2$ un entier. On note par φ la fonction d'Euler.

Soit d un diviseur de n. On pose

$$A_d = \{k \in \mathbb{N} \mid 1 \leqslant k \leqslant n \text{ et } \operatorname{pgcd}(k, n) = d\}.$$

(a) Pour $n = 16$, trouver A_4.

(b) Soit $k \in A_d$. Montrer que k s'écrit $k = dl$ avec $\operatorname{pgcd}(l, \frac{n}{d}) = 1$.

(c) Réciproquement, soit $k \in \mathbb{N}$ tel que $k = dl$ où $l \in \mathbb{N}$ avec $1 \leqslant l \leqslant \frac{n}{d}$ et $\operatorname{pgcd}(l, \frac{n}{d}) = 1$. Montrer que $k \in A_d$ (indication : utiliser le résultat de la question (1)).

(3) Montrer que card$A_d = \varphi(\frac{n}{d})$.

Chapitre V

Polynômes

V.1 Notations, premières propriétés et exemples

Soient :

• $\mathbb{F}$ un corps commutatif,

• $\mathbb{F}[X]$ est l'anneau des polynômes à coefficients dans $\mathbb{F}$, avec la variable X :

$$\mathbb{F}[X] = \{f(X) = f_0 + f_1 X + \cdots + f_m X^m \mid m \in \mathbb{N}, \quad f_i \in \mathbb{F}\}.$$

Pour $f(X) \in \mathbb{F}[X]$, on peut aussi écrire

$$f(X) = \sum_{i=0}^{m} f_i X^i = \sum_{i=0}^{m} f_i X^i + 0X^{m+1} + \cdots + 0X^{m+r}. \tag{V.1}$$

pour tout entier $r \geqslant 1$ (on ne change pas $f(X)$ en ajoutant les monômes $0X^j$ avec $j > m$).

• Le *polynôme nul* est $0(X) = 0 = 0 + 0X = 0 + 0X + \cdots + X^r$ où $r \in \mathbb{N}^*$.

• On dit que $f(X)$ est un polynôme *constant* si $f(X) = f_0 \in \mathbb{F}$. Le polynôme nul est donc un polynôme constant.

Soient $f(X), g(X) \in \mathbb{F}[X]$, avec

$$f(X) = f_0 + f_1 X + \cdots + f_m X^m$$
$$g(X) = g_0 + g_1 X + \cdots + g_n X^n.$$

Ces polynômes sont égaux si $f_i = g_i$ pour $i = 0, \ldots, \max(m, n)$ (en utilisant (V.1)).

• La somme de $f(X)$ et $g(X)$ est effectuée "coefficients par coefficients" :

$$f(X) + g(X) = (f_0 + g_0) + (f_1 + g_1)X + \cdots + (f_k + g_k)X^k + \cdots + (f_r + g_r)X^r \tag{V.2}$$

avec $r = \max(m, n)$. Dans cette formule, on prend $f_k = 0$ si $k > m$ et $g_k = 0$ si $k > n$.

• Le produit de $f(X)$ et $g(X)$ est :

$$\begin{aligned} f(X)g(X) &= \sum_{k=0}^{m+n} \Big(\sum_{i+j=k} f_i g_j \Big) X^k \\ &= \sum_{k=0}^{m+n} \Big(\sum_{\substack{0 \leqslant i \leqslant m \\ 0 \leqslant k-i \leqslant n \\ 0 \leqslant i \leqslant k}} f_i g_{k-i} \Big) X^k. \end{aligned} \tag{V.3}$$

Le produit est aussi appelé convolution.

Nous avons alors le résultat suivant ;

Proposition V.1.1 (L'algèbre des polynômes)**.** *L'ensemble* $(\mathbb{F}[X], +, \times)$ *des polynômes muni de l'addition et du produit est un anneau commutatif, i.e. :*

(1) $(\mathbb{F}[X], +, \times)$ *est groupe commutatif,*

(2) *La multiplication est associative, distributive par rapport à l'addition, admet* 1 *comme élément neutre et commutative.*

(3) *De plus, la multiplication d'un polynôme par un scalaire munit l'anneau* $(\mathbb{F}[X], \times, +)$ *d'un structure d'algèbre.*

Démonstration. Exercice. □

• Si $f(X)$ est non nul, avec $f(X) = f_0 + f_1 X + \cdots + f_m X^m$ le degré de $f(X)$ est

$$\deg f(X) = \deg f = \max\{i \in \{0, \ldots, m\} \mid f_i \neq 0\}.$$

• Si $f = f_0 \neq 0$ ($f(X)$ est constant et non nul), alors $\deg f = 0$.

• Si f est le polynôme nul : $f(X) = 0$, on pose $\deg 0 = -\infty$.

On a les propriétés suivantes pour le degré :

Proposition V.1.2 (Propriétés du degré)**.** *Soient* $f(X), g(X) \in \mathbb{F}[X]$*. Alors, on a :*

(1) $f(X) = f_0 + f_1 X + \cdots + f_{\deg f} X^{\deg f}$ *si* $f(X) \neq 0$,

(2) $\deg(f + g) \leqslant \max(\deg f, \deg g)$,

(3) $\deg(fg) = \deg f + \deg g$.

Démonstration. (1) Evident par la définition du degré : $f_i = 0$ pour $i > \deg f$.

(2) Par (V.2) (définition de la somme), l'exposant de X est au plus égale à $r = \max(\deg f, \deg g)$.

(3) Par (V.3) (définition du produit), l'exposant maximale de X est $m + n$ puisque le coefficient de X^{m+n} est $f_m g_n$, qui est non nul car f_m et g_n sont non nuls et que $\mathbb{F}$ est intègre. □

• soit $f(X) \neq 0 \in \mathbb{F}[X]$ avec $\deg f = m$. On a donc

$$f(X) = f_0 + f_1 X + \cdots + f_m X^m.$$

Le *coefficient dominant* $\mathrm{LC}(f)$, l'*exposant dominant* $\mathrm{LE}(f)$ et le monôme dominant $\mathrm{LM}(f)$ de $f(X)$ sont définis par

$$\mathrm{LC}(f) = f_{\deg f} = f_m, \quad \mathrm{LE}(f) = \deg f = m, \quad \mathrm{LM}(f) = X^{\deg f} = X^m. \tag{V.4}$$

• Le polynôme $f(X) = f_0 + f_1X + \cdots + f_mX^m$ (m n'est pas forcément le degré de f, on a $\deg f \leqslant m$) définit la suite finie d'éléments de $\mathbb{F}$

$$(f_0, f_1, \ldots, f_m) \quad \text{(sous forme vectorielle)}$$

ou tout simplement

$$f_0, f_1, \ldots, f_m \quad \text{ou} \quad f_0 f_1 \ldots f_m$$

(on a pris les coefficients suivant les puissances croissantes de X). Réciproquement, toute suite finie d'éléments de $\mathbb{F}$

$$s_0, s_1, \ldots, s_m$$

définit un polynôme de $\mathbb{F}[X]$ par

$$f(X) = s_0 + s_1X + \cdots + s_mX^m,$$

avec $\deg f \leqslant m$.

Exemples V.1.3. (1) Le corps fini à deux éléments est $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$. Les polynômes suivants sont des éléments de $\mathbb{F}_2[X]$:

• Le polynôme nul

$$\begin{aligned} f(X) =& 0 \\ =& 0 + 0X \\ =& 0 + 0X + 0X^2 \\ =& 0 + 0X + \cdots + 0X^m \quad (\text{pour } m \geqslant 2). \end{aligned}$$

On a $\deg f = -\infty$.

• Le (seul) polynôme constant non nul dans $\mathbb{F}_2[X]$ est

$$\begin{aligned} g(X) &= 1 \\ &= 1 + 0X \\ &= 1 + 0X + 0X^2 \\ &= 1 + 0X + 0X^2 + \cdots + 0X^m \ (\text{pour } m \geqslant 3). \end{aligned}$$

On a $\deg g = 0$.

• Autres polynôme

$$\begin{aligned} h(X) &= 1 + X^6 + X^{2020} \\ &= 1 + X^6 + X^{2020} + 0X^{2021} \\ &= 1 + X^6 + X^{2020} + \cdots + 0X^m (\text{pour } m \geqslant\ 2021) \end{aligned}$$

On a $\deg h = 2020$.

(2) Le corps fini à trois éléments est $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$. Soit

$$f(X) = 2 + X + 2X^3 + X^6 \in \mathbb{F}_3[X].$$

La suite des coefficients de $f(X)$ est

$$2,\ 1,\ 0,\ 2,\ 0,\ 0,\ 1.$$

La suite d'éléments de $\mathbb{F}_3$

$$1,\ 0,\ 0,\ 2,\ 2,\ 1,\ 0,\ 0,\ 2$$

définit le polynôme

$$g(X) = 1 + 2X^3 + 2X^4 + X^5 + 2X^8 \in \mathbb{F}_3[X].$$

Soient les polynômes de $\mathbb{F}_3[X]$ suivants

$$u(X) = 2 + 2X + 2X^2 + 2X^4$$
$$v(X) = 2 + 2X^2$$

On a

$$u(X) + v(X) = 1 + 2X + X^2 + 2X^4,$$
$$u(X)v(X) = 1 + X + 2X^2 + X^3 + 2X^4 + X^6.$$

V.2 Division euclidienne

Théorème V.2.1 (Division euclidienne des polynômes)**.** *Soient $f(X), g(X) \in \mathbb{F}[X]$ avec $g(X) \neq 0$. Alors il existe un couple unique de polynômes $(q(X), r(X)) \in \mathbb{F}[X] \times \mathbb{F}[X]$ tels que*

$$f(X) = g(X)q(X) + r(X)$$

avec $r(X) = 0$ ou $\deg r < \deg g$.
Le polynôme $q(X)$ est appelé le quotient et $r(X)$ le reste de la division euclidienne de $f(X)$ par $g(X)$.

Démonstration. Si $\deg f < \deg g$, on pose $q(X) = 0$ et $r(X) = f(X)$. Sinon posons $m = \mathrm{LE}(f)$ et $n = \mathrm{LE}(g)$, avec $m > n$. Prenons

$$q_1(X) = \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)} X^{\mathrm{LE}(f)-\mathrm{LE}(g)} = \frac{f_m}{g_n} X^{m-n}, \tag{V.5}$$

$$r_1(X) = f(X) - q_1(X)g(X) \quad \text{(on a } \deg q_1 g = m \text{ et } \mathrm{LE}(q_1 g) = m\text{)} \tag{V.6}$$

$$= (f_m X^m + f_{m-1}X^{m-1} + \cdots f_i X + \cdots f_0) - (f_m X^m + \text{termes de degrés} < m \text{ de } q_1(X)g(X)) \tag{V.7}$$

$$= (f_{m-1}X^{m-1} + \cdots f_i X + \cdots f_0) - (\text{termes de degrés} < m \text{ de } q_1(X)g(X)) \tag{V.8}$$

Nous avons $\deg r_1 < \deg f$. Si $\deg r_1 < \deg g$, alors $r(X) = r_1(X)$ et $q(X) = q_1(X)$ conviennent pour le reste et le quotient car (V.6) donne

$$f(X) = g(X)q_1(X) + r_1(X) \quad \text{avec } \deg r_1 < \deg g.$$

Sinon on remplace f par $r_1(X)$ et on recommence le processus : on obtient

$$q_2(X) = \frac{\mathrm{LC}(r_1)}{\mathrm{LC}(g)} X^{\mathrm{LE}(r_1)-\mathrm{LE}(g)}, \tag{V.9}$$

$$r_2(X) = r_1(X) - q_2(X)g(X) \quad (\text{on a } \deg q_2 g = m \text{ et } \mathrm{LE}(q_2 g) = \mathrm{LE}(r_1)) \tag{V.10}$$

$$= (f_{\mathrm{LE}(r_1)} X^{\mathrm{LE}(r_1)} + f_{\mathrm{LE}(r_1)-1} X^{\mathrm{LE}(r_1)-1} + \cdots f_i X^i + \cdots f_0) - (f_{\mathrm{LE}(r_1)} X^{\mathrm{LE}(r_1)} \tag{V.11}$$

$$+ \text{termes de degrés } < m \text{ de } q_2(X)g(X)) \tag{V.12}$$

$$= (f_{\mathrm{LE}(r_1)-1} X^{\mathrm{LE}(r_1)-1} + \cdots f_i X^i + \cdots f_0) - (\text{termes de degrés } < \mathrm{LE}(r_1) \text{ de } q_1(X)g(X)) \tag{V.13}$$

Nous avons, $\deg r_2 < \deg r_1$. Si $\deg r_2 < \deg g$, alors $r(X) = r_2(X)$ et $q(X) = q_1(X) + q_2(X)$ conviennent pour le reste et le quotient car (V.10) et (V.6) donnent

$$r_1(X) = r_2(X) + q_2(X)g(X)$$
$$f(X) = r_1(X) + q_1(X)g(X) = (q_1(X) + q_2(X))g(X) + r_1(X) \quad \text{avec } \deg r_2 < \deg g.$$

On continue ains le processus ; on obtient des polynômes $r_1, \ldots, r_i, \ldots$ et $g_1, \ldots, g_i \ldots$ avec

$$\deg r_1 > \deg r_2 > \cdots > \deg r_i > \cdots$$

et

$$f(X) = (q_1(X) + \cdots q_i(X))g(X) + r_i(X).$$

D'après le principe du bon ordre, il existe un entier plus petit entier N tel que $\deg r_N < \deg g$ (on peut aussi avoir $r_N(X) = 0$ dans ce cas). Alors $r(X) = r_N(X)$ et $q(X) = q_1(X) + \cdots q_N(X)$ conviennent pour le quotient et le reste. □

Notations. Le quotient $q(X)$ est noté par $f(X)$ div $g(X)$ ou $f(X)$ quot $g(X)$ et le reste $r(X)$ par $f(X) \mod g(X)$. On a donc

$$f(X) = g(X)(f(X)\mathrm{div}g(X)) + (f(X) \bmod g(X)).$$

V.3 Polynômes irréductibles

Définition V.3.1 (Polynômes irréductibles)**.** Un polynôme irréductible sur $\mathbb{F}_p$ est un polynôme $f(X)$ non constant de $\mathbb{F}_p[X]$ dont on ne peut plus factoriser en un produit de deux polynômes de moindres degrés : il n'existe pas de polynômes $g(X), h(X) \in \mathbb{F}_p[X]$ tels que

$$f(X) = g(X)h(X)$$

avec $\deg g < \deg f$ et $\deg h < \deg f$.

Autrement dit, le polynôme $f(X)$ est irréductible si lorsque l'on a

$$f(X) = g(X)h(X),$$

alors, forcément, $\deg g = \deg f$ ou $\deg h = \deg f$.

Exemples V.3.2. (1) Un polynôme de degré 1 est toujours irréductible sur $\mathbb{F}_p$: soit $f(X) = aX + b$ avec $a \neq 0$. Alors n'est pas constante. Si $f(X) = g(X)h(X)$, alors

$$\deg f = 1 = \deg g + \deg h.$$

Puisque $\deg g$ et $\deg h \in \mathbb{N}$, on a $(\deg g = 1$ et $\deg h = 0)$ ou $(\deg g = 0$ et $\deg h = 1)$. Donc, on a toujours $\deg g = \deg f$ ou $\deg h = \deg f$.
(2) Soit $f(X) = X^2 + X + 1 \in \mathbb{F}_2[X]$. Nous allons montrer que f est irréductible sur $\mathbb{F}_2$. Supposons que l'on ait $f(X) = g(X)h(X)$ avec $f, g \in \mathbb{F}_2\,|X]$. Enprenant les degrés, on a

$$\deg f = 2 = \deg g + \deg h.$$

Trois cas sont alors possibles :
$\underline{1^{\text{er}}\text{cas}}$: $\deg g = 1$ et $\deg h = 1$,
$\underline{\text{2ème cas}}$: $\deg g = 0$ et $\deg h = 2$,
$\underline{\text{3 ème cas}}$: $\deg g = 2$ et $\deg h = 0$.

Dans le premier cas, on a

$$g(X) = X + u, \quad h(X) = X + v$$

avec $u, v \in \{0, 1\}$ et

$$f(X) = (X + u)(X + v),$$
$$X^2 + X + 1 = X^2 + (u + v)X + uv.$$

En identifiant les coefficients, nous avons

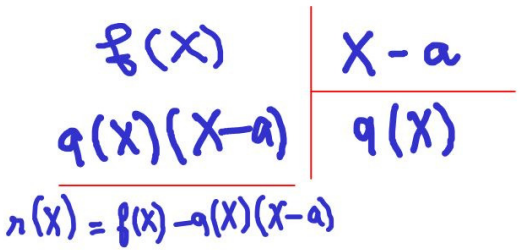
$$\begin{cases} 1 = u + v & (1) \\ 1 = uv & (2) \end{cases}$$

D'après l'équation (2), on a $u \neq 0$ et $v \neq 0$. Donc forcément, $u = v = 1$. En rapportant ce valeur dans (1), on a $1 = 1 + 1 = 0$, ce qui est faux. Donc ce système n'a pas de solution.
Donc seuls le deuxième et le troisième cas sont possibles. On obtient, $\deg h = \deg f$ ou $\deg g = \deg f$. Donc $X^2 + X + 1$ est irréductible.

Voici une propriété importante des polynômes irréductibles.

Proposition V.3.3. *Soit $f(X) \in \mathbb{F}_p[X]$ un polynôme irréductible de degré $\geqslant 2$. Alors $f(X)$ n'a pas de racines dans $\mathbb{F}_p$. Autrement dit, il n'existe aucun $a \in \mathbb{F}_p$ tel que $f(a) = 0$.*

Démonstration. Supposons que $f(a) = 0$ où $a \in \mathbb{F}_p$. Nous allons effectuer la division euclidienne de $f(X)$ par $X - a$:



Nous avons alors

$$f(X) = q(X)(X-a) + r(X)$$

avec

$$r(X) = 0 \quad \text{ou} \quad \deg r(X) < \deg(X-a) = 1.$$

Ainsi $r(X) = 0$ ou $\deg r(X) = 0$, c'est-à -dire que $r(X)$ est une constante non nulle. Donc, dans tous les cas, $r(X)$ est une constante $c \in \mathbb{F}_p$. Comme

$$r(X) = f(X) - q(X)(X-a) = c,$$

on a

$$\begin{aligned} r(a) &= f(a) - q(a)(a-a) \\ &= 0 - q(a) \cdot 0 = 0 = c. \end{aligned}$$

Ainsi, $r(X) = c = 0$ et

$$f(X) = q(X)(X-a).$$

De plus,

$$\begin{aligned} \deg f &= \deg q + \deg(x-a) \\ &= \deg q + 1. \end{aligned}$$

Il en résulte que $\deg q < \deg f$ et puisque $\deg f \geqslant 2$, on a aussi $\deg(X-1) < \deg f$. On a factorisé $f(X)$ en des polynômes de moindres degrés que celui de $f(X)$. Donc $f(X)$ n'est pas irréductible, ce qui est contraire à l'hypothèse. Par suite, $f(X)$ ne peut pas avoir une racine. □

La Proposition V.3.3 donne aussi une critère de non-réductiblilité.

Corollaire V.3.4. *Un polynôme de $\mathbb{F}_p[X]$ qui possède une racine dans $\mathbb{F}_p$ n'est pas irréductible sur $\mathbb{F}_p$.*

Remarques 1. (1) La Proposition V.3.3 ne s'applique pas pour les polynômes de degré 1 : le polynôme $f(X) = aX + b$ avec $a \neq 0$ est irréductible mais a pour racine $-\frac{b}{a}$.
(2) La réciproque de le Proposition V.3.3 n'est pas forcément vraie : la non-existence de racines n'entraîne pas l'irréductibilité. Par exemple,

$$f(X) = (X^2 + X + 1)^2 = X^4 + X^2 + 1 \in \mathbb{F}_2[X]$$

n'est pas irréductible même s'il n'a pas de racines (sinon X^2+X+1 en posséderait. Or, on a vu dans la partie (2) de Exemple V.3.2 que c'est irréductible sur $\mathbb{F}_2$).

Toutefois, la réciproque de la Proposition V.3.3 est vraie pour les polynômes de degrés 2 ou 3 :

Proposition V.3.5. *Soit $f(X) \in \mathbb{F}[X]$ avec $\deg f = 2$ ou 3. Si $f(X)$ n'a pas de racines dans $\mathbb{F}$, alors il est irréductible sur $\mathbb{F}$.*

Démonstration. Cas $\deg f = 2$. Supposons que $f(X)$ n'est pas irréductible sur $\mathbb{F}$. Alors, on peut écrire

$$f(X) = g(X)h(X)$$

où $g, h \in \mathbb{F}[X]$ avec $\deg g < \deg f$ et $\deg h < \deg f$. Puisque

$$\deg f = 2 = \deg g + \deg h,$$

on a forcément $\deg g = \deg h = 1$. Mais, étant de degré 1, g et h possède des racines, qui sont aussi racines de f, ce qui est faux, car f n'en a pas.

Cas $\deg f = 3$. Démonstration analogue à la précédente : si f n'était pas irréductible, il posséderait un facteur de degré 1 et qui posséderait alors une racine, ce qui est impossible. □

Exemples V.3.6. (1) Soit $f(X) = X^2+X+1 \in \mathbb{F}_2[X]$. On a $\deg f = 2$ et

$$\begin{aligned} f(0) &= 0^2+0+1 = 1 \neq 0, \\ f(1) &= 1^2+1+1 = 3 \mod 2 = 1 \neq 0. \end{aligned}$$

Ainsi, f n'a pas de racines dans $\mathbb{F}_2$. D'après la Proposition V.3.3, il est irréductible sur $\mathbb{F}_2$.

(2) Soit $f(X) = X^3+X+2 \in \mathbb{F}_3[X]$. On a $\deg f = 3$ et

$$\begin{aligned} f(0) &= 0^3+0+2 = 2 \neq 0, \\ f(1) &= 1^3+1+2 = 4 \mod 3 = 1 \neq 0, \\ f(2) &= 2^3+1+1 = 10 \mod 3 = 1 \neq 0. \end{aligned}$$

Ainsi, f n'a pas de racines dans $\mathbb{F}_3$. Donc, d'après la Proposition V.3.3 , il est irréductible sur $\mathbb{F}_3$.

Nous admettons le théorème suivant :

Théorème V.3.7 (Existence de polynômes irréductibles)**.** *Soit p un entier premier et $m \geqslant 1$ un entier quelconque. Alors il existe dans $\mathbb{F}[X]$ un polynôme irréductible de degré m.*

Exercices sur le Chapitre V

N.B. La notation $\mathbb{F}$ désigne un corps commutatif, X une variable et $\mathbb{F}[X]$ l'anneau des polynômes sur $\mathbb{F}$ avec la variable X.

Exercice 8. Montrer que $f(X) = X^4 + X + 1$ est irréductible sur $\mathbb{Z}/2\mathbb{Z}$.

Exercice 9. Montrer que les polynômes suivants sont irréductibles sur les corps donnés :
(1) $X^3 + X + 1$ sur $\mathbb{Z}/2\mathbb{Z}$,
(2) $X^2 + X + 2$ sur $\mathbb{Z}/3\mathbb{Z}$.

Exercice 10. Montrer qu'un polynôme $f(X) \in \mathbb{F}[X]$ est inversible dans $\mathbb{F}[X]$ si et seulement si c'est une constante non nulle. Autrement dit, $\mathbb{F}[X]^\times = \mathbb{F}^*$.

Exercice 11 (pgcd et Théorème de Bézout)**.** Si $f(X) \in \mathbb{F}[X]$, un *diviseur* de $f(X)$ est un polynôme non nul $d(X) \in \mathbb{F}[X]$ tel que $f(X) \mod d(X) = 0$, i.e. il existe $e(X) \in \mathbb{F}[X]$ tel que $f(X) = d(X)e(X)$. Dans ce cas, on écrit $d(X)|f(X)$.
Pour $f(X), g(X) \in \mathbb{F}[X]$ non tous nuls, un *plus grand commun diviseur* de $f(X)$ et de $g(X)$ est un diviseur commun $d(X) \in \mathbb{F}[X]$ à $f(X)$ et $g(X)$ tel que pour tout autre diviseur commun $d'(X)$ à $f(X)$ et $g(X)$, on a $d'(X)|d(X)$.
(1) Soit $f(X), g(X) \in \mathbb{F}[X]$ non tous nuls et

$$I = \{f(X)u(X) + g(X)v(X) | u, v \in \mathbb{F}[X]\}.$$

(a) Montrer que I est un idéal de $\mathbb{F}[X]$.
(b) Montrer qu'il existe $d(X) \in I$ tel que $I = \langle d(X) \rangle$.
(c) Montrer $d(X)$ est un plus grand commun diviseur de $f(X)$ et de $g(X)$.
(d) Montrer qu'il existe des polynômes $u(X), v(X) \in \mathbb{F}[X]$ tels que

$$d(X) = f(X)u(X) + g(X)v(X).$$

(2) Soient $f(X), g(X) \in \mathbb{F}[X]$ non tous nuls. Démontrer qu'il existe un unique pgcd de $f(X)$ qui est *unitaire*, c'est-à-dire dont le coefficient dominant est égal à 1. Ce plus grand commun diviseur est appelé le pgcd de $f(X)$ et de $g(X)$ et noté par $\mathrm{pgcd}(f(X), g(X))$.

Exercice 12 (Algorithme d'Euclide)**.** Les notations sont de l'Exercice 11.
(1) Soit $f(X) \in \mathbb{F}[X]$ un polynôme non nul. Trouver $\mathrm{pgcd}(f(X), 0)$.

(2) On suppose $f(X)$ et $g(X)$ sont non tous nuls, avec $\deg f > \deg g$. On effectue la division euclidienne de $f(X)$ par $g(X)$: il existe $q(X)$ et $r(X)$ tels que

$$f(X) = g(X)q(X) + r(X) \quad \text{avec } r(X) = 0 \text{ ou } \deg r(X) < \deg g(X).$$

Montrer que $\mathrm{pgcd}(f(X), g(X)) = \mathrm{pgcd}(g(X), r(X))$.

(3) Soient toujours $f(X), g(X) \in \mathbb{F}[X]$ non nuls avec $\deg f > \deg g$. On effectue la division euclidienne de $f(X)$ par $g(X)$:

$$f(X) = g(X)q_1(X) + r_1(X) \quad \text{avec } r_1(X) = 0 \text{ ou } \deg r_1 < \deg g.$$

Si $r_1(X) \neq 0$, on effectue la division euclidienne de $g(X)$ par $r_1(X)$

$$g(X) = r_1(X)q_2(X) + r_2(X) \quad \text{avec } r_2(X) = 0 \text{ ou } \deg r_2 < \deg g.$$

Si $r_2(X) \neq 0$, on effectue la division euclidienne de $r_1(X)$ par $r_2(X)$

$$r_1(X) = r_2(X)q_3(X) + r_3(X) \quad \text{avec } r_3(X) = 0 \text{ ou } \deg r_3 < \deg r_2.$$

On continue le processus : tant que $r_i(X) \neq 0$, on effectue la division euclidienne de $r_{i-1}(X)$ par $r_i(X)$:

$$r_{i-1}(X) = r_i(X)q_1(X) + r_{i+1}(X) \quad \text{avec } r_{i+1}(X) = 0 \text{ ou } \deg r_{i+1} < \deg r_i.$$

(1) Montrer qu'il existe N tel que $r_N(X) = 0$.

(2) Montrer que $\mathrm{pgcd}(f(X), g(X)) = r_{N-1}(X)$.

Exercice 13. Calculer $\mathrm{pgcd}(X^5 - 2X^4 + X^3 - X^2 + 2X - 1, X^3 - X^2 + 2X - 2)$ dans $\mathbb{R}[X]$.

Exercice 14. On dit que deux polynômes $f(X), g(X) \in \mathbb{F}[X]$ sont *premiers* entre eux s'ils possèdent un pgcd qui est une constante non nulle de $\mathbb{F}$. Demontrer qu'ils sont premiers entre eux si et seulement si $\mathrm{pgcd}(f(X), g(X)) = 1$.

Exercice 15. (1) Soit $f(X) \in \mathbb{F}[X]$ un polynôme non constant, de degré $m \in \mathbb{N}^*$. On définit la relation de *congruence modulo* $f(X)$ dans $\mathbb{F}[X]$ par

$$a(X) \equiv b(X) \pmod{f(X)} \iff a(X) - b(X) \in f(X)\,\mathbb{F}[X] \tag{V.14}$$

$$\iff \text{il existe } h(X) \in \mathbb{F}[X] \text{ tel que } a(X) - b(X) = h(X)f(X) \tag{V.15}$$

(1) Montrer que $\equiv \mathrm{mod} f(X)$ est une relation d"équivalence dans $\mathbb{F}[X]$.

(2) Montrer que $a(X) \equiv b(X) \pmod{f(X)}$ dans $\mathbb{F}[X]$ si et seulement si $a(X)$ et $b(X)$ ont le même reste par la division euclidienne par $f(X)$.

(3) Pour $a(X) \in \mathbb{F}[X]$, on note par $\overline{a(X)}$ la classe de $a(X)$ pour cette relation. Trouver cette classe.

(4) On note par $\mathbb{F}[X]/\langle f(X)$ l'ensemble-quotient pour cette relation :

$$\mathbb{F}[X]/\langle f(X)\rangle = \{\overline{g(X)} \mid g(X) \in \mathbb{F}[X]\}, \tag{V.16}$$

On munit $\mathbb{F}[X]/\langle f(X)\rangle$ des opérations d'addition et de multiplication définies par

$$\overline{a(X)} + \overline{b(X)} = \overline{a(X) + b(X)} \tag{V.17}$$

$$\overline{a(X)} \times \overline{b(X)} = \overline{a(X) \times b(X)}. \tag{V.18}$$

pour $a(X)$ et $b(X) \in \mathbb{F}[X]$.

(a) Montrer que $(\mathbb{F}[X]/\langle f(X)\rangle, +, \times)$ est un anneau commutatif.

(b) Montrer que $(\mathbb{F}[X]/\langle f(X)\rangle, +, \times)$ est un corps si et seulement si $f(X)$ est irréductible sur $\mathbb{F}$.

Chapitre VI

Le théorème fondamental de l'algèbre et ses conséquences

Dans ce chapitre, $\mathbb{F}$ désignera un corps commutatif et $\mathbb{F}[X]$ l'anneau des polynômes avec la variable X.

VI.1 Racines d'un polynôme

Proposition VI.1.1 (Nombre de racines d'un polyôme)**.** *Soit $n \geqslant 0$ un entier. Alors un polynôme non nul de degré n de $\mathbb{F}[X]$ a au plus n racines distinctes.*

Démonstration. : Par récurrence sur n. Pour $n = 0$, un polynôme constant non nul possède évidemment zéro racine, et un polynôme de degré 1 possède une seule racine. Soit n fixé, supposons le résultat vrai pour les polynômes de degré n ; soit maintenant$f(X)$ un polynôme de degré $n+1$. Si $f(X)$ n'a aucune racine, le résultat est vrai pour $f(X)$; sinon soit $a \in \mathbb{F}$ une racine de $f(X)$; on sait que l'on peut écrire $f(X) = (X-a)q(X)$ pour un polynôme $q(X) \in \mathbb{F}[X]$ qui est clairement de degré n. Maintenant, si b est une racine de $f(X)$, alors $0 = f(b) = (b-a)f(b)$, donc $b = a$ ou b est une racine de $q(X)$ (on utilise l'hypothèse d"intégrité de $\mathbb{F}$) ; or $q(X)$ a au plus n racines, donc $f(X)$ en a au plus $n+1$. □

Le corollaire suivant est immédiat :

Corollaire VI.1.2 (Polynôme nul)**.** *Le seul polynôme ayant une infinité de racines est le polynôme nul.*

Définition VI.1.3 (Ordre d'une racine)**.** Soient $f(X) \in \mathbb{F}[X], r \in \mathbb{N}^*$ et $a \in \mathbb{F}$. On dit que a est *racine d'ordre* r de $f(X)$ s'il existe un polynôme $q(X)$ tel que $f(X) = (X-a)^r q(X)$ avec $q(a) \neq 0$. Autrement dit, a est racine d"ordre r de $f(X)$ si $f(X)$ est divisible par $(X-a)^r$ mais pas par $(X-a)^{r+1}$.

Terminologie. Une racine est dite *simple* si elle est d'ordre 1, *double* si elle est d'ordre 2,. . .. D'une manière générale, l'entier r est appelé l'*ordre de multiplicité* de la racine.

VI.2 Les nombres complexes

Le polynôme $f(X) = X^2 + 1$ est de degré 2 et n'a pas de racines dans $\mathbb{R}$. On sait que dans ce cas, il est irréductible sur $\mathbb{R}$. Donc l'anneau-quotient

$$\mathbb{R}[X]/\langle X^2 + 1\rangle = \{a + b\overline{X} \,|a, b \in \mathbb{R}\}$$

est un corps (commutatif) qui contient $\mathbb{R}$ et que $\overline{X}$ est une racine de $f(X)$ dans ce corps (voir TD sur Chap. V) : on a

$$f(\overline{X}) = \overline{X}^2 + 1 = \overline{X^2 + 1} = \overline{0}.$$

Définition VI.2.1 (Le corps $\mathbb{C}$)**.** Le corps des *nombres complexes* est défini par

$$\mathbb{C} = \mathbb{R}[X]/\langle X^2 + 1\rangle = \{a + b\overline{X} \mid a, b \in \mathbb{R}\}.$$

Notation La classe $\overline{X}$ de X modulo $X^2 + 1$est noté par i. Donc i est racine de $X^2 + 1$, i.e. $i^2 = -1$.

Nous avons alors le théorème suivant

Théorème VI.2.2. *Soit $g(X)$ un polynôme de degré 2, irréductible sur $\mathbb{R}$. Alors, on l'isomorphisme de corps*

$$\mathbb{C} \longleftrightarrow \mathbb{R}[X]/\langle g(X)\rangle,$$
$$a + bi \longleftrightarrow a + b\overline{X},$$

de sorte que l'on peut identifier les deux corps.

Exemple VI.2.3. On a donc aussi

$$\mathbb{C} = \mathbb{R}[X]/\langle X^2 + 6\rangle = \mathbb{R}[X]/\langle 4X^2 + X + 7\rangle.$$

VI.3 Le théorème fondamental de l'algèbre et ses conséquences

Définition VI.3.1 (Polynôme scindé)**.** Un polynôme est dit *scindé* s"il peut s'ecrire comme produit de facteurs du premier degré.

Nous admettons le théorème fondamental de l'Algèbre, appelé aussi le théorème de d'Alembert-Gauß :

Théorème VI.3.2 (d'Alembert-Gauß)**.** *Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine complexe.*

Le corollaire suivant est alors immédiat :

Théorème VI.3.3 (Polynômes irréductibles sur $\mathbb{C}$)**.** *Les polynôммes irréductibles dans $\mathbb{C}[X]$ sont exactement les polynômes du premier degré.*

Démonstration. On sait déjà que les polynômes du premier degré sont irréductibles. Montrons que ce sont les seuls. Les polynômes constants n'étant pas irréductibles, soit $f(X)$ un polynôme de $\mathbb{C}[X]$ de degré au moins 2. Le polynôme $f(X)$ a alors au moins une racine a dans $\mathbb{C}$ et donc $f(X)$ peut s'écrire $f(X) = (X-a)q(X)$ avec $1 \leqslant \deg q(X) < \deg f$. Mais dans ce cas, $f(X)$ n'est pas irréductible, ce qui est contraire à l'hypothèse. Donc, nécessairement, $\deg f = 2$. □

Le corollaire suivant est alors immédiat :

Corollaire VI.3.4. *Tout polynôme de $\mathbb{C}[X]$ est scindé. Un polynôme de $\mathbb{C}[X]$ de degré d a donc exactement d racines complexes (comptées avec multiplicité).*

VI.4 Cas des polynômes à coefficients réels

Evidemment, tout polynôme à coefficients réels peut être vu comme polynôme à coefficients complexes (les réels étant des complexes particuliers).

Proposition VI.4.1. *Soient $f(X) \in \mathbb{C}[X]$ et $a \in \mathbb{C}$. Alors, a est racine de $f(X)$ (vu comme polynôme de $\mathbb{C}[X]$) si et seulement si son conjugué $\overline{a}$ est racine de $f(X)$. En particulier, les racines complexes non réelles de $f(X)$ sont deux à deux conjuguées.*

Démonstration. Exercice. □

Théorème VI.4.2 (Polynômes irréductibles sur $\mathbb{R}$)**.** *Les polynômes irréductibles dans $\mathbb{R}[X]$ sont :*
(1) *les polynômes de degré 1,*
(2) *les polynômes de degré 2 sans racine dans $\mathbb{R}$, i.e. de la forme aX^2+bX+c avec $b^2-4ac<0$. Tout polynôme non constant $f(X) \in \mathbb{R}[X]$ s'écrit donc comme produit de polynômes de ces types.*

Démonstration. Les polynômes mentionnés sont clairement irréductibles. Il reste à voir que tout $f(X) \in \mathbb{R}[X]$ avec $\deg f(X) > 1$ est divisible par un polynôme du type mentionné. Si $f(X)$ a une racine r réelle, c'est vrai, car il est divisible par $X-r$. Sinon, $f(X)$ peut être considéré comme appartenant à $\mathbb{C}[X]$ et il a une racine $a \in \mathbb{C}$, grâce au théorème de d'Alembert-Gauß. La proposition VI.4.1 montre alors que $\overline{a}$ est aussi racine de $f(X)$. Ainsi $f(X)$ est divisible dans $\mathbb{C}[X]$ par les deux polynômes irréductibles distincts $X-a$ et $X-\overline{a}$, donc aussi par le produit $g(X) = (X-a)(X-\overline{a}) = X^2 - 2\mathrm{Re}(a)X + |a|^2$., qui est un polynôme de degré 2 de $\mathbb{R}[X]$ irréductible. La division euclidienne de $f(X)$ par $g(X)$ dans $\mathbb{R}[X]$ s'écrit $f(X) = g(X)q(X) + r(X)$ avec $\deg r < 2$. Cette relation peut être vue comme

une égalité de polynômes de $\mathbb{C}[X]$ et c'est donc aussi la division euclidienne de $f(X)$ par $g(X)$ dans $\mathbb{C}[X]$. Par unicité du reste, on a $r(X) = 0$ et finalement $f(X) = g(X)q(X)$ est divisible par $g(X)$ dans $\mathbb{R}[X]$. □

Exercices sur le Chapitre VI

Exercice 16. (1) Soit $f(X) \in \mathbb{R}[X]$ un polynôme non constant, sans racine réelle. Montrer que $\deg f$ est pair.
(2) Soit $f(X) \in \mathbb{C}[X]$ un polynôme de degré impair. Montrer de deux façons (sans utiliser le théorème des valeurs intermédiaires) que $f(X)$ possède au moins une racine réelle.

Exercice 17. Soit $n \geqslant 2$ un entier. Quelles sont les racines de $Z^n - 1$? (racines n-ièmes de l'unité).

Exercice 18. (1) Soit $n \geqslant 2$ un entier et $\alpha \in \mathbb{C}^*$. Trouver les racines de $Z^n - \alpha$ dans $\mathbb{C}$ racines n-ième de $\mathbb{C}$).
(2) Trouver les racines de $X^4 - 3$ dans $\mathbb{C}$.
(3) Trouver les racines 6-ièmes de 5 dans $\mathbb{C}$.