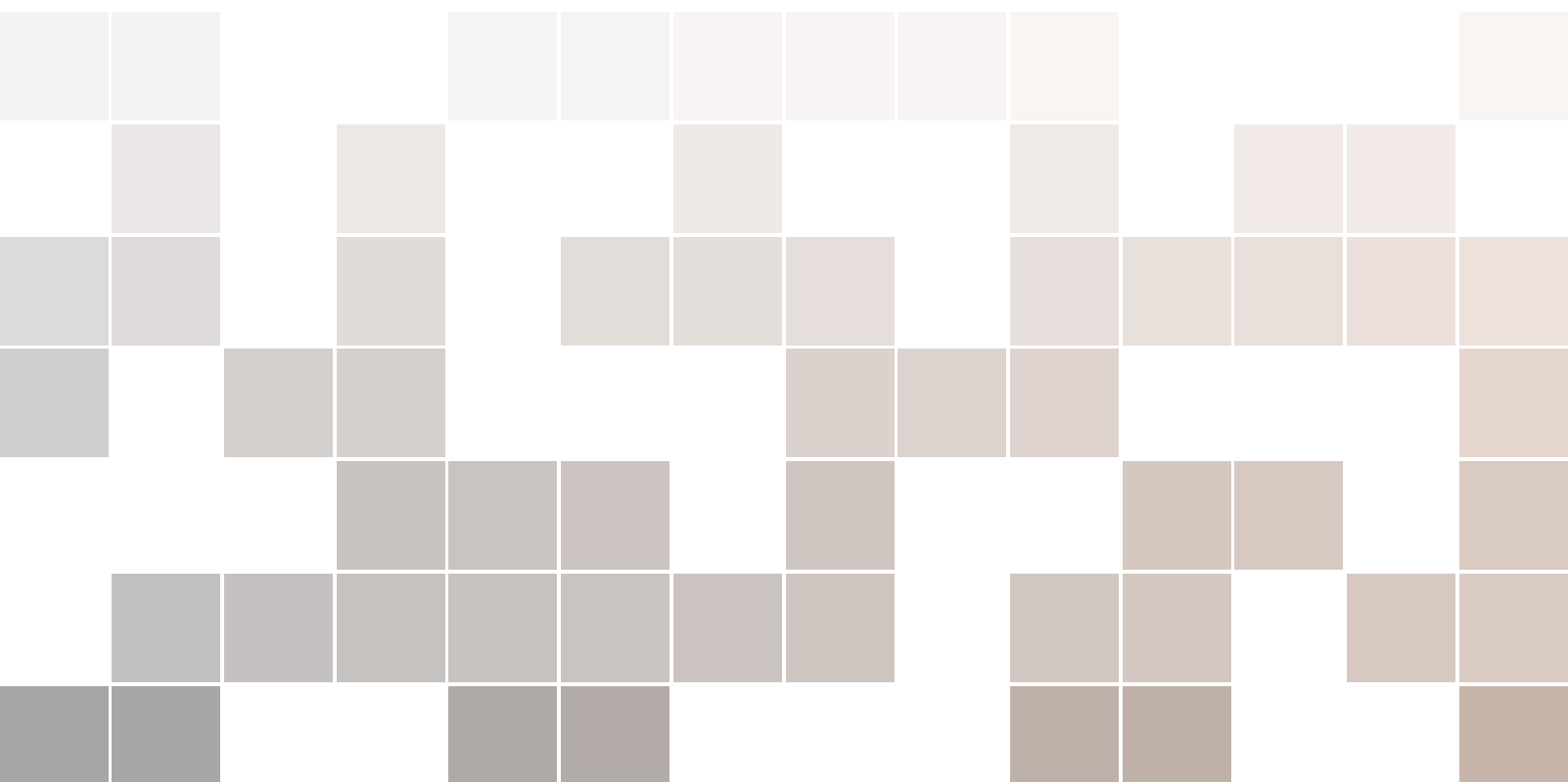


Algèbre I, polycopié

Printemps 2024

Michelle Bucher



Introduction

Ce cours concerne l'étude de trois objets algébriques fondamentaux : les groupes, les anneaux et les corps, qui sont trois objets omniprésents dans toutes les mathématiques. La théorie des groupe permet l'étude des symétries. La théorie des anneaux donne un cadre plus général aux propriétés arithmétiques bien connues de \mathbb{Z} . Pour les corps, nous nous concentreront sur les corps finis et leurs applications en théorie des nombres. Outre la théorie des nombres, nous verrons de nombreuses applications en arithmétique ou cryptographie.

Les notions introduites dans ce cours ne sont pas compliquées en soi. Mais elles sont à priori très abstraites. Votre plus grand travail sera de donner vie à toutes ces nouvelles définitions. C'est tout à fait possible en les exemplifiant, en les manipulant.

L'ordre de présentation de ce polycopié suit l'ordre de présentation du cours, à quelques exceptions près : Toutes les propriétés d'arithmétique, dont nous aurons par exemple crucialement besoin pour définir les lois d'addition et multiplications modulo n , sont détaillées dans l'Annexe, mais apparaîtront dans le cours au fur et à mesure. De même, un paragraphe spécifique est dédié au groupe symétrique, mais les diverses représentations d'éléments du groupe symétrique seront présentées plus tôt dans le cours.

Beaucoup d'erreurs typographiques ont été corrigées par la volée précédente ainsi que leurs assistants, que je remercie chaleureusement pour leur lecture attentive, mais il en reste certainement encore quelques unes pour votre volée. Je vous serai reconnaissante de me les signaler.

Table des matières

1	Groupes	7
1.1	Lois de compositions	7
1.2	Groupes : Définition et exemples	10
1.3	Sous-groupes	16
1.4	Homomorphismes et isomorphismes	18
1.5	Indice et Théorème de Lagrange	23
1.6	Sous-groupes normaux et quotients	27
1.7	Groupes simples	32
1.8	Groupes cycliques	33
1.9	Groupes symétriques	37
1.10	Actions de groupes	48
2	Anneaux	59
2.1	Définition et exemples	59
2.2	Homomorphismes d'anneaux	64
2.3	Idéaux et anneaux quotients	69
2.4	Idéaux maximaux et premiers	74
2.5	Factorisation dans un anneau intègre	80
2.6	L'anneau des polynômes	84
2.7	Anneaux Euclidiens	97
2.8	Théorème des restes chinois	101
2.9	Conjecture de Fermat / Théorème de Wiles	103

3	Corps	109
3.1	Corps finis	109
3.2	Polynômes cyclotomiques et Théorème de Dirichlet faible	116
A	Annexe : Arithmétique	121
A.1	Division Euclidienne ou division avec reste	121
A.2	Arithmétique modulaire	124
A.3	Cryptographie RSA	131

1. Groupes

La théorie des groupes est, pour ainsi dire, la Mathématique entière, dépouillée de sa matière et réduite à une forme pure.
Poincaré, 1915.

1.1 Lois de compositions

Les ensembles de nombres classiques, \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} ou \mathbb{C} , admettent des opérations (ou lois de compositions) naturelles comme l'addition, la soustraction, la multiplication, la division, etc. Le but de ce premier paragraphe est de généraliser ces opérations bien connues à des objets plus abstraits tout en en extrayant leurs propriétés.

Définition 1.1 Une loi de composition (interne) sur un ensemble E est une application

$$\begin{aligned}\circ : E \times E &\longrightarrow E \\ (x, y) &\longmapsto x \circ y.\end{aligned}$$

On dénote par (E, \circ) l'ensemble E muni de la loi \circ .

Par exemple l'addition $+$ est une loi de composition interne sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou \mathbb{C} . De même pour la multiplication \cdot . La soustraction $-$, elle, n'est pas une loi interne sur \mathbb{N} puisque $0 - 1 = -1 \notin \mathbb{N}$, alors que $0, 1 \in \mathbb{N}$. Mais elle l'est sur les autres ensembles de nombres ci-dessus, à savoir $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et \mathbb{C} . Quant à la division, puisque la division par 0 n'est pas définie, il faut considérer les ensembles de nombres privés de 0. Dans ce cas là, ce n'est pas une loi interne sur \mathbb{N}^* ou \mathbb{Z}^* , mais elle l'est sur $\mathbb{Q}^*, \mathbb{R}^*$ et \mathbb{C}^* .

Parmi les nombreuses propriétés qu'on pourrait exiger d'une loi de composition, voici les plus pertinentes pour les structures algébriques que nous allons considérer par la suite.

Définition 1.2 Soit (E, \circ) un ensemble E muni d'une loi de composition \circ . On dit que

— \circ est *associative* si

$$(x \circ y) \circ z = x \circ (y \circ z) \quad \forall x, y, z \in E,$$

— \circ est *commutative* si

$$x \circ y = y \circ x \quad \forall x, y \in E,$$

— \circ admet un *élément neutre à droite* si il existe $e_d \in E$ tel que

$$x \circ e_d = x \quad \forall x \in E,$$

— \circ admet un *élément neutre à gauche* si il existe $e_g \in E$ tel que

$$e_g \circ x = x \quad \forall x \in E,$$

— \circ admet un *élément neutre* si il existe $e \in E$ qui est à la fois un élément neutre à droite et à gauche.

En présence d'une loi de composition associative il est possible d'omettre les parenthèses des compositions de plus de 2 éléments. On se permettra d'écrire simplement

$$x \circ y \circ z$$

qu'on obtiendra soit en composant

$$(x \circ y) \circ z \quad \text{ou} \quad x \circ (y \circ z).$$

L'addition et la multiplication sont les premiers exemples de lois associatives, alors que la soustraction et la division ne le sont pas. Par exemple

$$\frac{1}{2} = (1 : 1) : 2 \neq 1 : (1 : 2) = 2.$$

De ce fait, l'expression $1 : 1 : 2$ n'a pas de sens. On ne peut donc pas omettre les parenthèses si la loi n'est pas associative.

- **Exemples 1.3**
1. $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des lois de compositions associatives, commutatives, avec 0 comme élément neutre.
 2. (\mathbb{N}, \cdot) , (\mathbb{Z}, \cdot) , (\mathbb{Q}, \cdot) , (\mathbb{R}, \cdot) et (\mathbb{C}, \cdot) sont des lois de compositions associatives, commutatives, avec 1 comme élément neutre.
 3. $(\mathbb{Z}, -)$, $(\mathbb{Q}, -)$, $(\mathbb{R}, -)$ et $(\mathbb{C}, -)$ sont des lois de compositions non associatives, non commutatives, avec 0 comme élément neutre à droite, et sans élément neutre à gauche. En contraste, la soustraction n'est pas une loi interne sur \mathbb{N} .
 4. $(\mathbb{Q}^*, :)$, $(\mathbb{R}^*, :)$ et $(\mathbb{C}^*, :)$ sont des lois de compositions non associatives, non commutatives, avec 1 comme élément neutre à droite, et sans élément neutre à gauche.
 5. Soit $n \in \mathbb{N}^*$. L'addition et la multiplication modulo n définies dans le paragraphe A.2 de l'Annexe sont deux lois internes associatives et commutatives sur $\{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$. L'addition modulo n admet 0 comme élément neutre et la multiplication modulo n admet 1 comme élément neutre.
 6. Soit V un espace vectoriel réel. L'addition vectorielle est une loi interne associative et commutative sur V , de neutre l'origine de V . Par contre, la multiplication par des

scalaires, qui est évidemment une loi essentielle sur un espace vectoriel,

$$\begin{aligned}\mathbb{R} \times V &\longrightarrow V \\ (\lambda, v) &\longmapsto \lambda v,\end{aligned}$$

n'est pas une loi *interne* sauf si $V = \mathbb{R}$.

7. Soit X un ensemble non vide et considérons l'ensemble $E = \{f : X \rightarrow X\}$ des applications de X dans X . On obtient une loi de composition interne en munissant E de la composition de fonctions. C'est une loi associative, non commutative (à moins que $|X| = 1$), admettant l'application identité comme élément neutre.
8. On peut affiner l'exemple précédent en imposant des restrictions sur les applications considérées, ceci à condition que ces restrictions soient préservées par la composition. Par exemple, puisque la composition de deux fonctions continues est encore continue, on peut munir l'espace $\mathcal{C}(\mathbb{R})$ des fonctions continues de \mathbb{R} dans \mathbb{R} de la composition de fonction. C'est bien une loi interne associative, non commutative, d'élément neutre l'application identité. Ou bien si $X = V$ est un espace vectoriel, on peut considérer l'espace $\mathcal{L}(V, V)$ des fonctions linéaires de V dans V muni de la composition de fonctions. C'est bien une loi interne associative, non commutative (sauf si $\dim(V) = 1$), d'élément neutre l'application identité.
9. L'ensemble $M_n(\mathbb{R})$ des matrices $n \times n$ à coefficients réels admet deux lois naturelles : l'addition de matrices (qui est un cas particulier de l'exemple 1.3.6) et la multiplication de matrices (qui est, après un choix de base, une réincarnation de l'exemple $\mathcal{L}(V, V)$ dans le cas où $V = \mathbb{R}^n$). Cette dernière loi n'est pas commutative (sauf si $n = 1$), est associative et admet la matrice identité comme élément neutre.
10. Il existe d'autres lois naturelles sur $\mathcal{C}(\mathbb{R})$. En effet on pourrait considérer l'addition ou la multiplication de fonctions :

$$(f + g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = f(x) \cdot g(x).$$

$(\mathcal{C}(\mathbb{R}), +)$ est une loi interne associative, commutative, d'élément neutre l'application identiquement nulle. $(\mathcal{C}(\mathbb{R}), \cdot)$ est une loi interne associative, commutative, d'élément neutre l'application constante 1.

11. Soit E un ensemble non vide. On peut toujours définir une loi de composition \circ_1 en projetant sur le premier facteur :

$$\begin{aligned}\circ_1 : E \times E &\longrightarrow E \\ (x, y) &\longmapsto x \circ_1 y := x.\end{aligned}$$

On vérifie facilement que cette loi est associative, non commutative sauf dans le cas trivial où $|E| = 1$, que n'importe quel $y \in E$ est neutre à droite (puisque $x \circ_1 y = x$ pour tout $y \in E$), mais qu'elle n'admet pas de neutre à gauche (sauf si $|E| = 1$). De même on pourrait définir une loi de composition \circ_2 en projetant sur le deuxième facteur, $x \circ_2 y := y$ qui est associative, admet autant de neutres à gauche que d'éléments de E et n'est commutative ou admet un neutre à droite seulement si $|E| = 1$.

12. Soit X un ensemble. Considérons $\mathcal{P}(X)$ l'ensemble des sous-ensembles de X . On peut le munir de plusieurs lois internes naturelles : par exemple l'union \cup , l'intersection \cap et la différence symétrique Δ . La différence symétrique $A \Delta B$ de deux sous-ensembles A, B de X est définie comme

$$A \Delta B = (A \cap B^c) \cup (A^c \cap B),$$

où $A^c = X \setminus A$. La loi $(\mathcal{P}(X), \cup)$ est une loi interne associative, commutative, d'élément neutre $\emptyset \in \mathcal{P}(X)$. La loi $(\mathcal{P}(X), \cap)$ est une loi interne associative, commutative, d'élément neutre $X \in \mathcal{P}(X)$. La loi $(\mathcal{P}(X), \Delta)$ est une loi interne associative, commutative, d'élément neutre $\emptyset \in \mathcal{P}(X)$.

Si E est fini, il peut être utile d'encoder une loi de composition \circ sur E par une table :

\circ	x	y	z	\dots
x	$x \circ x$	$x \circ y$	$x \circ z$	\dots
y	$y \circ x$	$y \circ y$	$y \circ z$	\dots
z	$z \circ x$	$z \circ y$	$z \circ z$	\dots
\vdots	\vdots	\vdots	\vdots	\vdots

Observons que la loi est alors commutative si et seulement si la table est symétrique par rapport à sa diagonale.

Par exemple, considérons $\{1, i, -1, -i\} \subset \mathbb{C}$ muni de la multiplication (qui est bien une loi interne). Sa table est donnée par :

\cdot	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Cette table est bien symétrique par rapport à sa diagonale, correspondant à la commutativité de la multiplication complexe.

Lemme 1.4 Soit (E, \circ) un ensemble muni d'une loi de composition. Supposons qu'il existe $e_g \in E$ neutre à gauche et $e_d \in E$ neutre à droite. Alors $e_d = e_g$ est un élément neutre.

Démonstration. On a

$$\begin{aligned} e_d &= e_g \circ e_d && \text{car } e_g \text{ est neutre à gauche,} \\ &= e_g && \text{car } e_d \text{ est neutre à droite.} \end{aligned}$$

■

En particulier, si une loi de composition (E, \circ) admet un élément neutre (donc neutre à droite et à gauche), celui-ci est forcément unique. En contraste, il existe des lois admettant plusieurs neutres à gauche, respectivement à droite (cf Exemple 1.3.11).

1.2 Groupes : Définition et exemples

Définition 1.5 Soit (G, \circ) un ensemble G muni d'une loi de composition interne

$$\circ : G \times G \longrightarrow G.$$

On dit que (G, \circ) est un *groupe* si

1. La loi \circ est associative.
2. Il existe un élément $e \in G$ neutre pour \circ ,
3. Pour tout $g \in G$, il existe $h \in G$ tel que

$$g \circ h = h \circ g = e.$$

(On appelle h *inverse* de g .)

Si de plus la loi \circ est commutative on dit que (G, \circ) est un groupe *commutatif* ou *abélien*.

- **Remarques**
1. Il découle du Lemme 1.4 que dans un groupe, le neutre est toujours unique. En effet, s'il en existait deux, l'un serait en particulier neutre à gauche, et l'autre neutre à droite, et donc égaux par le Lemme 1.4. De même, nous verrons ci-dessous dans le Lemme 1.9 que l'inverse est unique.
 2. L'inverse de l'élément neutre e est e .
 3. Puisqu'un groupe possède toujours un élément neutre, sa cardinalité est forcément plus grande ou égale à 1.

On définit l'ordre d'un groupe comme pour les ensembles.

Définition 1.6 Soit (G, \circ) un groupe. On appelle *ordre* de (G, \circ) la cardinalité $|G| \in \mathbb{N}^* \cup \{\infty\}$ de G . Si $|G| < \infty$ on dit que G est *fini*. Si $|G| = \infty$ on dit que G est *infini*.

■ **Exemple 1.7 — Groupe trivial.** Soit G un ensemble à 1 élément, $G = \{e\}$. La seule loi de composition possible sur G est

$$\begin{aligned} \circ : \{e\} \times \{e\} &\longrightarrow \{e\} \\ (e, e) &\longmapsto e. \end{aligned}$$

(G, \circ) est un groupe, appelé *groupe trivial*. Il en existe de nombreuses incarnations : $(\{0\}, +)$, $(\{1\}, \cdot)$, etc.

Revenons maintenant sur les exemples de lois de compositions du paragraphe précédent pour déterminer lesquelles définissent un groupe. Nous pouvons déjà écarter les lois non associatives ou celles n'admettant pas de neutre. En présence d'une loi interne associative admettant un élément neutre, il ne reste plus qu'à vérifier l'existence d'un inverse.

- **Exemples 1.8**
1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes commutatifs. L'inverse de x est $-x$. En revanche, $(\mathbb{N}, +)$ n'est pas un groupe puisque par exemple $1 \in \mathbb{N}$ n'a pas d'inverse dans \mathbb{N} pour l'addition.
 2. (\mathbb{N}, \cdot) , (\mathbb{Z}, \cdot) , (\mathbb{Q}, \cdot) , (\mathbb{R}, \cdot) et (\mathbb{C}, \cdot) ne sont pas des groupes puisque l'élément neutre de la multiplication est 1, mais 0 n'admet pas d'inverse : en effet, il n'existe pas de x dans \mathbb{C} (et donc dans \mathbb{N} , \mathbb{Z} , etc) tel que $0 \cdot x = 1$. Otons donc 0 à ces ensembles. (\mathbb{Q}^*, \cdot) , (\mathbb{R}^*, \cdot) et (\mathbb{C}^*, \cdot) sont des groupes commutatifs. L'inverse de x est $1/x$. En

revanche (\mathbb{N}^*, \cdot) et (\mathbb{Z}^*, \cdot) ne sont pas des groupes puisque 2 n'a pas d'inverse dans \mathbb{Z} (et donc dans \mathbb{N}) pour la multiplication. Observons que $(\mathbb{Q}_{>0}, \cdot)$ et $(\mathbb{R}_{>0}, \cdot)$ sont aussi des groupes commutatifs.

3. La soustraction est exclue puisque elle n'est pas associative et n'admet pas de neutre.
4. De même pour la division.
5. $(\{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}, + \text{ mod } n)$ est un groupe abélien que l'on dénote par C_n . On l'appellera *groupe cyclique d'ordre n* (voir Paragraphe 1.8 pour la justification de cette terminologie). L'inverse de $\overline{a} \in \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$ est $\overline{n-a} = -\overline{a}$. Les tables pour $n = 2$ et 3 sont données par (pour ne pas alourdir la notation, nous nous permettons d'omettre le surlignement des nombres 0, 1 et 0, 1, 2, mais n'oublions pas que 0 ou 1 n'ont pas la même signification dans le tableau de gauche et de droite) :

$+ \text{ mod } 2$	0	1
0	0	1
1	1	0

$+ \text{ mod } 3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Pour la multiplication modulo n nous rencontrons le même problème que pour la multiplication dans \mathbb{Q} ou \mathbb{R} : $\overline{0}$ ne peut pas avoir d'inverse multiplicatif. Si on l'ôte, on obtient parfois un groupe (par exemple pour $n = 2, 3$), mais un nouveau problème se présente : sans $\overline{0}$, la multiplication modulo n n'est plus forcément une loi interne. En effet pour $n = 4$ on a $2 \cdot 2 \equiv 0 \text{ mod } 4$, et donc $\overline{2} \cdot \overline{2} = \overline{0}$. On verra dans le Paragraphe 1.8 comment résoudre ce problème.

6. Un espace vectoriel V muni de l'addition vectoriel forme un groupe abélien. L'inverse de $v \in V$ est le vecteur $-v$.
7. Soit X un ensemble. Sur l'ensemble des applications $\{f : X \rightarrow X\}$, les seules applications $f : X \rightarrow X$ admettant une inverse pour la composition de fonctions sont naturellement les fonctions bijectives. Nous nous restreignons donc aux applications bijectives,

$$\text{Bij}(X) = \{f : X \rightarrow X \mid f \text{ bijective}\}$$

et observons que $(\text{Bij}(X), \circ)$ est bien un groupe, qui est commutatif si et seulement si $|X| \leq 2$. Un cas particulier d'une importance primordiale, qui sera étudié en détail dans le paragraphe 1.9, est le cas où $X = \{1, 2, \dots, n\}$ pour un $n \in \mathbb{N}^*$. Ce groupe s'appelle le *groupe symétrique (sur n éléments)* et on le dénote

$$\text{Sym}(n) := \text{Bij}(\{1, 2, \dots, n\}).$$

8. De même, l'espace des fonctions continues *bijectives* de \mathbb{R} dans \mathbb{R} , ou l'ensemble des applications linéaires *bijectives* sur un espace vectoriel, forment un groupe pour la composition d'application.
9. L'ensemble $\text{GL}(n, \mathbb{R})$ des matrices $n \times n$ inversibles est un groupe pour la multiplication matricielle. Pour rappel,

$$\text{GL}(n, \mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}.$$

De même (cf exercices),

$$\text{O}(n) = \{A \in M_n(\mathbb{R}) \mid AA^t = \text{Id}_n\}$$

est un groupe pour la multiplication matricielle.

10. $(\mathcal{C}(\mathbb{R}), +)$ est un groupe commutatif. L'inverse d'une application continue f est l'application $-f$. En revanche, $(\mathcal{C}(\mathbb{R}), \cdot)$ n'est pas un groupe puisque l'application identiquement nulle n'a pas d'inverse. Ceci se corrige facilement en considérant les fonctions continues sur \mathbb{R} à valeur dans \mathbb{R}^* (ou $\mathbb{R}_{>0}$) qui est un groupe commutatif (pour la multiplication de fonctions).
11. Un ensemble E muni de la projection sur le premier ou le deuxième facteur ne forme pas un groupe (à moins que $|E| = 1$ au quel cas on retrouve une incarnation du groupe trivial) puisque les projections n'admettent pas de neutre.
12. Soit X un ensemble. Vous vérifierez en exercice que $(\mathcal{P}(X), \Delta)$ est un groupe. $(\mathcal{P}(X), \cup)$ et $(\mathcal{P}(X), \cap)$ sont bien des lois internes associatives, commutatives, d'élément neutre \emptyset , respectivement $X \in \mathcal{P}(X)$. Si $X = \emptyset$, l'ensemble $\mathcal{P}(X)$ contient un élément (l'ensemble vide \emptyset) et on a à nouveau deux incarnations sans aucun doute pas très naturelles du groupe trivial. Par contre, si $X \neq \emptyset$, les lois $(\mathcal{P}(X), \cup)$ et $(\mathcal{P}(X), \cap)$ ne forment pas des groupes. En effet, vous pourrez vérifier que la plupart des éléments de $\mathcal{P}(X)$ n'admettent pas d'inverse pour ces lois.

Si vous deviez, malencontreusement, ne vous souvenir que de trois exemples de groupes, souvenez-vous de \mathbb{Z} , du groupe cyclique C_n (addition modulo n sur $\{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$), Exemple 1.8.5, et du groupe symétrique $\text{Sym}(n)$, Exemple 1.8.7.

Il existe de nombreuses façons de construire des groupes à partir d'un certain nombre de groupes donnés. La plus simple d'entre elle est le *produit direct* : Soient (G, \circ) , (H, \star) deux groupes. Leur produit direct est l'ensemble $G \times H$ muni de la loi de composition définie coordonnée par coordonnée :

$$\begin{aligned} (G \times H) \times (G \times H) &\longrightarrow G \times H \\ ((g_1, h_1), (g_2, h_2)) &\longmapsto (g_1 \circ g_2, h_1 \star h_2). \end{aligned}$$

Vous connaissez déjà très bien cette loi : l'addition vectorielle sur $\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$ et plus généralement sur \mathbb{R}^n est définie à partir de l'addition sur chaque facteur \mathbb{R} .

Par exemple, établissons la loi de groupe sur le produit direct $C_2 \times C_2$, où l'on rappelle que $C_2 = (\{\overline{0}, \overline{1}\}, + \text{ mod } 2)$. Pour ne pas alourdir la notation, nous nous privons de surligner les nombres 0, 1 :

$(+ \text{ mod } 2, + \text{ mod } 2)$	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
$(0, 0)$	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
$(0, 1)$	$(0, 1)$	$(0, 0)$	$(1, 1)$	$(1, 0)$
$(1, 0)$	$(1, 0)$	$(1, 1)$	$(0, 0)$	$(0, 1)$
$(1, 1)$	$(1, 1)$	$(1, 0)$	$(0, 1)$	$(0, 0)$

Lemme 1.9 Soit (G, \circ) un groupe. L'inverse de $g \in G$ est unique.

Démonstration. Supposons que g possède deux inverses h et h' , et montrons que $h = h'$:

$$\begin{aligned}
 h &= h \circ e && \text{car } e \text{ est neutre (à droite),} \\
 &= h \circ (g \circ h') && \text{car } h' \text{ inverse de } g, \\
 &= (h \circ g) \circ h' && \circ \text{ associative,} \\
 &= e \circ h' && \text{car } h \text{ inverse de } g, \\
 &= h' && \text{car } e \text{ est neutre (à gauche).}
 \end{aligned}$$

■

- **Remarques**
1. Puisque dans un groupe (G, \circ) , l'inverse d'un élément $g \in G$ est unique, nous le dénoterons désormais par g^{-1} .
 2. On omettra dorénavant souvent \circ de la notation : on dira simplement que G , au lieu de (G, \circ) , est un groupe, où l'on sous-entend que c'est par rapport à une loi interne qu'on n'écrira plus comme $g \circ h$ mais simplement comme

$$g \cdot h \quad \text{ou} \quad gh.$$

3. Le neutre d'un groupe G sera typiquement dénoté par e_G ou e sans d'avantage de précision.
4. Dans le cas d'un groupe G abélien, on préférera la notation additive, en écrivant $g + h$ pour $g \cdot h$, en dénotant le neutre e par 0 , et l'inverse de g par $-g$.
5. Dans le même esprit, si la loi est clairement sous-entendue, on ne la spécifiera plus. Par exemple, \mathbb{Z} est un groupe, où il est à comprendre que c'est un groupe pour l'addition.

Lemme 1.10 Soient g, h deux éléments d'un groupe G . Alors

1. $(g^{-1})^{-1} = g$,
2. $(gh)^{-1} = h^{-1}g^{-1}$.

Démonstration. Exercice. ■

■ **Remarque** Trop habitué aux calculs avec des lois commutatives (par exemple dans $(\mathbb{Z}, +)$ ou (\mathbb{R}^*, \cdot)), le deuxième point de ce lemme paraît parfois contre-intuitif. On oubliera parfois d'inverser l'ordre des éléments en prenant l'inverse d'un produit, comme on aurait le droit de le faire avec une loi commutative. Pourtant, dans la vie de tous les jours, il existe une multitude d'exemples démontrant le sens de cette égalité : Si on veut faire l'opération inverse de "mettre ses chaussettes", "mettre ses chaussures", il faut bien d'abord enlever ses chaussures, puis ses chaussettes.

Dans un groupe G on a le droit de simplifier : Pour tous $x, y, g \in G$ on a

- $xg = yg \implies x = y$,
- $gx = gy \implies x = y$.

En effet si $xg = yg$ on multiplie cette équation à droite par g^{-1} pour obtenir

$$x = xe = x(gg^{-1}) = \overbrace{(xg)g^{-1}}^{(xg=yg) \cdot g^{-1}} = (yg)g^{-1} = y(gg^{-1}) = ye = y.$$

Le calcul est identique pour $gx = gy$ où l'on multipliera cette fois l'équation à gauche par g^{-1} .

Une conséquence de la simplification autorisée dans un groupe, est que dans une table de loi de groupe, chaque élément du groupe apparaît exactement une seule fois sur chaque ligne et chaque colonne.

Définition 1.11 Soit G un groupe. Pour $g \in G$ et $n \in \mathbb{Z}$ on définit la n -ième puissance de g comme

$$g^n := \begin{cases} \underbrace{g \cdots g}_{n \text{ fois}} & \text{si } n > 0, \\ e & \text{si } n = 0, \\ \underbrace{g^{-1} \cdots g^{-1}}_{-n \text{ fois}} & \text{si } n < 0. \end{cases}$$

Observons que cette notation est cohérente avec notre notation pour l'inverse de g , puisque la (-1) -ième puissance de g n'est autre que l'inverse g^{-1} . Les vérifications des égalités

$$g^n g^m = g^{n+m} \quad \text{et} \quad (g^n)^m = g^{nm},$$

pour tous $g \in G$ et $n, m \in \mathbb{Z}$ sont laissées en exercice.

En présence d'un groupe abélien où la notation additive est choisie, la n -ième puissance d'un élément g s'écrit plutôt comme ng , puisque dans la notation additive, ceci correspond à $g + \cdots + g$ dans le cas $n > 0$. Les deux égalités précédentes prendront alors la forme

$$(ng) + (mg) = (n+m)g \quad \text{et} \quad m(ng) = (mn)g.$$

Définition 1.12 Soient G un groupe et $g \in G$. On définit l'ordre de g , qu'on notera $\text{ord}(g)$ (ou $|g|$) $\in \mathbb{N}^* \cup \{\infty\}$ comme suit :

- Si $g^k \neq e$ pour tout $k \in \mathbb{N}^*$, l'ordre de g est infini, $\text{ord}(g) := \infty$.
- Sinon,

$$\text{ord}(g) := \min\{k \in \mathbb{N}^* \mid g^k = e\}.$$

- **Exemples 1.13**
1. Dans tout groupe, l'élément neutre est le seul élément d'ordre 1.
 2. Dans \mathbb{R}^* , l'ordre de -1 est 2 puisque $(-1)^2 = 1$ mais $-1 = (-1)^1 \neq 1$.
 3. L'ordre de $\bar{1} \in C_n$ est n . L'ordre de $\bar{2} \in C_n$ est $n/2$ si n est pair et n si n est impair.
 4. L'ordre de $(1, 2, 3, 4) \in \text{Sym}(4)$ est 4 : En effet,

$$\begin{aligned} (1, 2, 3, 4)^1 &= (1, 2, 3, 4) \neq \text{Id} \\ (1, 2, 3, 4)^2 &= (1, 3)(2, 4) \neq \text{Id} \\ (1, 2, 3, 4)^3 &= (1, 4, 3, 2) \neq \text{Id} \\ (1, 2, 3, 4)^4 &= \text{Id}. \end{aligned}$$

Plus généralement, l'ordre d'un k -cycle de $\text{Sym}(n)$ est k .

Définition 1.14 Soient G un groupe et $x, y \in G$. On dit que x et y sont *conjugués* s'il existe $g \in G$ tel que

$$y = gxg^{-1}.$$

Observons qu'être conjugué est une relation d'équivalence. De plus, si x et y sont conjugués ils ont le même ordre puisque

$$\begin{aligned} y^m &= (gxg^{-1})^m = (gxg^{-1}) \underbrace{(gxg^{-1}) \cdots (gxg^{-1})}_{=e} \\ &= gx^m g^{-1}. \end{aligned}$$

En particulier, $y^m = e$ si et seulement si $x^m = e$.

1.3 Sous-groupes

Définition 1.15 Soit (G, \circ) un groupe. Un sous-ensemble $H \subset G$ est appelé *sous-groupe* si la loi \circ se restreint à une loi

$$\begin{aligned} \circ_H : H \times H &\longrightarrow H \\ (x, y) &\longmapsto x \circ y \end{aligned}$$

sur H (c'est-à-dire si $x \circ y \in H$ pour tous $x, y \in H$) telle que (H, \circ_H) est un groupe.

Si $H \subset G$ est un sous-groupe, on le dénote par $H < G$ (même si l'inclusion n'est pas forcément stricte).

■ **Remarque 1.16** Par définition, un sous-ensemble $H \subset G$ d'un groupe (G, \circ) est un sous-groupe, si et seulement si

1. $x \circ y \in H, \forall x, y \in H,$
2. $e \in H,$
3. $\forall x \in H, x^{-1} \in H.$

En effet la restriction d'une loi associative est automatiquement associative. De même pour l'existence dans H de l'inverse d'un élément $x \in H$, on sait déjà que x admet un inverse dans G , puisque G est un groupe. Il suffit donc de vérifier que cet inverse appartient bien à H . On verra dans le Lemme 1.19 ci-dessous qu'on peut reformuler ces conditions de façon encore plus concise.

Lemme 1.17 Soient K, H et G trois groupes. Si $K < H$ et $H < G$ alors $K < G$.

Démonstration. Exercice. ■

■ **Exemples 1.18** 1. Soit G un groupe d'élément neutre e . Alors $\{e\}$ et G sont toujours des sous-groupes de G .

2. $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}.$
3. $\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*.$
4. $\{+1\} < \{+1, -1\} < \{+1, i, -1, -i\} < S^1 < \mathbb{C}^*.$

5. Soit $n \in \mathbb{N}$. Alors $n\mathbb{Z} := \{nq \mid q \in \mathbb{Z}\}$ est un sous-groupe de \mathbb{Z} (exercice).
6. Soient G un groupe et $g \in G$. L'ensemble

$$\langle g \rangle := \{g^m \mid m \in \mathbb{Z}\}$$

est un sous-groupe de G appelé *groupe engendré par g* . Remarquons que l'ordre du groupe $\langle g \rangle$ est égal à l'ordre de l'élément g ,

$$\text{ord}(g) = |\langle g \rangle|.$$

En effet, si $\text{ord}(g) = \infty$, alors $g^k \neq e$ pour tout $k \geq 1$ et $g^m \neq g^n$ pour tous $m \neq n$ (car si $g^m = g^n$ avec $m < n$ alors $g^{n-m} = e$ pour $k = n - m \geq 1$, ce qui est impossible), de sorte que l'ensemble $\langle g \rangle$ a bien cardinalité infinie. Si $\text{ord}(g) = k < \infty$, alors $g^{qk+r} = g^r$ pour tous $q, r \in \mathbb{Z}$, et donc

$$\langle g \rangle = \{e, g, \dots, g^{k-1}\}.$$

De plus, ces k éléments de $\langle g \rangle$ sont bien distincts (ce qui implique que $\text{ord}(g) = |\langle g \rangle|$). Sinon on aurait $g^r = g^s$ pour $0 \leq r < s < k$ mais alors $g^{s-r} = e$ pour $1 \leq s - r < k$, ce qui contredirait la minimalité de k .

Lemme 1.19 Soit G un groupe et $H \subset G$ un sous-ensemble. Alors H est un sous-groupe de G si et seulement si

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

■ **Remarque** Si on compare les trois conditions de la Remarque 1.16 aux deux conditions du Lemme 1.19 on constate rapidement qu'on n'a pas gagné grand-chose. En effet pour montrer qu'un candidat H à être un sous-groupe est non vide, le plus simple à faire est souvent de montrer qu'il contient le neutre de G . Pour un sous-ensemble contenant l'élément neutre, le point 2. du lemme n'est quant à lui qu'une reformulation équivalente des points 1. et 3. de la remarque. Ce n'est pas ni plus dur ni moins dur à montrer en pratique. Ça peut être plus court en utilisant le point 2. du lemme, mais c'est souvent plus clair et intuitif en utilisant plutôt les points 1. et 3. de la remarque.

Preuve du Lemme 1.19. \implies : Soit $H < G$ un sous-groupe de G , donc un sous-ensemble satisfaisant les trois conditions de la Remarque 1.16. Montrons qu'il satisfait les deux conditions du lemme :

1. Par la condition 2. de la Remarque 1.16, $e \in H$ donc $H \neq \emptyset$.
2. Soient $x, y \in H$. Par la condition 3. de la Remarque 1.16, $y^{-1} \in H$. On applique la condition 1. de la remarque à x et y^{-1} pour en déduire que $xy^{-1} \in H$.

\impliedby : Soit $H \subset G$ un sous-ensemble satisfaisant les deux conditions du lemme. Montrons, dans le désordre, qu'il satisfait les trois conditions de la remarque 1.16 et est donc bien un sous-groupe de G :

2. Par la condition 1. du lemme, il existe $x \in H$. Appliquons la condition 2. du lemme à x et x pour en déduire que $xx^{-1} = e \in H$.
3. Soit $x \in H$. Par le point précédent, $e \in H$. On applique la condition 2. du lemme à e et x : $ex^{-1} = x^{-1} \in H$.

1. Soient $x, y \in H$. Par le point précédent, $y^{-1} \in H$. On applique la condition 2. du lemme à x et y^{-1} : $x(y^{-1})^{-1} = xy \in H$. ■

1.4 Homomorphismes et isomorphismes

Définition 1.20 Soient G, H deux groupes. Une application

$$f : G \longrightarrow H$$

est un *homomorphisme (de groupes)* si

$$f(xy) = f(x)f(y) \quad (1.1)$$

pour tous $x, y \in G$.

■ **Remarque** La condition (1.1) demande à ce qu'un homomorphisme soit compatible avec les lois des groupes G et H . Conceptuellement, il serait plus logique de demander à un homomorphisme de préserver aussi toutes les structures qu'on a dans un groupe, c'est-à-dire d'envoyer le neutre de G sur le neutre de H ($f(e_G) = e_H$), et d'envoyer l'inverse d'un élément sur l'inverse de son image ($f(x^{-1}) = (f(x))^{-1}$ pour tout $x \in G$). On verra dans la Proposition 1.22, après quelques exemples, que ces deux propriétés découlent de la condition (1.1) de la définition.

■ **Exemples 1.21** 1. Pour toute paire de groupes G, H l'application

$$\begin{aligned} G &\longrightarrow H \\ g &\longmapsto e_H \quad \forall g \in G \end{aligned}$$

est un homomorphisme appelé *homomorphisme trivial*.

2. Soient G un groupe et H un sous-groupe. Alors l'inclusion

$$H \hookrightarrow G$$

est un homomorphisme. En particulier, pour $H = G$, l'application identité est un homomorphisme.

3. Soit $k \in \mathbb{Z}$. L'application

$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathbb{Z} \\ n &\longmapsto kn \end{aligned}$$

est un homomorphisme de groupes.

4. L'application

$$\begin{aligned} \exp : (\mathbb{R}, +) &\longrightarrow (\mathbb{R}_{>0}, \cdot) \\ x &\longmapsto e^x \end{aligned}$$

est un homomorphisme de groupes.

5. L'application

$$\begin{aligned} (\mathbb{C}^*, \cdot) &\longrightarrow (\mathbb{R}_{>0}, \cdot) \\ z &\longmapsto |z| \end{aligned}$$

est un homomorphisme de groupes.

6. Pour tout groupe G et $g \in G$, l'application

$$\begin{aligned}\mathbb{Z} &\longrightarrow G \\ n &\longmapsto g^n\end{aligned}$$

est un homomorphisme de groupes.

7. La signature

$$\text{sign} : \text{Sym}(n) \longrightarrow \{+1, -1\}$$

est un homomorphisme de groupe (cf Définition 1.67 et Théorème 1.68).

8. Le déterminant

$$\text{Det} : \text{GL}(n, \mathbb{R}) \longrightarrow \mathbb{R}$$

est un homomorphisme de groupe.

Proposition 1.22 Soient G, H deux groupes et $f : G \rightarrow H$ un homomorphisme. Alors

1. $f(e_G) = e_H$,
2. $f(x^{-1}) = (f(x))^{-1}$ pour tout $x \in G$.

Démonstration. 1. On a

$$f(e_G) = f(e_G e_G) = f(e_G) f(e_G),$$

ce qui implique après multiplication à droite (ou à gauche) par $(f(e_G))^{-1}$ que

$$e_H = f(e_G).$$

2. Voyons que $f(x^{-1})$ est bien l'inverse de $f(x)$. On a d'une part

$$\begin{aligned}f(x)f(x^{-1}) &= f(xx^{-1}) && \text{car } f \text{ est un homomorphisme,} \\ &= f(e_G) && \text{car } xx^{-1} = e_G, \\ &= e_H && \text{par le point précédent.}\end{aligned}$$

De même on obtient

$$f(x^{-1})f(x) = f(x^{-1}x) = f(e_G) = e_H.$$

Ceci montre bien que $f(x^{-1})$ est l'inverse de $f(x)$, et donc que $f(x)^{-1} = f(x^{-1})$. ■

Lemme 1.23 Soient G, H, K des groupes, et

$$f_1 : G \longrightarrow H \quad \text{et} \quad f_2 : H \longrightarrow K$$

deux homomorphismes. Alors la composition

$$f_2 \circ f_1 : G \longrightarrow K$$

est un homomorphisme.

Démonstration. Exercice. ■

Définition 1.24 Soient G, H deux groupes et $f : G \rightarrow H$ un homomorphisme. On définit

$$\begin{aligned} \text{le noyau de } f \text{ par :} & \quad \text{Ker}(f) = \{x \in G \mid f(x) = e\} \subset G, \\ \text{l'image de } f \text{ par :} & \quad \text{Im}(f) = \{f(x) \in H \mid x \in G\} \subset H. \end{aligned}$$

Lemme 1.25 Soient G, H deux groupes et $f : G \rightarrow H$ un homomorphisme. Le noyau $\text{Ker}(f)$ est un sous-groupe de G et l'image $\text{Im}(f)$ est un sous-groupe de H .

Démonstration. Exercice. ■

Reprenons les exemples 1.21 pour déterminer leurs noyaux et images.

- **Exemples 1.26**
1. Le noyau de l'homomorphisme trivial $G \rightarrow H$ est G , son image est $\{e_H\}$.
 2. Le noyau de l'inclusion d'un sous-groupe H dans un groupe G est $\{e_H\}$, son image est H .
 3. L'homomorphisme $n \mapsto kn$ a pour noyau $\{0\}$ et image $k\mathbb{Z}$.
 4. L'application exponentielle a pour noyau $\{0\}$ et image $\mathbb{R}_{>0}$.
 5. L'homomorphisme $z \mapsto |z|$ a pour noyau S^1 et image $\mathbb{R}_{>0}$.
 6. L'homomorphisme $n \mapsto g^n$ a pour noyau $\text{ord}(g) \cdot \mathbb{Z}$ si $\text{ord} < \infty$ et $\{0\}$ sinon, et son image est dans tous les cas $\langle g \rangle$.
 7. La signature $\text{sign} : \text{Sym}(n) \rightarrow \{+1, -1\}$ a, par définition (cf Définition 1.70), pour noyau le groupe alterné $\text{Alt}(n)$ et son image est $\{+1, -1\}$.
 8. Le déterminant $\text{Det} : \text{GL}(n, \mathbb{R}) \rightarrow \mathbb{R}$ a par définition comme noyau le groupe *spécial linéaire*

$$\text{SL}(n, \mathbb{R}) := \{A \in M_n(\mathbb{R}) \mid \text{Det}(A) = 1\}$$

et image \mathbb{R} .

Rappelons qu'une application $f : G \rightarrow H$ est *injective* si et seulement si, pour tous $x, y \in G$:

$$f(x) = f(y) \implies x = y.$$

Lemme 1.27 Soient G, H deux groupes et $f : G \rightarrow H$ un homomorphisme. Alors f est injective si et seulement si $\text{Ker}(f) = \{e_G\}$.

■ **Remarque** Ceci devrait vous rappeler un énoncé similaire démontré pour les applications linéaires $f : V \rightarrow W$ entre deux espaces vectoriels V, W , qui est en fait un cas particulier du Lemme 1.27 puisque des espaces vectoriels sont des groupes abéliens pour l'addition vectorielle et qu'une application linéaire est en particulier un homomorphisme entre ces deux groupes abéliens.

Démonstration. \implies : Supposons que f est injective. Voyons que le noyau est réduit à l'identité, $\text{Ker}(f) = \{e_G\}$. Puisque $e_G \in \text{Ker}(f)$, il suffit de voir que tout élément du noyau est l'identité e_G . Soit donc $x \in \text{Ker}(f)$. Par définition, on a $f(x) = e_H$. D'autre part, $f(e_G) = e_H$. En particulier $f(x) = f(e_G)$ ce qui implique par injectivité de f que $x = e_G$.

\impliedby : Supposons que $\text{Ker}(f) = \{e_G\}$ et montrons que f est injective. Soient $x, y \in G$ tels que $f(x) = f(y)$. Il faut voir que $x = y$. Appliquons f à xy^{-1} :

$$\begin{aligned} f(xy^{-1}) &= f(x)f(y^{-1}) && f \text{ homomorphisme,} \\ &= f(x)f(y)^{-1} && \text{Proposition 1.22,} \\ &= f(x)f(x)^{-1} && f(x) = f(y) \text{ par hypothèse,} \\ &= e_H. \end{aligned}$$

Donc $xy^{-1} \in \text{Ker}(f)$, qui ne contient que l'élément neutre, ce qui implique que $xy^{-1} = e_G$ et donc après multiplication à droite par y , aussi que $x = y$. ■

Rappelons aussi qu'une application $f : G \rightarrow H$ est *surjective* si $\text{Im}(f) = H$, et qu'elle est *bijective* si elle est injective et surjective. On montre de plus facilement qu'une application $f : G \rightarrow H$ est bijective si et seulement si il existe une application $f' : H \rightarrow G$ telle que

$$f' \circ f = \text{Id}_G \quad \text{et} \quad f \circ f' = \text{Id}_H.$$

Notons que si une telle application f' existe, elle est forcément unique et on la dénote souvent par f^{-1} et on l'appelle *application inverse* de f . (Ceci est valide pour toute application, pas seulement pour les homomorphismes.)

Définition 1.28 Soient G, H deux groupes. Un homomorphisme $f : G \rightarrow H$ est un *isomorphisme* s'il existe un homomorphisme $f' : H \rightarrow G$ tel que

$$f' \circ f = \text{Id}_G \quad \text{et} \quad f \circ f' = \text{Id}_H.$$

S'il existe un isomorphisme $f : G \rightarrow H$ on dit que G et H sont *isomorphes* et on écrit $G \cong H$.

■ **Remarque** En d'autres termes un homomorphisme est un isomorphisme si et seulement si c'est un homomorphisme bijectif dont l'application inverse est aussi un homomorphisme.

Par exemple, tous les groupes à un élément sont isomorphes. En effet, l'unique application entre deux tels groupes $G = \{e_G\}$ et $H = \{e_H\}$ est un homomorphisme et son inverse aussi. De même, tous les groupes à deux éléments sont isomorphes : Soient $G = \{e_G, g\}$ et $H = \{e_H, h\}$ deux groupes d'ordre deux. Observons que $g^2 = e_G$ puisque, comme G n'a que deux éléments, si ce n'était pas le cas on aurait $g^2 = g$, ce qui implique après multiplication à gauche ou à droite par g^{-1} que $g = e_G$, impossible. De même $h^2 = e_H$. La bijection

$$\begin{array}{ccc} f : & G & \longrightarrow H \\ & e_G & \longmapsto e_H \\ & g & \longmapsto h \end{array}$$

est un homomorphisme puisque

$$\begin{aligned} f(e_G e_G) &= f(e_G) = e_H = e_H e_H = f(e_G) f(e_G), \\ f(e_G g) &= f(g) = h = e_H h = f(e_G) f(g), \\ f(g e_G) &= f(g) = h = h e_H = f(g) f(e_G), \\ f(g g) &= f(e_G) = e_H = h h = f(g) f(g). \end{aligned}$$

Par symétrie, son inverse est aussi un homomorphisme. En particulier, $C_2 \cong \{+1, -1\} \cong \text{Sym}(2)$. Plus généralement, nous verrons que tous groupes d'un même ordre p premier sont isomorphes. Le cas $p = 3$ pourra déjà être démontré similairement au cas $p = 2$ en exercice. En contraste, il existe à isomorphisme près deux groupes d'ordre 4 : C_4 et $C_2 \times C_2$. Ces deux groupes ne sont pas isomorphes puisque C_4 contient un élément d'ordre 4, mais pas $C_2 \times C_2$, et deux groupes isomorphes possèdent toujours des éléments de même ordre (exercice). Le fait que tout groupe d'ordre 4 est isomorphe à un de ces deux groupes est un exercice qu'on pourra s'amuser à résoudre à l'aide des tables de groupes par exemple.

■ **Exemple** L'homomorphisme exponentiel admet comme inverse l'homomorphisme

$$\begin{aligned} \log : (\mathbb{R}_{>0}, \cdot) &\longmapsto (\mathbb{R}, +) \\ y &\longmapsto \log(y). \end{aligned}$$

En particulier, les groupes $(\mathbb{R}_{>0}, \cdot)$ et $(\mathbb{R}, +)$ sont isomorphes.

Proposition 1.29 Soient G, H deux groupes et $f : G \rightarrow H$ un homomorphisme. Alors f est un isomorphisme si et seulement si f est bijective.

■ **Remarque** Cette proposition est très utile en pratique. Elle nous dit en clair que si un homomorphisme est bijectif, son inverse, qui existe d'un point de vue ensembliste, est automatiquement un homomorphisme. Par exemple, dans la preuve ci-dessus que tous les groupes d'ordre deux sont isomorphes, nous aurions pu nous épargner la phrase "Par symétrie, son inverse est aussi un homomorphisme".

Démonstration. \implies : Par définition.

\impliedby : Si $f : G \rightarrow H$ est bijective, elle admet une application (inverse) $f' : H \rightarrow G$, c'est-à-dire une application satisfaisant

$$f' \circ f = \text{Id}_G \quad \text{et} \quad f \circ f' = \text{Id}_H.$$

En effet, pour tout $h \in H$ il existe par surjectivité de f un élément $g \in G$ tel que $f(g) = h$. De plus, ce g est unique par injectivité de f . Il suffit donc de poser $f'(h) := g$.

Reste à voir que si f est un homomorphisme, cette application inverse f' est un homomorphisme. Soient $h, h' \in H$. On a

$$\begin{aligned} f(f'(hh')) &= hh' & \text{car } f \circ f' &= \text{Id}_H \\ &= f(f'(h))f(f'(h')) & \text{car } f \circ f' &= \text{Id}_H \\ &= f(f'(h))f'(h') & \text{car } f &\text{ homomorphisme.} \end{aligned}$$

Puisque f est injective, on en déduit que

$$f'(hh') = f'(h)f'(h'),$$

ce qui montre bien que f' est un homomorphisme. ■

1.5 Indice et Théorème de Lagrange

■ **Notation 1.1** Soient G un groupe, $X, Y \subset G$ des sous-ensembles et $g \in G$. On dénote les sous-ensembles suivants de G par

$$gX := \{gx \mid x \in X\} \subset G,$$

$$Xg := \{xg \mid x \in X\} \subset G,$$

$$XY := \{xy \mid x \in X, y \in Y\} \subset G,$$

Définition 1.30 Soient G un groupe, H un sous-groupe et $g \in G$. On appelle l'ensemble gH une *classe à gauche* (de H dans G). De même, l'ensemble Hg est appelé *classe à droite* (de H dans G).

Théorème 1.31 Soient G un groupe et $H < G$ un sous-groupe. Soient xH, yH deux classes à gauches. Alors

- ou bien $xH = yH$,
- ou bien $xH \cap yH = \emptyset$.

Démonstration. Supposons que $xH \cap yH \neq \emptyset$ et montrons que $xH = yH$. Puisque l'intersection $xH \cap yH$ est non vide, il existe $z \in xH \cap yH$. Comme $z \in xH$, il existe $h_1 \in H$ tel que $z = xh_1$. De même, comme $z \in yH$, il existe $h_2 \in H$ tel que $z = yh_2$. En particulier

$$xh_1 = yh_2.$$

Posons $h := h_2(h_1)^{-1} \in H$ et récrivons l'équation précédente comme

$$x = yh_2(h_1)^{-1} = yh.$$

On a

$$xH = yhH \subset yH,$$

où l'inclusion découle du fait que $hH \subset H$, puisque la loi de composition de G restreinte à H est interne. On a donc démontré que $xH \subset yH$ et on obtient l'inclusion inverse $xH \supset yH$ par symétrie. ■

Observons que nous avons en particulier montré que $xH = yH$ si et seulement si il existe $h \in H$ tel que $x = yh$.

■ **Exemples 1.32** 1. $G = \mathbb{Z} > 2\mathbb{Z} = H$. Il y a deux classes :

$$2\mathbb{Z} \quad \text{et} \quad 1 + 2\mathbb{Z},$$

la première est constituée des nombres pairs, la seconde des nombres impairs. En particulier elles sont bien disjointes.

2. Plus généralement, pour $n \in \mathbb{N}$, le sous-groupe $n\mathbb{Z}$ de \mathbb{Z} possède n classes :

$$n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}.$$

a. Preuve directe : En effet, par définition, toute classe a la forme

$$m + n\mathbb{Z}, \quad \text{pour } m \in \mathbb{Z}.$$

Si on applique la division Euclidienne par n à m on obtient

$$m = qn + r \quad \text{avec} \quad 0 \leq r < n.$$

Or puisque $qn \in n\mathbb{Z}$, notre classe arbitraire

$$m + n\mathbb{Z} = r + n\mathbb{Z},$$

pour un r satisfaisant $0 \leq r < n$. Ceci montre déjà qu'il y a au plus n classes. Montrons de plus qu'en variant r entre $0 \leq r < n$ on obtient bien n classes distinctes : Supposons qu'il existe r_1, r_2 tels que $0 \leq r_1 < r_2 < n$ et $r_1 + n\mathbb{Z} \cap r_2 + n\mathbb{Z} \neq \emptyset$. Par le Théorème 1.31, ceci implique que ces classes sont égales, donc

$$r_1 + n\mathbb{Z} = r_2 + n\mathbb{Z} \iff n\mathbb{Z} = r_2 - r_1 + n\mathbb{Z},$$

ce qui implique en particulier que $r_2 - r_1 \in n\mathbb{Z}$, ce qui n'est pas possible puisque

$$0 < r_2 - r_1 < n.$$

b. Alternativement, si l'on a déjà démontré qu'il y a n classes d'équivalences pour la relation de congruence modulo n , Théorème A.9, on observe simplement que

$$m + n\mathbb{Z} = \overline{m}. \tag{1.2}$$

\subset : Soit $m + nq \in m + n\mathbb{Z}$. Alors $m + nq \equiv m \pmod{n}$ et donc $m + nq \in \overline{m}$.

\supset : Soit $k \in \overline{m}$. Par définition, $k \equiv m \pmod{n}$ donc il existe $q \in \mathbb{Z}$ tel que $k - m = nq$ et donc $k = m + nq \in m + n\mathbb{Z}$.

3. Dans $G = \text{Sym}(n)$ considérons le sous-groupe

$$H = \{\sigma \in \text{Sym}(n) \mid \sigma(n) = n\},$$

qui est clairement isomorphe à $\text{Sym}(n-1)$. Déterminons l'ensemble des classes à gauche $\text{Sym}(n)/H$: Soient $\sigma, \tau \in \text{Sym}(n)$. Alors $\sigma H = \tau H$ si et seulement si $\tau^{-1}\sigma \in H$ donc si et seulement si $\tau^{-1}\sigma(n) = n$, autrement dit $\sigma(n) = \tau(n)$. En résumé

$$\sigma H = \{\tau \in \text{Sym}(n) \mid \sigma(n) = \tau(n)\}.$$

Donc une classe a la forme

$$\{\tau \in \text{Sym}(n) \mid k = \tau(n)\},$$

pour un $k \in \{1, 2, \dots, n\}$. Il y en a donc n .

4. Reprenons l'exemple précédent dans le cas où $n = 3$.

$$G = \text{Sym}(3) = \{\text{Id}, (1, 2, 3), (1, 3, 2), (1, 2), (1, 3), (2, 3)\}.$$

Les seules permutations qui fixent 3 sont l'identité et $(1, 2)$. On a donc $H = \{\text{Id}, (1, 2)\}$ qui est clairement isomorphe à $\text{Sym}(2)$. Il y a trois classes à gauche.

Chaque classe est formée des éléments de $\text{Sym}(3)$ qui envoient 3 sur k , pour $k = 1, 2, 3$. On a donc les trois classes

$$\begin{aligned} H &= \{\text{Id}, (1, 2)\}, \\ (1, 3)H &= \{(1, 3), (1, 2, 3)\}, \\ (2, 3)H &= \{(2, 3), (1, 3, 2)\}. \end{aligned}$$

■ **Notation 1.2** Soient G un groupe et H un sous-groupe. On dénote par G/H l'ensemble des classes à gauche,

$$G/H = \{gH \mid g \in G\}.$$

Définition 1.33 Soient G un groupe et H un sous-groupe. L'*indice* de H dans G , dénoté $[G : H]$ est la cardinalité de l'ensemble G/H .

Théorème 1.34 — Théorème de Lagrange. Soient G un groupe et H un sous-groupe. Alors

$$|G| = [G : H]|H|.$$

Cette formule fait sens aussi pour les groupes G de cardinalité infinie. Dans ce cas le théorème dit simplement que si G est infini, alors pour tout sous-groupe H , au moins l'un de $[G : H]$ ou $|H|$ est infini.

Reprenons les exemples ci-dessus : $n\mathbb{Z} < \mathbb{Z}$ possède n classes distinctes et donc

$$[\mathbb{Z}, n\mathbb{Z}] = n. \tag{1.3}$$

Le Théorème de Lagrange nous donne

$$\infty = |\mathbb{Z}| = |n\mathbb{Z}| \cdot [\mathbb{Z}, n\mathbb{Z}] = \infty \cdot n.$$

Le groupe symétrique $\text{Sym}(n)$ possède n classes pour le sous-groupe $H = \{\sigma \in \text{Sym}(n) \mid \sigma(n) = n\}$ isomorphe à $\text{Sym}(n-1)$. En particulier, $[\text{Sym}(n) : H] = n$ et

$$|\text{Sym}(n)| = [\text{Sym}(n) : H]|H| = n|\text{Sym}(n-1)|.$$

Ceci permet de montrer, par induction, que $|\text{Sym}(n)| = n!$, en partant de $|\text{Sym}(1)| = 1$.

Démonstration. Observons d'abord que toutes les classes de H ont la même cardinalité. En effet ceci découle du fait qu'il existe une bijection

$$\begin{aligned} H &\longrightarrow xH \\ h &\longmapsto xh. \end{aligned}$$

(C'est bien une bijection puisque elle admet l'application

$$\begin{aligned} xH &\longrightarrow H \\ k &\longmapsto x^{-1}k \end{aligned}$$

comme inverse.) Nous avons donc $|H| = |xH|$ pour tout $x \in G$.

Puisque la projection

$$\begin{aligned} G &\longrightarrow G/H \\ g &\longmapsto gH \end{aligned}$$

est une application surjective si G/H est de cardinalité infinie (et donc $[G : H] = \infty$) alors G aussi et il n'y a rien à montrer. Supposons donc $d = [G : H] < \infty$. Nous pouvons alors énumérer les d éléments de G/H comme

$$G/H = \{x_1H, \dots, x_dH\},$$

pour des $x_1, \dots, x_d \in G$. On a

$$G = \cup_{i=1}^d x_iH.$$

En effet il suffit de voir que G est inclu dans cette union : Soit $g \in G$. Alors gH est une classe de H . Elle doit figurer parmi une des d classes listée. Donc il existe i tel que $gH = x_iH$. Mais alors

$$g = g \cdot e \in gH = x_iH,$$

et g appartient bien à l'union $\cup_{i=1}^d x_iH$. De plus, par le théorème 1.31, cette union est une union disjointe, donc

$$G = \sqcup_{i=1}^d x_iH.$$

On en déduit que

$$|G| = \sum_{i=1}^d |x_iH| = \sum_{i=1}^d |H| = d|H| = [G : H]|H|,$$

où nous avons utilisé que $|x_iH| = |H|$. ■

- Corollaire 1.35**
1. Si $H < G$ alors $|H| \mid |G|$.
 2. Si $g \in G$ alors l'ordre de g divise $|G|$.
 3. Supposons $|K| < \infty$. Si $K < H < G$ alors

$$[G : K] = [G : H][H : K].$$

- **Remarques 1.36**
1. Observons que si G est fini, il découle du deuxième point du corollaire que $g^{|G|} = e$ pour tout $g \in G$. En effet, si l'ordre k de g divise $|G|$ alors $|G| = km$ pour un $m \in \mathbb{Z}$ et

$$g^{|G|} = g^{km} = (g^k)^m = e^m = e.$$

2. Le troisième point du corollaire est valide aussi pour des sous-groupes K de cardinalité infinie, mais ne s'obtient pas directement du Théorème de Lagrange. La démonstration de ce cas est laissée en exercice.

Démonstration. 1. Découle directement du Théorème de Lagrange.

2. Pour $g \in G$, le sous-groupe $\langle g \rangle < G$ est un sous-groupe de cardinalité l'ordre de g , qui divise G par le point précédent.

3. Par le théorème de Lagrange on a

$$\begin{aligned} |G| &= [G : K] \cdot |K|, \\ |G| &= [G : H] \cdot \underbrace{|H|}_{[H:K]|K|}. \end{aligned}$$

On en déduit que

$$[G : K]|K| = [G : H][H : K]|K|.$$

Puisque $|K| < \infty$, il suffit de diviser par $|K|$. ■

Application: Montrer que $m!n!$ divise $(m+n)!$. (Ceci implique que le coefficient binomial $\binom{m+n}{m} := (m+n)!/(m!n!)$ est bien un nombre entier.) Bien sûr, ce n'est pas très difficile à montrer directement, mais voici une preuve basée sur le théorème de Lagrange : Le produit $\text{Sym}(m) \times \text{Sym}(n)$ est un sous-groupe de $\text{Sym}(m+n)$, où l'on pense à $\text{Sym}(m)$ comme les permutations des m premiers éléments de $\{1, 2, \dots, m+n\}$ et $\text{Sym}(n)$ comme les permutations des n derniers éléments. Ces deux sous-groupes commutent et forment donc un produit direct puisque des permutations à support disjoint commutent. L'affirmation suit du fait que l'ordre d'un sous-groupe divise l'ordre d'un groupe.

Nous verrons comme autre application des preuves directes de Théorèmes de Fermat et d'Euler dans la Section 1.8.

Nous n'avons manipulé que des classes à gauche, mais nous aurions pu faire exactement pareil pour les classes à droite. (C'est un bon exercice : reformulez et démontrez tous les énoncés de ce paragraphe pour les classes à droite.) En particulier, on aurait pu définir un indice (à droite) comme la cardinalité de l'ensemble des classes à droite, avec lequel on aurait démontré le Théorème de Lagrange pour l'indice (à droite), duquel on aurait obtenu que l'indice à (droite) est $|G|/|H|$, donc égal à l'indice (à gauche). Ceci peut se montrer directement : il existe une bijection entre les classes à droite et les classes à gauche (cf exercices).

1.6 Sous-groupes normaux et quotients

Commençons par une discussion : Est-ce que l'ensemble des classes G/H est un groupe pour une loi de composition "raisonnable" ? Mais qu'entend-on par "raisonnable" ? On a une application quotient

$$\begin{aligned} \pi : G &\longrightarrow G/H \\ g &\longmapsto gH \end{aligned}$$

et on aimerait que la loi sur G/H , disons \circ , soit telle que cette application π est un homomorphisme, c'est-à-dire telle que

$$\pi(x) \circ \pi(y) = \pi(xy) \iff xH \circ yH = xyH \quad \forall x, y \in G.$$

On est donc obligé de définir

$$xH \circ yH := xyH.$$

Mais est-ce bien défini ? C'est-à-dire si $xH = x'H$ et $yH = y'H$ a-t-on bien $xyH = x'y'H$? Rappelons-nous que $xH = x'H$ si et seulement si $x' = xh$, avec $h \in H$. Et de même $yH = y'H$ si et seulement si $y' = yh'$, pour $h' \in H$. On a alors

$$x'y'H = xhyh'h'H = xhyH$$

qui est égal à xyH si et seulement si $hyH = yH$ ou encore $y^{-1}hy \in H$, et ceci pour tout $y \in G$ et $h \in H$. Ceci motive la définition suivante :

Définition 1.37 Soit G un groupe. Un sous-groupe $N < G$ est dit *normal* si

$$gNg^{-1} = N$$

pour tout $g \in G$. Si $N < G$ est normal, on dénote l'inclusion par $N \triangleleft G$.

■ **Remarque** Pour montrer qu'un sous-groupe est normal il suffit de démontrer l'une des deux inclusions de l'égalité. En effet, supposons que $gNg^{-1} \subset N$ pour tout $g \in G$. L'inclusion inverse s'obtient par

$$N = g(g^{-1}Ng)g^{-1} \subset gNg^{-1},$$

où on a appliqué la première inclusion avec g^{-1} au lieu de g . Autrement dit, pour montrer qu'un sous-groupe $N < G$ est normal il suffit de montrer que

$$gng^{-1} \in N, \quad \forall n \in N, g \in G.$$

- **Exemples 1.38**
1. Pour tout groupe G on a les deux sous-groupes normaux $\{e\} \triangleleft G$ et $G \triangleleft G$.
 2. Dans un groupe abélien, tout sous-groupe est normal.
 3. Dans $\text{Sym}(3)$ le sous-groupe $N = \{\text{Id}, (1,2,3), (1,3,2)\}$ est normal, mais $H = \{\text{Id}, (1,2)\}$ ne l'est pas puisque

$$(1,2,3)(1,2)(1,2,3)^{-1} = (1,2,3)(1,2)(1,3,2) = (2,3) \notin H.$$

4. Pour tout groupe G on peut définir son *centre* comme

$$Z(G) = \{z \in G \mid zg = gz \forall g \in G\}.$$

Vous vérifierez facilement que $Z(G)$ est un sous-groupe normal de G .

■ **Remarque** Observez que si $K < H < G$, alors $K \triangleleft H$ et $H \triangleleft G$ n'implique pas que $K \triangleleft G$ en général. Je vous laisse trouver le contre-exemple le plus simple dans $G = \text{Alt}(4)$. (Cf Définition 1.70.)

Théorème 1.39 Soient G un groupe et $N \triangleleft G$ un sous-groupe normal. Alors G/N muni de la loi

$$\begin{aligned} G/N \times G/N &\longrightarrow G/N \\ (xN, yN) &\longmapsto xN \circ yN := xyN \end{aligned}$$

est un groupe. De plus l'application quotient

$$\begin{aligned} \pi: G &\longrightarrow G/N \\ x &\longmapsto xN \end{aligned}$$

est un homomorphisme surjectif de noyau $\text{Ker}(\pi) = N$.

Le groupe G/N est appelé *groupe quotient*.

Démonstration. La seule vérification non immédiate, est le fait que le produit $xN \circ yN := xyN$ est bien défini, ce que nous avons déjà montré dans la discussion motivant la définition de sous-groupe normal. Puisque c'est le point crucial de cette preuve, nous incluons à nouveau l'argument, sous une forme un tout petit peu différente. Observons d'abord que puisque $N \triangleleft G$ est normal on a l'égalité

$$xyN = xNyN$$

pour tous $x, y \in G$. En effet, puisque $yNy^{-1} = N$ et donc $yN = Ny$ on a

$$xNyN = xyNN = xyN.$$

Nous pouvons donc écrire le produit comme

$$xN \circ yN := xyN = xNyN.$$

Il est maintenant immédiat que le produit est bien défini : Si $xN = x'N$ et $yN = y'N$ alors

$$xyN = xNyN = x'Ny'N = x'y'N.$$

Ne nous reste plus que quelques vérifications standard.

Le quotient G/N est un groupe :

— Associativité : Soient $xN, yN, zN \in G/N$. On a

$$\begin{aligned} (xN \circ yN) \circ zN &= (xyN) \circ zN = (xy)zN \\ &= x(yzN) = xN \circ (yzN) = xN \circ (yN \circ zN), \end{aligned}$$

où l'on a utilisé l'associativité de G pour le passage de la première ligne à la deuxième.

— Neutre dans G/N : Le neutre est la classe N . En effet pour tout $xN \in G/N$ on a

$$xN \circ N = xN \circ eN = xeN = xN = exN = eN \circ xN = N \circ xN.$$

— Inverse : L'inverse de $xN \in G/N$ est $x^{-1}N$:

$$xN \circ x^{-1}N = (xx^{-1}N) = eN = N = eN = (x^{-1}x)N = x^{-1}NxN.$$

La projection π est clairement un homomorphisme

$$(\pi(xy) = xyN = xN \circ yN = \pi(x) \circ \pi(y))$$

surjectif (pour tout $xN \in G/N$ on a $\pi(x) = xN$).

Le noyau de π est N : Soit $x \in G$. Alors $\pi(x) = xN = N$ si et seulement si $x \in N$. ■

■ **Exemple** Le groupe quotient $\mathbb{Z}/n\mathbb{Z}$: Soit $n \in \mathbb{N}$. Le sous-groupe $n\mathbb{Z}$ est normal dans \mathbb{Z} (puisque \mathbb{Z} est abélien). Nous avons déjà vu en (1.2) que

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\},$$

où l'on rappelle que \bar{k} dénote la classe d'équivalence de k pour la relation de congruence modulo n . De plus, on a pour tout $k, \ell \in \mathbb{Z}$,

$$(k + n\mathbb{Z}) + (\ell + n\mathbb{Z}) = (k + \ell) + n\mathbb{Z} = \overline{k + \ell} = \bar{k} + \bar{\ell}.$$

La loi induite sur le quotient $\mathbb{Z}/n\mathbb{Z}$ est donc précisément l'addition modulo n sur $\{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$, duquel on déduit que

$$\mathbb{Z}/n\mathbb{Z} = C_n.$$

Théorème 1.40 Soient G, H deux groupes, $N \triangleleft G$ un sous-groupe normal, $f : G \rightarrow H$ un homomorphisme. Si $N \subset \text{Ker}(f)$ alors il existe un unique homomorphisme $\bar{f} : G/N \rightarrow H$ tel que $f = \bar{f} \circ \pi$, c'est-à-dire tel que le diagramme

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \pi \downarrow & \nearrow \bar{f} & \\ G/N & & \end{array}$$

commute.

■ **Remarque** Puisque N et $\text{Ker}(f)$ sont des sous-groupes de G , la condition que N est un sous-groupe de $\text{Ker}(f)$ est équivalente à la condition que N est inclu dans $\text{Ker}(f)$.

De plus, si N n'est pas inclu dans $\text{Ker}(f)$, un tel homomorphisme \bar{f} n'a aucune chance d'exister : En effet il existerait $n \in N$ tel que $n \notin \text{Ker}(f)$. On aurait d'une part $f(n) \neq e_H$ et d'autre part, et pour n'importe quel homomorphisme $\bar{f} : G/N \rightarrow H$, $\bar{f} \circ \pi(n) = \bar{f}(e_{G/N}) = e_H$.

Démonstration. Observons d'abord que puisque nous voulons $f = \bar{f} \circ \pi$, nous n'avons aucun choix dans la définition de \bar{f} . En effet,

$$\bar{f}(xN) = \bar{f}(\pi(x)) = f(x).$$

Voyons que \bar{f} telle définie est bien définie, c'est-à-dire, si $xN = x'N$ alors $f(x) = f(x')$. Rappelons que $xN = x'N$ si et seulement si il existe $n \in N$ tel que $x' = xn$. Dans ce cas on obtient

$$f(x') = f(xn) = f(x)f(n) = f(x),$$

où pour la dernière égalité on a utilisé que N est contenu dans le noyau de f .

Ne reste plus qu'à vérifier que \bar{f} est bien un homomorphisme :

$$\begin{aligned} \bar{f}(xNyN) &= \bar{f}(xyN) && \text{par définition de la loi sur } G/N, \\ &= f(xy) && \text{par définition de } \bar{f}, \\ &= f(x)f(y), && \text{car } f \text{ est un homomorphisme,} \\ &= \bar{f}(xN)\bar{f}(yN) && \text{par définition de } \bar{f}. \end{aligned}$$

■

Lemme 1.41 Soient G, H deux groupes et $f : G \rightarrow H$ un homomorphisme. Alors le noyau $\text{Ker}(f)$ est un sous-groupe normal de G .

Démonstration. Nous avons déjà vérifié que le noyau (et l'image) d'un homomorphisme est un sous-groupe de G (respectivement de H). Ne reste plus qu'à montrer que $\text{Ker}(f)$ est normal, c'est-à-dire que $gkg^{-1} \in \text{Ker}(f)$ pour tout $g \in G$ et $k \in \text{Ker}(f)$. On calcule donc

$$\begin{aligned} f(gkg^{-1}) &= f(g)f(k)f(g)^{-1} && \text{car } f \text{ est un homomorphisme,} \\ &= f(g)f(g)^{-1} && \text{car } f(k) = e \text{ puisque } k \in \text{Ker}(f), \\ &= e, \end{aligned}$$

ce qui montre bien que $gkg^{-1} \in \text{Ker}(f)$. ■

Corollaire 1.42 Soit G un groupe. Un sous-groupe $N < G$ est normal si et seulement si il existe un groupe H et un homomorphisme $f : G \rightarrow H$ tel que $N = \text{Ker}(f)$.

Démonstration. Si N est normal, prendre $H = G/N$ et $f = \pi : G \rightarrow G/N$.

Inversément, si N est le noyau d'un homomorphisme, il est normal par le Lemme 1.41. ■

Malgré ce corollaire, il est parfois difficile ou tout au moins pénible de déterminer si un sous-groupe est normal. Le critère suivant est très utile en pratique :

Lemme 1.43 Soient G un groupe et $H < G$ un sous-groupe. Si $[G : H] = 2$ alors $H \triangleleft G$.

Démonstration. Première preuve, n'utilisant pas l'égalité entre le nombre de classes à droite et à gauche : Puisque l'indice est 2, le groupe G se décompose comme l'union disjointe de deux classes à gauche :

$$G = H \sqcup gH,$$

pour tout $g \in G$ n'appartenant pas à H . Soient $x \in G, h \in H$. A voir : $xhx^{-1} \in H$. Si $x \in H$ c'est clair. Supposons que $x \notin H$ de sorte que l'on a

$$G = H \sqcup xH.$$

Supposons par l'absurde que $xhx^{-1} \notin H$. Alors $xhx^{-1} \in xH$ et donc $hx^{-1} \in H$ et après multiplication à gauche par h^{-1} aussi $x^{-1} \in H$ et finalement $x \in H$, contradiction.

Deuxième preuve, plus élégante, à n'utiliser que si vous avez démontré l'égalité entre le nombre de classes à droite et à gauche : Si $x \in H$ il est clair que $xH = Hx$. Si $x \notin H$ alors

$$G = H \sqcup xH = H \sqcup Hx.$$

Donc $xH = Hx$. ■

Théorème 1.44 Soient G, H deux groupes. Tout homomorphisme $f : G \rightarrow H$ induit un isomorphisme

$$\bar{f} : G/\text{Ker}(f) \longrightarrow \text{Im}(f).$$

Démonstration. Soit $f : G \rightarrow H$ un homomorphisme. Appliquons le Théorème 1.40 à f et $N = \text{Ker}(f)$ pour déduire qu'il existe un (unique) homomorphisme $\bar{f} : G/\text{Ker}(f) \rightarrow H$ tel que le diagramme

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \pi \downarrow & \nearrow \bar{f} & \\ G/\text{Ker}(f) & & \end{array}$$

commute. Puisque le diagramme commute, les deux homomorphismes f et \bar{f} ont la même image et nous pouvons considérer \bar{f} comme un homomorphisme $\bar{f} : G/\text{Ker}(f) \rightarrow \text{Im}(f)$.

Finalement, \bar{f} est injectif puisque si $g\text{Ker}(f)$ est dans le noyau, alors $e_H = \bar{f}(g\text{Ker}(f)) = \bar{f}\pi(g) = f(g)$ et donc $g \in \text{Ker}(f)$ et $g\text{Ker}(f) = \text{Ker}(f)$. ■

Corollaire 1.45 Soit $f : G \rightarrow H$ un homomorphisme surjectif. Alors

$$[G : \text{Ker}(f)] = |H|.$$

Démonstration. Par le Théoreme 1.44, l'homomorphisme f induit un isomorphisme

$$G/\text{Ker}(f) \cong H.$$

Ces deux groupes ont donc la même cardinalité. Mais la cardinalité de $G/\text{Ker}(f)$ n'est autre que l'indice $[G : \text{Ker}(f)]$, par définition. ■

1.7 Groupes simples

Discussion : Soit G un groupe. S'il admet un sous-groupe normal $N \triangleleft G$, alors il existe un groupe H et un homomorphisme surjectif $f : G \rightarrow H$ tel que $G/N \cong H$. (En effet prendre $H = G/N$ et f la projection $G \rightarrow G/N$). Oublions G et posons-nous la question de savoir comment retrouver G à partir de N et H . Le groupe G est caractérisé par le fait qu'il existe un homomorphisme injectif $i : N \rightarrow$ et un homomorphisme surjectif $\pi : G \rightarrow H$ tels que $\text{Im}(i) = \text{Ker}(\pi)$,

$$N \xrightarrow{i} G \xrightarrow{\pi} H.$$

Un tel groupe G est appelé *extension de H par N* . Les groupes H et N ne déterminent pas G uniquement (par exemple pour $H = N = C_2$ on peut obtenir $G = C_4$ ou $G = C_2 \times C_2$). La chose à retenir est que G se construit (par extensions) à partir de groupes "plus petits", à condition d'admettre un sous-groupe normal.

Définition 1.46 Un groupe G est dit simple si ses seuls sous-groupes normaux sont $\{e\}$ et G .

L'idée sous-jacente est que les groupes simples forment les "blocs de constructions" des groupes.

Proposition 1.47 Soit G un groupe d'ordre p premier. Alors G est simple.

Démonstration. On montre plus généralement que G ne contient pas de sous-groupes différents de $\{e\}$ et G . Soit $N < G$ un sous-groupe. Alors par Lagrange, $|N|$ divise $|G| = p$. Donc soit $|N| = 1$ et $N = \{e\}$, soit $|N| = p = |G|$ et $N = G$. ■

Plus généralement, tout groupe d'ordre p premier est simple, simplement parce qu'il est isomorphe à C_p :

Lemme 1.48 Soit G un groupe tel que $|G| = p$ est premier. Alors $G \cong C_p$.

Remarquons que la Proposition 1.47 combinée avec le Lemme 1.48 montrent en particulier que le groupe cycle C_p est simple pour p premier. En contraste C_n n'est jamais simple si n n'est pas premier. En effet, si $n = ab$ avec $1 < a, b < n$ alors C_n contient le sous groupe normal

$$\{\bar{0}, \bar{a}, \bar{2a}, \dots, \overline{(b-1)a}\}.$$

Démonstration. Soit $e \neq x \in G$. Comme dans la preuve du lemme précédent, on sait que $\text{ord}(x) = p$. On définit un homomorphisme

$$f: \begin{array}{ccc} C_p & \longrightarrow & G \\ \bar{k} & \longmapsto & x^k \end{array}$$

qui est bien défini car $\text{ord} x = p$. Il est de plus injectif car

$$e = f(\bar{k}) = x^k$$

implique que p divise k et donc que $\bar{k} = 0$. Un homomorphisme injectif entre deux groupes de même cardinalité est aussi surjectif, et c'est donc un isomorphisme. ■

Nous démontrerons aussi dans le Paragraphe 1.9 (Théorème 1.73) que le groupe alterné $\text{Alt}(n)$ est simple pour $n \geq 5$. (Aussi pour $n = 1, 2$ trivialement et $n = 3$ puisque $\text{Alt}(3) \cong C_3$.) Ceci établit déjà deux familles infinies de groupes simples. A titre informatif, les groupes finis simples sont complètement classifiés. Plus précisément si G est simple alors il est isomorphe à un (unique) groupe parmi la liste suivante :

- C_p pour p premier,
- $\text{Alt}(n)$ pour $n \geq 5$,
- "groupes de type de Lie", par exemple $\text{PSL}(2, \mathbb{Z}/5\mathbb{Z})$, subdivisés en 12 familles infinies et 4 groupes additionnels,
- un des 26 groupes appelés "sporadiques". Le plus grand, appelé "monstre" a cardinalité $\sim 8 \cdot 10^{53}$.

Cette classification est un travail titanesque. Débutée en 1955, affirmée comme établie en 1983, elle n'est finalisée qu'en 2004 après plus de 50 articles par plus de 100 mathématiciens, détaillée sur plus de 10'000 pages. Typiquement elle sera considérée comme une "boîte noire" par la plupart des mathématiciens.

1.8 Groupes cycliques

Définition 1.49 Un groupe G est dit *cyclique* s'il existe $x \in G$ tel que $G = \langle x \rangle$.

- **Exemples 1.50** 1. \mathbb{Z} est cyclique puisque $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.
2. $C_n = \mathbb{Z}/n\mathbb{Z}$ est cyclique, $C_n = \langle \bar{1} \rangle$ ou de façon équivalente $\mathbb{Z}/n\mathbb{Z} = \langle 1 + \mathbb{Z} \rangle$.
- **Remarques** 1. Rappelons que si $G = \langle x \rangle$ est cyclique, alors l'ordre de x est égal à $|G|$. En particulier :

$$\begin{array}{ll} \text{si } |G| = \infty : & G = \{\dots, x^{-1}, x^{-1}, e, x, x^2, \dots\}, \\ \text{si } |G| = n < \infty : & G = \{e, x, x^2, \dots, x^{n-1}\}. \end{array}$$

2. Si G est cyclique, alors G est abélien.

Théorème 1.51 Soit $H < \mathbb{Z}$ un sous-groupe. Alors H est cyclique et il existe un unique $n \in \mathbb{N}$ tel que

$$H = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}.$$

De plus, si $H \neq \{0\}$ alors $n = [\mathbb{Z} : H]$.

Preuve du Théorème 1.51. Existence de n : Soit $H < \mathbb{Z}$ un sous-groupe. Si $H = \{0\}$ on prend $n = 0$. Supposons dorénavant que $H \neq \{0\}$ et considérons l'ensemble $H \cap \mathbb{N}^*$. Cet ensemble est non vide (puisque $H \neq \{0\}$, il existe $h \neq 0 \in H$, et comme H est un sous-groupe, $-h$ aussi appartient à H , donc $\{h, -h\} \subset H$ et $|h| \in H \cap \mathbb{N}^*$) et minoré (tous ses éléments sont ≥ 1), dont on conclut qu'il existe un plus petit élément que nous appellerons h_0 .

Affirmation: $H = \langle h_0 \rangle$.

Preuve de l'affirmation. Puisque $h_0 \in H$, on a l'inclusion $\langle h_0 \rangle < H$. Pour l'autre inclusion, soit $h \in H$, et montrons que $h \in \langle h_0 \rangle$. Par la Division Euclidienne, il existe (des uniques) $q, r \in \mathbb{Z}$ tels que

$$h = qh_0 + r \quad \text{et} \quad 0 \leq r < h_0.$$

Mais alors

$$r = h - qh_0 = h + \underbrace{(-h) + \cdots + (-h)}_{q \text{ fois}} \in H.$$

Il en découle que $r = 0$, sinon on aurait $r \in H \cap \mathbb{N}^*$ avec $r < h_0$, ce qui contredirait la minimalité de h_0 dans $H \cap \mathbb{N}^*$. Mais si $r = 0$, alors $h = qh_0 \in \langle h_0 \rangle$. ■

Dans le théorème, on prend donc $n = h_0$, et on a bien l'affirmation que

$$H = \langle n \rangle = n\mathbb{Z}.$$

Unicité : Elle est évidente puisque $n\mathbb{Z} = m\mathbb{Z}$ si et seulement si $n = \pm m$.

Finalement, l'indice $[\mathbb{Z} : n\mathbb{Z}] = n$ a été établie dans (1.44). ■

Corollaire 1.52 — Classification des groupes cycliques. Soit G un groupe cyclique.

Si $|G| = \infty$ alors $G \cong \mathbb{Z}$.

Si $|G| = n < \infty$ alors $G \cong \mathbb{Z}/n\mathbb{Z}$.

Notons qu'en particulier, tout groupe cyclique est quotient de \mathbb{Z} .

Démonstration. Soit $G = \langle x \rangle$ un groupe cyclique et considérons l'homomorphisme

$$\begin{aligned} f: \mathbb{Z} &\longrightarrow G \\ m &\longmapsto x^m. \end{aligned}$$

Puisque tout élément de G est une puissance de x , l'homomorphisme f est clairement surjectif. Il découle du Théorème 1.44 que $\mathbb{Z}/\text{Ker}(f) \cong G$.

Si $|G| = |x| = \infty$ alors $\text{Ker}(f) = \{0\}$ et $G \cong \mathbb{Z}$.

Si $|G| = |x| = n < \infty$ alors $\text{Ker}(f) = n\mathbb{Z}$ et $G \cong \mathbb{Z}/n\mathbb{Z}$.

■

La définition du plus grand commun diviseur $\text{pgcd}(a, b)$ de deux nombres entiers $a, b \in \mathbb{Z}$ est rappelée dans la Définition A.2 de l'Annexe.

Corollaire 1.53 Soient $a, b \in \mathbb{Z}$. Alors

$$\{am + bn \mid m, n \in \mathbb{Z}\} \subset \mathbb{Z}$$

est un sous-groupe cyclique engendré par $\text{pgcd}(a, b)$.

Sans parler de groupes, on peut reformuler ce corollaire en disant que donnés a, b tout nombre de la forme $am + bn$, pour $m, n \in \mathbb{Z}$ est un multiple de $\text{pgcd}(a, b)$. Et inversement que tout multiple du pgcd s'écrit sous cette forme. C'est la formulation du Théorème A.5 dont une preuve constructive n'impliquant pas la théorie des groupes est donnée dans l'annexe, avec en particulier aussi un algorithme pour trouver le pgcd de deux nombres.

Dans le cas où a et b sont premiers entre eux, c'est-à-dire par définition si $\text{pgcd}(a, b) = 1$, on obtient en particulier :

Théorème 1.54 — Théorème de Bézout. Deux nombres $a, b \in \mathbb{Z}$ sont premiers entre eux si et seulement si il existe $m, n \in \mathbb{Z}$ tels que $am + bn = 1$.

Preuve du Théorème de Bézout. Soient a, b tels que $\text{pgcd}(a, b) = 1$. Alors par le Corollaire 1.53,

$$\{am + bn \mid m, n \in \mathbb{Z}\} = \mathbb{Z}.$$

Puisque $1 \in \mathbb{Z}$ il existe $m, n \in \mathbb{Z}$ tels que $am + bn = 1$.

Inversement s'il existe $m, n \in \mathbb{Z}$ tels que $am + bn = 1$ alors par le Corollaire 1.53, 1 appartient au sous-groupe cyclique engendré par $\text{pgcd}(a, b)$. C'est donc un multiple de $\text{pgcd}(a, b)$, ce qui n'est possible que si $1 = \text{pgcd}(a, b)$. ■

Preuve du Corollaire 1.53. Le fait que

$$H := \{am + bn \mid m, n \in \mathbb{Z}\}$$

est un sous-groupe de \mathbb{Z} devrait dorénavant vous sauter aux yeux comme une évidence. (Si ce n'est pas le cas, vérifiez les axiomes !) Par le Théorème 1.51, H est un groupe cyclique de la forme $H = k\mathbb{Z}$, avec $k \in \mathbb{N}$. A voir : $k = \text{pgcd}(a, b)$. Observons qu'un nombre entier x appartient à H si et seulement si $k \mid x$.

On a

$$a = 1 \cdot a + 0 \cdot b \in H \implies k \mid a,$$

$$b = 0 \cdot a + 1 \cdot b \in H \implies k \mid b,$$

en particulier k divise a et b et donc $k \leq \text{pgcd}(a, b)$.

Par définition $\text{pgcd}(a, b) \mid a$ et $\text{pgcd}(a, b) \mid b$ donc $\text{pgcd}(a, b)$ divise n'importe quelle combinaison \mathbb{Z} -linéaire de a et b , donc tout élément de H . En effet, soient $u, v \in \mathbb{Z}$ tels que $a = pu$ et $b = pv$. Alors un élément arbitraire de H a la forme

$$am + bn = pum + pvn = p(um + vn),$$

qui est bien divisible par p . En particulier, p divise $k \in H$ et donc $p \leq k$. ■

Multiplication modulo n

Rappelons-nous que

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

et posons

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{m} \mid \text{pgcd}(m, n) = 1\}.$$

Par exemple, $(\mathbb{Z}/6\mathbb{Z})^\times = \{\bar{1}, \bar{5}\}$ et si p est premier,

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\}.$$

Proposition 1.55 $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot \bmod n)$ est un groupe abélien.

Démonstration. Observons d'abord que nous avons enlevé les éléments qu'il fallait à $\mathbb{Z}/n\mathbb{Z}$ pour que la multiplication modulo n définisse bien une loi interne. En effet, soient $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Alors par définition $\text{pgcd}(a, n) = 1 = \text{pgcd}(b, n)$, ce qui revient à dire qu'aucun diviseur p premier de n ne divise a ou b . En particulier il ne peut pas diviser leur produit ab , et on obtient bien que $\text{pgcd}(ab, n) = 1$, et donc $\overline{ab} = \overline{ab}$ par le Lemme A.10 appartient bien à $(\mathbb{Z}/n\mathbb{Z})^\times$. Il est clair que la multiplication modulo n est une loi associative, commutative, de neutre 1. Ne reste plus qu'à montrer que tout élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ admet un inverse multiplicatif. Pour ceci, nous invoquerons le Théorème de Bézout. Soit $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Puisque $\text{pgcd}(a, n) = 1$, il existe, par Bézout (appliqué à a et n), des entiers $m, n \in \mathbb{Z}$ tels que

$$ma + np = 1.$$

Mais cette équation modulo p donne précisément

$$ma \equiv 1 \pmod{p}.$$

Il en découle que \bar{m} est l'inverse de \bar{a} . ■

Par exemple, cherchons l'inverse de $\bar{5}$ dans $(\mathbb{Z}/7\mathbb{Z})^\times$. Pour trouver $m, n \in \mathbb{Z}$ tels que $m \cdot 5 + n \cdot 7 = 1$ on pourra utiliser l'algorithme de l'Annexe, donnant par ailleurs une preuve directe du Théorème de Bézout. En utilisant cet algorithme, ou dans ce cas même à l'oeil nu, on trouve $m = -4$ et $n = 3$,

$$(-4) \cdot 5 + 3 \cdot 7 = 1.$$

Donc $-4 \equiv 3 \pmod{7}$, et $\overline{-4} = \bar{3}$ est l'inverse multiplicatif de $\bar{5}$. On contrôle pour être sûrs : $3 \cdot 5 = 15 = 1 + 14 \equiv 1 \pmod{7}$.

Définition 1.56 On définit, pour tout $n \in \mathbb{N}^*$ la fonction d'Euler par

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

Par exemple, $\varphi(6) = 2$ et $\varphi(p) = p - 1$ pour p premier.

Théorème 1.57 — Petit Théorème de Fermat. Soient p premier, $a \in \mathbb{Z}$ avec $\text{pgcd}(a, p) = 1$. Alors

$$a^{p-1} \equiv 1 \pmod{p}.$$

On obtient une façon alternative de trouver l'inverse d'un élément $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$. En effet il découle du Petit Théorème de Fermat que l'inverse de \bar{a} est $\overline{a^{p-2}}$. Par exemple, recalculons l'inverse de 5 modulo 7 :

$$5^{7-2} = 5^5 = 5^2 \cdot 5^2 \cdot 5 = 25^2 \cdot 5 \equiv 3^2 \cdot 5 \pmod{7} \equiv 2 \cdot 5 \pmod{7} \equiv 3 \pmod{7}.$$

Notons quand même que pour des p premiers grands, il peut être plus économique d'utiliser plutôt le Théorème de Bézout pour trouver l'inverse.

Théorème 1.58 — Théorème d'Euler. Soient $a, n \in \mathbb{Z}$ avec $n \geq 2$ et $\text{pgcd}(a, n) = 1$. Alors

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

Le Théorème d'Euler implique clairement le Petit Théorème de Fermat : Si $n = p$ est premier, alors $\varphi(p) = p - 1$. Démontrons le Théorème d'Euler :

Démonstration. Observons que puisque $\text{pgcd}(a, n) = 1$, la classe \bar{a} appartient à $(\mathbb{Z}/n\mathbb{Z})^\times$. Il découle de la Remarque 1.36.1 (qui est une conséquence directe du Théorème de Lagrange) que $a^{\varphi(n)} \equiv 1 \pmod{n}$. ■

Une preuve purement arithmétique du Petit Théorème de Fermat est présentée dans l'Annexe. Il existe aussi des preuves du Théorème d'Euler n'invoquant pas le Théorème de Lagrange, mais la plupart exploitent quand même le fait que les éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$ admettent des inverses multiplicatifs (ce qu'on peut faire, par Bézout, sans mentionner de groupes).

Les Théorèmes d'Euler et de Fermat sont à la base de certains systèmes de cryptographie moderne, connus sous le nom de système RSA, dont vous trouverez une description dans l'Annexe.

1.9 Groupes symétriques

Le groupe symétrique est le groupe fini par excellence, dans le sens où tout groupe fini est isomorphe à un sous-groupe d'un groupe symétrique. (Vous verrez ceci dans le cours de Géométrie I en utilisant des actions de groupe. Ce n'est pas difficile de le montrer avec seulement les notions introduites jusqu'ici dans ce cours.) Autrement dit, pour étudier tous les groupes finis, il "suffit" d'étudier les groupes symétriques et leurs

sous-groupes. Le groupe symétrique apparaît aussi naturellement dans de nombreuses formules mathématiques, comme par exemple dans le déterminant d'une matrice.

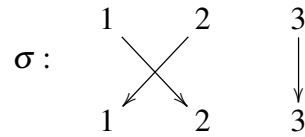
On appelle les éléments du groupe symétrique $\sigma \in \text{Sym}(n)$ des *permutations*. Il existe plusieurs façon de dépicter ces permutation. Par définition, une permutation est une bijection

$$\begin{aligned} \sigma : \{1, 2, \dots, n\} &\longrightarrow \{1, 2, \dots, n\} \\ 1 &\longmapsto \sigma(1) \\ 2 &\longmapsto \sigma(2) \\ &\vdots \\ n &\longmapsto \sigma(n). \end{aligned}$$

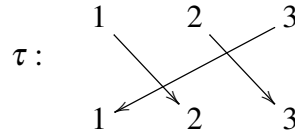
On aimera (ou pas) encoder cette information sous forme de matrice :

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

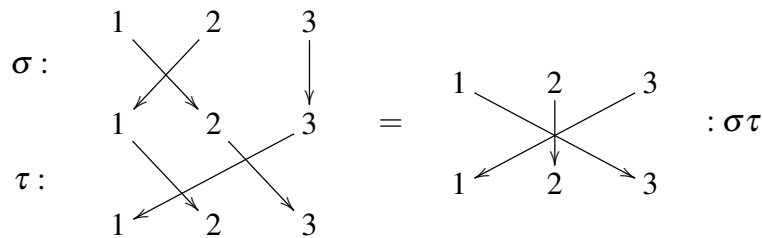
Une variante à priori minime de cette écriture mais qui présente d'énormes avantages pour la lecture de compositions de permutations ou le calcul de la signature (voir plus bas) est de faire deux lignes avec les éléments $1, 2, \dots, n$ (dans cet ordre), et d'ajouter une flèche entre i et $\sigma(i)$. Par exemple la permutation $\sigma \in \text{Sym}(3)$ qui échange 1 et 2 et fixe 3 est représentée par le diagramme



De même la permutation $\tau \in \text{Sym}(3)$ qui envoie 1 sur 2, 2 sur 3 et 3 sur 1 est représentée par le diagramme



Leur composition $\tau\sigma$ s'obtient alors immédiatement en suivant les flèches :



On aboutira à une troisième façon de représenter des permutations, en pratique la plus utile, dans le Théorème 1.64, dont l'idée est de décomposer toute permutation en cycles, que nous définissons maintenant :

Définition 1.59 Soit $1 \leq \ell \leq n$. Une permutation $\sigma \in \text{Sym}(n)$ est appelée un ℓ -cycle s'il existe un sous-ensemble $\{i_1, \dots, i_\ell\} \subset \{1, \dots, n\}$ de cardinalité ℓ tel que

1. $\sigma(i_k) = i_{k+1}$ pour $1 \leq k < \ell$,
2. $\sigma(i_\ell) = i_1$,
3. $\sigma(j) = j$ pour tout $j \in \{1, \dots, n\} \setminus \{i_1, \dots, i_\ell\}$.

On dénotera ce ℓ -cycle σ par $(i_1, i_2, \dots, i_\ell)$ et on appellera ℓ la *longueur* de σ . Un 2-cycle est appelé *transposition*. Un 2-cycle de la forme $(i, i+1)$, pour $1 \leq i < n$ est appelé *transposition élémentaire*.

Par exemple la permutation σ considérée ci-dessus est un 2-cycle, c'est-à-dire une transposition (même élémentaire), que l'on peut écrire comme $\sigma = (1, 2)$. La permutation τ ci-dessus est un 3-cycle, $\tau = (1, 2, 3)$. Avec cette notation, la composition devient encore plus évidente puisqu'il suffit de suivre chaque élément à travers les cycles. Par exemple montrons que

$$\tau\sigma = (1, 2)(1, 2, 3) = (2, 3).$$

On commence par 1 : On part du cycle le plus à droite, 1 est envoyé sur 2 par ce cycle, on prend le suivant qui renvoie 2 sur 1. Donc la composition envoie 1 sur 1. Essayons encore 2 : Le cycle le plus à droite envoie 2 sur 3, et le cycle suivant laisse 3 invariant. Donc la composition envoie 2 sur 3. Vous pourrez vérifier que cet algorithme envoie bien 3 sur 2, ou le déduire directement du fait que la composition est une bijection.

Le seul 1-cycle est l'identité, même si en tant que 1-cycle il admet d'après la définition différentes écritures : $(1) = \dots = (n) = \text{Id}$.

Proposition 1.60 Soit $(i_1, i_2, \dots, i_\ell) \in \text{Sym}(n)$ un ℓ -cycle. Alors

1. $(i_1, i_2, \dots, i_\ell) = (i_2, i_3, \dots, i_\ell, i_1)$,
2. $(i_1, \dots, i_\ell) = (i_1, \dots, i_k)(i_k, \dots, i_\ell)$ pour $1 < k < \ell$,
3. $\text{ord}((i_1, i_2, \dots, i_\ell)) = \ell$,
4. $\tau(i_1, i_2, \dots, i_\ell)\tau^{-1} = (\tau(i_1), \dots, \tau(i_\ell))$ pour tous $\tau \in \text{Sym}(n)$.

Démonstration. 1. et 3. Evident par définition. 2. Faites impérativement la vérification ! Ne reste que 4.

L'assertion est équivalente à

$$(i_1, i_2, \dots, i_\ell) = \tau^{-1}(\tau(i_1), \dots, \tau(i_\ell))\tau.$$

Montrons donc que le terme de droite est bien le ℓ -cycle (i_1, \dots, i_ℓ) . Pour $1 \leq k < \ell$, on a

$$\tau^{-1} \underbrace{(\tau(i_1), \dots, \tau(i_\ell))\tau(i_k)}_{=\tau(i_{k+1})} = i_{k+1}.$$

Similairement,

$$\tau^{-1} \underbrace{(\tau(i_1), \dots, \tau(i_\ell))\tau(i_\ell)}_{=\tau(i_1)} = i_1.$$

Finalement, si $j \in \{1, \dots, n\} \setminus \{i_1, \dots, i_\ell\}$ alors

$$\tau(j) \in \{1, \dots, n\} \setminus \{\tau(i_1), \dots, \tau(i_\ell)\}$$

est fixé par le ℓ -cycle $(\tau(i_1), \dots, \tau(i_\ell))$. De ce fait,

$$\tau^{-1} \underbrace{(\tau(i_1), \dots, \tau(i_\ell))\tau(j)}_{=\tau(j)} = j.$$

■

Proposition 1.61 Dans $\text{Sym}(n)$, tous les ℓ -cycles sont conjugués.

Démonstration. Soient $(i_1, \dots, i_\ell), (j_1, \dots, j_\ell)$ deux ℓ -cycles. Par le point 4. de la Proposition 1.60, il suffit de voir qu'il existe $\tau \in \text{Sym}(n)$ tel que $\tau(i_1) = j_1, \dots, \tau(i_\ell) = j_\ell$. On pose donc $\tau(i_k) := j_k$ pour tout $1 \leq k \leq \ell$, qui est une bijection entre

$$\{i_1, \dots, i_\ell\} \quad \text{et} \quad \{j_1, \dots, j_\ell\},$$

qu'on étend à une bijection de $\{1, 2, \dots, n\}$ en choisissant une bijection entre

$$\{1, 2, \dots, n\} \setminus \{i_1, \dots, i_\ell\} \quad \text{et} \quad \{1, 2, \dots, n\} \setminus \{j_1, \dots, j_\ell\},$$

ce qui est possible puisque ce sont deux ensembles de même cardinalité $n - \ell$. ■

Définition 1.62 Pour $\sigma \in \text{Sym}(n)$ on définit son support comme

$$\text{supp}(\sigma) = \{i \in \{1, \dots, n\} \mid \sigma(i) \neq i\}.$$

Par exemple le support d'un ℓ -cycle $(i_1, i_2, \dots, i_\ell)$ est $\{i_1, \dots, i_\ell\}$.

Observons que si i appartient au support d'une permutation σ , alors $\sigma(i)$ est aussi dans le support. En effet, sinon on aurait $\sigma(\sigma(i)) = \sigma(i)$ qui par injectivité de σ impliquerait $\sigma(i) = i$, qui contredirait $i \in \text{supp}(\sigma)$.

Lemme 1.63 Soient $\sigma, \tau \in \text{Sym}(n)$. Si $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$ alors σ et τ commutent : $\sigma\tau = \tau\sigma$.

Démonstration. Exercice. ■

Théorème 1.64 Toute permutation est composition de cycles à supports contenus dans $\text{supp}(\sigma)$ disjoints.

Démonstration. Soit $\sigma \in \text{Sym}(n)$. On fait une induction sur $|\text{supp}(\sigma)|$. Si $|\text{supp}(\sigma)| = 0$ alors $\sigma(i) = i$ pour tout $i \in \{1, 2, \dots, n\}$. C'est donc l'identité qui est une composition de zéro cycles. On pourrait passer directement à l'étape d'induction, mais regardons encore les cas $|\text{supp}(\sigma)| = 1$ ou 2. Le cas $|\text{supp}(\sigma)| = 1$ est en fait exclu : Par l'observation ci-dessus, si le support contient un élément i , il contient aussi $\sigma(i) \neq i$. Supposons $|\text{supp}(\sigma)| = 2$ et soient i, j dans $\text{supp}(\sigma)$. Puisque $\sigma(i) \neq i$ et $\sigma(j) \neq j$ appartiennent forcément au support, ils sont forcément permutés par σ . Donc $\sigma = (i, j)$, qui est bien composition d'un 2-cycle.

Supposons maintenant le théorème démontré pour des permutations dont la cardinalité du support est strictement plus petite que $|\text{supp}(\sigma)|$. Soit $i \in \text{supp}(\sigma)$ et regardons les images successives de i :

$$i, \sigma(i), \sigma^2(i), \dots, \sigma^k(i), \dots$$

Puisque n est fini il existe par le principe des tiroirs forcément $k < k'$ tels que $\sigma^k(i) = \sigma^{k'}(i)$. Puisque σ est bijective, $i = \sigma^{k'-k}(i)$. Soit $1 < \ell$ minimal tel que $i = \sigma^\ell(i)$ et considérons le ℓ -cycle

$$\tau = (i, \sigma(i), \dots, \sigma^{\ell-1}(i)).$$

On a clairement pour tout k

$$\tau(\sigma^k(i)) = \sigma(\sigma^k(i)).$$

Il en découle que la composition $\tau^{-1}\sigma$ fixe chaque $\sigma^k(i)$. De plus, pour $j \in \{1, 2, \dots, n\} \setminus \{i, \sigma(i), \dots, \sigma^{\ell-1}(i)\}$, on a

$$\sigma(j) \in \{1, 2, \dots, n\} \setminus \{i, \sigma(i), \dots, \sigma^{\ell-1}(i)\}$$

et donc $\tau^{-1}(\sigma(j)) = \sigma(j)$. Par conséquent, $\tau^{-1}\sigma(j) = \sigma(j)$. On en déduit que

$$\text{supp}(\sigma\tau^{-1}) = \text{supp}(\sigma) \setminus \{i, \sigma(i), \dots, \sigma^{\ell-1}(i)\}.$$

Par hypothèse d'induction, $\tau^{-1}\sigma = \tau_1 \dots \tau_m$ est un produit de cycles τ_j de supports contenus dans $\text{supp}(\tau^{-1}\sigma)$ disjoints, en particulier disjoints de $\text{supp}(\tau)$. Finalement

$$\sigma = \tau\tau_1 \dots \tau_m,$$

est le produit désiré. ■

On peut remarquer que la décomposition d'une permutation en cycles à support disjoints est unique si on exclut les 1-cycles, ou si l'on demande comme dans le théorème que le support des cycles est inclus dans le support de la permutation.

Corollaire 1.65 1. Tout $\sigma \in \text{Sym}(n)$ est composition de transpositions.
2. Tout $\sigma \in \text{Sym}(n)$ est composition de transpositions élémentaires.

Evidemment le point 1. est un cas particulier du point 2. mais peut être intéressant indépendamment de la preuve du point 2.

Démonstration. 1. Par le Théorème 1.64 il suffit de montrer que tout cycle est composition de transpositions. Pour ceci, on itère le point 2. de la Proposition 1.60 pour obtenir

$$(i_1, \dots, i_\ell) = (i_1, i_2)(i_2, i_3) \dots (i_{\ell-1}, i_\ell).$$

2. Par le point précédent il suffit de montrer que toute transposition est composition de transpositions élémentaires. Soient $1 \leq i < j \leq n$ et considérons la transposition (i, j) . Par le point 4. de la Proposition 1.60, pour toute permutation $\tau \in \text{Sym}(n)$ telle que $\tau(i) = i$ et $\tau(j) = i + 1$ on a

$$(i, j) = \tau(i, i + 1)\tau^{-1}.$$

Pour τ on peut par exemple prendre le cycle

$$\tau = (i + 1, i + 2, \dots, j - 1, j),$$

qui est, comme le montre le calcul du point précédent une composition de transpositions,

$$\tau = (i + 1, i + 2) \dots (j - 1, j),$$

où l'on observe de plus que chacune des transpositions est élémentaire. Son inverse τ^{-1} et $(i, j) = \tau(i, i+1)\tau^{-1}$ sont donc aussi des compositions de transpositions élémentaires. ■

D'après le point 2. du corollaire, il ne faut que $n - 1$ éléments pour écrire chacune des $n!$ permutations de $\text{Sym}(n)$. On peut faire encore mieux si l'on veut : Avec les deux permutations $(1, 2)$ et $(1, 2, \dots, n)$ on peut écrire tout élément du groupe symétrique. En formulation plus sophistiquée : $(1, 2)$ et $(1, 2, \dots, n)$ engendrent $\text{Sym}(n)$. La preuve, qui est très facile en vue du point 2. du Corollaire 1.65, est laissée en exercice.

Théorème 1.66 Deux permutations $\sigma, \sigma' \in \text{Sym}(n)$ sont conjuguées si et seulement si elles admettent toutes deux une décomposition en cycles disjoints de longueurs ℓ_1, \dots, ℓ_m pour les mêmes valeurs ℓ_1, \dots, ℓ_m .

Démonstration. Si σ et σ' sont conjugués, alors, par définition, il existe $\tau \in \text{Sym}(n)$ tel que $\sigma' = \tau\sigma\tau^{-1}$. Soit

$$\sigma = c_{\ell_1} \circ \dots \circ c_{\ell_m}$$

une décomposition de σ en cycles à support disjoints de longueurs ℓ_1, \dots, ℓ_m . Alors

$$\begin{aligned} \sigma' &= \tau\sigma\tau^{-1} = \tau(c_{\ell_1} \circ \dots \circ c_{\ell_m})\tau^{-1} \\ &= (\tau c_{\ell_1} \tau^{-1}) \circ \dots \circ (\tau c_{\ell_m} \tau^{-1}) \end{aligned}$$

est une décomposition de σ' en cycles de longueurs ℓ_1, \dots, ℓ_m par le point 4. de la Proposition 1.60. De plus, ces cycles ont support disjoint puisque

$$\text{supp}(\tau c_{\ell_j} \tau^{-1}) = \tau(\text{supp}(c_{\ell_j})),$$

et que τ est une bijection. Inversément, soient

$$\sigma = c_{\ell_1} \circ \dots \circ c_{\ell_m}$$

et

$$\sigma' = c'_{\ell_1} \circ \dots \circ c'_{\ell_m}$$

deux décompositions en cycles à support disjoint, où $c_{\ell_k} = (i_1^k, \dots, i_{\ell_k}^k)$ et $c'_{\ell_k} = (j_1^k, \dots, j_{\ell_k}^k)$ sont des cycles de longueur ℓ_k . Alors, par le point 4. de la Proposition 1.60, la conjugaison sera réalisée par n'importe quelle bijection envoyant i_s^k sur j_s^k pour tous $1 \leq k \leq m$, $1 \leq s \leq \ell_k$. ■

Signature

Définition 1.67 On définit la *signature* $\text{sign}(\sigma) \in \mathbb{Q}^*$ d'une permutation $\sigma \in \text{Sym}(n)$ par la formule

$$\text{sign}(\sigma) = \prod_{i < j} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Notons que la signature a bien valeur dans \mathbb{Q}^* puisque, i et j étant distincts, le dénominateur de chaque facteur est non nul, et par injectivité de σ , le numérateur aussi.

Personne ne calculera jamais la signature avec cette formule, mais faisons-le quand même pour la permutation $\sigma = (1, 2, 3) \in \text{Sym}(3)$:

$$\begin{aligned} \text{sign}((1, 2, 3)) &= \frac{\sigma(1) - \sigma(2)}{1 - 2} \cdot \frac{\sigma(1) - \sigma(3)}{1 - 3} \cdot \frac{\sigma(2) - \sigma(3)}{2 - 3} \\ &= \frac{2 - 3}{1 - 2} \cdot \frac{2 - 1}{1 - 3} \cdot \frac{3 - 1}{2 - 3} \\ &= \frac{-1}{-1} \cdot \frac{1}{-2} \cdot \frac{2}{-1} = 1. \end{aligned}$$

Le seul calcul, utilisant cette formule, dont nous aurons vraiment besoin, c'est la signature d'une permutation élémentaire $\sigma = (k, k+1)$ pour $1 \leq k < n$. Observons que dans le produit définissant la signature, les facteurs correspondant à $i < j$, pour $i, j \neq k$ ou $k+1$ sont égaux à 1 puisque $\sigma(i) = i$ et $\sigma(j) = j$. On peut donc les oublier. Ne reste plus que les facteurs de $i < k$, $k \neq i < k+1$, $k < k+1$, $k < j \neq k+1$ et $k < j+1$. Décomposons le produit en trois : Pour le produit d'éléments correspondant à $i < k$ et $k \neq i < k+1$ on obtient

$$\begin{aligned} &\prod_{i < k} \frac{\sigma(i) - \sigma(k)}{i - k} \cdot \prod_{k \neq i < k+1} \frac{\sigma(i) - \sigma(k+1)}{i - (k+1)} \\ &= \prod_{i < k} \left(\frac{\sigma(i) - \sigma(k)}{i - k} \cdot \frac{\sigma(i) - \sigma(k+1)}{i - (k+1)} \right) \\ &= \prod_{i < k} \left(\underbrace{\frac{i - (k+1)}{i - k} \cdot \frac{i - k}{i - (k+1)}}_{=1} \right) = 1. \end{aligned}$$

Pour le terme $k < k+1$ on a

$$\frac{\sigma(k) - \sigma(k+1)}{k - (k+1)} = \frac{k+1 - k}{k - (k+1)} = -1.$$

Pour le produit d'éléments correspondant à $k < j \neq k+1$ et $k < j+1$ on obtient

$$\begin{aligned} &\prod_{k < j \neq k+1} \frac{\sigma(k) - \sigma(j)}{k - j} \cdot \prod_{k+1 < j} \frac{\sigma(k+1) - \sigma(j)}{k+1 - j} \\ &= \prod_{k < j \neq k+1} \left(\frac{\sigma(k) - \sigma(j)}{k - j} \cdot \frac{\sigma(k+1) - \sigma(j)}{k+1 - j} \right) \\ &= \prod_{k < j \neq k+1} \left(\underbrace{\frac{k+1 - j}{k - j} \cdot \frac{k - j}{k+1 - j}}_{=1} \right) = 1. \end{aligned}$$

La signature de la permutation élémentaire $\sigma = (k, k+1)$ est le produit de ces trois facteurs et donc

$$\text{sign}((k, k+1)) = -1. \quad (1.4)$$

Cette définition a pour principale utilité de pouvoir démontrer facilement le théorème suivant, à partir duquel nous pourrions déduire une façon beaucoup plus efficace de calculer la signature d'une permutation.

Théorème 1.68 La signature d'une permutation $\sigma \in \text{Sym}(n)$ est $+1$ ou -1 et définit un homomorphisme

$$\text{sign} : \text{Sym}(n) \longrightarrow \{\pm 1\}.$$

Démonstration. Montrons d'abord que la signature vue comme application à valeur dans \mathbb{Q}^* est un homomorphisme. Soient $\sigma, \tau \in \text{Sym}(n)$. On a

$$\begin{aligned} \text{sign}(\sigma\tau) &= \prod_{i < j} \frac{\sigma(\tau(i)) - \sigma\tau(j)}{i - j} \\ &= \prod_{i < j} \frac{\sigma(\tau(i)) - \sigma\tau(j)}{\tau(i) - \tau(j)} \cdot \prod_{i < j} \frac{\tau(i) - \tau(j)}{i - j} \\ &= \prod_{i < j} \frac{\sigma(\tau(i)) - \sigma\tau(j)}{\tau(i) - \tau(j)} \text{sign}(\tau). \end{aligned}$$

Reste à voir que le produit restant est bien la signature de σ . Faisons le changement de variable $i' = \tau(i)$, $j' = \tau(j)$. On a alors

$$\prod_{i < j} \frac{\sigma(\tau(i)) - \sigma\tau(j)}{\tau(i) - \tau(j)} = \prod_{\substack{i', j' \text{ tels que} \\ \tau^{-1}(i') < \tau^{-1}(j')}} \frac{\sigma(i') - \sigma(j')}{i' - j'}. \quad (1.5)$$

Dans ce produit, toute paire de i', j' distincts apparaît exactement une fois, puisque soit $\tau^{-1}(i') < \tau^{-1}(j')$ soit $\tau^{-1}(j') < \tau^{-1}(i')$. Donc une paire $i < j$ apparaît soit comme $i = i'$, $j = j'$ si $\tau^{-1}(i') < \tau^{-1}(j')$, soit comme $j = i'$, $i = j'$ si $\tau^{-1}(j') < \tau^{-1}(i')$. Mais dans le deuxième cas, échanger l'ordre de i' et j' change le signe du numérateur et du dénominateur et donc ne change pas la fraction

$$\frac{\sigma(i') - \sigma(j')}{i' - j'} = \frac{\sigma(j') - \sigma(i')}{j' - i'}.$$

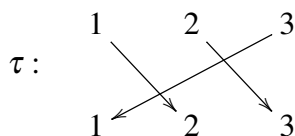
On en conclut que le produit en (1.5) est bien égal à

$$\prod_{i < j} \frac{\sigma(i) - \sigma(j)}{i - j} = \text{sign}(\sigma).$$

Finalement, puisque par le Corollaire 1.65, toute permutation est un produit de transpositions élémentaires et que la signature d'une transposition élémentaire calculée en (1.4) est -1 , la signature d'une permutation est un produit de -1 , donc bien $+1$ ou -1 . ■

■ **Exemple 1.69** Nous avons vu dans la preuve du Corollaire 1.65 une décomposition explicite de tout ℓ -cycle en un produit de $\ell - 1$ transpositions. On en déduit que la signature d'un ℓ -cycle est $(-1)^{\ell-1}$. Pour une permutation arbitraire, on la décompose d'abord en produit de cycles (par exemples disjoints comme dans le Théorème 1.64), sa signature est alors le produit des signatures de ces cycles.

Il existe une autre façon de calculer la signature d'une permutation : C'est (-1) à la puissance le nombre de croisements dans notre 2ème façon de représenter une permutation. Donc $+1$ si le nombre de croisements est pair, et -1 sinon (où on s'arrangera pour qu'il n'y ait pas de croisements multiples). Par exemple :



a 2 croisements et donc $\text{sign}(\tau) = +1$. Si vous aimez la combinatoire, vous pourrez vous amuser à démontrer cette formule, et gagner ainsi le droit à son utilisation.

Groupe alterné

Définition 1.70 Une permutation $\sigma \in \text{Sym}(n)$ est dite *paire* si $\text{sign}(\sigma) = +1$ et *impaire* si $\text{sign}(\sigma) = -1$.

Le sous-groupe $\text{Ker}(\text{sign}) \triangleleft \text{Sym}(n)$ est appelé *groupe alterné* et on le dénote par $\text{Alt}(n)$.

- $\text{Sym}(1) = \{\text{Id}\} = \text{Alt}(1)$.
- $\text{Sym}(2) = \{\text{Id}, (1, 2)\}$. L'identité est paire et la transposition $(1, 2)$ est impaire. Par conséquent $\text{Alt}(2) = \{\text{Id}\}$ est le groupe trivial.
- $\text{Sym}(3) = \{\text{Id}, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}$. Les éléments pairs sont l'identité et les deux 3 cycles $(1, 2, 3)$ et $(1, 3, 2)$ et les éléments impairs sont les transpositions $(1, 2), (1, 3), (2, 3)$. Par conséquent $\text{Alt}(3) = \{\text{Id}, (1, 2, 3), (1, 3, 2)\}$ est le groupe cyclique d'ordre 3.
- Dans $\text{Sym}(4)$ le sous-groupe alterné est formé des 12 éléments suivants :

$$\begin{aligned} \text{Alt}(4) = \{ & \text{Id}, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3) \\ & (1, 2, 3), (1, 2, 4), (1, 3, 4), (2, 3, 4) \\ & (1, 3, 2), (1, 4, 2), (1, 4, 3), (2, 4, 3) \}. \end{aligned}$$

Observons que puisque le groupe alterné est le noyau d'un homomorphisme surjectif dans un groupe à deux éléments, son indice est 2,

$$[\text{Sym}(n), \text{Alt}(n)] = 2,$$

par le Corollaire 1.45. Par le Théorème de Lagrange 1.34, sa cardinalité est

$$|\text{Alt}(n)| = \frac{n!}{2}.$$

Il existe donc deux classes dans $\text{Sym}(n)/\text{Alt}(n)$: La première, $\text{Alt}(n)$ est formée des permutations paires. La deuxième, $\text{Sym}(n)/\text{Alt}(n)$ est formée des permutations impaires.

Lemme 1.71 Le groupe alterné $\text{Alt}(n)$ est engendré par ses 3-cycles.

C'est clair pour $n = 2$ et 3 d'après la liste des éléments de $\text{Alt}(n)$ établie ci-dessus.

Démonstration. Puisque tout élément de $\text{Alt}(n)$ est produit d'un nombre pair de transpositions, il suffit de montrer que le produit de deux transpositions τ_1, τ_2 est un produit de 3-cycles. On se souvient que le support d'une transposition contient deux éléments. Nous considérons donc les trois cas d'intersections possibles :

1. $\text{supp}(\tau_1) = \text{supp}(\tau_2)$: Dans ce cas $\tau_1 = \tau_2$ et le produit $\tau_1 \tau_2$ est l'identité, qui est bien un produit de zéro 3-cycle.
2. $\text{supp}(\tau_1) \cap \text{supp}(\tau_2) = \{j\}$. Dans ce cas $\tau_1 = (i, j)$, $\tau_2 = (j, k)$ avec i, j, k tous distincts et

$$\tau_1 \tau_2 = (i, j)(j, k) = (i, j, k)$$

est un 3-cycle.

3. $\text{supp}(\tau_1) \cap \text{supp}(\tau_2) = \emptyset$. Dans ce cas $\tau_1 = (i, j)$, $\tau_2 = (k, \ell)$ avec i, j, k, ℓ tous distincts et

$$\tau_1 \tau_2 = (i, j)(k, \ell) = (i, j)(j, k)(j, k)(k, \ell) = (i, j, k)(j, k, \ell),$$

où l'on a utilisé deux fois l'égalité établie au point précédent. ■

Lemme 1.72 Pour $n \geq 5$, tous les 3-cycles sont conjugués dans $\text{Alt}(n)$.

Pour $n = 1$ ou 2 l'énoncé est aussi vrai mais vide ($\text{Alt}(1)$ et $\text{Alt}(2)$ sont triviaux et ne contiennent aucun 3-cycle). Pour $n = 3$ il existe deux 3-cycles : $(1, 2, 3)$ et son inverse $(1, 3, 2)$. On ne peut les conjuguer puisque $\text{Alt}(3)$ est un groupe abélien. Vous pourrez montrer en exercice que l'énoncé est faux aussi pour $n = 4$.

Démonstration. Il suffit de montrer que tout 3-cycle est conjugué à $(1, 2, 3)$, c'est-à-dire que pour tout 3-cycle σ il existe $\tau \in \text{Alt}(n)$ tel que $\tau \sigma \tau^{-1} = (1, 2, 3)$. En effet ceci implique immédiatement que toute paire de 3-cycles σ, σ' est conjuguée : S'il existe $\tau, \tau' \in \text{Alt}(n)$ tels que $\tau \sigma \tau^{-1} = (1, 2, 3)$ et $\tau' \sigma' (\tau')^{-1} = (1, 2, 3)$ alors

$$\sigma = \tau^{-1}(1, 2, 3)\tau = \tau^{-1}\tau'\sigma'(\tau')^{-1}\tau = (\tau^{-1}\tau')\sigma'(\tau^{-1}\tau')^{-1}.$$

Soit donc $\sigma = (i, j, k)$ un 3-cycle arbitraire, c'est-à-dire avec i, j, k tous distincts. Considérons une permutation quelconque $\tau \in \text{Sym}(n)$ envoyant i sur 1, j sur 2 et k sur 3. Alors par le point 4. de la Proposition 1.60.

$$\tau(i, j, k)\tau^{-1} = (\tau(i), \tau(j), \tau(k)) = (1, 2, 3).$$

Si $\tau \in \text{Alt}(n)$ alors on a terminé. Sinon, on remplace τ par $\tau' = (4, 5)\tau$ qui appartient bien à $\text{Alt}(n)$ puisque $\text{sign}(\tau') = \text{sign}((4, 5))\text{sign}(\tau) = (-1)(-1) = 1$ (la signature de τ est bien -1 puisque l'on suppose ici que τ n'appartient pas à $\text{Alt}(n)$). Ce nouveau τ' réalise bien la conjugaison désirée :

$$\tau'(i, j, k)(\tau')^{-1} = (4, 5)\tau(i, j, k)\tau^{-1}(4, 5) = (4, 5)(1, 2, 3)(4, 5) = (1, 2, 3),$$

où pour la dernière égalité on a utilisé que des cycles à support disjoint commutent. ■

Théorème 1.73 Le groupe alterné $\text{Alt}(n)$ est simple pour $n \geq 5$.

L'énoncé est trivialement vrai pour $n = 1, 2$ et valide aussi pour $n = 3$ puisque $\text{Alt}(3)$ est un groupe cyclique d'ordre 3 premier. Mais le Théorème est faux pour $n = 4$ (exercice).

Démonstration. Soit $N \triangleleft \text{Alt}(n)$ un sous-groupe normal qu'on suppose différent du groupe trivial $N \neq \{\text{Id}\}$. On veut montrer que $N = \text{Alt}(n)$. La stratégie est simple : Nous allons montrer que N contient un 3-cycle τ . S'il en contient un, il les contient tous puisque par le lemme 1.72 ils sont tous conjugués et donc ont tous la forme $\sigma\tau\sigma^{-1}$ pour notre 3-cycle τ fixé et $\sigma \in \text{Alt}(n)$. Or puisque N est normal, $\sigma\tau\sigma^{-1} \in N$. On invoque ensuite le Lemme 1.71 pour conclure que $N = \text{Alt}(n)$.

Avant de démontrer l'existence d'un 3-cycle dans N observons que si $\tau \in N$ alors $\tau\sigma\tau^{-1}\sigma^{-1} \in N$ pour tout $\sigma \in \text{Alt}(n)$. En effet puisque N est un sous-groupe, τ^{-1} appartient à N ; puisque N est normal, $\sigma\tau^{-1}\sigma^{-1}$ appartient à N ; et puisque N est un sous-groupe le produit $\tau(\sigma\tau^{-1}\sigma^{-1})$ appartient à N . Puisque nous avons supposé que N n'est pas trivial, il existe $\tau \in N$ différent de l'identité. Analysons les différentes possibilités pour τ :

Cas 1 : La décomposition de τ en produit de cycles à support disjoint contient au moins un cycle de longueur ≥ 4 , disons (i, j, k, ℓ, \dots) . Posons $\sigma = (i, j, k)$. Alors par le point 4. de la Proposition 1.60 on a

$$\tau\sigma\tau^{-1} = \tau(i, j, k)\tau^{-1} = (\tau(i), \tau(j), \tau(k)) = (j, k, \ell)$$

et donc

$$\tau\sigma\tau^{-1}\sigma^{-1} = (j, k, \ell)(i, k, j) = (i, \ell, j) \in N$$

et N contient un 3-cycle.

Cas 2 : τ est un produit de 2 et 3-cycles à support disjoint. On décompose ce cas en deux :

- Cas 2a : τ contient au moins un 3-cycle (i, j, k) . S'il ne contient pas d'autres 2 et 3-cycles, on a terminé. Sinon il contient un 2-cycle (ℓ, m) ou un 3-cycle (ℓ, m, p) . Dans les deux cas, posons $\sigma = (i, j, \ell)$. Par le point 4. de la Proposition 1.60 on a

$$\tau\sigma\tau^{-1} = \tau(i, j, \ell)\tau^{-1} = (\tau(i), \tau(j), \tau(\ell)) = (j, k, m)$$

et donc

$$\tau\sigma\tau^{-1}\sigma^{-1} = (j, k, m)(i, \ell, j) = (i, \ell, k, m, j) \in N.$$

Il existe donc un 5-cycle dans N et on peut appliquer le Cas 1 pour en déduire l'existence d'un 3-cycle dans N .

- Cas 2b : τ est produit de 2-cycles à support disjoints. Puisque $\text{Id} \neq \tau \in \text{Alt}(n)$, le nombre de cycles est pair ≥ 2 . Soient (i, j) et (k, ℓ) deux 2-cycles apparaissant dans τ . Posons $\sigma = (i, k, m)$ pour un $m \notin \{i, j, k, \ell\}$ (un tel m existe puisque $n \geq 5$). Par le point 4. de la Proposition 1.60 on a

$$\tau\sigma\tau^{-1} = \tau(i, k, m)\tau^{-1} = (\tau(i), \tau(k), \tau(m)) = (j, \ell, \tau(m))$$

On a encore deux sous-cas : $\tau(m) = m$ ou $\tau(m) \neq m$. Dans le premier sous-cas on obtient

$$\tau\sigma\tau^{-1}\sigma^{-1} = (j, \ell, m)(i, m, k) = (i, j, \ell, m, k) \in N.$$

On a donc un 5-cycle dans N et on peut se ramener au Cas 1. Dans le deuxième sous-cas, observons que si $\tau(m) = p \neq m$, alors $p \neq i, j, k, \ell$ (puisque ces derniers 4 éléments sont déjà l'image par τ de j, i, ℓ, k respectivement). On obtient

$$\tau\sigma\tau^{-1}\sigma^{-1} = (j, \ell, p)(i, m, k) \in N,$$

qui est un produit de deux 3-cycles à support disjoint et on peut appliquer le Cas 2a. ■

1.10 Actions de groupes

Définition 1.74 Soient G un groupe et X un ensemble. Une *action (à gauche)* de G sur X est une application

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

telle que

1. $e \cdot x = x$ pour tout $x \in X$,
2. $(gh) \cdot x = g \cdot (h \cdot x)$ pour tous $g, h \in G, x \in X$.

On dit aussi que G agit sur X et on le dénote par $G \curvearrowright X$.

- **Exemples 1.75** 1. Pour tous groupes G et ensembles X on peut considérer l'*action triviale* :

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x := x. \end{aligned}$$

2. Le groupe $G = \text{Sym}(n)$ agit sur $X = \{1, 2, \dots, n\}$:

$$\begin{aligned} \text{Sym}(n) \times \{1, 2, \dots, n\} &\longrightarrow \{1, 2, \dots, n\} \\ (\sigma, i) &\longmapsto \sigma(i). \end{aligned}$$

3. Le groupe $G = \text{GL}(n, \mathbb{R})$ agit sur $X = \mathbb{R}^n$:

$$\begin{aligned} \text{GL}(n, \mathbb{R}) \times \mathbb{R}^n &\longrightarrow \mathbb{R}^n \\ (A, v) &\longmapsto A(v). \end{aligned}$$

4. Un groupe G agit sur lui-même de plusieurs façons :

- a. *Action par multiplication à gauche* :

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, h) &\longmapsto gh. \end{aligned}$$

- b. *Action par multiplication à droite par l'inverse* :

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, h) &\longmapsto hg^{-1}. \end{aligned}$$

- c. *Action par multiplication conjugaison* :

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, h) &\longmapsto ghg^{-1}. \end{aligned}$$

Vous pouvez vérifier en exercice que ces applications définissent bien des actions.

5. Soient G un groupe et $H < G$ un sous-groupe. L'application

$$\begin{aligned} G \times G/H &\longrightarrow G/H \\ (g, g'H) &\longmapsto gg'H \end{aligned}$$

définit une action de G sur G/H .

Nous utiliserons souvent l'identité

$$g^{-1} \cdot (g \cdot x) = x, \quad (1.6)$$

pour tous $g \in G, x \in X$ qui se justifie facilement comme suit :

$$\begin{aligned} g^{-1} \cdot (g \cdot x) &= (g^{-1}g) \cdot x && \text{par le point 1. de la définition,} \\ &= e \cdot x && \text{car } g^{-1}g = e, \\ &= x && \text{par le point 2. de la définition.} \end{aligned}$$

Observons qu'une action $G \curvearrowright X$ définit une application

$$\begin{aligned} G &\longrightarrow \{X \rightarrow X\} \\ g &\longmapsto \varphi_g, \end{aligned}$$

où l'application $\varphi_g : X \rightarrow X$ est définie par

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

Montrons que cette application φ_g est bijective pour tout $g \in G$: Elle est injective puisque

$$\varphi_g(x) = \varphi_g(y) \iff g \cdot x = g \cdot y.$$

Agissons par g^{-1} sur cette dernière équation pour obtenir

$$g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot y) \iff x = y,$$

par l'identité (1.6) appliquée à gauche et à droite. Elle est surjective puisque tout $y \in X$ est dans l'image de φ_g :

$$\varphi_g(g^{-1} \cdot y) = g \cdot (g^{-1} \cdot y) = y$$

par l'identité (1.6). Il découle qu'une action $G \curvearrowright X$ définit une application

$$\begin{aligned} \varphi : G &\longrightarrow \text{Bij}(X) \\ g &\longmapsto \varphi_g, \end{aligned}$$

Vous pourrez vérifier en exercice que φ est un homomorphisme et inversément, que tout homomorphisme $G \rightarrow \text{Bij}(X)$ définit une action de groupe $G \curvearrowright X$. De plus cette correspondance est bijective.

Identifions l'homomorphisme $G \rightarrow \text{Bij}(X)$ dans quelques-uns des exemples vus ci-dessus.

■ **Exemples 1.76** 1. L'homomorphisme correspondant à l'action triviale est l'homomorphisme trivial

$$\begin{aligned} G &\longrightarrow \text{Bij}(X) \\ g &\longmapsto \text{Id}_X. \end{aligned}$$

2. L'homomorphisme correspondant à l'action naturelle de $\text{Sym}(n)$ sur $\{1, 2, \dots, n\}$ n'est autre que l'identité.
4. (a) Supposons que G est fini. L'action de G sur G par multiplication à gauche donne lieu à un homomorphisme

$$\begin{aligned} G &\longrightarrow \text{Bij}(G) \cong \text{Sym}(|G|) \\ g &\longmapsto \{h \mapsto gh\}. \end{aligned}$$

Définition 1.77 Soit $G \curvearrowright X$ un action de groupe.

- L'action est *transitive* si pour tous $x, y \in X$ il existe $g \in G$ tel que $g \cdot x = y$.
- Soit $x \in X$. L'*orbite* de x est l'ensemble

$$G \cdot x = \{g \cdot x \mid g \in G\}.$$

- On dénote par $G \backslash X$ l'ensemble des orbites.

Observons qu'une action $G \curvearrowright X$ est transitive si et seulement si il n'existe qu'une seule orbite, ou de façon équivalente, $G \cdot x = X$ pour tous $x \in X$, ou encore il existe $x \in X$ tel que $G \cdot x = X$.

Définition 1.78 Une action $G \curvearrowright X$ est *fidèle* si le seul élément de G à agir comme l'identité de X est le neutre, c'est-à-dire si il existe $g \in G$ tel que $g \cdot x = x$ pour tous $x \in X$ alors $g = e$.

Observons qu'une action est fidèle si et seulement si l'homomorphisme correspondant $G \rightarrow \text{Bij}(X)$ est injectif.

- **Exemples 1.79**
1. L'action triviale a pour orbites les singletons $\{x\}$. Elle est transitive si et seulement si $|X| = 1$ et fidèle si et seulement si $|G| = 1$.
 2. Considérons l'action naturelle de $\text{Sym}(n)$ sur $\{1, 2, \dots, n\}$. L'orbite de tout élément $i \in \{1, 2, \dots, n\}$ est $\{1, 2, \dots, n\}$. C'est une action transitive et fidèle.
 3. L'action naturelle de $\text{GL}(n, \mathbb{R})$ sur \mathbb{R}^n a deux orbites : $\mathbb{R}^n \setminus \{0\}$ et $\{0\}$. Elle n'est donc pas transitive. (Mais elle le serait si on la considère comme action sur $\mathbb{R}^n \setminus \{0\}$. C'est une action fidèle.
 4. a. L'action de G sur lui-même par multiplication à gauche est transitive et fidèle.
b. Considérons l'action de G sur lui-même par conjugaison. L'orbite d'un élément $h \in G$ consiste en l'ensemble

$$\{ghg^{-1} \mid g \in G\}$$

des conjugués de h . En particulier l'orbite de l'identité est le singleton $\{e\}$. Cette action n'est donc pas transitive si $|G| \geq 2$. On vérifie facilement qu'elle est fidèle si et seulement si $Z(G) = \{e\}$.

Lemme 1.80 Soit $G \curvearrowright X$ une action de groupes. Deux orbites sont soit égales, soit disjointes. Plus précisément, pour tous $x, y \in X$, ou bien $G \cdot x = G \cdot y$, ou bien $G \cdot x \cap G \cdot y = \emptyset$.

Démonstration. Soient $x, y \in X$ et supposons que $G \cdot x \cap G \cdot y \neq \emptyset$. Il existe donc un élément z dans l'intersection $G \cdot x \cap G \cdot y$. Puisque $z \in G \cdot x$ il existe $g_1 \in G$ tel que $z = g_1 \cdot x$. De même puisque $z \in G \cdot y$ il existe $g_2 \in G$ tel que $z = g_2 \cdot y$. En particulier $g_1 \cdot x = z = g_2 \cdot y$ et donc $y = g \cdot x$ pour $g = g_2^{-1} g_1$. Montrons que $G \cdot y \subset G \cdot x$: Un élément arbitraire de $G \cdot y$ a la forme $g' \cdot y$, pour un $g' \in G$. Mais alors

$$g' \cdot y = g'(g \cdot x) = (gg') \cdot x \in G \cdot x.$$

L'inclusion inverse $G \cdot y \supset G \cdot x$ s'obtient par symétrie. ■

Définition 1.81 Soit $G \curvearrowright X$ une action de groupe. On appelle un *ensemble de représentant (des orbites)* un sous-ensemble $S \subset X$ contenant un et un seul élément de chaque orbite.

Observons que si S est un ensemble de représentants des orbites, alors

$$X = \coprod_{s \in S} G \cdot s.$$

Définition 1.82 Soit $G \curvearrowright X$ une action de groupe. On définit, pour tout $x \in X$, son *stabilisateur* comme

$$\text{Stab}(x) = \{g \in G \mid g \cdot x = x\}.$$

Proposition 1.83 Soit $G \curvearrowright X$ une action de groupe.

1. $\text{Stab}(x) < G$ pour tout $x \in X$.
2. Si $x \in X$ et $y \in X$ sont dans la même orbite alors $\text{Stab}(x) \cong \text{Stab}(y)$.

Démonstration. 1. Vérifions que $\text{Stab}(x)$ est un sous-groupe de G :

- $e \in \text{Stab}(x)$ puisque par la propriété 1. des actions de groupes, $e \cdot x = x$.
- Si $g, h \in \text{Stab}(x)$ alors

$$\begin{aligned} (gh) \cdot x &= g \cdot (h \cdot x) && \text{par le point 2. de la définition,} \\ &= g \cdot x && \text{car } h \in \text{Stab}(x), \\ &= x && \text{car } g \in \text{Stab}(x), \end{aligned}$$

de sorte que $gh \in \text{Stab}(x)$.

- Si $g \in \text{Stab}(x)$ alors

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

et $g^{-1} \in \text{Stab}(x)$.

2. Supposons que x et y appartiennent à la même orbite. Alors il existe $g \in G$ tel que $y = g \cdot x$. Considérons l'homomorphisme injectif

$$\begin{aligned} \Psi_g : \text{Stab}(x) &\longrightarrow G \\ h &\longmapsto ghg^{-1}. \end{aligned}$$

Observons que l'image de Ψ_g est contenue dans $\text{Stab}(y)$:

$$\Psi_g(h) \cdot y = (ghg^{-1}) \cdot y = (gh) \cdot \underbrace{(g^{-1}(y))}_{=x} = g \cdot (h \cdot x) = g \cdot x = y,$$

où l'on a utilisé que $h \in \text{Stab}(x)$. Par symétrie, $\Psi_{g^{-1}}$ est un homomorphisme injectif de $\text{Stab}(y)$ avec image $\text{Stab}(x)$. Finalement, Ψ_g et $\Psi_{g^{-1}}$ sont clairement inverses l'un de l'autre et réalisent l'isomorphisme entre $\text{Stab}(x)$ et $\text{Stab}(y)$. ■

Théorème 1.84 — Formule des orbites. Soient $G \curvearrowright X$ une action de groupe et $x \in X$. Alors

$$|G| = |G \cdot x| \cdot |\text{Stab}(x)|.$$

- **Exemples 1.85** 1. Considérons l'action naturelle de $\text{Sym}(n)$ sur $\{1, 2, \dots, n\}$ et prenons $x = n$. Alors son stabilisateur est isomorphe à $\text{Sym}(n-1)$ et son orbite est l'ensemble $\{1, 2, \dots, n\}$ de sorte que la formule des orbites nous redonne l'expression récurrente

$$|\text{Sym}(n)| = n \cdot |\text{Sym}(n-1)|.$$

2. Théorème de Lagrange : Soient G un groupe et $H < G$ un sous-groupe. On considère l'action naturelle de G sur G/H suivante :

$$\begin{aligned} G \times G/H &\longrightarrow G/H \\ (g, g'H) &\longmapsto gg'H. \end{aligned}$$

Appliquons la formule des orbites à $x = H$: Son orbite est clairement G/H tout entier et son stabilisateur n'est rien d'autre que H de sorte que

$$|G| = |G/H| \cdot |H|,$$

qui est précisément le Théorème de Lagrange puisque $|G/H| = [G : H]$.

Démonstration. Soit $y \in G \cdot x$ de sorte qu'il existe $g \in G$ tel que $y = g \cdot x$. On pose

$$K_y := \{g \in G \mid g \cdot x = y\}.$$

Observons que pour $y = x$ on a $K_x = \text{Stab}(x)$, mais pour $y \neq x$, l'ensemble K_y n'est jamais un groupe puisque $e \notin K_y$.

L'application

$$\begin{aligned} \text{Stab}(x) &\longrightarrow K_y \\ h &\longmapsto gh \end{aligned}$$

est une bijection entre K_y et $\text{Stab}(x)$. En effet

$$\begin{aligned} h \in \text{Stab}(x) &\iff h \cdot x = x \\ &\iff (gh) \cdot x = g(h \cdot x) = g \cdot x = y \\ &\iff gh \in K_y \end{aligned}$$

et l'application inverse est donnée par la multiplication à gauche par g^{-1} . On en déduit que $|K_y| = |\text{Stab}(x)|$ pour tout $y \in G \cdot x$.

Si $y \neq y' \in G \cdot x$ alors $K_y \cap K_{y'} = \emptyset$ par définition. De plus, tout $g \in G$ appartient à un (unique) de ces ensembles : $g \in K_{g \cdot x}$. Il en découle que

$$G = \coprod_{y \in G \cdot x} K_y$$

et

$$|G| = \sum_{y \in G \cdot x} \underbrace{|K_y|}_{=|\text{Stab}(x)|} = |G \cdot x| |\text{Stab}(x)|,$$

ce qui démontre la formule des orbites. ■

Corollaire 1.86 Soient $G \curvearrowright X$ une action de groupe et $x \in X$. Alors

$$|G \cdot x| = [G : \text{Stab}(x)].$$

Démonstration. Immédiat par la formule des orbites et le Théorème de Lagrange. ■

Corollaire 1.87 Soient $G \curvearrowright X$ fini une action de groupe avec X et $x \in X$ et $S \subset X$ un ensemble de représentants des orbites. Alors

$$|X| = \sum_{s \in S} [G : \text{Stab}(s)].$$

Démonstration. Par définition nous avons $X = \coprod_{s \in S} G \cdot s$. Il suffit d'appliquer le corollaire précédent. ■

Equation des classes

Considérons désormais l'action de G sur lui-même par conjugaison, où nous supposons que G est fini. Le stabilisateur de $x \in G$ est le sous-groupe

$$\{g \in G \mid gxg^{-1} = x\} =: C_G(x),$$

appelé *centralisateur* de x . Notons que $Z(G) = \cap_{x \in G} C_G(x)$.

Supposons que l'orbite de $x \in G$ est de cardinalité 1 :

$$\begin{aligned}
 |G \cdot x| = 1 &\iff G \cdot x = \{x\} \\
 &\iff gxg^{-1} = x \forall g \in G \\
 &\iff gx = xg \forall g \in G \\
 &\iff x \in Z(G) \\
 &\iff C_G(x) = G.
 \end{aligned}$$

On en déduit que

$$|G \cdot x| > 1 \iff C_G(x) \neq G.$$

Soit S un ensemble de représentant des orbites. Puisque l'orbite de $x \in Z(G)$ est un singleton, S contient $Z(G)$. Nous pouvons donc écrire

$$S = Z(G) \coprod (S \setminus Z(G)).$$

Les Corollaires 1.86 et 1.87 donnent

$$|G| = \sum_{s \in Z(G)} 1 + \sum_{s \in S \setminus Z(G)} [G : C_G(s)].$$

Le corollaire suivant est maintenant immédiat :

Corollaire 1.88 — Equation des classes. Soit G un groupe fini et S un ensemble de représentant des orbites pour l'action de G par conjugaison. Alors

$$|G| = |Z(G)| + \sum_{s \in S \setminus Z(G)} \underbrace{[G : C_G(s)]}_{\geq 2}.$$

Trois applications de l'Equation des classes

1. Eléments d'ordre premier dans un groupe. Nous avons vu en corollaire du Théorème de Lagrange que l'ordre d'un élément d'un groupe, divise toujours la cardinalité du groupe. Posons-nous la question inverse : si n divise $|G|$, existe-t-il un élément d'ordre n dans G ? En général, non : Dans $C_p \times C_p$, pour p premier, les éléments ont ordre p ou 1 (pour l'identité); il n'y a donc pas d'éléments d'ordre $p^2 = |C_p \times C_p|$. Le théorème de Cauchy donne néanmoins une réponse affirmative dans le cas où n est premier :

Théorème 1.89 — Théorème de Cauchy. Soient G un groupe fini et p un nombre premier divisant $|G|$. Alors il existe un élément d'ordre p dans G .

Ceci peut être vu comme un cas particulier des Théorèmes de Sylow, affirmant en particulier que si p^k divise $|G|$ alors G contient un sous-groupe d'ordre p^k . En effet pour $k = 1$, un sous-groupe d'ordre p contient un (ou plus précisément $p - 1$) élément(s) d'ordre p .

Démonstration 1. Cette preuve est basée sur les actions de groupe et la formule des orbites.

On considère l'ensemble

$$X = \{(x_1, \dots, x_p) \in G^p \mid x_1 x_2 \dots x_p = e\}.$$

Observons que la cardinalité de X est $|G|^{p-1}$ puisque les $p+1$ premières coordonnées x_1, \dots, x_{p-1} d'un élément de X , qui peuvent être choisies librement dans G^{p-1} , déterminent la dernière coordonnée $x_p = x_{p-1}^{-1} \dots x_2^{-1} x_1^{-1}$. Il existe donc une bijection

$$\begin{aligned} X &\longrightarrow G^{p-1} \\ (x_1, \dots, x_p) &\longmapsto (x_1, \dots, x_{p-1}). \end{aligned}$$

En particulier p divise $|X|$. (On a même p^{p-1} divise $|X|$.)

Si $(x_1, \dots, x_p) \in X$, alors toute permutation cyclique

$$(x_{i+1}, \dots, x_p, x_1, \dots, x_i),$$

pour $0 \leq i \leq p-1$ appartient encore à X . En effet il suffit de le vérifier pour la permutation (x_2, \dots, x_p, x_1) , le cas général découlant par induction. Dans ce cas on vérifie

$$x_2 \dots x_p x_1 = x_1^{-1} \underbrace{(x_1 x_2 \dots x_p)}_{=e} x_1 = x_1^{-1} x_1 = e.$$

En particulier, on peut définir une action du groupe cyclique C_p sur X par

$$\begin{aligned} C_p \times X &\longrightarrow X \\ (\bar{i}, (x_1, \dots, x_p)) &\longmapsto (x_{i+1}, \dots, x_p, x_1, \dots, x_i). \end{aligned}$$

Par la formule des orbites, nous savons que toute orbite pour cette action a cardinalité 1 ou p puisqu'elle doit diviser $|C_p| = p$. Observons qu'une orbite de cardinalité 1 consiste en un singleton de la forme $\{(x, \dots, x)\}$, pour $(x, \dots, x) \in X$, et donc $x^p = e$, ce qui nous donne un élément d'ordre p à condition que $x \neq e$. Nous allons donc établir qu'il existe deux (en fait au moins p) orbites de cardinalité 1, donc au moins deux éléments de G satisfaisant $x^p = e$. L'un d'eux n'est pas l'identité et a donc ordre p .

Définissons k_1 comme le nombre d'orbites de cardinalité 1, et k_p comme le nombre d'orbites de cardinalité p . Puisque X est l'union disjointe de ses orbites, nous avons

$$|X| = k_1 + p k_p.$$

Nous savons que p divise $|X|$, de sorte que cette équation modulo p devient

$$k_1 \equiv 0 \pmod{p}.$$

Or $k_1 \geq 1$ car l'orbite de (e, \dots, e) a cardinalité 1 et donc $k_1 \geq p \geq 2$, ce qui termine cette première démonstration. ■

Démonstration 2. Cette preuve est basée sur une induction et l'équation des classes.

Montrons d'abord le théorème dans le cas où G est abélien par induction sur $n = |G|$. Précisons ce que l'on entend par induction sur $n = |G|$. Nous allons montrer que

1. Le théorème est vrai pour tous les groupes (abéliens) d'ordre p .
2. Soit G un groupe abélien tel que p divise $|G|$. Si le théorème est vrai pour tous les groupes abéliens H tels que p divise $|H|$, $|H|$ divise $|G|$, avec $|H| < |G|$ alors le théorème est vrai pour G .

Ceci implique que le théorème est valide pour tout groupe abélien d'ordre fini tel que p divise $|G|$. En effet, un tel groupe a ordre $p \cdot q_1 \cdot \dots \cdot q_n$ pour des premiers q_1, \dots, q_n pas forcément distincts. Faisons une induction sur n : Le cas $n = 0$ est le cas 1 : $|G| = p$. Supposons le cas abélien du théorème démontré pour tout groupe de cardinalité $p \cdot q_1 \cdot \dots \cdot q_k$ avec $k < n$ et des premiers q_1, \dots, q_k pas forcément distincts. Alors l'hypothèse de notre point 2. est vérifiée puisqu'un groupe (abélien) H tel que p divise $|H|$ et $|H|$ divise $|G|$ a, si $|H| < |G|$, forcément cardinalité $p \cdot q_{i_1} \cdot \dots \cdot q_{i_k}$, pour un sous-ensemble strict $\{i_1, \dots, i_k\} \subset \{1, \dots, n\}$. Ainsi le cas abélien du théorème est valide pour G .

1. Si $n = p$ alors tout élément différent de l'identité a ordre p .
2. Supposons le théorème valide pour les groupes abéliens de cardinalité $< n$. Soit $x \in G$ différent de l'identité et considérons le sous-groupe cyclique

$$H := \langle x \rangle = \{e, x, x^2, \dots, x^m\},$$

où m dénote l'ordre de x et de H . Si p divise m , il existe $k \in \mathbb{N}$ tel que $m = kp$ et l'élément $y := x^k \in H < G$ a ordre p . En effet

$$y^p = (x^k)^p = x^m = e$$

et si $1 < \ell < p$ alors

$$y^\ell = (x^k)^\ell = x^{k\ell} \neq e$$

puisque $1 < k\ell < m$ et x a ordre m .

Si p ne divise pas l'ordre m de $|H|$ alors il divise l'indice $[G : H]$ et donc la cardinalité du groupe quotient G/H qui est un groupe abélien. De plus $|G/H| < |G|$ puisque $|H| > 1$. Nous pouvons donc appliquer l'hypothèse d'induction au groupe quotient G/H . Il existe donc une classe $zH \in G/H$ d'ordre p . Soit m l'ordre du représentant $z \in G$ de cette classe. On a

$$(zH)^m = z^m H = H$$

donc l'ordre p de zH divise m et comme ci-dessus $z^{m/p}$ a ordre p .

Montrons maintenant le théorème pour des groupes G non nécessairement abéliens, toujours par induction sur $n = |G|$. Si $n = p$, alors G est isomorphe au groupe cyclique d'ordre p et le théorème est vrai. Supposons le théorème valide pour les groupes de cardinalité $< n$. Le centre $Z(G)$ est un sous-groupe abélien de G . Si p divise $|Z(G)|$ alors $Z(G)$ contient un élément d'ordre p (et donc G aussi) par le cas abélien. Supposons donc que p ne divise pas $|Z(G)|$, autrement dit $|Z(G)| \not\equiv 0 \pmod{p}$.

Soit S un ensemble de représentants des classes de conjugaison de G . L'équation des classes donne

$$|G| = |Z(G)| + \sum_{s \in S \setminus Z(G)} [G : C_G(s)],$$

et modulo p ,

$$|Z(G)| + \sum_{s \in S \setminus Z(G)} [G : C_G(s)] \equiv 0 \pmod{p}.$$

Puisque $|Z(G)| \not\equiv 0 \pmod{p}$ il doit exister $s \in S \setminus Z(G)$ tel que $[G : C_G(s)] \not\equiv 0 \pmod{p}$. En particulier, p ne divise pas l'indice $[G : C_G(s)]$, ce qui implique par Lagrange que p divise $|C_G(s)|$, qui est strictement plus petit que $|G|$ puisque $s \notin Z(G)$. Par induction $C_G(s)$ (et donc G) possède un élément d'ordre p . ■

2. Centre d'un p -groupe. Un p -groupe est simplement un groupe d'ordre p^k pour un p premier.

Lemme 1.90 Soit G un groupe d'ordre p^k , pour p premier et $k \geq 1$. Alors son centre $Z(G)$ est non trivial.

Démonstration. Soit S un ensemble de représentants des classes de conjugaison de G . L'équation des classes donne

$$|G| = |Z(G)| + \sum_{s \in S \setminus Z(G)} [G : C_G(s)].$$

Observons que pour $s \in S \setminus Z(G)$, l'indice $[G : C_G(s)]$ est divisible par p puisqu'il divise $|G| = p^k$ et ne peut pas être égal à 1 car $C_G(s) \neq G$ pour $s \notin Z(G)$. L'équation des classes modulo p devient

$$|Z(G)| \equiv 0 \pmod{p}.$$

Or $|Z(G)| \geq 1$ car $e \in Z(G)$, et donc $|Z(G)| \geq p$. ■

3. Classification des p -groupes simples. Pour classifier les groupes simples finis il faut d'une part montrer que les groupes de la liste de la classification sont bien simples (c'est la partie facile), et par d'innombrables cas et sous-cas, montrer que tous les autres ne le sont pas. Voici une toute petite contribution dans cette direction.

Corollaire 1.91 Un groupe G d'ordre p^k , pour p premier et $k > 1$ ne peut pas être simple.

Puisque tout groupe d'ordre p est simple, nous pourrions reformuler ce corollaire comme : Un groupe d'ordre p^k , avec p premier et $k \geq 1$ est simple si et seulement si $k = 1$.

Démonstration. Par le lemme précédent, un tel groupe a centre $Z(G) \neq \{e\}$. Si $Z(G) \neq G$ alors G n'est pas simple puisqu'il contient le sous-groupe normal $Z(G)$, différent de $\{e\}$ et G . Si $Z(G) = G$ alors G est abélien. Par le théorème de Cauchy, il contient un élément et donc un sous-groupe d'ordre p . Ce sous-groupe est différent de $\{e\}$ et G et est normal puisque tout sous-groupe d'un groupe abélien est normal. ■

2. Anneaux

2.1 Définition et exemples

Définition 2.1 Un *anneau* est un ensemble A muni de deux lois de composition internes

$$\begin{array}{ccc} + : A \times A & \longrightarrow & A \\ (x, y) & \longmapsto & x + y \end{array} \quad \text{et} \quad \begin{array}{ccc} \cdot : A \times A & \longrightarrow & A \\ (x, y) & \longmapsto & x \cdot y \end{array}$$

telles que

1. $(A, +)$ est un groupe abélien,
2. la loi \cdot est associative ($x(yz) = (xy)z$ pour tous $x, y, z \in A$),
3. il existe un neutre pour la loi \cdot ,
4. distributivité :

$$x(y + z) = xy + xz \quad \text{et} \quad (x + y)z = xz + yz$$

pour tous $x, y, z \in A$.

Si de plus la loi \cdot est commutative on dit que $A = (A, +, \cdot)$ est un anneau *commutatif*.

- **Remarques**
1. On dénotera le neutre de $(A, +)$ par 0 (ou 0_A s'il y a risque de confusion) et l'inverse de $a \in A$ (pour la loi $+$) par $-a$.
 2. Le neutre pour la loi \cdot sera noté 1 (ou 1_A).
 3. On appelle la loi $+$ l'addition et la loi \cdot la multiplication.
 4. Les termes de droite du point 4. de la définition ne sont pas bien définis puisqu'on ne sait pas à priori qu'elle opération effectuer en premier. Par exemple le terme $xy + xz$ pourrait être $x \cdot (y + (x \cdot z))$ ou $x \cdot (y + x) \cdot z$. Mais l'expression est bien définie si on admet la convention que la multiplication passe avant l'addition, donc $xy + xz = (xy) + (xz)$.
 5. Parfois l'existence d'un neutre pour la multiplication n'est pas incluse dans la définition d'anneau. D'autres fois, la commutativité de la multiplication fait partie de la définition.

■ **Exemples 2.2** 0. L'anneau trivial $(\{0\}, +, \cdot)$.

1. Les ensembles de nombres $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des anneaux pour l'addition et multiplication.
2. $\mathbb{Z}/n\mathbb{Z}$ est un anneau pour l'addition et la multiplication modulo n .
3. Si A est un anneau, alors

$$M_n(A) = \{(a_{ij})_{1 \leq i, j \leq n} \mid a_{ij} \in A\}$$

est un anneau pour l'addition et multiplication de matrices. En effet, l'addition de matrice est définie coordonnée par coordonnée et ne dépend que de l'addition sur A . La multiplication elle requiert l'addition et la multiplication dans A . Le neutre pour l'addition est la matrice nulle et le neutre pour la multiplication est la matrice identité (où l'on comprend que les termes 1 sur la diagonales sont le neutre multiplicatif dans A). Ce n'est pas un anneau commutatif quand $n \geq 2$, à moins que $0 = 1$.

4. Si A est un anneau, on peut considérer l'anneau des polynômes $A[X]$ à coefficients dans A . Formellement, $A[X]$ est défini comme les suites $(a_0, a_1, a_2, \dots, a_k, \dots)$ avec $a_k \in A$ et $a_i \neq 0$ pour un nombre fini de $i \geq 0$. La notation

$$a_0 + a_1X + a_2X^2 + \dots + a_nX^n$$

pour $(a_0, a_1, a_2, \dots, a_n, 0, \dots)$ est très utile en pratique, ne serait-ce que pour définir la multiplication sur $A[X]$. Commençons par l'addition qui est donnée par

$$\begin{aligned} (a_0, a_1, \dots, a_k, \dots) + (b_0, b_1, \dots, b_k, \dots) \\ = (a_0 + b_0, a_1 + b_1, \dots, a_k + b_k, 0, \dots). \end{aligned}$$

Observons qu'on obtient bien un élément de $A[X]$ car les sommes $a_k + b_k$ sont non nulles pour un nombre fini de k . La multiplication est définie par

$$(a_0, a_1, \dots, a_k, \dots) \cdot (b_0, b_1, \dots, b_k, \dots) = (c_0, c_1, \dots, c_k, \dots),$$

où

$$c_k = \sum_{i=0}^k a_i b_{k-i}.$$

Ici aussi on obtient bien un élément de $A[X]$. Nous le démontrerons formellement dans la première partie de la preuve du point 1. de la Proposition 2.58.

Par exemple, prenons $A = \mathbb{Z}$. Alors l'élément $(0, 2, 3, 0, \dots) \in \mathbb{Z}[X]$ s'écrit $2X + 3X^2$, et l'élément $(1, 1, 0, \dots) \in \mathbb{Z}[X]$ s'écrit $1 + X$. Leur somme est

$$(2X + 3X^2) + (1 + X) = 1 + 3X + 3X^2$$

et leur produit est

$$(2X + 3X^2) \cdot (1 + X) = 2X + 5X^2 + 3X^3.$$

5. L'ensemble $\mathcal{C}(\mathbb{R})$ des fonctions continues de \mathbb{R} dans \mathbb{R} est un anneau pour l'addition et la multiplication de fonctions.

6. Pour tous anneau A et ensemble X on peut munir l'ensemble des fonctions de X dans A ,

$$A^X := \{f : X \longrightarrow A\}$$

de l'addition et de la multiplication de fonctions (en utilisant l'addition et la multiplication de A). C'est un anneau qui sera commutatif si et seulement si A est commutatif.

Comme pour les groupes, on peut considérer le produit direct $A_1 \times A_2$ de deux anneaux A_1, A_2 , où l'on définit l'addition et la multiplication sur le produit coordonnée par coordonnée. Il est facile de vérifier que c'est un anneau, qui sera commutatif si et seulement si A_1 et A_2 le sont.

Lemme 2.3 Soit A un anneau. Alors

1. $0 \cdot x = 0 = x \cdot 0$ pour tout $x \in A$,
2. $-(x \cdot y) = (-x) \cdot y = x \cdot (-y)$ pour tous $x, y \in A$.

Démonstration. 1. On a

$$\begin{aligned} 0 \cdot x &= (0 + 0) \cdot x && \text{car } 0 \text{ neutre pour } +, \\ &= 0 \cdot x + 0 \cdot x && \text{distributivité,} \end{aligned}$$

auquel on additionne $-0 \cdot x$ pour obtenir

$$0 = 0 \cdot x.$$

L'identité $x \cdot 0 = 0$ se démontre identiquement.

2. On a

$$xy + (-x)y = \underbrace{(x + (-x))}_{=0}y = 0 \cdot y = 0,$$

où l'on a utilisé la distributivité et l'identité $0 \cdot y = 0$ prouvée au point précédent. Ceci implique que

$$-(xy) = (-x)y.$$

La preuve de $-(xy) = x(-y)$ est identique. ■

Remarquons qu'à l'exception de l'anneau trivial à un élément, le neutre pour l'addition est différent du neutre pour la multiplication, $0 \neq 1$. En effet, si $0 = 1$, alors

$$x = x \cdot 1 = x \cdot 0 = 0$$

pour tout $x \in A$. Il sera parfois nécessaire d'exclure ce cas dans les hypothèses de certains résultats. On se souviendra qu'un anneau tel que $0 \neq 1$ est simplement un anneau non réduit à un élément.

Par définition, dans un anneau A , l'ensemble A muni de l'addition, $(A, +)$, est un groupe commutatif. Qu'en est-il de (A, \cdot) ? On est en présence d'une loi interne associative, avec élément neutre, mais l'existence d'un inverse n'est pas assurée (et 0 n'a aucune chance d'en avoir sauf si $0 = 1$).

Définition 2.4 Soit A un anneau. Le sous-ensemble

$$U(A) := \{u \in A \mid \exists v \in A \text{ tel que } uv = 1 = vu\} \subset A$$

est appelé *unités* de A .

Il est immédiat que la multiplication de A se restreint à une loi interne sur $U(A)$ faisant de $U(A)$ un groupe. De plus, $(U(A), \cdot)$ est un groupe abélien si A est un anneau commutatif. Observons de plus que $0 \in U(A)$ si et seulement si $0 = 1$. Pour $u \in U(A)$ nous dénoterons par u^{-1} l'unique inverse (multiplicatif) de u .

- **Exemples 2.5**
1. $U(\mathbb{Z}) = \{+1, -1\}$, $U(\mathbb{Q}) = \mathbb{Q}^*$, $U(\mathbb{R}) = \mathbb{R}^*$ et $U(\mathbb{C}) = \mathbb{C}^*$.
 2. $U(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^\times$.
 3. $U(M_n(\mathbb{R})) = \text{GL}(n, \mathbb{R})$.

Définition 2.6 Un anneau A est un corps si A est commutatif et $U(A) = A \setminus \{0\}$.

Par exemple, \mathbb{Q} , \mathbb{R} et \mathbb{C} sont des corps, mais pas \mathbb{Z} . Aussi, $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier. On aimera le dénoter par

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z},$$

pour p premier, où le \mathbb{F} vient de "fields", corps en anglais.

Observons que si A est un corps, alors $|A| \geq 2$. En effet, $|A| < 2$ si et seulement si $|A| = 1$ et $A = \{0\}$ ou de façon équivalente $0 = 1$. Mais 1 est toujours une unité même dans l'anneau trivial, or dans l'anneau trivial $A \setminus \{0\}$ est vide.

Définition 2.7 Soit A un anneau. Un élément $a \in A \setminus \{0\}$ est un *diviseur de 0* si il existe $0 \neq b \in A$ tel que

$$ab = 0 \quad \text{ou} \quad ba = 0.$$

Par exemple $\mathbb{Z}/n\mathbb{Z}$ contient des diviseurs de 0 si n n'est pas premier. En effet, si $n = ab$ avec $1 < a, b < n$ alors \bar{a} et \bar{b} sont des diviseurs de 0 puisque $ab \equiv 0 \pmod{n}$. Mais il n'en contient pas si $n = p$ est premier.

L'anneau $M_n(\mathbb{Z})$ contient des diviseur de 0 pour $n \geq 2$. Par exemple pour $n = 2$,

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

- **Remarques 2.8**
1. Si $a \neq 0$ n'est pas un diviseur de 0, alors on peut simplifier par a . Plus précisément, pour tous $x, y \in A$, on a

$$ax = ay \implies x = y \quad \text{et} \quad xa = ya \implies x = y.$$

En effet, si $ax = ay$ alors $0 = ax - ay = a(x - y)$ et donc $x - y = 0$ et $x = y$. De même de l'autre côté.

2. Si $u \in U(A)$ alors u n'est pas un diviseur de 0. En effet, supposons que $u \in U(A)$. Si on avait $u \cdot b = 0$ pour un $b \in A$ alors on aurait $b = u^{-1}ub = u^{-1}0 = 0$. Observons que l'implication inverse est fausse. Par exemple $2 \in \mathbb{Z}$ n'est pas un diviseur de 0, mais $2 \notin U(\mathbb{Z})$.

Définition 2.9 Un anneau commutatif $A \neq \{0\}$ est dit *intègre* s'il ne contient pas de diviseurs de 0.

Autrement dit, un anneau $A \neq \{0\}$ est intègre s'il est commutatif et si $ab = 0$ implique $a = 0$ ou $b = 0$ pour tous $a, b \in A$.

Par exemple, \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} sont intègres, ainsi que $\mathbb{Z}/p\mathbb{Z}$ pour p premier. Mais $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre quand n est un nombre composé.

Si A_1 et A_2 sont des anneaux non-triviaux, alors le produit $A_1 \times A_2$ n'est jamais intègre. En effet pour tous $0 \neq a_1 \in A_1$ et $0 \neq a_2 \in A_2$ on a

$$(a_1, 0) \cdot (0, a_2) = (0, 0) \in A_1 \times A_2.$$

■ **Remarque** Un corps est forcément intègre. Ceci découle de la Remarque 2.8.2.

Proposition 2.10 Soit A un anneau fini. Alors A est un corps si et seulement si A est intègre.

Pour des anneaux de cardinalité infinie, cette équivalence est clairement fausse : \mathbb{Z} est intègre, mais ce n'est pas un corps.

Démonstration. Nous avons déjà observé qu'un corps est intègre. Supposons maintenant qu'un anneau fini A est intègre et montrons que c'est un corps, c'est-à-dire que $U(A) = A \setminus \{0\}$. Soit donc $a \in A \setminus \{0\}$. A voir : $a \in U(A)$. Montrons d'abord que $a^k \neq 0$ pour tout $k \in \mathbb{N}^*$. On montre ceci par induction sur k . Pour $k = 1$, c'est notre hypothèse que $a \in A \setminus \{0\}$. Supposons que $a^{k-1} \neq 0$. Alors

$$a^k = a^{k-1}a$$

est différent de 0 puisque c'est un produit, dans un corps intègre, de deux éléments non nuls.

Considérons maintenant le sous-ensemble

$$\{a, a^2, a^3, \dots\} \subset A.$$

Puisque A est fini, par le principe des tiroirs, il existe $k, \ell \in \mathbb{N}^*$ avec $k < \ell$ tels que $a^k = a^\ell$. Mais alors

$$0 = a^\ell - a^k = (a^{\ell-k} - 1)a^k.$$

Mais comme $a^k \neq 0$, on a forcément, puisque A est intègre, $a^{\ell-k} - 1 = 0$ et donc $1 = a^{\ell-k} = a^{\ell-k-1}a$. L'élément $a^{\ell-k-1}$ est donc l'inverse multiplicatif de a et $a \in U(A)$. ■

Par exemple, $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si c'est un corps, si et seulement si $n = p$ est premier.

Définition 2.11 Soit A un anneau. Un sous-ensemble $B \subset A$ est un *sous-anneau* si l'addition et la multiplication de A se restreignent à des lois internes sur B tel que $(B, +, \cdot)$ est un anneau avec $1_B = 1_A$.

Par exemple $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sont tous des sous-anneaux.

Un exemple où toutes les conditions d'être un sous-anneau sauf $1_B = 1_A$ sont réalisées est le suivant : Prendre $A = M_2(\mathbb{R})$ et

$$B = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \middle| x \in \mathbb{R} \right\}.$$

Les lois de A se restreignent à B et B est un anneau pour ces lois (c'est une incarnation de \mathbb{R}), mais

$$1_B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{alors que} \quad 1_A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Nous verrons que, contrairement au cas des sous-groupes dans les groupes, les sous-anneaux ne jouent pas un rôle très important dans la théorie des anneaux.

2.2 Homomorphismes d'anneaux

Définition 2.12 Soient A, B deux anneaux. Une application $f : A \rightarrow B$ est un *homomorphisme (d'anneaux)* si

1. $f(x + y) = f(x) + f(y)$ pour tous $x, y \in A$,
2. $f(1_A) = 1_B$,
3. $f(xy) = f(x)f(y)$ pour tous $x, y \in A$.

De plus, s'il existe un homomorphisme d'anneaux $f' : B \rightarrow A$ tel que

$$f' \circ f = \text{Id}_A \quad \text{et} \quad f \circ f' = \text{Id}_B$$

alors f est un *isomorphisme (d'anneaux)*. Dans ce cas, on dira que A et B sont *isomorphes* et on le dénote par $A \cong B$.

Le premier point de cette définition n'est rien d'autre que la condition que $f : (A, +) \rightarrow (B, +)$ soit un homomorphisme de groupe, ce qui implique en particulier que $f(0_A) = 0_B$ et $f(-a) = -f(a)$ pour tout $a \in A$. On appellera souvent le troisième point de la définition la *multiplicativité* de f .

■ **Exemples 2.13** 1. Pour tout anneau A et tout sous-anneau B , l'inclusion $B \hookrightarrow A$ est un homomorphisme. En particulier, les inclusions $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sont toutes des homomorphismes d'anneaux.

2. Mais l'inclusion

$$\begin{aligned} \mathbb{R} &\longrightarrow M_2(\mathbb{R}) \\ x &\longmapsto \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

n'est pas un homomorphisme d'anneaux.

3. Pour tous anneaux A et B , l'application nulle

$$\begin{aligned} 0 : A &\longrightarrow B \\ a &\longmapsto 0 \end{aligned}$$

n'est un homomorphisme que si B est l'anneau trivial.

4. La réduction modulo n ,

$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ k &\longmapsto \bar{k} \end{aligned}$$

est un homomorphisme d'anneaux. Le fait que la réduction modulo n est un homomorphisme d'anneaux est à la base des critères de divisibilité exposés dans l'Annexe.

Un homomorphisme d'anneaux $f : A \rightarrow B$ se restreint à un homomorphisme de groupes $f : U(A) \rightarrow U(B)$. Pour voir ceci il suffit, par la multiplicativité de f , de montrer que $f(U(A)) \subset U(B)$. Soit donc $u \in U(A)$ et $u^{-1} \in U(A)$ son inverse multiplicatif. Alors

$$f(u)f(u^{-1}) = f(uu^{-1}) = f(1_A) = 1_B$$

et de même $f(u^{-1})f(u) = 1_B$ de sorte que $f(u) \in U(B)$.

Observons que la composition de deux homomorphismes d'anneaux est clairement encore un homomorphisme d'anneaux.

Comme pour les isomorphismes de groupes, on montre facilement le critère suivant très utile.

Proposition 2.14 Un homomorphisme d'anneaux est un isomorphisme si et seulement si il est bijectif.

Démonstration. \implies : clair, puisque l'existence de l'application inverse f' implique que f (et f') sont bijectifs.

\impliedby : Soit $f : A \rightarrow B$ un homomorphisme d'anneau bijectif. En particulier, $f : (A, +) \rightarrow (B, +)$ est un homomorphisme de groupes bijectif. Par la Proposition 1.29 il existe un homomorphisme de groupes $f' : B \rightarrow A$ tel que

$$f' \circ f = \text{Id}_A \quad \text{et} \quad f \circ f' = \text{Id}_B.$$

Puisque f' est un homomorphisme de groupe, on a $f'(x+y) = f'(x) + f'(y)$ pour tous $x, y \in A$.

Comme $f(1_A) = 1_B$ on a $f'(1_B) = f'(f(1_A)) = 1_A$.

Il reste à voir que $f'(xy) = f'(x)f'(y)$ pour tous $x, y \in B$. Puisque f est injective, cette égalité est équivalente à

$$f(f'(xy)) = f(f'(x)f'(y)).$$

Le terme de gauche n'est autre que xy puisque $f \circ f' = \text{Id}_B$. Quant au terme de droite, on utilise d'abord la multiplicativité de f pour obtenir

$$f(f'(x)f'(y)) = f(f'(x))f(f'(y)) = xy.$$

Les deux termes étant bien égaux, l'égalité demandée est vérifiée. ■

On définit le noyau et l'image d'un homomorphisme d'anneau $f : A \rightarrow B$ comme pour les homomorphismes de groupes :

$$\text{Ker}(f) = \{a \in A \mid f(a) = 0_B\} \subset A,$$

$$\text{Im}(f) = \{f(a) \mid a \in A\} \subset B.$$

On vérifie facilement que $\text{Im}(f)$ est toujours un sous-anneau de B . Mais $\text{Ker}(f)$ ne sera un sous-anneau de A que si $B = \{0_B\}$. En effet, si $B \neq \{0_B\}$ ou autrement dit $0_B \neq 1_B$ alors $1_A \notin \text{Ker}(f)$ puisque $0_B \neq 1_B = f(1_A)$. Voici les propriétés qui comme nous le montrerons plus tard caractérisent les noyaux d'homomorphismes d'anneaux.

Lemme 2.15 Soit $f : A \rightarrow B$ un homomorphisme d'anneaux. Alors

1. $\text{Ker}(f)$ est un sous-groupe de $(A, +)$,
2. pour tous $k \in \text{Ker}(f)$ et $a \in A$ on a $ak \in \text{Ker}(f)$ et $ka \in \text{Ker}(f)$.

Démonstration. 1. Simplemenent car f est en particulier un homomorphisme de groupes.

2. Pour $k \in \text{Ker}(f)$ et $a \in A$ on a

$$f(ak) = f(a) \underbrace{f(k)}_{=0_B} = f(a) \cdot 0_B = 0_B$$

et de façon identique $f(ka) = 0_B$. ■

Montrons à présent que pour tout anneau A il existe un unique homomorphisme d'anneaux

$$\varepsilon : \mathbb{Z} \longrightarrow A.$$

Avant d'examiner la forme de ε , rappelons que $(A, +)$ étant un groupe abélien, il est possible pour tous $a \in A$ et $n \in \mathbb{Z}$ de considérer la n -ième puissance de a , qui en notation additive s'écrit

$$na = \begin{cases} \underbrace{a + \cdots + a}_{n \text{ fois}} & \text{si } n > 0, \\ 0_A & \text{si } n = 0, \\ \underbrace{(-a) + \cdots + (-a)}_{-n \text{ fois}} & \text{si } n < 0. \end{cases}$$

et satisfait les relations

$$(P1) \ m \cdot a + n \cdot a = (m+n) \cdot a \quad \text{et} \quad (P2) \ m \cdot (n \cdot a) = (mn) \cdot a$$

pour tous $m, n \in \mathbb{Z}$, $a \in A$.

Pour qu'une telle application ε soit un homomorphisme d'anneaux, on doit, par définition, avoir $\varepsilon(0) = 0_A$ et $\varepsilon(1) = 1_A$ et par conséquent, pour tout $n \in \mathbb{Z}$.

$$\varepsilon(n) = n \cdot 1_A.$$

Vérifions qu'on n'a, en effet, pas d'autre choix que de poser $\varepsilon(n) = n \cdot 1_A$. Traitons d'abord le cas $n \in \mathbb{N}$ par induction sur n . Pour $n = 0$ et $n = 1$ cela a déjà été observé. Supposons que $\varepsilon(n-1) = (n-1) \cdot 1_A$. Alors

$$\begin{aligned}\varepsilon(n) &= \varepsilon((n-1) + 1) \\ &= \varepsilon(n-1) + \varepsilon(1) && \text{si } \varepsilon \text{ homomorphisme de groupes,} \\ &= (n-1) \cdot 1_A + 1 \cdot 1_A && \text{par induction,} \\ &= n \cdot 1_A && (P1).\end{aligned}$$

Finalement pour $n < 0$ on a

$$\begin{aligned}\varepsilon(n) &= -\varepsilon(-n) && \text{si } \varepsilon \text{ homomorphisme de groupes,} \\ &= (-1) \cdot \varepsilon(-n) && \text{car } -a \text{ est la } (-1)\text{-ème puissance de } a, \\ &= (-1) \cdot ((-n) \cdot 1_A) && \text{car } -n > 0, \\ &= n \cdot 1_A && (P2).\end{aligned}$$

Vérifions que l'application ε définie ainsi est bien un homomorphisme d'anneaux. Il est clair que $\varepsilon(m+n) = \varepsilon(m) + \varepsilon(n)$ pour tous $m, n \in \mathbb{Z}$. Ceci découle des propriétés des puissances n -ièmes. (Plus généralement, nous avons déjà observé que dans tout groupe G et pour tout $g \in G$, l'application

$$\begin{aligned}\mathbb{Z} &\longrightarrow G \\ n &\longmapsto g^n\end{aligned}$$

est un homomorphisme de groupe. Prendre ici $G = (A, +)$ et $g = 1_A$ en notation additive.) Nous avons aussi $\varepsilon(1) = 1_A$ par définition de ε . Ne reste plus qu'à vérifier que $\varepsilon(m \cdot n) = \varepsilon(m) \cdot \varepsilon(n)$ pour tous $m, n \in \mathbb{Z}$. Pour ceci, nous utiliserons le lemme suivant :

Lemme 2.16 Soient A un anneau, $a \in A$ et $m \in \mathbb{Z}$. Alors $(m \cdot 1_A)a = m \cdot a$.

Avant de le démontrer, voyons comment ceci implique la multiplicativité de ε :

$$\varepsilon(m \cdot n) = (mn) \cdot 1_A = m \cdot (n \cdot 1_A) = (m \cdot 1_A)(n \cdot 1_A) = \varepsilon(m)\varepsilon(n),$$

où l'on a appliqué le lemme à $a = n \cdot 1_A$ dans la 3-ème égalité.

Démonstration. Si $m = 0$ on a bien

$$\underbrace{(0 \cdot 1_A)}_{0_A} a = 0_A \cdot a = 0_A \quad \text{et} \quad 0 \cdot a = 0_A.$$

Si $m > 0$ alors

$$\begin{aligned}(m \cdot 1_A)a &= \underbrace{(1_A + \cdots + 1_A)}_{m \text{ fois}} a && \text{définition } m\text{-ième puissance} \\ &= \underbrace{(a + \cdots + a)}_{m \text{ fois}} && \text{distributivité} \\ &= m \cdot a && \text{définition } m\text{-ième puissance.}\end{aligned}$$

Si $m < 0$ alors

$$\begin{aligned}
 (m \cdot 1_A)a &= (((-1)(-m)) \cdot 1_A)a \\
 &= ((-1)((-m) \cdot 1_A))a && (P2) \\
 &= (-((-m) \cdot 1_A))a && \text{car } -b \text{ est la } (-1)\text{-ème puissance de } b, \\
 &= -(((-m) \cdot 1_A)a) && (-x)y = -(xy) \\
 &= -((-m)a) && \text{cas } -m > 0 \\
 &= (-1)((-m)a) && \text{car } -b \text{ est la } (-1)\text{-ème puissance de } b, \\
 &= ((-1)(-m))a && (P2) \\
 &= ma.
 \end{aligned}$$

■

Un corollaire immédiat du Lemme 2.16 est :

Corollaire 2.17 Soit A un anneau. Si il existe $m \in \mathbb{Z}$ tel que $m \cdot 1_A = 0_A$ alors $m \cdot a = 0_A$ pour tout $a \in A$.

Définition 2.18 La *caractéristique* d'un anneau, $\text{car}(A) \in \mathbb{N}$ est définie comme suit :

- Si $m \cdot 1_A \neq 0$ pour tout $m \in \mathbb{N}$ on pose $\text{car}(A) := 0$.
- Sinon,

$$\text{car}(A) := \min\{m \in \mathbb{N} \mid m \cdot 1_A = 0\}.$$

En d'autres termes, la caractéristique d'un anneau A , dans le cas où $\text{car}(A) > 0$, n'est rien d'autre que l'ordre de 1_A dans le groupe abélien $(A, +)$. En particulier le noyau de l'unique homomorphisme d'anneaux $\varepsilon : \mathbb{Z} \rightarrow A$ défini ci-dessus est $\text{Ker}(\varepsilon) = \text{car}(A)\mathbb{Z} \subset \mathbb{Z}$. Nous avons déjà observé ceci dans le cadre plus général d'un homomorphisme de groupe

$$\begin{aligned}
 \varphi : \mathbb{Z} &\longrightarrow G \\
 n &\longmapsto g^n,
 \end{aligned}$$

pour un groupe G et un élément $g \in G$, où l'on sait que $\text{Ker}(\varphi) = \text{ord}(g)\mathbb{Z}$ si $\text{ord}(g) < \infty$ et $\text{Ker}(\varphi) = \{0\}$ si $\text{ord}(g) = \infty$.

Par exemple, les caractéristiques de $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont 0 et la caractéristique de $\mathbb{Z}/n\mathbb{Z}$ est n . Le seul anneau de caractéristique 1 est l'anneau trivial $A = \{0_A\}$.

Lemme 2.19 Soient A un anneau de caractéristique non nulle et $a \in A$. Alors l'ordre (pour l'addition) de a divise $\text{car}(A)$.

Démonstration. Par définition de la caractéristique on a $\text{car}(A) \cdot 1_A = 0_A$, ce qui implique par le Corollaire 2.17, que $\text{car}(A) \cdot a = 0$ et que l'ordre de a divise $\text{car}(A)$. ■

Proposition 2.20 Soit $A \neq \{0\}$ un anneau intègre. Alors ou bien $\text{car}(A) = 0$ ou bien $\text{car}(A)$ est un nombre premier.

Démonstration. Supposons que $k \cdot \ell = m = \text{car}(A) > 0$, avec $k, \ell \in \mathbb{N}$ tels que $1 < k, \ell < m$. Alors

$$(k \cdot 1_A) \cdot (\ell \cdot 1_A) = \varepsilon(k)\varepsilon(\ell) = \varepsilon(k\ell) = (k\ell) \cdot 1_A = 0_A,$$

qui est impossible dans un anneau intègre puisque $k \cdot 1_A$ et $\ell \cdot 1_A$ sont différents de 0_A . ■

Proposition 2.21 Soit A un anneau fini de caractéristique p un nombre premier. Alors il existe $n \geq 1$ tel que $|A| = p^n$.

Observons que ceci est faux si la caractéristique n'est pas un nombre premier : $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ a caractéristique 4 mais son ordre 8 n'est pas une puissance de 4.

Démonstration. Montrons que le seul premier divisant $|A|$ est p . Soit q un nombre premier divisant $|A|$. Par le Théorème de Cauchy 1.89 il existe un élément d'ordre q dans A , mais par le Lemme 2.19, cet ordre doit diviser p , et donc $q = p$. ■

Lemme 2.22 Soit $f : A \rightarrow B$ un homomorphisme d'anneaux. Alors $\text{car}(B)$ divise $\text{car}(A)$.

Démonstration. Soient $\varepsilon_A : \mathbb{Z} \rightarrow A$ et $\varepsilon_B : \mathbb{Z} \rightarrow B$ les deux uniques homomorphismes d'anneaux entre \mathbb{Z} et A , respectivement B . La composition $f \circ \varepsilon_A$ est aussi un homomorphisme d'anneaux de \mathbb{Z} dans B et donc égale à ε_B par unicité. On a donc

$$\text{car}(A)\mathbb{Z} = \text{Ker}(\varepsilon_A) \subset \text{Ker}(f \circ \varepsilon_A) = \text{Ker}(\varepsilon_B) = \text{car}(B)\mathbb{Z},$$

ce qui implique que $\text{car}(B)$ divise $\text{car}(A)$. ■

2.3 Idéaux et anneaux quotients

Définition 2.23 Soit A un anneau. Un sous-ensemble $I \subset A$ est un *idéal (bilatère)* si

- $(I, +)$ est un groupe (abélien),
- $xa \in I$ et $ax \in I$ pour tous $x \in I$ et $a \in A$.

Si I est un idéal d'un anneau A , on le note $I < A$.

Dans tout anneau A , les sous-ensembles $\{0\}$ et A sont des idéaux de A , qu'on appellera idéaux *triviaux*.

Le Lemme 2.15 dit précisément que le noyau d'un homomorphisme d'anneaux $f : A \rightarrow B$ est un idéal, $\text{Ker}(f) < A$. Inversément, nous verrons bientôt ci-dessous dans le Corollaire 2.29 que tout idéal est le noyau d'un homomorphisme d'anneaux.

Dans un anneau commutatif A , il est facile de définir le plus petit idéal de A contenant un nombre fini d'éléments $x_1, \dots, x_k \in A$ (pour un $k \in \mathbb{N}^*$). En effet, il suffit de poser

$$(x_1, \dots, x_k) := \{a_1x_1 + \dots + a_kx_k \mid a_i \in A\}.$$

La vérification du fait que (x_1, \dots, x_k) est bien un idéal contenant x_1, \dots, x_k et que tout idéal $I < A$ contenant x_1, \dots, x_k contient l'idéal (x_1, \dots, x_k) est laissée en exercice.

Définition 2.24 Soient A un anneau commutatif et $x \in A$. Un idéal de la forme $I = (x)$ est appelé idéal *principal*.

Un anneau commutatif dont tous les idéaux sont des idéaux principaux est un anneau *principal*.

- **Exemples 2.25** 1. Les idéaux de \mathbb{Z} étant en particulier des sous-groupes de \mathbb{Z} ont forcément la forme $n\mathbb{Z}$, pour un $n \in \mathbb{N}$. On vérifiera facilement que $n\mathbb{Z}$ est bien un idéal de \mathbb{Z} qui est clairement principal puisque $n\mathbb{Z} = (n)$. En particulier \mathbb{Z} est un anneau principal.

Notons que $I = (4, 6)$ est aussi un idéal de \mathbb{Z} et est donc aussi principal, même s'il n'en a pas l'air au premier abord. En effet $(4, 6) = (2)$.

2. Dans $\mathbb{R}[X]$ on a les idéaux principaux suivants :

$$\begin{aligned} (X) &= \{a_1X + a_2X^2 + \dots + a_nX^n \mid a_i \in \mathbb{R}\}, \\ (X^2) &= \{a_2X^2 + a_3X^3 + \dots + a_nX^n \mid a_i \in \mathbb{R}\}. \end{aligned}$$

De même, on pourrait considérer des idéaux principaux arbitraires $(p(X))$ pour tout polynôme $p(X) \in \mathbb{R}[X]$. Nous verrons que $\mathbb{R}[X]$ est un anneau principal.

3. En contraste, vous verrez en exercice que dans $A = \mathbb{Z}[X]$ l'idéal

$$(2, X) = \{2a_0 + a_1X + \dots + a_nX^n \mid a_i \in \mathbb{Z}\}$$

n'est pas principal.

Lemme 2.26 Soient A un anneau non trivial et $I < A$ un idéal. Alors

$$I = A \iff \exists u \in U(A) \text{ tel que } u \in I.$$

Démonstration. \implies : Supposons que $I = A$. Alors $1_A \in A = I$.

\impliedby : Soit $u \in U(A) \cap I$. Montrons que $A \subset I$. Soit $a \in A$. Alors

$$a = \underbrace{u}_{\in I} \underbrace{(u^{-1}a)}_{\in A} \in I.$$

■

En particulier, un idéal $I < A$ différent de A n'est jamais un sous-anneau de A puisqu'il ne contient pas le neutre multiplicatif de A .

Lemme 2.27 Dans un corps, tout idéal est trivial.

Démonstration. Soient A un corps et $\{0\} \neq I < A$ un idéal. Il existe donc $0 \neq u \in I \subset A \setminus \{0\} = U(A)$. Par le Lemme 2.26, $I = A$. ■

Théorème 2.28 Soient A un anneau et $I < A$ un idéal. Le groupe abélien $(A/I, +)$ muni de la multiplication

$$(a + I)(b + I) = ab + I$$

est un anneau de neutre multiplicatif $1 + I$. De plus, la projection

$$\begin{aligned} A &\longrightarrow A/I \\ a &\longmapsto a + I \end{aligned}$$

est un homomorphisme d'anneaux.

Corollaire 2.29 Soit A un anneau. Un sous-ensemble $I \subset A$ est un idéal si et seulement si il existe un homomorphisme d'anneaux $f : A \rightarrow B$ tel que $\text{Ker}(f) = I$.

Démonstration. \Leftarrow : C'est le Lemme 2.15.

\Rightarrow : Prendre f la projection $A \rightarrow A/I$ du Théorème 2.28. ■

En contraste, un sous-ensemble A' d'un anneau A est un sous-anneau si et seulement si il existe un homomorphisme d'anneaux $f : B \rightarrow A$ tel que $\text{Im}(f) = A'$. En effet, nous avons déjà observé que l'image d'un homomorphisme d'anneaux est un sous-anneau. Inversément, si $A' \subset A$ est un sous-anneau, il suffit de prendre $B = A'$ et l'inclusion de A' dans A .

Avant de voir la preuve du Théorème 2.28, revenons sur les exemples vus ci-dessus pour essayer de comprendre les quotients A/I correspondants.

- **Exemples 2.30**
1. $A = \mathbb{Z} > n\mathbb{Z} = I$. Alors l'anneau quotient A/I n'est rien d'autre que $\mathbb{Z}/n\mathbb{Z}$ muni de l'addition et la multiplication modulo n .
 2. $A = \mathbb{R}[X]$. Examinons le quotient A/I pour les trois idéaux $I = (X)$, (X^2) et $(X^2 + 1)$. Pour $I = (X)$, la projection prend la forme

$$\begin{aligned} \mathbb{R}[X] &\longrightarrow \mathbb{R}[X]/(X) \cong \mathbb{R} \\ a_0 + \underbrace{a_1X + \cdots + a_nX^n}_{\in (X)} &\longmapsto a_0 + (X) \mapsto a_0, \end{aligned}$$

et le quotient $\mathbb{R}[X]/(X)$ s'identifie (c'est-à-dire est isomorphe) à \mathbb{R} .

Pour $I = (X^2)$, la projection prend la forme

$$\begin{aligned} \mathbb{R}[X] &\longrightarrow \mathbb{R}[X]/(X^2) \cong (\mathbb{R}^2, +, \circ) \\ a_0 + a_1X + \underbrace{a_2X^2 + \cdots + a_nX^n}_{\in (X^2)} &\longmapsto a_0 + a_1X + (X^2) \mapsto (a_0, a_1). \end{aligned}$$

Ici il faut être un peu plus prudent. En effet l'identification entre le quotient $\mathbb{R}[X]/(X^2)$ et \mathbb{R}^2 est bien un isomorphisme de groupes abéliens pour l'addition usuelle sur \mathbb{R}^2 , mais ce n'est pas un isomorphisme d'anneaux pour la structure d'anneau produit sur \mathbb{R}^2 . En effet

$$(a_0 + a_1X)(b_0 + b_1X) = a_0b_0 + (a_0b_1 + a_1b_0)X + \underbrace{a_1b_1X^2}_{\in (X^2)}$$

alors que

$$(a_0, a_1)(b_0, b_1) = (a_0b_0, a_1b_1) \in \mathbb{R}^2.$$

Pour que l'identification soit un isomorphisme d'anneaux, il faut définir une multiplication différente sur \mathbb{R}^2 :

$$\begin{aligned} \circ : \quad \mathbb{R}^2 \times \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ ((a_0, a_1), (b_0, b_1)) &\longmapsto (a_0b_0, a_0b_1 + a_1b_0). \end{aligned}$$

Il est maintenant clair que $\mathbb{R}[X]/(X^2) \cong (\mathbb{R}^2, +, \circ)$.

Finalement, pour $I = (X^2 + 1)$ observons d'abord que tout polynôme $f(X) \in \mathbb{R}[X]$ s'écrit de façon unique comme

$$f(X) = b_0 + b_1X + (X^2 + 1)g(X),$$

pour un polynôme $g(X) \in \mathbb{R}[X]$ et $b_0, b_1 \in \mathbb{R}$. Nous démontrerons ceci formellement par la suite : c'est la division polynômiale. La projection prend maintenant la forme

$$\begin{aligned} \mathbb{R}[X] &\longrightarrow \mathbb{R}[X]/(X^2) \cong \mathbb{C} \\ b_0 + b_1X + \underbrace{(X^2 + 1)g(X)}_{\in (X^2 + 1)} &\longmapsto b_0 + b_1X + (X^2 + 1) \mapsto b_0 + b_1i. \end{aligned}$$

L'identification

$$\begin{aligned} f : \quad \mathbb{R}[X]/(X^2) &\longrightarrow \mathbb{C} \\ b_0 + b_1X + (X^2 + 1) &\longmapsto b_0 + b_1i \end{aligned}$$

est bien un isomorphisme d'anneaux : Il est clair que f est un isomorphisme de groupes. De plus

$$\begin{aligned} &f((b_0 + b_1X + (X^2 + 1))(c_0 + c_1X + (X^2 + 1))) \\ &= f(b_0c_0 + (b_1c_0 + b_0c_1)X + b_1c_1X^2 + (X^2 + 1)) \\ &= f((b_0c_0 - b_1c_1 + (b_1c_0 + b_0c_1)X + \underbrace{b_1c_1(X^2 + 1)}_{\in (X^2 + 1)} + (X^2 + 1))) \\ &= (b_0c_0 - b_1c_1) + (b_1c_0 + b_0c_1)i \\ &= (b_0 + b_1i)(c_0 + c_1i) \\ &= f((b_0 + b_1X + (X^2 + 1))f((c_0 + c_1X + (X^2 + 1)))). \end{aligned}$$

3. Pour $A = \mathbb{Z}[X]$, on obtient

$$\mathbb{Z}[X]/(X) \cong \mathbb{Z} \quad \text{et} \quad \mathbb{Z}[X]/(2, X) \cong \mathbb{Z}/2\mathbb{Z}.$$

Démonstration du Théorème 2.28. Soient A un anneau et I un idéal. Puisque $(A, +)$ est abélien, le sous-groupe $I < A$ est normal de sorte que nous pouvons considérer le groupe quotient A/I . Vérifions que la multiplication

$$(a + I)(b + I) = ab + I$$

est bien définie. Rappelons que tout représentant de la classe $a + I$ a la forme $a + x$ pour $x \in I$. De même un représentant de la classe $b + I$ a la forme $b + y$ pour $y \in I$. Calculons le produit

$$(a + x)(b + y) = ab + \underbrace{ay + xb + xy}_{\in I}$$

pour conclure que $(a + x)(b + y) + I = ab + I$. L'associativité et la distributivité est un calcul direct laissé en exercice. Le neutre multiplicatif est clairement $1 + I$, ce qui finit d'établir que A/I est un anneau.

Le fait que la projection est un homomorphisme d'anneaux est évident. ■

Nous obtenons, pour les anneaux aussi, l'analogue du Théorème 1.40 :

Théorème 2.31 Soient A, B deux anneaux, $I < A$ un idéal, $f : A \rightarrow B$ un homomorphisme d'anneaux. Si $I < \text{Ker}(f)$ alors il existe un unique homomorphisme d'anneaux $\bar{f} : A/I \rightarrow B$ tel que $f = \bar{f} \circ \pi$, c'est-à-dire tel que le diagramme

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \pi \downarrow & \nearrow \bar{f} & \\ A/I & & \end{array}$$

commute.

Démonstration. Par le Théorème 1.40, nous savons déjà qu'il existe un unique homomorphisme de groupes $\bar{f} : (A/I, +) \rightarrow (B, +)$ tel que $f = \bar{f} \circ \pi$. Vérifions que \bar{f} est automatiquement un homomorphisme d'anneaux : Soient $a + I, b + I \in A/I$. Alors

$$\begin{aligned} \bar{f}((a + I)(b + I)) &= \bar{f}(ab + I) \\ &= f(ab) \\ &= f(a)f(b) \\ &= \bar{f}(a + I)\bar{f}(b + I). \end{aligned}$$

Et finalement,

$$\bar{f}(1_{A/I}) = \bar{f}(1_A + I) = f(1_A) = 1_B.$$

■

Théorème 2.32 Soient A, B deux anneaux. Tout homomorphisme d'anneaux $f : A \rightarrow B$ induit un isomorphisme

$$\bar{f} : A/\text{Ker}(f) \longrightarrow \text{Im}(f).$$

Démonstration. Nous savons déjà, par le Théorème 1.44, que f induit un isomorphisme de groupes $\bar{f} : A/\text{Ker}(f) \rightarrow \text{Im}(f)$, qui est un homomorphisme d'anneaux par le Théorème 2.31. Finalement, un homomorphisme d'anneaux bijectif est un isomorphisme d'anneaux. ■

2.4 Idéaux maximaux et premiers

Définition 2.33 Soit A un anneau. Un idéal $I < A$ est *maximal* si $I \neq A$ et si $I \subset J \subset A$ pour un idéal $J < A$ alors $I = J$ ou $J = A$.

- **Exemples 2.34** 1. Quels sont les idéaux maximaux de \mathbb{Z} ? Nous savons que tout idéal de \mathbb{Z} a la forme $n\mathbb{Z}$ pour $n \in \mathbb{Z}$. De plus

$$n\mathbb{Z} < m\mathbb{Z} < \mathbb{Z}$$

si et seulement si m divise n . De ce fait, un idéal $n\mathbb{Z}$ est maximal si et seulement si n est un nombre premier.

2. Est-ce que les idéaux (X) , (X^2) et $(X^2 + 1)$ sont maximaux dans $\mathbb{R}[X]$? Pour le moment nous pouvons seulement conclure que (X^2) n'est pas maximal. En effet,

$$(X^2) < (X) < \mathbb{R}[X]$$

et ces inclusions sont strictes puisque $X \in (X)$ mais $X \notin (X^2)$ et $1 \in \mathbb{R}[X]$ mais $1 \notin (X)$. Nous verrons bientôt comment traiter les deux autres idéaux.

3. Dans $\mathbb{Z}[X]$ l'idéal (X) n'est pas maximal puisque

$$(X) < (2, X) < \mathbb{Z}[X].$$

Et nous pouvons d'ores et déjà montrer que $(2, X)$ est maximal. L'argument est un peu plus laborieux que nécessaire (on préférera sans doute invoquer la Proposition 2.36 ci-dessous) mais peut être instructif. Supposons que

$$(2, X) < I < \mathbb{Z}[X].$$

On applique le Théorème 1.40 à l'homomorphisme $\pi : \mathbb{Z}[X] \rightarrow \mathbb{Z}[X]/I$ et le sous-groupe normal $(2, X)$, ce que l'on peut faire puisque $(2, X) < I = \text{Ker}(\pi)$ par hypothèse, pour conclure qu'il existe un homomorphisme surjectif

$$\mathbb{Z}[X]/(2, X) \rightarrow \mathbb{Z}[X]/I.$$

Mais $\mathbb{Z}[X]/(2, X) \cong \mathbb{Z}/2\mathbb{Z}$ n'a que deux éléments, donc $\mathbb{Z}[X]/I$ en a 1 ou 2. Dans le premier cas on conclut que $I = \mathbb{Z}[X]$ et dans le deuxième que $I = (2, X)$.

Proposition 2.35 Soit A un anneau commutatif. Alors A est un corps si et seulement si $\{0\}$ est un idéal maximal.

Démonstration. \Rightarrow : Car $\{0\}$ et A sont les seuls idéaux dans un corps A .

\Leftarrow : Supposons que $\{0\}$ est un idéal maximal. Notons que ceci implique que $A \neq \{0\}$ car un idéal maximal est strictement contenu dans son anneau. Voyons que A est un corps, ou de façon équivalente, que $U(A) \supset A \setminus \{0\}$. Soit donc $0 \neq x \in A$. On a

$$\{0\} \subset (x) \subset A.$$

Puisque $x \neq 0$, la première inclusion est stricte, et comme $\{0\}$ est un idéal maximal, $(x) = A$. En particulier, $1 \in A = (x) = \{ax \mid a \in A\}$. Il existe donc $a \in A$ tel que $ax = 1$ et $x \in U(A)$. ■

Proposition 2.36 Soit A un anneau commutatif. Alors $I < A$ est un idéal maximal si et seulement si A/I est un corps.

Démonstration. Soient A un anneau commutatif et $I < A$ un idéal. Montrons d'abord qu'il existe une bijection entre les idéaux de A/I et les idéaux de A contenant I . Pour ceci, considérons la projection canonique

$$\pi : A \longrightarrow A/I.$$

Vous verrez en exercice que l'image d'un idéal par un homomorphisme d'anneaux est toujours un idéal. En particulier, si $J < A$ est un idéal alors $\pi(J) < A/I$ est un idéal.

De même, la préimage d'un idéal est aussi un idéal contenant le noyau de l'homomorphisme. Donc si $K < A/I$ est un idéal de l'anneau quotient A/I , alors

$$\pi^{-1}(K) = \{a \in A \mid \pi(a) \in K\}$$

est un idéal de A contenant $I = \text{Ker}(\pi)$. La bijection recherchée est donnée par

$$\begin{aligned} \{J < A \text{ idéal} \mid I < J\} &\longrightarrow \{K < A/I \text{ idéal}\} \\ J &\longmapsto \pi(J) \\ \pi^{-1}(K) &\longleftarrow K. \end{aligned}$$

Ceci définit bien une bijection puisque d'une part l'égalité $\pi(\pi^{-1}(K)) = K$ est vraie pour une application surjective quelconque et un sous-ensemble quelconque de l'ensemble d'arrivée. D'autre part, vérifions l'égalité $\pi^{-1}(\pi(J)) = J$ pour un idéal $J < A$ contenant I . Observons d'abord que l'inclusion $\pi^{-1}(\pi(J)) \supset J$ est elle aussi vraie pour une application quelconque et un sous-ensemble quelconque de l'ensemble de départ. Montrons que $\pi^{-1}(\pi(J)) \subset J$. Soit $x \in \pi^{-1}(\pi(J))$. Par définition, $\pi(x) \in \pi(J)$. Il existe donc $y \in J$ tel que $\pi(x) = \pi(y)$. De ce fait, $x - y \in \text{Ker}\pi = I$ et il existe $z \in I$ tel que $x = y + z \in J$ puisque $y \in J$ et $z \in I < J$.

En effet I n'est pas maximal si et seulement si il existe un idéal $J \neq I$, A tel que $I < J < A$. Avec la bijection ci-dessus ceci est équivalent à l'existence d'un idéal non trivial $K < A/I$, ce qui par la Proposition 2.35 est équivalent à ce que A/I ne soit pas un corps. ■

Revenons sur les exemples d'idéaux ci-dessus :

- **Exemples 2.37** 1. $(n) = n\mathbb{Z} < \mathbb{Z}$ est maximal si et seulement si $\mathbb{Z}/(n)$ est un corps et donc si et seulement si n est un nombre premier.
2. (X) et $(X^2 + 1) < \mathbb{R}[X]$ sont maximaux puisque $\mathbb{R}[X]/(X) \cong \mathbb{R}$ et $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$ sont des corps. On pourrait aussi utiliser la Proposition 2.36 pour montrer que (X^2) n'est pas maximal : Le quotient $\mathbb{R}[X]/(X^2)$ n'est pas un corps puisque $X + (X^2)$ est un diviseur de zéro. En effet,

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

De façon équivalente, \mathbb{R}^2 muni de la multiplication

$$\begin{aligned} \circ : \quad \mathbb{R}^2 \times \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ ((a_0, a_1), (b_0, b_1)) &\longmapsto (a_0b_0, a_0b_1 + a_1b_0) \end{aligned}$$

n'est pas un corps puisque $(0, 1)$ est un diviseur de zéro, $(0, 1) \circ (0, 1) = (0, 0 + 0) = (0, 0)$.

3. $(X) < \mathbb{Z}[X]$ n'est pas maximal puisque $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$ n'est pas un corps, et $(2, X) < \mathbb{Z}[X]$ est maximal puisque $\mathbb{Z}[X]/(2, X) \cong \mathbb{Z}/2\mathbb{Z}$ est un corps.

Définition 2.38 Soit A un anneau commutatif. Un idéal $I < A$ est *premier*, si $I \neq A$ et pour tous $a, b \in A$:

$$ab \in I \implies a \in I \text{ ou } b \in I.$$

- **Exemples 2.39** 1. Considérons $(n) < \mathbb{Z}$ pour $n \in \mathbb{N}$.
- Si $n = 0$ alors $(0) = \{0\}$ est premier.
 - Si $n = k\ell$ avec $1 < k, \ell < n$ alors (n) n'est pas premier puisque $k\ell = n \in (n)$ mais $k, \ell \notin (n)$.
 - Si p est un nombre premier alors (p) est premier. En effet,

$$\begin{aligned} ab \in (p) &\iff p \mid ab \\ &\implies p \mid a \text{ ou } p \mid b \\ &\iff a \in (p) \text{ ou } b \in (p). \end{aligned}$$

2. Il est clair que $(X^2) < \mathbb{R}[X]$ n'est pas premier : $X \cdot X \in (X^2)$ mais $X \notin (X^2)$. Qu'en est-il de (X) et $(X^2 + 1)$?

Par définition que dans un anneau commutatif différent de $\{0\}$ l'idéal $\{0\}$ est premier si et seulement si A est intègre. Plus généralement, on a :

Proposition 2.40 Soit A un anneau commutatif. Un idéal $I < A$ est premier si et seulement si A/I est intègre.

Démonstration. Soient $I < A$ un idéal et $\pi : A \rightarrow A/I$ la projection canonique. L'idéal I est par définition premier si et seulement si, pour tous $a, b \in A$,

$$ab \in I \implies a \in I \text{ ou } b \in I.$$

Réécrivons cette condition en utilisant que $x \in I$ si et seulement si $\pi(x) = 0_{A/I}$:

$$\pi(ab) = \pi(a)\pi(b) = 0_{A/I} \implies \pi(a) = 0_{A/I} \text{ ou } \pi(b) = 0_{A/I}.$$

Mais puisque π est surjective, c'est exactement la condition pour que A/I soit intègre. ■

Corollaire 2.41 Soient A un anneau commutatif et $I < A$ un idéal. Si I est maximal alors I est premier.

Observons que l'implication inverse est fausse en générale : $\{0\} < \mathbb{Z}$ et $(X) < \mathbb{Z}[X]$ sont premiers mais pas maximaux.

Démonstration. $I < A$ est maximal si et seulement si A/I est un corps et donc intègre, ce qui est équivalent à ce que I soit premier. ■

Idéaux de la forme (n) dans $\mathbb{Z}[i]$

Pour terminer ce paragraphe, étudions les idéaux de la forme (n) , pour $n \in \mathbb{Z}$, ou de façon équivalente $n \in \mathbb{N}$, dans

$$\mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}\} \subset \mathbb{C},$$

l'anneau des entiers de Gauss. Observons que

$$\begin{aligned} (n) &= \{n(a + ib) \mid a, b \in \mathbb{Z}\} \\ &= \{a + ib \mid n \mid a \text{ et } n \mid b\}. \end{aligned}$$

Si $n = k\ell$ est un nombre composé avec $1 < k, \ell < n$ on montre facilement, exactement comme pour \mathbb{Z} , que l'idéal (n) n'est pas premier et donc pas maximal non plus.

Si $n = 0$ alors $(0) < \mathbb{Z}[i]$ est premier car $\mathbb{Z}[i] \subset \mathbb{C}$ est intègre, mais certainement pas maximal car $\mathbb{Z}[i]$ contient des idéaux non triviaux.

Le but de la fin de ce paragraphe est d'établir :

Théorème 2.42 Soit $p \in \mathbb{N}$ un nombre premier. Alors

$$\begin{aligned} (p) < \mathbb{Z}[i] \text{ est maximal} &\iff (p) < \mathbb{Z}[i] \text{ est premier} \\ &\iff p \equiv 3 \pmod{4}. \end{aligned}$$

Notons que seul 2 est un nombre premier pair et que les nombres premiers impairs se divisent naturellement en deux sous-ensembles selon que p est congru à 1 ou 3 modulo 4. Ces deux sous-ensembles jouent souvent un rôle différent en théorie des nombres dont on en voit ici une première illustration. D'autres exemples sans doute un peu plus concrets sont donnés par les Théorème 2.45 et 2.83 ci-dessous. Remarquons déjà qu'il y a une infinité de nombres premiers congru à 1, respectivement à 3 modulo 4. Avant de montrer ceci, rappelons une preuve élémentaire de l'infinité des nombres premiers.

Théorème 2.43 Il existe une infinité de nombres premiers.

Démonstration. Supposons qu'il en existe un nombre fini p_1, \dots, p_k . Posons

$$N := p_1 \cdots p_k + 1.$$

Alors il doit exister un premier divisant N mais aucun des p_i ne divise N puisque p_i divise $N - 1$. ■

Similairement, on peut montrer (cf exercice) qu'il existe une infinité de nombres premiers congrus à 3 modulo 4. La preuve repose sur le fait qu'un nombre congru à 3 modulo 4 contient forcément un facteur premier congru à 3 modulo 4. Ce fait est faux si l'on remplace 3 par 1 et il nous faut un argument additionnel pour traiter ce cas :

Théorème 2.44 Il existe une infinité de nombres premiers congrus à 1 modulo 4.

Démonstration. Supposons qu'il en existe un nombre fini p_1, \dots, p_k . Posons

$$N := \underbrace{(2p_1 \cdots p_k)}_x^2 + 1 = 4p_1^2 \cdots p_k^2 + 1.$$

Observons que $N \equiv 1 \pmod{4}$ et $N \equiv 1 \pmod{p_i}$. En particulier aucun des p_i ne divise N . Soit q un facteur premier de N . Observons que $q \neq 2$. Puisque q divise $N = x^2 + 1$ on a $x^2 + 1 \equiv 0 \pmod{q}$ ou de façon équivalente $x^2 \equiv -1 \pmod{q}$. En particulier

$$x^4 \equiv 1 \pmod{q} \text{ et } x^2 \equiv -1 \not\equiv 1 \pmod{q}$$

et il existe un élément d'ordre 4 dans $(\mathbb{Z}/q\mathbb{Z})^\times$. Ce dernier groupe a cardinalité $q - 1$. Il découle de Lagrange ou plus précisément du point 2. du Corollaire 1.35 que 4 divise $q - 1$ et que $q \equiv 1 \pmod{4}$, une contradiction. ■

Plus généralement, montrons que l'existence d'une solution à l'équation $x^2 \equiv -1 \pmod{p}$ est une caractérisation des nombres premiers impairs $p \equiv 1 \pmod{4}$:

Théorème 2.45 Soit $p \neq 2$ premier. Alors $x^2 \equiv -1 \pmod{p}$ a une solution $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ si et seulement si $p \equiv 1 \pmod{4}$.

Par exemple pour $p = 5$ on a $2^2 = 4 \equiv -1 \pmod{5}$, pour $p = 13$ on a $5^2 = 25 \equiv -1 \pmod{13}$, et on vérifie aisément qu'il n'existe pas de solution pour $p = 3$ ou 7.

Nous aurons besoin du Théorème de Wilson suivant :

Théorème 2.46 (Théorème de Wilson) Soit $n \in \mathbb{N}$, $n \geq 2$. Alors $(n - 1)! \equiv -1 \pmod{n}$ si et seulement si n est premier.

Démonstration. \Leftarrow : Supposons que $(n-1)! \equiv -1 \pmod n$. Soit $d \in \mathbb{N}$ tel que $d \mid n$ et $d < n$. À voir : $d = 1$. Puisque $d < n$ on a $d \mid (n-1)!$. Mais d divise aussi n qui lui-même divise $(n-1)! + 1$. Donc d divise la différence de ces deux nombres, soit ± 1 , et $d = 1$.

\Rightarrow : Supposons que $n = p$ est un nombre premier. Le produit $(p-1)!$ est congru à -1 modulo p si et seulement si le produit de tous les éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$ est égal à $\overline{-1}$,

$$\prod_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} x = \overline{-1}.$$

Si x est un élément d'inverse $x^{-1} \neq x$, ou de façon équivalente, $x^2 \neq \overline{1}$, alors le produit des deux facteurs xx^{-1} s'annulera. Notre produit devient donc

$$\prod_{x \in (\mathbb{Z}/p\mathbb{Z})^\times, x^2 \neq \overline{1}} x.$$

Certainement, $x = \overline{1}$ et $x = \overline{-1}$ satisfont $x^2 = \overline{1}$. Voyons que ce sont les seuls éléments : $x^2 = \overline{1}$ est équivalent à $0 = (x^2 - \overline{1}) \equiv (x - \overline{1})(x + \overline{1})$. Puisque $\mathbb{Z}/p\mathbb{Z}$ est intègre, ceci implique bien que $x - \overline{1} = 0$ ou $x + \overline{1} = 0$. Il ne reste donc plus que les facteurs $x = \overline{1}$ et $x = \overline{-1}$ dans notre produit, qui est donc bien égal à $\overline{-1}$. ■

Démonstration du Théorème 2.45. Nous avons déjà montré, dans la preuve du Théorème 2.44, que si $x^2 \equiv -1 \pmod p$ a une solution alors $p \equiv 1 \pmod 4$. Inversément supposons que $p \equiv 1 \pmod 4$ et soit $k \in \mathbb{N}$ tel que $p = 4k + 1$. Par le Théorème de Wilson,

$$\begin{aligned} -1 \pmod p &\equiv 1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \dots \cdot (p-2) \cdot (p-1) \\ &\equiv 1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \cdot \dots \cdot (-2) \cdot (-1) \\ &\equiv (-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2}\right)^2. \end{aligned}$$

Mais $(p-1)/2 = 4k/2 = 2k$ est pair, donc l'équation admet la solution $1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2}$. ■

Démonstration du Théorème 2.42. Soit p un nombre premier. Observons tout d'abord que $\mathbb{Z}[i]/(p)$ a cardinalité p^2 . En effet, toute classe dans le quotient s'écrit de façon unique comme $a + ib + (p)$ avec $0 \leq a, b < p$. En particulier, l'idéal (p) est maximal si et seulement si $\mathbb{Z}[i]/(p)$ est un corps si et seulement si $\mathbb{Z}[i]/(p)$ est intègre (car c'est un anneau fini) si et seulement si (p) est premier.

$p = 2$: (2) n'est pas premier puisque $(1+i)(1-i) = 2 \in (2)$ mais $1 \pm i \notin (2)$.

$p \equiv 1 \pmod 4$: Par le Théorème 2.45 nous savons qu'il existe $x \in \mathbb{Z}$ tel que $x^2 \equiv -1 \pmod p$ ou de façon équivalente $x^2 + 1 \equiv 0 \pmod p$. En particulier l'entier $x^2 + 1 = (x+i)(x-i)$ appartient à (p) , mais $x \pm i \notin (p)$. Donc (p) n'est pas premier.

$p \equiv 3 \pmod 4$: Nous allons établir que $R_p := \mathbb{Z}[i]/(p)$ est un corps en montrant que tout idéal est trivial. Soit donc $I < R_p$ un idéal. Voyons que $I = \{0\}$ ou R_p . Puisque $|I|$ divise $|R_p| = p^2$ il y a trois choix pour $|I|$. Si $|I| = 0$ alors $I = \{0\}$. Si $|I| = p^2$ alors $I = R_p$. Ne reste plus qu'à exclure le cas $|I| = p$. Supposons donc que I a cardinalité p . Le quotient R_p/I a cardinalité $p^2/p = p$. C'est donc un anneau isomorphe à $\mathbb{Z}/p\mathbb{Z}$ (cf exercices). On considère la composition φ des deux projections ainsi que de l'isomorphisme $R_p/I \cong \mathbb{Z}/p\mathbb{Z}$:

$$\varphi : \mathbb{Z}[i] \longrightarrow \mathbb{Z}[i]/(p) \longrightarrow R_p/I \cong \mathbb{Z}/p\mathbb{Z}.$$

Soit $a := \varphi(i) \in \mathbb{Z}/p\mathbb{Z}$. Observons que puisque φ est un homomorphisme d'anneaux, $\varphi(-1) = -\varphi(1) = -1$. De plus,

$$a^2 = \varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -1.$$

Ce n'est pas possible puisqu'il n'existe pas de solution à $x^2 \equiv -1 \pmod{p}$ pour $p \equiv 3 \pmod{4}$. ■

2.5 Factorisation dans un anneau intègre

Dans \mathbb{Z} , on peut écrire, au signe près, tout entier comme un produit de premiers. Plus précisément, dénotons

$$\mathbb{P} := \{2, 3, 5, 7, 11, 13, 17, \dots\}$$

l'ensemble des nombres premiers (positifs).

Théorème 2.47 — Théorème fondamental de l'arithmétique. Pour tout $n \in \mathbb{Z} \setminus \{0\}$ il existe $\varepsilon \in \{\pm 1\}$ et des premiers p_1, \dots, p_k tels que

$$n = \varepsilon \cdot p_1 \cdot \dots \cdot p_k.$$

De plus, cette écriture est unique à permutation des p_i près.

Peut-on généraliser ce théorème à d'autres anneaux ? Mais comment formaliser la notion d'être premier dans \mathbb{Z} à d'autres anneaux ? Dans \mathbb{Z} il y a deux façons naturelles de caractériser un nombre premier p : si p divise un produit, alors p divise un des facteurs, ou bien si $p = ab$ est un produit, alors $a = \pm 1$ ou $b = \pm 1$. Nous pouvons formaliser ces deux caractérisations à des anneaux intègres, et nous verrons qu'elles donnent lieu, en général, à deux notions différentes.

Définition 2.48 Soient A un anneau commutatif et $a, b \in A$. On dit que a *divise* b , que l'on écrit $a \mid b$ si il existe $q \in A$ tel que $aq = b$.

Notons qu'une unité $u \in U(A)$ divise tout élément $b \in A$. En effet $u(u^{-1}b) = b$. En particulier dans \mathbb{Z} , $1 \mid n$ et $(-1) \mid n$ pour tout $n \in \mathbb{Z}$.

Définition 2.49 Soit A un anneau intègre. Soit $p \in A \setminus \{0\}$. On dit que p est *premier* si $p \notin U(A)$ et pour tous $a, b \in A$,

$$p \mid ab \implies p \mid a \text{ ou } p \mid b.$$

irréductible si $p \notin U(A)$ et pour tous $a, b \in A$,

$$p = ab \implies a \in U(A) \text{ ou } b \in U(A).$$

Remarquons que comme observé ci-dessus, dans $A = \mathbb{Z}$, ces deux notions sont équivalentes.

Lemme 2.50 Soit A un anneau intègre. Si $p \in A$ est premier, alors p est irréductible.

Démonstration. Supposons que $p \in A$ est premier. En particulier, $p \notin U(A)$. Si $p = ab$ pour $a, b \in A$ alors $p \mid ab$ et puisque p est premier, $p \mid a$ ou $p \mid b$. Par symétrie (A est un anneau commutatif), nous pouvons supposer que $p \mid a$. Alors il existe $q \in A$ tel que

$$a = pq = abq$$

et donc $a(1 - bq) = 0$. Comme A est intègre, $a = 0$ ou $1 - bq = 0$. Mais si $a = 0$ alors $p = ab = 0$, impossible. Donc $bq = 1$ et $b \in U(A)$. ■

L'implication inverse est fausse en général. En effet, vous verrez en exercice que dans l'anneau intègre $A = \mathbb{Z}[\sqrt{-5}]$ l'élément 3 est irréductible mais pas premier. Néanmoins, dans un anneau intègre principal, par exemple \mathbb{Z} les deux notions sont équivalentes (Corollaire 2.52).

Nous pouvons résumer nos connaissances actuelles par le diagramme suivant, pour un anneau intègre A et pour tout élément $0 \neq p \in A$. (Les implications horizontales seront démontrées en exercice.)

$$\begin{array}{ccc} p \text{ premier} & \Longleftrightarrow & (p) \text{ premier} \\ \Downarrow & & \Uparrow \\ p \text{ irréductible} & \Longleftarrow & (p) \text{ maximal.} \end{array}$$

Voyons finalement que dans un anneau intègre principal, la dernière implication horizontale est une équivalence :

Proposition 2.51 Soient A un anneau intègre principal et $0 \neq p \in A$. Alors

$$p \text{ est irréductible} \Longleftrightarrow (p) \text{ maximal.}$$

Ainsi dans un anneau intègre principal, toutes les implications du diagramme ci-dessus sont des équivalences et on déduit :

Corollaire 2.52 Soient A un anneau intègre principal et $p \in A$. Alors

$$p \text{ est premier} \Longleftrightarrow p \text{ est irréductible.}$$

Démonstration. Il suffit de démontrer que pour un élément irréductible p d'un anneau intègre principal A , l'idéal (p) est maximal. Observons que $(p) \neq A$ sinon on aurait $p \in U(A)$. Supposons que

$$(p) < I < A.$$

Puisque A est principal, il existe $x \in A$ tel que $I = (x)$. Puisque $p \in (p) < (x)$ il existe $a \in A$ tel que $p = xa$ et donc soit $x \in U(A)$, auquel cas $(x) = A$, soit $a \in U(A)$ auquel cas $(p) = (x)$. ■

Soit A un anneau intègre. Soit $\text{Irr}(A) \subset A$ l'ensemble des irréductibles de A . Alors $U(A)$ agit sur $\text{Irr}(A)$ par multiplication :

$$\begin{aligned} U(A) \times \text{Irr}(A) &\longrightarrow \text{Irr}(A) \\ (u, p) &\longmapsto u \cdot p. \end{aligned}$$

Par exemple les irréductibles de \mathbb{Z} sont les nombres premiers et (-1) fois les nombres premiers,

$$\text{Irr}(\mathbb{Z}) = \{\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \dots\}.$$

Définition 2.53 Soit A un anneau intègre. On dit que A est *factoriel* si pour tout $a \in A \setminus \{0\}$ il existe $u \in U(A)$ et $p_1, \dots, p_k \in \text{Irr}(A)$ tels que

$$a = u \cdot p_1 \cdot \dots \cdot p_k.$$

De plus, cette factorisation est unique à permutation des p_1, \dots, p_k près et à unité près dans le sens suivant : Si $u \cdot p_1 \cdot \dots \cdot p_k = v \cdot q_1 \cdot \dots \cdot q_\ell$ avec $u, v \in U(A)$ et $p_i, q_i \in \text{Irr}(A)$, alors $k = \ell$ et il existe une permutation $\sigma \in \text{Sym}(k)$ et des unités $u_i \in U(A)$ tels que

$$q_{\sigma(i)} = u_i \cdot p_i,$$

pour tous $1 \leq i \leq k$.

Par exemple dans \mathbb{Z} on a $6 = 2 \cdot 3 = (-3) \cdot (-2)$. Ces deux expressions sont des produits d'irréductibles, et on passe de l'une à l'autre en permutant les facteurs et en les multipliant par l'unité -1 . Le Théorème fondamental de l'arithmétique est équivalent à l'affirmation que \mathbb{Z} est un anneau factoriel.

Théorème 2.54 Un anneau intègre principal est factoriel.

Nous aurons besoin du lemme préliminaire suivant :

Lemme 2.55 Soit $\{I_\alpha\}_{\alpha \in \Delta}$ une famille non vide d'idéaux d'un anneau principal A . Alors cette famille possède un élément maximal. C'est-à-dire il existe $\alpha_0 \in \Delta$ tel que pour tout $\alpha \in \Delta$,

$$I_{\alpha_0} \subset I_\alpha \implies I_{\alpha_0} = I_\alpha.$$

Démonstration. Supposons qu'il n'existe pas de tel α_0 . Alors il existe une suite

$$I_{\alpha_1} \subsetneq I_{\alpha_2} \subsetneq I_{\alpha_3} \subsetneq \dots$$

avec $\alpha_i \in \Delta$. Considérons l'idéal $I = \bigcup_{i \geq 1} I_{\alpha_i}$. (La vérification du fait que c'est bien un idéal est laissée en exercice.) Puisque A est principal, il existe $x \in A$ tel que $I = (x)$. Puisque x appartient à cette union, il existe n tel que $x \in I_{\alpha_n}$. En particulier $(x) = I \subset I_{\alpha_n}$ et

$$I_{\alpha_n} = I_{\alpha_{n+1}} = I_{\alpha_{n+2}} = \dots = I,$$

une contradiction. ■

Preuve du Théorème 2.54. Existence : On montre d'abord que tout $a \in A \setminus \{0\}$ est un produit d'éléments irréductibles. Soit

$$Y \subset A \setminus \{0\}$$

l'ensemble des éléments de A qui n'ont pas la forme $u \cdot p_1 \cdot \dots \cdot p_k$, pour $u \in U(A)$ et $p_1, \dots, p_k \in \text{Irr}(A)$. À voir : $Y = \emptyset$. On considère la famille d'idéaux $\{(y)\}_{y \in Y}$. Si $Y \neq \emptyset$ alors cette famille possède un élément (y_0) maximal (au sens du Lemme 2.55). L'élément $y_0 \in Y$ n'est en particulier pas irréductible et n'est pas une unité. Il existe donc $a, b \in A$, $a, b \notin U(A)$ tels que $y_0 = ab$. Puisque $b \notin U(A)$, l'inclusion $(y_0) \subsetneq (a)$ est stricte de sorte que $a \notin Y$ par maximalité de (y_0) . De même, par symétrie, $b \notin Y$. Il en découle que $a = u \cdot p_1 \dots p_k$, $b = v \cdot q_1 \dots q_\ell$ et donc $y_0 = (uv) \cdot p_1 \dots p_k q_1 \dots q_\ell$ pour $p_1, \dots, p_k, q_1, \dots, q_\ell \in \text{Irr}(A)$ et $y_0 \notin Y$, ce qui montre que $Y = \emptyset$.

Unicité : On montre par induction sur $m = \min\{k, \ell\}$ que si

$$u \cdot p_1 \cdot \dots \cdot p_k = v \cdot q_1 \cdot \dots \cdot q_\ell,$$

avec $u, v \in U(A)$ et $p_i, q_i \in \text{Irr}(A)$, alors $k = \ell$ et il existe une permutation $\sigma \in \text{Sym}(k)$ et des unités $u_i \in U(A)$ tels que

$$q_{\sigma(i)} = u_i \cdot p_i,$$

pour tous $1 \leq i \leq k$.

Supposons $m = \min\{k, \ell\} = 0$. Par symétrie on peut supposer que $k = 0$. Alors

$$u = v \cdot q_1 \cdot \dots \cdot q_\ell$$

et donc

$$1 = u^{-1} \cdot v \cdot q_1 \cdot \dots \cdot q_\ell,$$

et $q_i \in U(A)$, ce qui est impossible et implique $\ell = 0$.

Supposons

$$x = u \cdot p_1 \cdot \dots \cdot p_k = v \cdot q_1 \cdot \dots \cdot q_\ell$$

avec $m = \min\{k, \ell\} > 0$ et l'unicité démontrée pour un nombre minimal de facteurs irréductibles égal à $m - 1$. En particulier, $k, \ell \geq 1$. Observons que p_1 est premier car p_1 est irréductible et A est principal. En conséquence, puisque p_1 divise x et ne divise pas l'unité u , il divise un des facteurs q_i . Quitte à renuméroter les q_1, \dots, q_ℓ on peut supposer que c'est q_1 . Il existe donc $b \in A$ tel que $q_1 = bp_1$, mais puisque q_1 est irréductible, $b = u_1 \in U(A)$. On a donc

$$\begin{aligned} p_1 \cdot p_2 \cdot \dots \cdot p_k &= (p_1 \cdot u_1) \cdot q_2 \cdot \dots \cdot q_\ell \\ &= p_1 \cdot (u_1 \cdot q_2) \cdot \dots \cdot q_\ell. \end{aligned}$$

Puisque A est intègre, il découle que

$$p_2 \cdot \dots \cdot p_k = (u \cdot q_2) \cdot \dots \cdot q_\ell.$$

Observons que $u_1 q_2 \in \text{Irr}(A)$ et diffère d'un p_i par une unité si et seulement si q_2 diffère de p_i par une unité, de sorte que l'unicité est établie par induction. ■

2.6 L'anneau des polynômes

Soit A un anneau commutatif. Rappelons que l'anneau commutatif des polynômes $A[X]$ à coefficients dans A est formellement défini comme les suites (a_0, a_1, a_2, \dots) avec $a_i \in A$ et $a_i \neq 0$ pour un nombre fini de $i \geq 0$. Un élément $(a_0, \dots, a_n, 0, 0, 0, \dots)$ s'écrit

$$a_0 + a_1X + a_2X^2 + \dots + a_nX^n.$$

L'addition et la multiplication sur $A[X]$ définies dans l'Exemple 2.2.4, induites de l'addition et multiplication de polynômes usuelles font de $A[X]$ un anneau commutatif (car A est supposé commutatif).

Il est clair qu'il existe toujours un homomorphisme d'anneaux injectif

$$\begin{aligned} \iota_A : A &\longrightarrow A[X] \\ a &\longmapsto (a, 0, 0, \dots) = a + 0 \cdot X + 0 \cdot X^2 + \dots = a. \end{aligned}$$

Ceci nous permet d'identifier A à un sous-anneau de $A[X]$ et on appelle un élément $a = \iota_A(a)$ de l'image un *polynôme constant*.

Lemme 2.56 Soient A, B deux anneaux commutatifs. Tout homomorphisme d'anneau $\varphi : A \rightarrow B$ induit un homomorphisme d'anneaux $\bar{\varphi} : A[X] \rightarrow B[X]$ tel que

$$\iota_B \circ \varphi = \bar{\varphi} \circ \iota_A.$$

Démonstration. Exercice. ■

Définition 2.57 Soient A un anneau et $f(X) = a_0 + a_1X + \dots + a_nX^n \in A[X]$ avec $a_n \neq 0$. Le *degré* de $f(x)$ est l'entier $\deg(f) = n$ et on appelle a_n *coefficient dominant*.

Nous n'avons pas défini le degré du polynôme 0. Si on voulait le définir, il faudrait poser $\deg(0) := -\infty$ pour que tous les énoncés ci-dessous gardent leur sens.

Soient $f, g \in A[X] \setminus \{0\}$. Il est clair qu'on a toujours l'inégalité

$$\deg(f + g) \leq \max(\deg(f), \deg(g)).$$

Dans la preuve de la proposition suivante, nous verrons aussi que

$$\deg(fg) \leq \deg(f) + \deg(g),$$

et que cette inégalité devient une égalité quand A est intègre.

Proposition 2.58 Soit A un anneau intègre. Alors

1. $A[X]$ est intègre et $\deg(fg) = \deg(f) + \deg(g)$ pour tous $f, g \in A[X] \setminus \{0\}$,
2. $U(A[X]) = \iota_A(U(A))$.

Démonstration. 1. Soient $f, g \in A[X] \setminus \{0\}$. A voir : $f \cdot g \neq 0$. Soient n et m les degrés de f et g respectivement, de sorte que

$$\begin{aligned} f(X) &= a_0 + a_1X + \cdots + a_nX^n, & a_n &\neq 0 \\ g(X) &= b_0 + b_1X + \cdots + b_mX^m, & b_m &\neq 0. \end{aligned}$$

Le produit $f \cdot g$ s'obtient comme

$$(f \cdot g)(X) = \sum_{k \geq 0} \underbrace{\left(\sum_{i=0}^k a_i b_{k-i} \right)}_{c_k} X^k.$$

Si $k > n + m$ alors

$$c_k = \sum_{i=0}^n a_i \underbrace{b_{k-i}}_{=0} + \sum_{i=n+1}^k \underbrace{a_i}_{=0} b_{k-i} = 0,$$

puisque dans la première somme $k - i > n + m - i \geq m$ et $b_{k-i} = 0$ et dans la deuxième somme, $i > n$ de sorte que $a_i = 0$. Similairement

$$c_{n+m} = \sum_{i=0}^{n-1} a_i \underbrace{b_{n+m-i}}_{=0} + a_n b_m + \sum_{i=n+1}^{n+m} \underbrace{a_i}_{=0} b_{n+m-i} = a_n b_m \neq 0,$$

puisque A est intègre et $a_n, b_m \neq 0$. En particulier, $f \cdot g \neq 0$ et $\deg(fg) = \deg(f) + \deg(g)$.

2. Clairement, si $u \in U(A)$ alors $\iota_A(u) \in U(A[X])$. Supposons $f \in U(A[X])$. Il existe $g \in A[X]$ tel que $f \cdot g = 1$. Alors

$$0 = \deg(1) = \deg(f \cdot g) = \deg(f) + \deg(g),$$

où l'on a utilisé l'égalité démontrée dans le premier point du Lemme. Puisque $\deg(f), \deg(g) \geq 0$, cette égalité implique que $\deg(f) = \deg(g) = 0$. Donc $f = \iota_A(a)$ et $g = \iota_A(b)$, pour $a, b \in A$. L'égalité

$$\iota_A(1) = 1 = f \cdot g = \iota_A(a) \cdot \iota_A(b)$$

implique maintenant par injectivité de ι_A que $a \cdot b = 1$ et $a \in U(A)$. ■

Théorème 2.59 (Division polynômiale) Soit A un anneau intègre. Soit $g \in A[X]$ un polynôme dont le coefficient dominant est une unité. Alors pour tout $f \in A[X]$ il existe des uniques $q, r \in A[X]$ tels que

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

Démonstration. Unicité : Supposons que $g \cdot q + r = f = g \cdot q' + r'$ avec $r = 0$ ou $\deg(r) < \deg(g)$ et de même $r' = 0$ ou $\deg(r') < \deg(g)$. Alors

$$g(q - q') = r' - r.$$

Supposons que $r' \neq r$. Alors

$$\deg(g) > \deg(r' - r) = \deg(g(q - q')) = \deg(g) + \deg(q - q'),$$

ce qui est impossible puisque $\deg(q - q') \geq 0$. Donc $r = r'$ et $g(q - q') = 0$. Mais comme $A[X]$ est intègre et $g \neq 0$, ceci implique bien que $q - q' = 0$.

Existence : Par induction sur $\deg(f)$. Si $f = 0$ il n'y a rien à montrer : prendre $q = r = 0$. Si $\deg(f) = 0$ de sorte que $f(X) = a_0$ il y a deux cas :

- $\deg(g) \geq 1$: prendre $q = 0$ et $r = f$, ce qui donne bien $\deg(r) = \deg(f) = 0 < 1 \leq \deg(g)$.
- $\deg(g) = 0$: Puisque le coefficient dominant de g est une unité, $g(x) = u$ avec $u \in U(A)$. On prend $q(X) = u^{-1} \cdot f(X)$ et $r = 0$.

Soit $\deg(f) = n \geq 1$ et supposons le théorème démontré pour tous les polynômes de degré $\leq n - 1$. Comme pour le cas $\deg(f) = 0$ on distingue deux cas :

- $\deg(f) < \deg(g)$: prendre $q = 0$ et $r = f$.
- $n = \deg(f) \geq \deg(g) = m$: On a

$$\begin{aligned} f(X) &= a_0 + a_1X + \cdots + a_nX^n, & a_n &\neq 0 \\ g(X) &= b_0 + b_1X + \cdots + b_mX^m, & b_m &\in U(A). \end{aligned}$$

On pose

$$h(X) = f(X) - g(X)a_nb_m^{-1}X^{n-m}.$$

Si $h = 0$ alors $f = g \cdot q$ pour $q = a_nb_m^{-1}X^{n-m}$. Si $h \neq 0$ alors $\deg(h) \leq \deg(f) - 1$. Par hypothèse d'induction, il existe $q', r' \in A[X]$ tels que $h = g \cdot q' + r'$ avec $r' = 0$ ou $\deg(r') < \deg(g)$. Finalement

$$\begin{aligned} f(X) &= h(X) + g(X)a_nb_m^{-1}X^{n-m} \\ &= g(X)(q'(X) + a_nb_m^{-1}X^{n-m}) + r'(X), \end{aligned}$$

et l'on a bien la division attendue avec $q(X) = q'(X) + a_nb_m^{-1}X^{n-m}$ et $r(X) = r'(X)$. ■

Un polynôme dans $A[X]$ n'est en général pas une application de A dans A , mais il en définit une. Soyons plus précis. Rappelons que l'ensemble $\text{Map}(A, A)$ des applications de A dans A est un anneau pour l'addition et la multiplication de fonctions. Il existe toujours un homomorphisme d'anneaux

$$\begin{aligned} \varphi : A[X] &\longrightarrow \text{Map}(A, A) \\ f(X) &\longmapsto \{b \mapsto f(b) := \sum_{i \geq 0} a_i b^i\} \end{aligned}$$

mais cet homomorphisme n'est pas injectif en général. En effet, $f(X) = X + X^2 \in \mathbb{Z}/2\mathbb{Z}[X]$ est un polynôme non nul mais son image par φ est la fonction envoyant $\bar{0}$ sur $f(\bar{0}) = \bar{0} + \bar{0}^2 = \bar{0}$ et $\bar{1}$ sur $f(\bar{1}) = \bar{1} + \bar{1}^2 = \bar{1} + \bar{1} = \bar{0}$, c'est donc la fonction identiquement nulle. Nous ne pouvons donc pas identifier $A[X]$ à son image par φ en général. Mais nous verrons que φ est un homomorphisme injectif si A est un anneau intègre infini.

Définition 2.60 Un élément $a \in A$ est une *racine* (ou un *zéro*) du polynôme $f \in A[X] \setminus \{0\}$ si $f(a) = 0$.

Lemme 2.61 Soient A un anneau intègre et $a \in A$ une racine de $f \in A[X] \setminus \{0\}$. Alors il existe $g \in A[X]$ tel que

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

Observons qu'en particulier $\deg(g) = \deg(f) - 1$.

Démonstration. Le polynôme $X - a$ a degré 1 et son coefficient dominant est l'unité $1 \in U(A)$. Nous pouvons donc appliquer la division du Théorème 2.59 de sorte qu'il existe $g, r \in A[X]$ tels que

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

Si $\deg(r) < \deg(X - a) = 1$ alors $\deg(r) = 0$ et $r(X) = r_0$ pour un $r_0 \in A$. Mais

$$0 = f(a) = g(a)(a - a) + r(a) = r(a) = r_0$$

et $r = 0$. ■

Théorème 2.62 Soient A un anneau intègre et $f \in A[X] \setminus \{0\}$ de degré n . Alors f a au plus n racines dans A .

Démonstration. Induction sur n . Si $n = 0$ alors f est une constante non nulle et n'a aucune racine. Soit $n \geq 1$ et supposons le théorème démontré pour tous les polynômes de degré $\leq n - 1$. Si f n'a pas de racine il n'y a rien à montrer. Supposons que f a une racine $a \in A$. Alors par le Lemme 2.61 il existe $g \in A[X]$ tel que $f(X) = g(X)(X - a)$. Soit $a' \in A$ une racine de f quelconque. Alors

$$0 = f(a') = g(a')(a' - a).$$

Puisque A est intègre, ceci implique soit que $g(a') = 0$ et a' est une racine de g , soit que $a' = a$. En particulier, les racines de f sont contenues dans l'ensemble des racines de g union $\{a\}$. Par induction il y en a au plus $(n - 1) + 1 = n$. ■

Observons que ce théorème est faux si l'anneau n'est pas intègre : $2X + 2X^2 \in \mathbb{Z}/8\mathbb{Z}$ a degré 2 mais 4 racines $\overline{0}, \overline{3}, \overline{4}, \overline{7} = \overline{-1}$.

Proposition 2.63 Soit A un anneau intègre infini. Alors l'homomorphisme d'anneaux

$$\begin{aligned} \varphi : A[X] &\longrightarrow \text{Map}(A, A) \\ f(X) &\longmapsto \{b \mapsto f(b) := \sum_{i \geq 0} a_i b^i\} \end{aligned}$$

est injectif.

Démonstration. Soit $0 \neq f \in A[X]$ de degré n . Si $\varphi(f) = 0$ alors $f(a) = 0$ pour tout $a \in A$ et puisque A est infini, f a un nombre infini de racines, ce qui contredit le fait que f a au plus n racines établi au Théorème 2.62. ■

Voyons à présent une application extrêmement utile du Théorème 2.62 nous informant précisément sur la structure du groupe des unités d'un corps fini :

Théorème 2.64 Soit K un corps fini. Alors $U(K) = K \setminus \{0\}$ est un groupe cyclique.

Un cas particulier déjà largement non trivial est le cas de $K = \mathbb{Z}/p\mathbb{Z}$ pour p premier :

Corollaire 2.65 Soit $p \in \mathbb{N}$ premier. Alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est un groupe cyclique (d'ordre $p - 1$).

Pour information, on peut plus généralement montrer que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n = 2, 4, p^k$ ou $2p^k$ pour un premier p impair.

Par exemple, pour $p = 5$, le groupe des unités est $\{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ et on vérifie facilement que $\bar{2}$ (et $\bar{3}$) sont des générateurs. En effet $\bar{2}^2 = \bar{4}$, $\bar{2}^3 = \bar{3}$ et $\bar{2}^4 = \bar{1}$. Par conséquent, $(\mathbb{Z}/5\mathbb{Z})^\times = \langle \bar{2} \rangle \cong C_4$. En contraste $(\mathbb{Z}/8\mathbb{Z})^\times$ n'est pas cyclique. C'est aussi un groupe d'ordre 4 puisque $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$, mais tous ses éléments différents de $\bar{1}$ ont ordre 2, de sorte que ce groupe est isomorphe à $C_2 \times C_2$.

Dans la preuve du Théorème 2.64 nous aurons besoin de l'observation suivante :

Lemme 2.66 Soit A un groupe abélien. S'il existe deux éléments d'ordre m et n dans A alors A possède un élément d'ordre $\text{ppcm}(m, n)$.

Notons que cet élément d'ordre $\text{ppcm}(m, n)$ n'est en général pas le produit des éléments d'ordre m et n . Par exemple on pourrait prendre un élément a d'ordre $m > 1$ et son inverse a^{-1} qui a aussi ordre m et leur produit aa^{-1} a ordre 1, et non $\text{ppcm}(m, m) = m$. C'est néanmoins le cas pour le produit de deux cycles de support disjoints, ou en toute généralité, quand $\text{pgcd}(m, n) = 1$, qui est la première étape de la preuve de ce lemme.

Démonstration. Montrons d'abord le cas où $\text{pgcd}(m, n) = 1$. Soit $a \in A$ d'ordre m et $b \in A$ d'ordre n . Montrons que ab a ordre mn . Il est clair que $(ab)^{mn} = e$. Supposons que $(ab)^k = e$ pour $k > 0$. Alors $a^k = b^{-k}$. Cette expression à la puissance n donne

$$a^{nk} = (a^k)^n = (b^{-k})^n = (b^n)^{-k} = e.$$

On en déduit que l'ordre de a divise nk , c'est-à-dire $m \mid nk$. Puisque $\text{pgcd}(m, n) = 1$, ceci implique que $m \mid k$. Par symétrie, on a aussi $n \mid k$, et donc, utilisant encore le fait que $\text{pgcd}(m, n) = 1$, que $mn \mid k$ de sorte que $\text{ord}(ab) = mn = \text{ppcm}(m, n)$.

Avant de poursuivre avec le cas général, observons que si il existe dans A un élément d'ordre n , alors il existe un élément d'ordre k pour tout $k \mid n$.

Soient maintenant $m = \prod_{i=1}^k p_i^{r_i}$ et $n = \prod_{i=1}^k p_i^{s_i}$, où l'on suppose que les p_i sont des nombres premiers tous distincts. Observons que

$$\text{ppcm}(m, n) = \prod_{i=1}^k p_i^{\max(r_i, s_i)}.$$

Quitte à réordonner ces factorisations, on peut supposer qu'il existe $1 \leq \ell \leq k$ tel que $r_i > s_i$ pour $i \leq \ell$ et $r_i \leq s_i$ pour $i > \ell$ de sorte que

$$\text{ppcm}(m, n) = \prod_{i=1}^{\ell} p_i^{r_i} \cdot \prod_{i=\ell+1}^k p_i^{s_i}.$$

Posons

$$p = \prod_{i=1}^{\ell} p_i^{r_i} \quad \text{et} \quad q = \prod_{i=\ell+1}^k p_i^{s_i}$$

et observons que $pq = \text{ppcm}(m, n)$ et $\text{pgcd}(p, q) = 1$. Il est clair que $p \mid m$ et $q \mid n$ de sorte qu'il existe des éléments d'ordre p et q dans A et il existe donc par le cas particulier démontré ci-dessus un élément d'ordre pq dans A . ■

Démonstration du Théorème 2.64. Posons $q = |K|$. Soient k_1, \dots, k_{q-1} les ordres des $q-1$ éléments de $U(K) = K \setminus \{0\}$. Alors par le Lemme 2.66 il existe un élément d'ordre $m = \text{ppcm}(k_1, \dots, k_{q-1})$. Donc d'une part il existe i tel que $k_i = m$ et d'autre part $k_j \mid (q-1)$ pour tous $1 \leq j \leq q-1$. En particulier m divise l'ordre du groupe $q-1$, et $m \leq q-1$. Le polynôme $f(X) = X^m - 1$ a $q-1$ racines dans K ce qui implique par le Théorème 2.62 que $q-1 \leq m$. On en conclut que $m = q-1$. ■

Éléments irréductibles dans $K[X]$

Soit K un corps. Nous verrons dans le prochain paragraphe que $K[X]$ est principal, ce qui implique, par le Théorème 2.54, que $K[X]$ est factoriel. L'étude des polynômes irréductibles est donc cruciale pour la décomposition de polynômes arbitraires.

Observons qu'un polynôme $f(X) \in K[X]$ est une unité si et seulement si il a degré 0.

Lemme 2.67 Soit K un corps. Un polynôme $a + bX$ de degré 1 est irréductible.

Démonstration. Si $a + bX = g(X)h(X)$, alors $1 = \deg(g) + \deg(h)$ de sorte que g ou h a degré 0 et est une unité. ■

Polynômes irréductibles dans $\mathbb{C}[X]$

Pour pouvoir caractériser les polynômes irréductibles de $\mathbb{C}[X]$ nous aurons besoin du

Théorème 2.68 — Théorème Fondamental de l'Algèbre. Soit $f(X) \in \mathbb{C}[X] \setminus \{0\}$. Alors f a une racine dans \mathbb{C} .

Ce théorème, malgré son nom, n'est pas un résultat algébrique. Il n'en existe en effet aucune preuve purement algébrique. Toutes les nombreuses preuves existantes reposent sur un argument de continuité. La preuve ci-dessous est peut-être la preuve la moins

technologique, reposant sur un minimum de notions d'analyse. Elle est aussi et de loin bien moins élégante que les preuves que l'on peut produire avec un peu de topologie ou d'analyse complexe.

Démonstration. 1ère étape : Montrons qu'il existe $r > 0$ tel que $|f(z)| \geq |f(0)|$ pour $|z| \geq r$. Sans restreindre la généralité, nous pouvons supposer que le coefficient dominant de f est 1. Ecrivons

$$f(X) = a_0 + a_1X + \dots + a_{n-1}X^{n-1} + X^n.$$

Soit $r \in \mathbb{R}$ tel que

$$r \geq \max \left\{ \sqrt[n]{|a_0|2n}, \dots, \sqrt[n]{|a_{n-2}|2n}, |a_{n-1}|2n \right\}$$

Soit $z \in \mathbb{C}$ tel que $|z| \geq r$. Alors

$$\begin{aligned} |f(z)| &= |z|^n \left| 1 + \frac{a_{n-1}}{z} + \dots + \frac{a_0}{z^n} \right| \\ &\geq |z|^n \left(1 - \left| \frac{a_{n-1}}{z} + \dots + \frac{a_0}{z^n} \right| \right). \end{aligned}$$

Mais

$$\begin{aligned} \left| \frac{a_{n-1}}{z} + \dots + \frac{a_0}{z^n} \right| &\leq \frac{|a_{n-1}|}{|z|} + \dots + \frac{|a_0|}{|z|^n} \\ &\leq \frac{|a_{n-1}|}{r} + \dots + \frac{|a_0|}{r^n} \\ &\leq \frac{1}{2}, \end{aligned}$$

puisque $\frac{|a_{n-k}|}{r^k} \leq 1/(2n)$ pour $1 \leq k \leq n$ par notre hypothèse sur r . On conclut que

$$|f(z)| \geq \frac{|z|^n}{2} \geq \frac{r^n}{2} \geq n|a_0| \geq |a_0| = |f(0)|.$$

2ème étape : La fonction

$$\begin{aligned} \mathbb{C} &\longrightarrow \mathbb{R} \\ z &\longmapsto |f(z)| \end{aligned}$$

possède un minimum global. En effet, si on restreint cette fonction (continue) à la boule fermée $\overline{B(0, r)}$ alors elle admet un minimum $z_0 \in \overline{B(0, r)}$ puisque toute fonction continue à valeur réelle définie sur un compact admet un minimum (cf Théorème 27 du Polycopié d'Analyse). Puisque par la première étape $|f(z)| \geq |f(0)| = |f(z_0)|$, ce minimum est un minimum global.

3ème étape : $f(z_0) = 0$. Le développement de Taylor de f en z_0 donne

$$f(z) = f(z_0) + c_1(z - z_0) + \dots + c_n(z - z_0)^n.$$

Soit $k \geq 1$ tel que $c_k \neq 0$ et $c_i = 0$ pour $1 \leq i \leq k$, de sorte que

$$f(z) = f(z_0) + c_k(z - z_0)^k + \dots + c_n(z - z_0)^n.$$

Supposons $f(z_0) \neq 0$ et soit $a \in \mathbb{C}^*$ tel que $c_k a^k = -f(z_0)$. Soit $0 \leq t$ et

$$\begin{aligned} f(z_0 + ta) &= f(z_0) + c_k (ta)^k + \dots + c_n (ta)^n \\ &= f(z_0)(1 - t^k) + t^{k+1} \cdot g(t), \end{aligned}$$

où $g(t)$ est un polynôme (à coefficients complexes et de degré $n - k - 1$). Observons que puisque $g : [0, 1] \rightarrow \mathbb{C}$ est continue, il existe $C_0 \in \mathbb{R}_{\geq 0}$ tel que $|g(t)| \leq C_0$ pour tout $t \in [0, 1]$.

Finalement, pour tout $0 < t \leq \min\{1, |f(z_0)|/2C_0\}$, on a

$$\begin{aligned} |f(z_0 + ta)| &= |f(z_0)(1 - t^k) + t^{k+1} \cdot g(t)| \\ &\leq |f(z_0)(1 - t^k) + t^{k+1}| |g(t)| \\ &\leq |f(z_0)(1 - t^k) + t^{k+1}| C_0 \\ &\leq |f(z_0)| (1 - t^k) + t^k \frac{|f(z_0)|}{2} \\ &= |f(z_0)| \left(1 - \frac{t^k}{2}\right) \\ &< |f(z_0)|, \end{aligned}$$

ce qui contredit la minimalité de $|f(z_0)|$ et conclut la preuve. ■

Corollaire 2.69 Un polynôme est irréductible dans $\mathbb{C}[X]$ si et seulement si il a degré 1.

Démonstration. Une direction de cette équivalence est donnée par le Lemme 2.67. Pour l'autre direction, soit $f(X) \in \mathbb{C}[X] \setminus \{0\}$ un polynôme. Si $\deg(f) = 0$ alors f est une unité, puisque $f \in \iota_{\mathbb{C}}(\mathbb{C} \setminus \{0\}) = \iota_{\mathbb{C}}(U(\mathbb{C})) = U(\mathbb{C}[X])$. Si $\deg(f) \geq 2$, alors f a une racine $a \in \mathbb{C}$ par le Théorème Fondamental de l'Algèbre, et il existe par le Lemme 2.61 un polynôme $g(x) \in \mathbb{C}[X]$ tel que

$$f(X) = g(X)(X - a). \quad (2.1)$$

Aucun des facteurs n'est une unité puisqu'ils ont tous les deux degré ≥ 1 . En effet, le degré de g est $\deg(f) - 1 \geq 1$. ■

Corollaire 2.70 Tout polynôme $f(X) \in \mathbb{C}[X] \setminus \{0\}$ se décompose de façon unique comme

$$f(X) = c(X - a_1) \cdot \dots \cdot (X - a_n),$$

où $n = \deg(f)$, $c \in \mathbb{C}^*$ et $a_1, \dots, a_n \in \mathbb{C}$ sont les n racines de f (comptées avec multiplicité).

Démonstration. Découle du Corollaire 2.69 combiné avec le fait que $\mathbb{C}[X]$ est factoriel qui sera démontré dans le prochain paragraphe. ■

Polynômes irréductibles dans $\mathbb{R}[X]$

Avant de caractériser les polynômes irréductibles dans $\mathbb{R}[X]$, rappelons une formule bien connue :

Lemme 2.71 — Formule de Viète. Soit $f(X) = aX^2 + bX + c$ avec $a, b, c \in \mathbb{R}$ et $a \neq 0$. Alors les racines complexes de f sont

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Elles sont réelles si et seulement si $b^2 - 4ac \geq 0$.

Démonstration non constructive. On vérifie facilement que dans $\mathbb{C}[X]$ on a la factorisation

$$f(X) = a \left(X - \frac{-b + \sqrt{b^2 - 4ac}}{2a} \right) \left(X + \frac{-b - \sqrt{b^2 - 4ac}}{2a} \right).$$

Puisque la factorisation est unique, les deux racines de f sont $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. ■

Démonstration constructive. Quitte à diviser f par a , on peut sans restreindre la généralité supposer que $a = 1$. La première étape de la preuve consiste en ce qu'on appelle la complétion en carré de $X^2 + bX$, c'est-à-dire réécrire $f(X) = X^2 + bX + c$ comme $(X + d)^2 + e$, avec $d, e \in \mathbb{R}$. On a

$$\begin{aligned} f(X) = X^2 + bX + c &= \left(X^2 + bX + \left(\frac{b}{2} \right)^2 \right) - \left(\frac{b}{2} \right)^2 + c \\ &= \left(X + \frac{b}{2} \right)^2 - \frac{b^2 - 4c}{4}. \end{aligned}$$

Posons $\Delta := b^2 - 4c$ de sorte que

$$f(X) = \left(X + \frac{b}{2} \right)^2 - \frac{\Delta}{4}.$$

Si $f(r) = 0$ pour $r \in \mathbb{C}$, alors

$$\left(r + \frac{b}{2} \right)^2 = \frac{\Delta}{4}$$

et donc

$$r + \frac{b}{2} = \pm \sqrt{\frac{\Delta}{4}}$$

et

$$r = -\frac{b}{2} \pm \sqrt{\frac{\Delta}{4}} = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Si $\Delta = b^2 - 4c < 0$, alors pour tout $r \in \mathbb{R}$,

$$f(r) = \underbrace{\left(r + \frac{b}{2} \right)^2}_{\geq 0} - \underbrace{\frac{\Delta}{4}}_{> 0} > 0,$$

et il n'y a pas de racines. ■

Théorème 2.72 Un polynôme $f(X)$ est irréductible dans $\mathbb{R}[X]$ si et seulement si

- $\deg(f) = 1$, ou
- $\deg(f) = 2$ et si $f(X) = aX^2 + bX + c$, alors

$$b^2 - 4ac < 0.$$

Démonstration. \Leftarrow : Si $f(X)$ a degré 1 il est irréductible par le Lemme 2.67. Si $f(X) = aX^2 + bX + c$ a degré 2, il est irréductible si et seulement si il n'est pas un produit de deux polynômes de degré 1, autrement dit si et seulement si il n'a pas de racines dans \mathbb{R} . Par Viète, ceci est équivalent à $b^2 - 4ac < 0$.

\Rightarrow : Il reste à montrer qu'un polynôme de degré ≥ 3 n'est pas irréductible. Si f a une racine réelle, alors f n'est pas irréductible par le Lemme 2.61. Supposons que ce n'est pas le cas. Pour toute racine $\alpha \in \mathbb{C} \setminus \mathbb{R}$ de f , le conjugué $\bar{\alpha}$ est aussi une racine de f puisque pour un polynôme à coefficients réels,

$$f(\bar{\alpha}) = \overline{f(\alpha)}.$$

Par conséquent, les $\deg(f)$ racines complexes de f viennent par paire $\alpha, \bar{\alpha}$. En particulier

$$f(X) = c(X - \alpha_1)(X - \bar{\alpha}_1) \cdot \dots \cdot (X - \alpha_k)(X - \bar{\alpha}_k),$$

où $2k = n = \deg(f)$ et $c = a_n \in \mathbb{R}$. Finalement observons que pour tout $\alpha \in \mathbb{C}$,

$$(X - \alpha)(X - \bar{\alpha}) = X^2 - 2\operatorname{Re}(\alpha)X + |\alpha|^2 \in \mathbb{R}[X]$$

de sorte que f est un produit de k polynômes à coefficients réels de degré 2 et est donc non irréductible. ■

Polynômes irréductibles dans $\mathbb{Q}[X]$

L'analyse des polynômes irréductibles à coefficients rationnels est beaucoup plus subtile que le cas complexe ou même réel. Il n'existe pas de caractérisation globale, mais seulement divers critères, s'appliquant au cas par cas, permettant de déterminer, quand certaines hypothèses sont réunies, qu'un polynôme est irréductible. Nous en verrons deux : Le critère d'Eisenstein, Théorème 2.75, et le critère de réduction, Théorème 2.76.

Rappelons le peu que nous savons déjà : Soit $f \in \mathbb{Q}[X] \setminus \{0\}$.

- $\deg(f) = 0$ si et seulement si $f \in U(\mathbb{Q}[X])$. En particulier f n'est pas irréductible.
- Si $\deg(f) = 1$ alors f est irréductible (Lemme 2.67).
- Si f possède une racine dans \mathbb{Q} alors f n'est pas irréductible.

Observons que $f(X)$ est irréductible dans $\mathbb{Q}[X]$ si et seulement si tout multiple non nul $q \cdot f(X)$ est irréductible, pour $q \in \mathbb{Q}^*$. En particulier, en prenant $q \in \mathbb{N}$ égal au plus petit commun multiple des dénominateurs des coefficients de f , on peut toujours se ramener au cas où notre polynôme a coefficients entiers. On aimerait maintenant pouvoir déduire qu'un polynôme $f(X) \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Q}[X]$ si et seulement si il l'est dans $\mathbb{Z}[X]$. C'est faux en général : Par exemple, $2X - 2$ est irréductible dans \mathbb{Q} mais pas dans $\mathbb{Z}[X]$. Plus généralement, soit $f(X) \in \mathbb{Z}[X]$ un polynôme irréductible dans $\mathbb{Q}[X]$ alors pour tout

$n \in \mathbb{Z} \setminus \{0, \pm 1\}$, le polynôme à coefficients entiers $n \cdot f(X)$ est aussi irréductible dans $\mathbb{Q}[X]$, mais pas dans $\mathbb{Z}[X]$. Le Lemme de Gauss ci-dessous montre que c'est la seule pathologie qui peut se produire, et se résoud facilement en se restreignant aux polynômes primitifs, que nous définissons maintenant :

Définition 2.73 Un polynôme $f(X) = a_0 + a_1X + \dots + a_nX \in \mathbb{Z}[X] \setminus \{0\}$ est *primitif* si

$$\text{pgcd}(a_0, a_1, \dots, a_n) = 1.$$

Pour tout $f(X) = a_0 + a_1X + \dots + a_nX \in \mathbb{Z}[X] \setminus \{0\}$, le polynôme

$$\frac{1}{\text{pgcd}(a_0, a_1, \dots, a_n)} \cdot f(X)$$

est encore dans $\mathbb{Z}[X]$ et est primitif.

Lemme 2.74 — Lemme de Gauss. Soit $f \in \mathbb{Z}[X]$ avec $\deg(f) \geq 1$. Alors f est irréductible dans $\mathbb{Z}[X]$ si et seulement si il est primitif et irréductible dans $\mathbb{Q}[X]$.

L'hypothèse $\deg(f) \geq 1$ est nécessaire puisqu'un polynôme constant $f(X) = p$ pour $p \in \mathbb{N}$ premier est irréductible dans $\mathbb{Z}[X]$, mais n'est ni primitif, ni irréductible dans $\mathbb{Q}[X]$

Démonstration. \Leftarrow : Supposons que $f = g \cdot h$ pour $g, h \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$. Puisque f est irréductible dans $\mathbb{Q}[X]$, l'un des facteurs g ou h est unité et donc de degré 0. Supposons que c'est $g(X) = n \in \mathbb{Z}$. Alors $f(X) = n \cdot h(X)$ et n divise tous les coefficients de f . Puisque f est primitif, ceci implique que $n = \pm 1$ et $g(X) = \pm 1$ est une unité dans $\mathbb{Z}[X]$.

\Rightarrow : Supposons que $f(X) = c_0 + \dots + c_nX^n$ est irréductible dans $\mathbb{Z}[X]$. Montrons d'abord que f est primitif. Posons $q = \text{pgcd}(c_0, \dots, c_n)$. Alors $(1/q) \cdot f(X)$ appartient à $\mathbb{Z}[X]$ et $f = q \cdot ((1/q) \cdot f(X))$, ce qui implique, puisque f est irréductible dans $\mathbb{Z}[X]$ que q est une unité de $\mathbb{Z}[X]$ et donc $q = 1$.

Montrons maintenant que f est irréductible dans $\mathbb{Q}[X]$. Soient $A, B \in \mathbb{Q}[X]$ tels que

$$f(X) = A(X) \cdot B(X).$$

Posons

$$m_A := \text{ppcm}\{\text{dénominateurs des coefficients de } A\},$$

$$m_B := \text{ppcm}\{\text{dénominateurs des coefficients de } B\},$$

de sorte que $m_A \cdot A$ et $m_B \cdot B$ sont des polynômes à coefficients dans $\mathbb{Z}[X]$. Prenons maintenant

$$\ell_A := \text{pgcd}\{\text{coefficients de } m_A \cdot A\},$$

$$\ell_B := \text{pgcd}\{\text{coefficients de } m_B \cdot B\},$$

de sorte que

$$a(X) := \frac{m_A}{\ell_A} \cdot A(X) \quad \text{et} \quad b(X) := \frac{m_B}{\ell_B} \cdot B(X)$$

sont des polynômes primitifs à coefficients entiers. Soient de plus $m, \ell \in \mathbb{Z}$ avec $\text{pgcd}(m, \ell) = 1$ tels que

$$\frac{m}{\ell} = \frac{m_A}{\ell_A} \frac{m_B}{\ell_B}.$$

Observons que

$$f(X) = A(X) \cdot B(X) = \frac{\ell_A}{m_A} \frac{\ell_B}{m_B} a(X) \cdot b(X) = \frac{\ell}{m} a(X) \cdot b(X). \quad (2.2)$$

Affirmation: $\frac{\ell}{m} = \pm 1$.

L'affirmation implique clairement le théorème puisque alors, par irréductibilité de f dans $\mathbb{Z}[X]$, un des facteurs $a(X)$ ou $b(X)$ doit être une unité de $\mathbb{Z}[X]$, disons $a(X) = \pm 1$. Mais alors $A(X) = \pm \frac{\ell_A}{m_A}$ est une unité dans $\mathbb{Q}[X]$ et f est bien irréductible dans $\mathbb{Q}[X]$.

Il ne reste plus qu'à démontrer l'affirmation. L'équation (2.2) est équivalente à

$$mf(X) = \ell a(X) \cdot b(X).$$

En particulier, ℓ divise tous les coefficients de $mf(X)$. Comme on a supposé que $\text{pgcd}(m, \ell) = 1$, ℓ doit diviser tous les coefficients de $f(X)$ et donc aussi le plus grand commun diviseur de ces coefficients, qui est 1 puisque f est primitif. Ceci implique que $\ell = \pm 1$. Sans restreindre la généralité, supposons que $\ell = 1$. Nous avons donc

$$mf(X) = a(X) \cdot b(X).$$

Soit $p \in \mathbb{N}$ un nombre premier divisant m . Considérons l'homomorphisme d'anneaux

$$\pi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}/p\mathbb{Z}[X].$$

Alors puisque a et b sont primitifs, $\pi(a)$ et $\pi(b)$ sont non nuls, et comme l'anneau $\mathbb{Z}/p\mathbb{Z}[X]$ est intègre, leur produit

$$\pi(a \cdot b) = \pi(a) \cdot \pi(b) \neq 0$$

est aussi non nul. Mais puisque $p \mid m$, on a $\pi(m \cdot f) = 0$, une contradiction. Il n'existe donc pas de premier p divisant m , et $m = \pm 1$, ce qui termine la démonstration de l'affirmation et du Théorème. ■

Théorème 2.75 — Critère d'Eisenstein. Soit $f(X) = a_0 + a_1X + \dots + a_nX^n \in \mathbb{Z}[X]$ et $p \in \mathbb{N}$ premier. Si

$$a_n \not\equiv 0 \pmod{p}, \quad a_i \equiv 0 \pmod{p} \quad \forall 0 \leq i \leq n-1, \quad \text{et} \quad a_0 \not\equiv 0 \pmod{p^2}$$

alors $f(X)$ est irréductible dans $\mathbb{Q}[X]$.

Démonstration. Exercice. ■

Par exemple, le Critère d'Eisenstein implique immédiatement que $3X^5 - 15$ (prendre $p = 5$) ou $2X^{10} - 21$ (prendre $p = 3$ ou 7) sont irréductibles. De même si $a \in \mathbb{Z}^*$, $a \neq \pm 1$ n'a pas de facteurs carrés, c'est-à-dire qu'aucun nombre entier au carré ne divise a , alors

$X^n + a$ est irréductible pour tout $n \geq 1$. En effet il suffit d'appliquer le critère d'Eisenstein à un p premier divisant a . Par exemple $X^n \pm 2$ est toujours irréductible.

Dans certains cas où le Critère d'Eisenstein ne s'applique à priori pas, comme par exemple

$$f(X) = 1 + X + \dots + X^{p-1} \in \mathbb{Z}[X],$$

pour un $p \in \mathbb{N}$ premier, il est possible de se ramener à un cas où le critère s'applique par un simple changement de variable. En effet vous verrez en exercice que le critère s'applique à $g(X) := f(X+1)$, impliquant l'irréductibilité de $f(X)$.

Théorème 2.76 — Critère de Réduction. Soient $p \in \mathbb{N}$ un nombre premier et $\pi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}/p\mathbb{Z}[X]$ l'homomorphisme d'anneaux canonique. Soit $f \in \mathbb{Z}[X]$ primitif. Si $\deg(f) = \deg(\pi(f))$ et $\pi(f)$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ alors f est irréductible dans $\mathbb{Q}[X]$.

Démonstration. Par le Lemme de Gauss, il suffit de montrer que f est irréductible dans $\mathbb{Z}[X]$. Supposons que $f(X) = A(X) \cdot B(X)$ avec $A, B \in \mathbb{Z}[X]$. Alors

$$\pi(f) = \pi(A \cdot B) = \pi(A) \cdot \pi(B).$$

Puisque $\pi(f)$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, ceci implique que $\pi(A)$ ou $\pi(B)$ est une unité de $\mathbb{Z}/p\mathbb{Z}[X]$ donc un polynôme de degré 0. Supposons que $\deg(\pi(A)) = 0$. On a toujours l'inégalité

$$\deg(\pi(f)) = \deg(\pi(A)) + \deg(\pi(B)) \leq \deg(A) + \deg(B) = \deg(f).$$

Mais puisque nous avons supposé que $\deg(\pi(f)) = \deg(f)$, on a nécessairement $0 = \deg(\pi(A)) = \deg(A)$ (et aussi $\deg(\pi(B)) = \deg(B)$). Donc $A(X) = n \in \mathbb{Z}$ et $f(X) = nB(X)$. Mais puisque f est primitif, $n = \pm 1$ et A est bien une unité de $\mathbb{Z}[X]$. ■

Par exemple, vous verrez en exercice que les polynômes $X^p - X - 1$ sont irréductibles dans $\mathbb{Z}/p\mathbb{Z}[X]$ pour $p = 2, 3$ et 5 . (C'est vrai plus généralement pour tout premier p). Le Critère de Réduction implique immédiatement que ces polynômes sont irréductibles dans $\mathbb{Q}[X]$.

Notons que le Critère de Réduction ne détectera pas l'irréductibilité de tous les irréductibles de $\mathbb{Q}[X]$, même en considérant tous les nombres premiers p . En effet il existe des polynômes $f(X) \in \mathbb{Z}[X]$, irréductibles dans $\mathbb{Q}[X]$, tels que $\pi(f)$ est réductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ pour tout premier p . Un tel exemple est donné par $f(X) = X^4 + 1$:

$X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$: Par le Lemme de Gauss, il suffit de montrer qu'il est irréductible dans $\mathbb{Z}[X]$. Supposons que $X^4 + 1$ est produit de deux polynômes de degrés $k \leq \ell$ avec $k + \ell = 4$. Le cas $k = 0$ est exclu car $X^4 + 1$ est primitif. Le cas $k = 1$ aussi puisque $X^4 + 1$ n'a clairement pas de racines dans \mathbb{R} (car $x^4 + 1 \geq 1$ pour tout $x \in \mathbb{R}$) et donc dans \mathbb{Q} . Ne reste que le cas $k = \ell = 2$. Soient donc $a, b, c, d \in \mathbb{Z}$ tels que

$$\begin{aligned} X^4 + 1 &= (X^2 + aX + b)(X^2 + cX + d) \\ &= X^4 + (a+c)X^3 + (b+ac+d)X^2 + (ad+bc)X + bd \end{aligned}$$

ou de façon équivalente

$$\begin{cases} a + c = 0 \\ b + ac + d = 0 \\ ad + bc = 0 \\ bd = 1, \end{cases}$$

qui mène à

$$b = d = \pm 1, \quad a = -c \quad \text{et} \quad \pm 2 = 2b = a^2.$$

Puisque ± 2 n'a pas de racine carrée dans \mathbb{Z} , une telle factorisation est impossible.

$X^4 + 1$ n'est pas irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$: Montrons qu'il est toujours possible de factoriser $X^4 + 1$ comme un produit de deux polynômes de degré 2 dans $\mathbb{Z}/p\mathbb{Z}[X]$. On reprend les équations ci-dessus avec $a, b, c, d \in \mathbb{Z}/p\mathbb{Z}$.

Si $a = 0$ on obtient $b = -d$ et $bd = -b^2 = 1$. En particulier, si il existe $u \in \mathbb{Z}/p\mathbb{Z}$ tel que $u^2 = -1$ alors

$$X^4 + 1 = (X^2 + u)(X^2 - u).$$

Si $a \neq 0$ alors $b = d$ et $bd = 1$ mène à $b = d = \pm 1$ et $a^2 = \pm 2$. En particulier, si il existe $u \in \mathbb{Z}/p\mathbb{Z}$ tel que $u^2 = 2$ alors

$$X^4 + 1 = (X^2 + uX + 1)(X^2 - uX + 1),$$

et si il existe $u \in \mathbb{Z}/p\mathbb{Z}$ tel que $u^2 = -2$ alors

$$X^4 + 1 = (X^2 + uX - 1)(X^2 - uX - 1).$$

Il ne reste plus qu'à montrer que l'une de ces trois conditions (l'existence de u tel que $u^2 = -1, 2$ ou -2) est toujours vérifiée pour tout premier p . Pour $p = 2$, on a $1^2 = 1 = -1$. Supposons dorénavant que p est un premier impair. On considère

$$H := \{u^2 \mid u \in (\mathbb{Z}/p\mathbb{Z})^*\}$$

qui est clairement un sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^*$. Nous devons donc vérifier que si ni -1 ni 2 n'appartiennent à H , alors $-2 \in H$. Calculons l'indice de H dans $(\mathbb{Z}/p\mathbb{Z})^*$. Pour ceci, on considère l'homomorphisme surjectif

$$\begin{aligned} f: (\mathbb{Z}/p\mathbb{Z})^* &\longrightarrow H \\ u &\longmapsto u^2. \end{aligned}$$

Le noyau de f est égal à $\{\pm 1\}$ puisque ce sont les seuls éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ satisfaisant $u^2 = 1$, comme nous l'avons déjà vu dans la preuve du Théorème de Wilson. Ceci implique que $|H| = (p-1)/2$ et que $[(\mathbb{Z}/p\mathbb{Z})^* : H] = 2$. Considérons maintenant la projection

$$\pi: (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*/H \cong \{\pm 1\}.$$

Rappelons que $u \in H$ si et seulement si $\pi(u) = 1$. Si -1 et 2 n'appartiennent pas à H alors $\pi(-1) = -1$ et $\pi(2) = -1$. Par conséquent, $\pi(-2) = \pi((-1) \cdot 2) = \pi(-1)\pi(2) = (-1)(-1) = 1$ et -2 appartient à H .

2.7 Anneaux Euclidiens

Définition 2.77 Soit A un anneau intègre. On dit que A est un anneau *euclidien* s'il existe une fonction

$$\delta : A \setminus \{0\} \longrightarrow \mathbb{N}$$

telle que

- $\delta(a) \leq \delta(ab)$ pour tous $a, b \in A \setminus \{0\}$,
- pour tous $a, b \in A, b \neq 0$ il existe $q, r \in A$ tels que

$$a = bq + r \text{ avec } r = 0 \text{ ou bien } \delta(r) < \delta(b).$$

- **Exemples 2.78**
1. \mathbb{Z} est un anneau euclidien pour $\delta(n) = |n|$.
 2. Si \mathbb{K} est un corps, alors $\mathbb{K}[X]$ est un anneau euclidien pour $\delta(f(X)) = \deg(f(x))$.
 3. Un corps \mathbb{K} est un anneau euclidien pour $\delta(x) = 0$ pour tout $x \in \mathbb{K} \setminus \{0\}$.

Lemme 2.79 Soit A un anneau euclidien. Alors

1. $\delta(1) \leq \delta(a)$ pour tous $a \in A \setminus \{0\}$,
2. pour $a \in A \setminus \{0\}$ on a $\delta(1) = \delta(a)$ si et seulement si $a \in U(A)$.

Démonstration.

1. Par la première propriété de la fonction δ , on a $\delta(1) \leq \delta(1 \cdot a) = \delta(a)$.
2. \Leftarrow : Soit $a \in U(A)$. Alors par la première propriété de la fonction δ on a $\delta(a) \leq \delta(aa^{-1}) = \delta(1)$, qui combiné avec le premier point du lemme, donne bien $\delta(a) = \delta(1)$.
 \Rightarrow : Soit $a \neq 0$ avec $\delta(1) = \delta(a)$. Appliquons la deuxième propriété de la fonction δ à 1 et $a \neq 0$. Il existe donc q et r tels que $1 = qa + r$ avec $r = 0$ puisque $\delta(r) < \delta(a) = \delta(1)$ est impossible par le premier point du lemme. ■

■ **Exemple 2.80** L'anneau des entiers de Gauss

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

est euclidien pour

$$\delta(a + ib) = a^2 + b^2 = |a + ib|^2 \in \mathbb{N}.$$

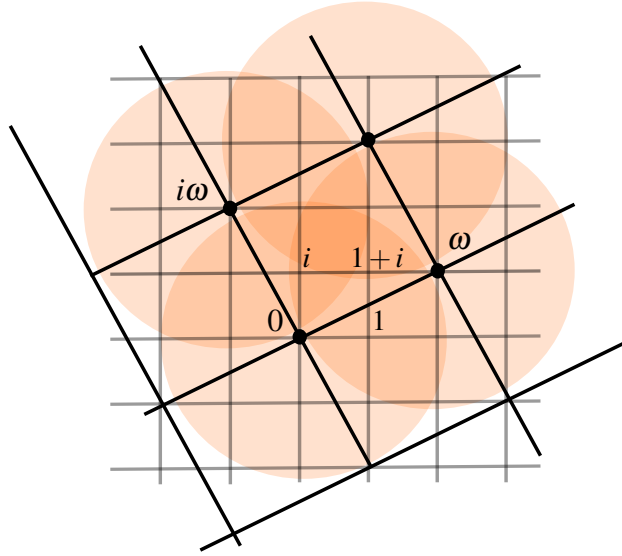
Avant de vérifier que δ fait bien de $\mathbb{Z}[i]$ un anneau euclidien, rappelons que $|z||w| = |zw|$ pour tous $z, w \in \mathbb{C}$. Si $0 \neq w = a + ib \in \mathbb{Z}[i]$ alors $|w| \geq 1$. La première propriété est maintenant évidente : pour tous $z, w \in \mathbb{Z}[i] \setminus \{0\}$ on a bien

$$\delta(z) = |z| \leq |z||w| = |zw| = \delta(zw).$$

Pour la deuxième propriété, soit $w \in \mathbb{Z}[i]$ avec $w \neq 0$. Considérons l'idéal

$$(w) = \{(a + ib)w \mid a, b \in \mathbb{Z}\} = \{aw + b(iw) \mid a, b \in \mathbb{Z}\}.$$

Il consiste en toutes les combinaisons \mathbb{Z} -linéaires de w et iw . Géométriquement, les points de (w) forment ce que l'on appelle un réseau, ce sont les sommets de carrés de côtés de longueur $|w| = \sqrt{\delta(w)}$.



Montrons que pour tout $z \in \mathbb{C}$, il existe un point de $qw \in (w)$ (donc un $q \in \mathbb{Z}[i]$) tel que $\delta(z - qw) < \delta(w)$. Si de plus, $z \in \mathbb{Z}[i]$ alors $r := z - qw \in \mathbb{Z}[i]$ et on a terminé. Géométriquement, ceci veut dire que la distance de qw à z est strictement plus petite que $|w|$. Or il est clair que les disques ouverts centrés en les points de (w) de rayon $|w|$ recouvrent le plan complexe. Voyons ceci algébriquement. L'ensemble $\{w, iw\}$ forme une base de \mathbb{C} considéré comme espace vectoriel réel (de dimension 2). En particulier, tout $z \in \mathbb{C}$ s'écrit comme

$$z = xw + yiw$$

avec $x, y \in \mathbb{R}$. Soient $a, b \in \mathbb{Z}$ tels que $|x - a|, |y - b| \leq 1/2$. Pour $q = a + ib$ on obtient bien

$$\begin{aligned} \delta(z - qw) &= |xw + yiw - (a + ib)w|^2 \\ &= |(x - a) + i(y - b)|^2 |w|^2 = (|x - a|^2 + |y - b|^2) |w|^2 \\ &\leq (1/4 + 1/4) |w|^2 \\ &= \frac{1}{2} \delta(w) < \delta(w), \end{aligned}$$

ce qui termine de démontrer que $\mathbb{Z}[i]$ est euclidien.

Théorème 2.81 Un anneau euclidien est principal.

Puisqu'un anneau principal est factoriel (Théorème 2.54), le corollaire suivant est immédiat.

Corollaire 2.82 Un anneau euclidien est factoriel.

Le théorème se démontre exactement comme le Théorème 1.51, qui classe les sous-groupes de \mathbb{Z} , et du quel on déduit que \mathbb{Z} est principal.

Démonstration du Théorème 2.81. Soit $(0) \neq I < A$ un idéal dans un anneau euclidien A . On pose

$$\mathcal{S} = \{\delta(x) \mid x \in I, x \neq 0\} \subset \mathbb{N}.$$

Puisque $I \setminus \{0\}$ est non vide, \mathcal{S} aussi, et il admet un plus petit élément n_0 . Soit $x_0 \in I$ tel que $\delta(x_0) = n_0$. Voyons que $I = (x_0)$. Il est évident que $(x_0) \subset I$. Montrons que $I \subset (x_0)$. Soit $x \in I$. Par la deuxième propriété de la fonction δ appliquée à x et x_0 il existe $q, r \in A$ tels que $x = qx_0 + r$ avec $r = 0$ ou $\delta(r) < \delta(x_0)$. Puisque $x, x_0 \in I$, le reste $r = x - qx_0$ appartient aussi à I . Ainsi si $r \neq 0$ alors $\delta(r) < \delta(x_0)$ contredit la minimalité de $n_0 = \delta(x_0)$. On a donc $r = 0$ et $x = qx_0 \in (x_0)$. ■

Théorème 2.83 Soit $p \in \mathbb{N}$ premier. Alors il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$ si et seulement si $p = 2$ ou $p \equiv 1 \pmod{4}$.

Par exemple

$$\begin{aligned} 2 &= 1^2 + 1^2 \\ 5 &= 2^2 + 1^2 \\ 13 &= 3^2 + 2^2 \\ 17 &= 4^2 + 1^2, \end{aligned}$$

mais il n'existe pas de $a, b \in \mathbb{Z}$ tels que 3, 7 ou 11 soient égaux à $a^2 + b^2$.

Démonstration. \implies (Première preuve élémentaire) : Puisque les seuls carrés modulo 4 sont $\bar{0}$ et $\bar{1}$ (Lemme A.14) un nombre congru à 3 modulo 4 n'est jamais somme de deux carrés (Lemme A.15).

\implies (Deuxième preuve plus technologique) : Supposons que $p = a^2 + b^2 = (a + ib)(a - ib)$. Remarquons que puisque $\delta(p) = p^2 \neq 1 = \delta(1)$, par le Lemme 2.79, le premier p n'est pas une unité de $\mathbb{Z}[i]$. De plus, comme $a + ib \in U(\mathbb{Z}[i]) = \{\pm 1 \pm i\}$ si et seulement si $a - ib \in U(\mathbb{Z}[i])$, les deux entiers de Gauss $a \pm ib$ ne sont pas non plus des unités sinon leur produit p le serait. En particulier, p n'est pas irréductible ce qui est équivalent à (p) n'est pas premier, et par le Théorème 2.42 $p \neq 3 \pmod{4}$.

\Leftarrow : Supposons que $p \not\equiv 3 \pmod{4}$. Alors $p \in \mathbb{Z}[i]$ n'est pas irréductible. Il existe donc $a + ib, c + id \in \mathbb{Z}[i]$ tels que

$$p = (a + ib)(c + id) \tag{2.3}$$

avec $a + ib, c + id \notin U(\mathbb{Z}[i])$. En particulier, par le Lemme 2.79 $\delta(a + ib), \delta(c + id) \neq 1 = \delta(1)$. Comme

$$p^2 = \delta(p) = \delta(a + ib)\delta(c + id)$$

on a forcément que $p = \delta(a + ib) = a^2 + b^2$ (et de même pour $c + id$). ■

Théorème 2.84 Soit $m = p_1^{k_1} \cdots p_\ell^{k_\ell} \in \mathbb{N}$ avec $p_i \in \mathbb{Z}$ des premiers distincts. Alors m est somme de deux carrés si et seulement si k_i est pair si $p_i \equiv 3 \pmod{4}$.

Démonstration. \implies : Supposons que $p_1^{k_1} \cdots p_\ell^{k_\ell} = m = a^2 + b^2 = (a + ib)(a - ib)$. Supposons qu'il existe un facteur, que l'on suppose par symétrie être p_1 tel que $p_1 \equiv 3 \pmod{4}$.

Voyons que k_1 est pair. Puisque $\mathbb{Z}[i]$ est factoriel et que p^{k_1} divise le produit $(a+ib)(a-ib)$, chaque facteur est un produit

$$a+ib = p_1^{r_1} z_1, \quad a-ib = p_1^{r_2} z_2$$

avec $r_1 + r_2 = k_1$, $z_1, z_2 \in \mathbb{Z}[i]$ tels que p_1 ne divise ni z_1 ni z_2 . Mais pour $r \in \mathbb{N}$, on a $p_1^r \mid a+ib$ si et seulement si $p_1^r \mid a-ib$. En particulier $r_1 = r_2$ et $k_1 = 2r_1$ est pair.

\Leftarrow : Induction sur $\sum_{i=1}^{\ell} k_i$. Observons d'abord que si $m = a^2 + b^2$ et $n = c^2 + d^2$ sont sommes de deux carrés, alors leur produit l'est aussi,

$$mn = (ac + bd)^2 + (ad - bc)^2.$$

Si $1 = \sum_{i=1}^{\ell} k_i = k_1$ alors $m = p_1$ avec $p_1 = 2$ ou $p_1 \equiv 1 \pmod{4}$, qui est bien somme de deux carrés par le Théorème 2.83. Supposons le théorème démontré pour tout nombre avec somme des exposants $< \sum_{i=1}^{\ell} k_i$. Observons que si tous les k_i sont pairs, alors $m = n^2$ est un carré et donc somme de deux carrés $m = n^2 + 0^2$. S'il existe un k_i , disons k_1 , impair, alors par hypothèse $p_1 \not\equiv 3 \pmod{4}$ et p_1 est somme de deux carrés par le Théorème 2.83. On a

$$m = p_1(p_1^{k_1-1} \cdots p_{\ell}^{k_{\ell}}).$$

Le second facteur satisfait encore l'hypothèse du théorème et est donc somme de deux carrés par induction. Le produit m aussi. ■

2.8 Théorème des restes chinois

Théorème 2.85 Soient A un anneau commutatif, $I, J < A$ deux idéaux de A tels que

$$I \cap J = \{0\} \quad \text{et} \quad I + J = A.$$

Alors l'homomorphisme d'anneaux

$$\begin{aligned} A &\longrightarrow A/I \times A/J \\ a &\longmapsto (a+I, a+J) \end{aligned}$$

est un isomorphisme d'anneaux.

Démonstration. Il suffit de montrer que l'homomorphisme est bijectif.

Injectivité : Soit $a \in A$ tel que $(a+I, a+J) = (0_{A/I}, 0_{A/J})$. En particulier $a \in I$ et $a \in J$ et $a \in I \cap J = \{0\}$.

Surjectivité : Soit $(b+I, c+J)$ un élément arbitraire du produit $A/I \times A/J$. Il faut montrer qu'il existe $a \in A$ tel que

$$a+I = b+I \quad \text{et} \quad a+J = c+J.$$

La différence $b-c \in A$. Par hypothèse, $A = I+J$ et il existe $x \in I, y \in J$ tels que $b-c = x+y$. Posons $a := b-x$. Alors clairement, $a+I = b+I$ et $a+J = b-x+J = c+y+J = c+J$. ■

Corollaire 2.86 Soient $m, n \in \mathbb{Z}$ tels que $\text{pgcd}(m, n) = 1$. Alors

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Démonstration. Dans l'anneau $A = \mathbb{Z}/mn\mathbb{Z}$ on considère les idéaux $I = m\mathbb{Z}/mn\mathbb{Z}$ et $J = n\mathbb{Z}/mn\mathbb{Z}$. Vérifions que ces idéaux satisfont les hypothèses du théorème : Pour voir que $I + J = A$ il suffit de montrer, puisque $A = \mathbb{Z}/mn\mathbb{Z}$ est cyclique, que $\bar{1} \in I + J$. Puisque $\text{pgcd}(m, n) = 1$, il existe $a, b \in \mathbb{Z}$ tels que $am + bn = 1$. En particulier $\overline{am} \in I$, $\overline{bn} \in J$ et $\bar{1} \in I + J$. Montrons que $I \cap J = \{0\}$: Soit $\bar{c} \in I \cap J$. Alors tout représentant $c \in \mathbb{Z}$ est à la fois un multiple de m et de n , donc un multiple du plus petit commun multiple de m et n qui n'est autre que mn puisque $\text{pgcd}(m, n) = 1$. En particulier $\bar{c} = 0$.

Le théorème implique donc l'existence d'un isomorphisme

$$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/mn\mathbb{Z})/I \times (\mathbb{Z}/mn\mathbb{Z})/J,$$

donné par la projection naturelle sur chaque facteur. L'isomorphisme annoncé découle du fait que l'application

$$\begin{aligned} (\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z}) &\longrightarrow \mathbb{Z}/m\mathbb{Z} \\ \bar{c} + m\mathbb{Z}/mn\mathbb{Z} &\longmapsto \bar{c}, \end{aligned}$$

est un isomorphisme d'anneaux. (Les vérifications sont laissées en exercice.) ■

Par exemple

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Le produit à gauche contient donc un élément d'ordre 6 : c'est $(\bar{1}, \bar{1})$ (ou aussi $(\bar{1}, -\bar{1})$). Si $\text{pgcd}(m, n) \neq 1$, on a bien un homomorphisme, mais il ne sera jamais bijectif. Par exemple

$$\mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Par induction on obtient immédiatement :

Corollaire 2.87 Soient $m_1, \dots, m_k \in \mathbb{Z}$ tels que $\text{pgcd}(m_i, m_j) = 1$ pour $i \neq j$. Alors

$$\mathbb{Z}/(m_1 \dots m_k)\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z}.$$

Observons que l'isomorphisme est valide en particulier pour les groupes additifs sous-jacents. Mentionnons au passage, sans aucune preuve, que tout groupe abélien fini est un produit de groupes cycliques finis.

Une reformulation plus explicite du dernier corollaire est la suivante :

Corollaire 2.88 Soient $m_1, \dots, m_k \in \mathbb{Z}$ tels que $\text{pgcd}(m_i, m_j) = 1$ pour $i \neq j$. Alors pour tous $a_1, \dots, a_k \in \mathbb{Z}$ il existe un unique $a \in \mathbb{Z}$ tel que $0 \leq a < m_1 \dots m_k$ et

$$\begin{cases} a \equiv a_1 \pmod{m_1} \\ \vdots \\ a \equiv a_k \pmod{m_k}. \end{cases}$$

Démonstration constructive de l'existence. Supposons d'abord $k = 2$. Il faut donc trouver une solution $a \in \mathbb{Z}$ de

$$\begin{cases} a \equiv a_1 \pmod{m_1} \\ a \equiv a_2 \pmod{m_2}. \end{cases}$$

Puisque $\text{pgcd}(m_1, m_2) = 1$ il existe $u_1, u_2 \in \mathbb{Z}$ tels que $u_1 m_1 + u_2 m_2 = 1$. Posons

$$a := a_1 u_2 m_2 + a_2 u_1 m_1.$$

Alors

$$\begin{aligned} a &= a_1 u_2 m_2 + a_2 u_1 m_1 \\ &\equiv a_1 u_2 m_2 \pmod{m_1} \\ &\equiv a_1 (1 - u_1 m_1) \pmod{m_1} \\ &\equiv a_1 \pmod{m_1}. \end{aligned}$$

Par symétrie, on obtient aussi $a \equiv a_2 \pmod{m_2}$. Il suffit maintenant de prendre le reste de la division de a par $m_1 m_2$.

Pour un système avec $k \geq 3$ équations, on procède par induction. En effet, on considère d'abord les deux premières équations comme dans le cas $k = 2$ qui implique que les deux premières équations sont équivalentes à

$$a \equiv a_{12} \pmod{(m_1 m_2)},$$

où a_{12} est la solution a trouvée ci-dessus. Puisque $\text{pgcd}(m_1 m_2, m_i) = 1$ pour $i \geq 3$, on continue par récurrence. ■

2.9 Conjecture de Fermat / Théorème de Wiles

Rappelons la conjecture de Fermat, désormais un théorème de Wiles :

Théorème 2.89 — Wiles, 1995. Soit $n \geq 3$. Si $x, y, z \in \mathbb{Z}$ satisfont l'équation $x^n + y^n = z^n$ alors $xyz = 0$.

Bien sûr, pour $n = 2$, ce théorème est faux, puisqu'il existe une infinité de solutions non triviales que nous détaillerons ci-dessous de l'équation $x^2 + y^2 = z^2$, par exemple $3^2 + 4^2 = 5^2$.

Fermat a énoncé ce théorème dans la marge du recueil "Arithmétiques" de Diophante, avec le fameux commentaire que la marge est trop étroite pour contenir sa preuve. Fermat aura une preuve de ce théorème pour $n = 4$ et il mentionne le cas $n = 3$ dans ses correspondances, dont on peut imaginer qu'il en possédait une démonstration. Cette annotation n'était pas destinée à être publiée et il est probable qu'il s'est rapidement rendu compte qu'il n'en avait pas de preuve pour $n \geq 5$.

Puisque $(x^k)^\ell + (y^k)^\ell = (z^k)^\ell$, il suffit clairement de démontrer la conjecture pour $n = 4$ et n un nombre premier impair. La preuve ci-dessous, remontant à Euler, peut se généraliser si tôt que l'anneau $\mathbb{Z}[e^{2i\pi/n}]$ est factoriel, pour $n = 4$ ou n un nombre premier impair. C'est le cas pour $n = 4$ (dans ce cas on retrouve les entiers de Gauss $\mathbb{Z}[i]$) et pour $p < 23$ premier, car ce sont des anneaux principaux. Mais l'anneau $\mathbb{Z}[e^{2i\pi/p}]$ n'est pas factoriel pour les premiers $p \geq 23$.

Triples pythagoriciens

Théorème 2.90 Soient $a, b, c \in \mathbb{Z}$. Alors $a^2 + b^2 = c^2$ si et seulement si il existe $k, u, v \in \mathbb{Z}$ tels que

$$a = k(u^2 - v^2), \quad b = k2uv \quad \text{et} \quad c = k(u^2 + v^2)$$

ou

$$a = k2uv, \quad b = k(u^2 - v^2) \quad \text{et} \quad c = k(u^2 + v^2).$$

Démonstration. Il est clair que des entiers de cette forme satisfont $a^2 + b^2 = c^2$. Soient donc $a, b, c \in \mathbb{Z}$ tels que $a^2 + b^2 = c^2$. Sans restreindre la généralité, nous pouvons supposer que $\text{pgcd}(a, b) = \text{pgcd}(a, c) = \text{pgcd}(b, c) = 1$. Puisque $a^2 \equiv 0, 1 \pmod{4}$, l'un de a ou b doit être pair. (Ce ne peut pas être les deux puisque $\text{pgcd}(a, b) = 1$.) Et c est impair. Considérons la factorisation

$$c^2 = a^2 + b^2 = (a + bi)(a - bi).$$

Voyons que $a + ib$ et $a - ib$ n'ont pas de facteurs irréductibles en commun : Soit $\pi \in \mathbb{Z}[i]$ tel que $\pi \mid a + ib$ et $\pi \mid a - ib$. Alors $\delta(\pi)$ divise $\delta(a + ib) = a^2 + b^2 = c^2$, qui est impair. En particulier $\delta(\pi)$ est impair. Puisque π divise $a \pm ib$, il divise leurs sommes et différences, qui sont $2a$ et $2ib$. Donc $\delta(\pi)$ divise $4a^2$ et $4b^2$. Puisque $\delta(\pi)$ est impair, ceci implique $\delta(\pi)$ divise a^2 et b^2 . Comme $\text{pgcd}(a, b) = 1$, on obtient $\delta(\pi) = 1$ et donc $\pi = \pm 1, \pm i$ est une unité. Puisque $(a + ib)(a - ib) = c^2$ et que $a + ib$ et $a - ib$ n'ont pas de facteurs irréductibles communs, chacun des deux facteurs doit être un carré, à une unité près. Il existe donc $u + iv \in \mathbb{Z}[i]$ et une unité $w \in \{\pm 1, \pm i\}$ tels que

$$a + ib = w(u + iv)^2.$$

Puisque $-1 = i^2$, on peut quitte à absorber un facteur -1 dans le carré supposer que $w = 1$ ou $w = i$. Si $w = 1$ alors $a + ib = (u + iv)^2 = (u^2 - v^2) + 2iuv$, ce qui implique bien que $a = u^2 - v^2$, $b = 2uv$ et automatiquement $c = u^2 + v^2$, qui est bien de la forme annoncée (avec $k = 1$). Si $w = i$ alors $a + ib = i(u + iv)^2 = -2uv + i(u^2 - v^2)$, ce qui implique bien que $a = -2uv$, $b = u^2 - v^2$ et automatiquement $c = u^2 + v^2$, qui est bien de la forme annoncée (avec $k = 1$, et u remplacé par $-u$). ■

Conjecture de Fermat pour $n = 3$

Ce paragraphe est hors champs d'examen.

Soit $(x, y, z) \in \mathbb{Z}^3$ une solution de $x^3 + y^3 = z^3$ tel que $0 < |xyz|$ est minimal. On montre qu'il existe $(x', y', z') \in \mathbb{Z}^3$ tels que $(x')^3 + (y')^3 = (z')^3$ avec $|x'y'z'| < |xyz|$, que l'on appellera une solution plus petite, ce qui mène à une contradiction.

Posons $\omega := e^{2i\pi/3}$. Rappelons que l'anneau

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$$

est euclidien pour la fonction

$$\delta(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2.$$

Les éléments irréductibles sont de la forme

- $\pi \in \mathbb{Z}[\omega]$ tel que $\delta(\pi) \in \mathbb{N}$ est un nombre premier. Dans ce cas $\pi = a + ib$ avec $a^2 - ab + b^2$ un nombre premier,
- $\pi = u \cdot p$, où u est une unité et p est un nombre premier de \mathbb{N} qu'on ne peut pas écrire sous la forme $p = a^2 - ab + b^2$, pour $a, b \in \mathbb{N}$.

La factorisation en irréductible de 3 sera cruciale dans ce qui suit :

$$3 = (1 - \omega)(\overline{1 - \omega}) = (-\omega^2)(1 - \omega)^2,$$

avec $1 - \omega, \overline{1 - \omega}$ irréductibles.

Remarque préliminaire : Si $\pi \in \mathbb{Z}[\omega]$ est irréductible avec $\delta(\pi) \in \mathbb{N}$ un nombre premier, alors pour tout $m \in \mathbb{Z}$, si π divise m , on a aussi $\delta(\pi)$ divise m . En effet c'est immédiat du fait que $\delta(\pi)$ divise $\delta(m) = m^2$.

Par le Lemme A.16, nous savons déjà que 3 doit diviser x, y ou z . Sans restreindre la généralité, nous pouvons supposer que 3 divise z . En effet, si 3 divise x (et par symétrie, de même pour y), on considère l'équation $x^3 = (-y)^3 + z^3$. Il existe donc $k \geq 1$ et $n \in \mathbb{Z}$ tels que

$$z = 3^k n,$$

où 3 ne divise pas n . On calcule

$$\begin{aligned} (x+y)(x+\omega y)(x+\omega^2 y) &= x^3 + x^y \underbrace{(1+\omega+\omega^2)}_{=0} + xy^2 \underbrace{(1+\omega+\omega^2)}_{=0} + y^3 \\ &= x^3 + y^3 = z^3 = 3^{3k} n^3 = (1-\omega)^{3k} (\overline{1-\omega})^{3k} n^3 \\ &= (-\omega^2)^{3k} (1-\omega)^{6k} n^3. \end{aligned}$$

On se demande maintenant comment sont répartis les $6k$ facteurs irréductibles $1 - \omega$ dans le produit

$$(x+y)(x+\omega y)(x+\omega^2 y).$$

Affirmation: Il y a au moins un facteur $1 - \omega$ dans chacun des trois facteurs.

Démonstration. On a $x+y = x+\omega y + y(1-\omega)$. Par conséquent, $1-\omega$ divise $x+y$ si et seulement si il divise $x+\omega y$. Et $1-\omega$ divise $x+\omega y$ si et seulement si $\overline{1-\omega}$ divise $\overline{x+\omega y} = x+\omega^2 y$, ce qui, puisque $\overline{1-\omega} = (-\omega)^2(1-\omega)$, est équivalent à ce que $1-\omega$ divise $x+\omega^2 y$. Donc, si $1-\omega$ divise un des facteurs, il les divise tous. Puisque le nombre de facteurs $1-\omega$ est non nul (même égal à $6k > 0$), l'affirmation est démontrée. ■

Affirmation: Il y a exactement un facteur $1 - \omega$ dans $x+\omega y$ et $x+\omega^2 y$.

Démonstration. Observons que par la remarque préliminaire puisque par l'affirmation précédente, $1-\omega$ divise $x+y \in \mathbb{Z}$, on a $3 \mid x+y$. Si $(1-\omega)^2$ divise $x+\omega y$ alors $(-\omega^2)(1-\omega)^2 = 3$ divise $x+\omega y$. Mais si 3 divise $x+y$ et $x+\omega y$, il divise aussi leur différence $y(1-\omega)$. En particulier, $(1-\omega)$ divise y , et par la remarque préliminaire, 3 divise y . Mais dans ce cas $(x/3, y/3, z/3)$ est une solution plus petite : contradiction. Puisque $(1-\omega)^2$ divise $x+\omega y$, si et seulement si $(1-\omega)^2$ divise $x+\omega^2 y$, l'affirmation est démontrée. ■

En particulier, nous savons désormais que

$$\begin{cases} x+y &= 3^{3k-1}m \\ x+\omega y &= (1-\omega)\alpha \\ x+\omega^2 y &= (\overline{1-\omega})\overline{\alpha}, \end{cases}$$

où $m \in \mathbb{Z}$, $\alpha \in \mathbb{Z}[\omega]$, $1 - \omega$ ne divise ni m ni α et

$$m\alpha\bar{\alpha} = n^3.$$

Affirmation:

1. m et α n'ont pas de facteurs irréductibles communs,
2. m et $\bar{\alpha}$ n'ont pas de facteurs irréductibles communs,
3. α et $\bar{\alpha}$ n'ont pas de facteurs irréductibles communs.

Démonstration. Nous démontrons la première assertion. Les deux autres sont identiques. Soit $\pi \in \mathbb{Z}[\omega]$ irréductible. Supposons que $\pi \mid m$ et $\pi \mid \alpha$. Puisque π divise m il divise aussi $x + y$. Et puisque π divise α il divise aussi $x + \omega y$. Il divise donc aussi la différence

$$x + y - (x + \omega y) = (1 - \omega)y.$$

On sait que ni m ni α ne sont divisibles par $(1 - \omega)$ donc π ne peut pas diviser $1 - \omega$ et doit donc diviser y . Comme il divise aussi $x + y$, il doit diviser x . L'équation $x^3 + y^3 = z^3$ implique qu'il divise aussi z . On a maintenant deux cas :

1. π est à une unité près un nombre premier $p \in \mathbb{N}$. On a alors une solution plus petite $(x/p, y/p, z/p)$,
2. $\delta(\pi)$ est un nombre premier de \mathbb{N} . Alors par la remarque préliminaire $\delta(\pi)$ divise x, y et z et on a la solution plus petite $(x/\delta(\pi), y/\delta(\pi), z/\delta(\pi))$.

■

En particulier m et $\alpha\bar{\alpha}$ n'ont pas de facteurs irréductibles communs et il découle de $m\alpha\bar{\alpha} = n^3$ qu'il existe $q, r \in \mathbb{Z}$ tels que $m = \pm q^3$ et $\alpha\bar{\alpha} = \pm r^3$. Puisque $-q^3 = (-q)^3$ on peut supposer, quitte à remplacer q et r par $-q$ et $-r$ que $m = q^3$ et $\alpha\bar{\alpha} = r^3$. De même, comme α et $\bar{\alpha}$ n'ont pas de facteurs irréductibles communs, il existe $\beta \in \mathbb{Z}[\omega]$ et $u \in U(\mathbb{Z}[\omega])$ tels que

$$\alpha = u\beta^3 \quad \text{et} \quad \bar{\alpha} = \bar{u}\bar{\beta}^3.$$

Affirmation: $u = \pm 1$

Démonstration. Puisque $x + y = 3^{3k-1}q^3$ avec $k \geq 1$, nous savons que 3^2 divise $x + y$. En particulier, dans le quotient $\mathbb{Z}[\omega]/(9) = \mathbb{Z}[\omega]/(1 - \omega)^4$ nous obtenons l'égalité

$$x + y \equiv 0 \pmod{(1 - \omega)^4}.$$

mais alors

$$(1 - \omega)u\beta^3 = x + \omega y = x + y - y(1 - \omega) \equiv -y(1 - \omega) \pmod{(1 - \omega)^4}.$$

On en déduit que

$$u\beta^3 \equiv -y \pmod{(1 - \omega)^3}$$

et de même

$$\bar{u}\bar{\beta}^3 \equiv -y \pmod{(1 - \omega)^3}.$$

Soustrayons ces deux équations pour obtenir

$$u\beta^3 \equiv \bar{u}\bar{\beta}^3 \equiv u^{-1}\bar{\beta}^3 \pmod{(1 - \omega)^3}$$

et donc

$$u^2\beta^3 \equiv \bar{\beta}^3 \pmod{(1 - \omega)^3}.$$

Cette égalité est d'autant plus valide modulo $(1 - \omega)^2$, c'est-à-dire modulo 3 :

$$u^2 \beta^3 \equiv \bar{\beta}^3 \pmod{3}.$$

Or modulo 3, on a $\beta^3 \equiv \bar{\beta}^3 \pmod{3}$. En effet, si $\beta = a + b\omega$, alors

$$\beta^3 = a^3 + 3a^2b\omega + 3ab^2\omega^2 + b^3 \equiv a^3 + b^3 \pmod{3}.$$

Nous avons donc

$$(u^2 - 1)\beta^3 \equiv 3 \pmod{3}.$$

Puisque $(1 - \omega)$ ne divise pas β , on a forcément $u^2 \equiv 1 \pmod{3}$. Ceci n'est pas valide pour les unités $u = \pm\omega, \pm\omega^2$ et nous en déduisons que $u = \pm 1$. ■

Quitte à remplacer β par $-\beta$ nous avons maintenant

$$\begin{cases} x + y &= 3^{3k-1}q^3 \\ x + \omega y &= (1 - \omega)\beta^3 \\ x + \omega^2 y &= (\overline{1 - \omega})\bar{\beta}^3. \end{cases}$$

Examinons cette deuxième équation pour $\beta = a + b\omega \in \mathbb{Z}[\omega]$. On calcule

$$\begin{aligned} x + \omega y &= (1 - \omega)(a + b\omega)^3 \\ &= (a^3 - 6ab^2 + 3a^2 + b^3) + \omega(-a^3 + 6a^2b - 3ab^3 - b^3). \end{aligned}$$

On en déduit que

$$\begin{aligned} x &= a^3 - 6ab^2 + 3a^2 + b^3 \\ y &= -a^3 + 6a^2b - 3ab^3 - b^3 \end{aligned}$$

et

$$3^{3k-1}q^3 = x + y = 9ab(a - b).$$

En particulier

$$ab(a - b) = (3^{k-1}q)^3.$$

Observons que $\text{pgcd}(a, b) = \text{pgcd}(a, a - b) = \text{pgcd}(b, a - b) = 1$ car un diviseur commun de a et b divise aussi $x + y = 3^{3k-1}q^3$ et β , et est donc une unité. Puisque le produit $ab(a - b)$ est un cube ($= (3^{k-1}q)^3$), il existe A, B, C tels que

$$a = A^3, \quad b = B^3 \quad \text{et} \quad a - b = C^3.$$

Mais alors $(A, -B, C)$ est une nouvelle solution puisque

$$A^3 + (-B)^3 = a - b = C^3.$$

Cette solution est plus petite :

$$\begin{aligned} |ABC|^3 &= |ab(a - b)| = \frac{|x + y|}{9} \\ &< |x + y| \leq |x + y| \underbrace{|x + \omega y|}_{\geq 1} \underbrace{|x + \omega^2 y|}_{\geq 1} \\ &= |z^3| \leq |xyz|^3, \end{aligned}$$

ce qui termine la démonstration.

3. Corps

Rappelons qu'un anneau K est un *corps* si K est commutatif et $U(K) = K \setminus \{0\}$. Définissons $K^* := K \setminus \{0\}$.

Nous avons vu plusieurs exemples importants de corps. Les plus classiques sont $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ et $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ pour p un nombre premier. Nous avons vu quelques autres corps de cardinalité p^2 , notamment $\mathbb{Z}[i]/(p)$ pour $p \equiv 3 \pmod{4}$.

Vous en verrez une multitude d'autres en Algèbre II. Parmi eux, on peut par exemple pour tout $\alpha \in \mathbb{R}$ considérer le plus petit corps contenant \mathbb{Q} et α . Pour $\alpha = \sqrt{2}$ c'est simplement $\{x + \sqrt{2}y \mid x, y \in \mathbb{Q}\}$ et pour $\alpha = \pi$ ce corps est formé de toutes les combinaisons \mathbb{Q} -linéaires finies de puissances positives et négatives de π .

Nous nous concentrons ici sur les corps finis et allons en particulier démontrer :

Théorème 3.1 Soit $p \in \mathbb{N}$ un nombre premier. Pour tout $n \in \mathbb{N}^*$ il existe un corps de cardinalité p^n .

Vous démontrerez de plus en Algèbre II qu'il existe à isomorphisme près un unique corps d'ordre p^n , mais vous êtes d'ores et déjà invités à tester cette unicité sur les corps de cardinalité p^n que vous rencontrerez ici. (Ce n'est pas évident en général, mais peut être amusant sur des corps de petite cardinalité.)

Pour $n = 1$, ce corps est \mathbb{F}_p , mais notez que pour $n > 1$ ce n'est jamais $(\mathbb{F}_p)^n$, qui est un anneau, mais pas un corps puisqu'il contient des diviseurs de zéro.

3.1 Corps finis

Soit K un corps fini. Observons que sa caractéristique est forcément un nombre premier p . En effet, la caractéristique d'un anneau intègre est, d'après la Proposition 2.20 soit un nombre premier, soit 0, mais dans ce cas l'ordre de 1 est infini et l'anneau de cardinalité infinie. De plus, par la Proposition 2.21 l'ordre de K est une puissance de p , $|K| = p^n$ pour $n \geq 1$.

Une façon de construire des corps de cardinalité p^n est de choisir un polynôme irréductible de degré n dans $\mathbb{Z}_p[X]$ et de considérer $\mathbb{Z}_p[X]/(f)$. Tout élément dans le quotient peut être représenté par un unique polynôme de degré $< n$. Il y en a bien p^n . Vous verrez

en exercice que tout corps a cette forme. (Ceci ne démontre pas encore l'unicité de corps de cardinalité p^n : Il reste à montrer que deux polynômes irréductibles de même degré sur le même corps fini donnent lieu à deux corps isomorphes. Vous verrez ceci en Algèbre II.) Par exemple, prenons $f(X) = X^2 + X + 1 \in \mathbb{F}_2[X]$. Alors

$$\mathbb{F}_2[X]/(f) = \{0 + (f), 1 + (f), X + (f), X + 1 + (f)\}.$$

Définition 3.2 Un polynôme $f(X) \in \mathbb{F}_p[X]$ est dit *unitaire* si son coefficient dominant est 1. On définit

$$\text{Irr}_p(n) := \{f \in \mathbb{Z}_p[X] \mid \deg(f) = n, \text{unitaire et irréductible}\}.$$

Puisque pour $f \in \text{Irr}_p(n)$ le quotient $\mathbb{Z}_p[X]/(f)$ est un corps de cardinalité p^n , l'existence de corps de telle cardinalité (Théorème 3.1) découle immédiatement du

Théorème 3.3 $\text{Irr}_p(n) \neq \emptyset$.

Par exemple en degré 1,

$$\text{Irr}_p(1) = \{X, X + 1, \dots, X + (p - 1)\}.$$

En degré 2, un polynôme est irréductible si et seulement si il n'a pas de zéro. Pour $p = 2$ on a

$$\text{Irr}_2(2) = \{X^2 + X + 1\}.$$

Pour $p \geq 3$, pour chacun des $\frac{p-1}{2}$ choix de $a \notin \{b^2 \mid b \in \mathbb{F}_p\}$ on a

$$X^2 - a \in \text{Irr}_p(2).$$

Alternativement, pour montrer que $\text{Irr}_p(2) \neq \emptyset$, on pourrait comparer le nombre de polynômes unitaires de degré 2 (il y en a p^2) et le nombre de polynômes non irréductibles unitaires de degré 2. Ces derniers polynômes ont une racine et donc la forme $(X + a)(X + b)$ pour $a, b \in \mathbb{F}_p$. Puisque si $a \neq b$ on peut échanger a et b et tomber sur le même polynôme de degré 2, il y a exactement $\frac{p(p+1)}{2}$ tels polynômes réductibles, et donc

$$|\text{Irr}_p(2)| = p^2 - \frac{p(p+1)}{2} = \frac{p(p-1)}{2}.$$

La preuve du Théorème 3.3 requiert quelques résultats intermédiaires d'intérêt indépendant :

Théorème 3.4 Dans $\mathbb{F}_p[X]$ on a

$$X^{p^n} - X = \prod_{d|n} \prod_{f \in \text{Irr}_p(d)} f(X).$$

Par exemple pour $p = 2$ nous avons déjà remarqué que

$$\begin{aligned}\text{Irr}_2(1) &= \{X, X+1\} \\ \text{Irr}_2(2) &= \{X^2+X+1\}\end{aligned}$$

et pour $n = 2$ on a bien

$$X^4 - 1 = X(X+1)(X^2+X+1).$$

Commençons par un lemme :

Lemme 3.5 $X^{p^n} - X$ n'a pas de facteurs multiples dans $\mathbb{F}_p[X]$. C'est-à-dire il n'existe pas de polynômes $f, g \in \mathbb{F}_p[X]$ avec $\deg(f) \geq 1$ et $X^{p^n} - X = f(X)^2 \cdot g(X)$.

Démonstration. Supposons que $X^{p^n} - X = f(X)^2 \cdot g(X)$ pour $f, g \in \mathbb{F}_p[X]$. Prenons la dérivée de cette expression. (La dérivée $f(X)'$ d'un polynôme $f(X)$ est donnée par la formule que vous connaissez bien d'analyse. On peut ici la définir formellement, et vous vérifierez en exercice que la dérivée d'un produit $f(X) \cdot g(X)$ est dans notre cadre aussi donné par la formule $f(X)'g(X) + f(X)g(X)'$.) On obtient

$$p^n X^{p^n-1} - 1 = f(X)(2f(X)'g(X) + g(X)').$$

Dans $\mathbb{F}_p[X]$ le premier terme $p^n X^{p^n-1}$ est nul, de sorte qu'on a

$$-1 = f(X)(2f(X)'g(X) + g(X)'),$$

et donc puisque \mathbb{F}_p est intègre, $0 = \deg(-1) \geq \deg(f)$. ■

Rappelons que dans un anneau intègre A de caractéristique un nombre premier p , l'application

$$\begin{aligned}\text{Fr} : A &\longrightarrow A \\ x &\longmapsto x^p\end{aligned}$$

est un homomorphisme d'anneau (cf Série 7), appelé *homomorphisme de Fröbenius*. En effet, dans un anneau de caractéristique p on a l'identité remarquable

$$(a+b)^p = a^p + b^p.$$

Lemme 3.6 Soit K un corps fini de cardinalité $|K| = p^n$. Alors $\text{Fr}^n = \underbrace{\text{Fr} \circ \dots \circ \text{Fr}}_{n \text{ fois}} = \text{Id}_K$ et $\text{Fr}^k \neq \text{Id}$ pour $1 \leq k < n$.

Démonstration. On a

$$\begin{aligned}\text{Fr}^n(x) &= \text{Fr}^{n-1}(x^p) = \text{Fr}^{n-2}(x^{p^2}) = \dots \\ &= (x^{p^{n-1}}) = x^{p^n}.\end{aligned}$$

Il est clair que $x^{p^n} = x$: Pour $x = 0$ c'est évident, et tout $0 \neq x \in K$ a un ordre divisant $|K^*| = p^n - 1$ et satisfait $x^{p^n-1} = 1$ et donc $x^{p^n} = x^{p^n-1} \cdot x = x$. Voyons maintenant que

$\text{Fr}^k \neq \text{Id}$ pour $1 \leq k < n$. Puisque K^* est un groupe cyclique, il contient un élément y d'ordre $p^n - 1$. Pour cet élément, on a

$$\text{Fr}^k(y) = y^{p^k} = y^{p^k-1} \cdot y \neq y$$

puisque $y^{p^k-1} \neq 1$ car $1 \leq p \leq p^k - 1 < p^n - 1$. Il découle que $\text{Fr}^k \neq \text{Id}$. ■

Démonstration du Théorème 3.4. Pour $f \in \text{Irr}_p(d)$ on considère la projection canonique

$$\pi : \mathbb{F}_p[X] \longrightarrow \mathbb{F}_p[X]/(f) =: K.$$

Observons que K est un corps de cardinalité $|K| = p^d$. Posons $\alpha := \pi(X)$. Montrons que

$$\deg(f) \mid n \iff f \mid X^{p^n} - X.$$

\implies : Puisque par le Lemme 3.6 on a $\text{Fr}^d = \text{Id}_K$, on a aussi $\text{Fr}^n = (\text{Fr}^d)^{n/d} = \text{Id}_K$ et donc $\alpha^{p^n} = \alpha$. Ceci implique que

$$\pi(X^{p^n} - X) = \alpha^{p^n} - \alpha = 0.$$

Il en découle que $X^{p^n} - X$ appartient au noyau de la projection π , qui est précisément (f) , et donc $f \mid X^{p^n} - X$.

\impliedby : Supposons que $f \mid X^{p^n} - X$ ou de façon équivalente, que $X^{p^n} - X \in (f) = \text{Ker}(\pi)$. On a donc

$$\alpha^{p^n} - \alpha = \pi(X^{p^n} - X) = 0.$$

Considérons le sous-ensemble

$$A = \{\beta \in K \mid \text{Fr}^n(\beta) = \beta\} \subset K.$$

Observons que A est un sous-anneau de K contenant α et toute ses puissances. Puisque tout élément de K est une combinaison \mathbb{F}_p -linéaire de puissances de α (car tout élément de $\mathbb{F}_p[X]$ est une combinaison \mathbb{F}_p -linéaire de puissances de X), l'anneau A est égal à K . Nous avons donc $\text{Fr}^n = \text{Id}_K$ et aussi $\text{Fr}^{\text{pgcd}(n,d)} = \text{Id}_K$. Ceci implique par le Lemme 3.6, que $\text{pgcd}(n,d) \geq d$ et donc $\text{pgcd}(n,d) = d$ et d divise n .

Finalement, puisque $\mathbb{F}_p[X]$ est factoriel, $X^{p^n} - X$ admet une factorisation en produits d'irréductibles,

$$X^{p^n} - X = u \cdot f_1 \cdot \dots \cdot f_r,$$

où $u \in (\mathbb{F}_p)^*$ et les polynômes f_1, \dots, f_r sont irréductibles. Quitte à multiplier les f_i par une unité, on peut supposer que leurs coefficients dominants sont tous égaux à 1, de sorte que $f_i \in \text{Irr}_p(\deg(f_i))$. Puisque le coefficient dominant de $X^{p^n} - X$ est aussi 1, l'unité u de la factorisation est 1. Par l'équivalence ci-dessus, les seuls facteurs irréductibles de $X^{p^n} - X$ appartiennent à $\text{Irr}_p(d)$ pour un d divisant n . Par le Lemme 3.5, ils apparaissent tous avec multiplicité 1, ce qui termine la démonstration du théorème. ■

Posons $I_p(d) := |\text{Irr}_p(d)|$. En prenant le degré de l'équation du Théorème 3.4 on obtient immédiatement :

Corollaire 3.7 $p^n = \sum_{d|n} d I_p(d).$

Par exemple pour $n = 2$ on obtient

$$p^2 = 1 \cdot I_p(1) + 2 \cdot I_p(2).$$

Puisque tous les polynômes de degré 1 sont irréductibles, on a $I_p(1) = p$ et on retrouve

$$I_p(2) = \frac{p^2 - p}{2}.$$

Plus généralement, cette formule permet de déterminer $I_p(n)$ par induction sur les facteurs premiers de n . Par exemple, si $n = q$ est premier alors

$$p^q = 1 \cdot I_p(1) + q \cdot I_p(q),$$

du quel on déduit

$$I_p(q) = \frac{p^q - p}{q}.$$

Si $n = q^2$ avec q premier, on a

$$p^{q^2} = 1 \cdot I_p(1) + q \cdot I_p(q) + q^2 I_p(q^2),$$

du quel on calcule

$$I_p(q^2) = \frac{1}{q^2} \left(p^{q^2} - q \frac{p^q - p}{q} - p \right) = \frac{1}{q^2} (p^{q^2} - p^q).$$

Si $n = q_1 q_2$ avec q_1, q_2 premiers on a

$$p^{q_1 q_2} = 1 \cdot I_p(1) + q_1 \cdot I_p(q_1) + q_2 \cdot I_p(q_2) + q_1 q_2 \cdot I_p(q_1 q_2),$$

du quel on peut déduire une expression pour $I_p(q_1 q_2)$.

Pour obtenir une formule générale pour $I_p(n)$, définissons

$$\begin{aligned} \mu : \quad \mathbb{N} \setminus \{0\} &\longrightarrow \{1, 0, -1\} \\ k = p_1^{r_1} \cdot \dots \cdot p_s^{r_s} &\longmapsto \begin{cases} 0 & \text{si } \exists i \text{ tel que } r_i \geq 2 \\ (-1)^s & \text{sinon.} \end{cases} \end{aligned}$$

Théorème 3.8 $I_p(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$

Corollaire 3.9 $I_p(n) > \frac{1}{n} > 0.$

Ceci démontre immédiatement le Théorème 3.3, qui affirme que $\text{Irr}_p(n) \neq \emptyset$.

Démonstration du Corollaire 3.9. On a

$$\begin{aligned} I_p(n) &= \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d \\ &= \frac{1}{n} \left(\mu(1)p^n + \sum_{d|n, d \neq n} \mu\left(\frac{n}{d}\right) p^d \right). \end{aligned}$$

Puisque $-1 \leq \mu(k) \in \{1, 0, -1\}$, cette expression est minorée par

$$\begin{aligned} &\geq \frac{1}{n} \left(p^n - \sum_{d|n, d \neq n} p^d \right) \\ &\geq \frac{1}{n} \left(p^n - \underbrace{\sum_{d=0}^{n-1} p^d}_{= \frac{p^n - 1}{p - 1} < p^n - 1} \right) \\ &> \frac{1}{n} \end{aligned}$$

■

Ne reste plus qu'à démontrer le Théorème 3.8. Pour ceci nous utiliserons :

Théorème 3.10 — Inversion de Möbius. Soient $f, F : \mathbb{N} \setminus \{0\} \rightarrow \mathbb{C}$ deux fonctions. Si

$$F(n) = \sum_{d|n} f(d)$$

alors

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d).$$

Voyons déjà comment l'inversion de Möbius implique immédiatement le Théorème 3.8 :

Démonstration du Théorème 3.8. Prenons $F(n) = p^n$ et $f(d) = dI_p(d)$. Nous avons établi dans le Corollaire 3.7 que

$$p^n = \sum_{d|n} dI_p(d),$$

ce qui est précisément l'identité

$$F(n) = \sum_{d|n} f(d),$$

qui implique par l'inversion de Möbius que

$$nI_p(n) = f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

■

Pour démontrer l'inversion de Möbius, étudions un peu la fonction μ .

Lemme 3.11 Soient $m, n \in \mathbb{N} \setminus \{0\}$ tels que $\text{pgcd}(m, n) = 1$. Alors

$$\mu(m \cdot n) = \mu(m) \cdot \mu(n).$$

Démonstration. Évident. ■

Proposition 3.12 Soit $n \in \mathbb{N} \setminus \{0\}$. Alors

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1. \end{cases}$$

Démonstration. Pour $n = 1$ on a $\mu(1) = 1$ par définition. Soit $n > 1$. On a

$$n = p_1^{r_1} \cdot \dots \cdot p_m^{r_m},$$

où les p_i sont des premiers distincts, et $r_i \geq 1$. Observons que $d \mid n$ si et seulement si

$$d = p_1^{s_1} \cdot \dots \cdot p_m^{s_m},$$

avec $0 \leq s_i \leq r_i$. Si il existe i tel que $s_i \geq 2$ alors $\mu(d) = 0$ par définition. En particulier, dans la somme sur $d \mid n$ nous pouvons nous restreindre aux diviseurs d de la forme $d = p_{i_1} \cdot \dots \cdot p_{i_k}$ pour un sous-ensemble $\{i_1, \dots, i_k\} \subset \{1, \dots, m\}$. On obtient

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{k=0}^m \sum_{\{i_1, \dots, i_k\} \subset \{1, \dots, m\}} \mu(p_{i_1} \cdot \dots \cdot p_{i_k}) \\ &= \sum_{k=0}^m \sum_{\{i_1, \dots, i_k\} \subset \{1, \dots, m\}} (-1)^k \\ &= \sum_{k=0}^m \binom{m}{k} (-1)^k \\ &= (-1 + 1)^m = 0. \end{aligned}$$
■

Démonstration du Théorème 3.10. On a

$$\begin{aligned} f(n) &= f(n) \cdot \underbrace{1}_{=\mu(1)} + \sum_{d'|n, d' \neq n} f(d') \cdot \underbrace{0}_{=\sum_{d|\frac{n}{d'}} \mu(d)} \\ &= \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d) \\ &= \sum_{d'|n} \sum_{d|\frac{n}{d'}} f(d') \mu(d). \end{aligned}$$

Nous devons donc sommer sur l'ensemble

$$\begin{aligned} \{(d', d) \mid d' \mid n, d \mid \frac{n}{d'}\} &= \{(d', d) \mid dd' \mid n\} \\ &= \{(d', d) \mid d \mid n, d' \mid \frac{n}{d}\}, \end{aligned}$$

de sorte que nous pouvons réécrire cette somme comme

$$\sum_{d \mid n} \underbrace{\sum_{d' \mid \frac{n}{d}} f(d') \mu(d)}_{=F(\frac{n}{d})} = \sum_{d \mid n} F(d) \mu\left(\frac{n}{d}\right),$$

puisque d divise n si et seulement si n/d divise n . ■

3.2 Polynômes cyclotomiques et Théorème de Dirichlet faible

Soit $n \in \mathbb{N}^*$. On considère le polynôme

$$f(X) = X^n - 1 \in \mathbb{Z}[X].$$

Ce polynôme, considéré comme un polynôme dans $\mathbb{C}[X]$ admet une décomposition en produit de polynômes de degré 1. Posons $\omega_n := e^{\frac{2i\pi}{n}}$. Alors

$$f(X) = X^n - 1 = \prod_{k=1}^n (X - \omega_n^k) \in \mathbb{C}[X].$$

Posons

$$\Phi_n(X) := \prod_{\substack{1 \leq k \leq n \\ \text{pgcd}(k, n) = 1}} (X - \omega_n^k).$$

Par exemple

$$\begin{aligned} \Phi_1(X) &= X - 1, \\ \Phi_2(X) &= X + 1, \\ \Phi_3(X) &= (X - \omega_3)(X - \overline{\omega_3}) = X^2 + X + 1, \\ \Phi_4(X) &= (X - i)(X + i) = X^2 + 1. \end{aligned}$$

Lemme 3.13 $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$.

Par exemple pour $n = 4$ on a bien

$$X^4 - 1 = \Phi_4(X) \Phi_2(X) \Phi_1(X) = (X^2 + 1)(X + 1)(X - 1).$$

Démonstration. On a

$$\begin{aligned} X^n - 1 &= \prod_{i=1}^n (X - \omega_n^i) \\ &= \prod_{d \mid n} \prod_{\substack{1 \leq k \leq n \\ \text{pgcd}(k, n) = d}} (X - \omega_n^k), \end{aligned}$$

où l'on a simplement utilisé le fait que

$$\{1 \leq k \leq n\} = \coprod_{d|n} \{1 \leq k \leq n \mid \text{pgcd}(k, n) = d\}.$$

Observons de plus que si $d = \text{pgcd}(k, n)$, on a

$$\omega_n^k = (e^{\frac{2i\pi}{n}})^k = (e^{\frac{2i\pi}{n/d}})^{k/d} = \omega_{n/d}^{k/d}$$

et une bijection

$$\begin{aligned} \{1 \leq k \leq n \mid \text{pgcd}(k, n) = d\} &\longrightarrow \{1 \leq k' \leq \frac{n}{d} \mid \text{pgcd}(k', \frac{n}{d}) = 1\} \\ k &\longmapsto \frac{k}{d}. \end{aligned}$$

Ceci permet de réécrire le dernier produit comme

$$\begin{aligned} X^n - 1 &= \prod_{d|n} \underbrace{\prod_{\substack{1 \leq k' \leq \frac{n}{d} \\ \text{pgcd}(k', \frac{n}{d}) = 1}} (X - \omega_{n/d}^{k'})}_{=\Phi_{n/d}(X)} \\ &= \prod_{d|n} \Phi_{n/d}(X) \\ &= \prod_{d|n} \Phi_d(X), \end{aligned}$$

où la dernière égalité découle du fait que d divise n si et seulement si n/d divise n . ■

Une conséquence immédiate, en appliquant le degré à l'équation du Lemme 3.13, est que

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

Posons $\Psi_n(X) = \prod_{d|n, d \neq n} \Phi_d(X)$ de sorte que

$$X^n - 1 = \Phi_n(X) \Psi_n(X).$$

Lemme 3.14 $\Phi_n(X) \in \mathbb{Z}[X]$.

Démonstration. Induction sur n : Pour $n = 1$ on a $\Phi_1(X) = X - 1$ qui a bien coefficients entiers. Supposons maintenant que $\Phi_d(X) \in \mathbb{Z}[X]$ pour tous $d < n$. En particulier $\Psi_n(X) \in \mathbb{Z}[X]$. Effectuons la division avec reste de $X^n - 1$ par $\Psi_n(X)$ dans $\mathbb{Z}[X]$. (C'est autorisé puisque le coefficient dominant de $\Psi_n(X)$ est 1.) Il existe donc $q(X), r(X) \in \mathbb{Z}[X]$ tels que

$$X^n - 1 = \Psi_n(X) \cdot q(X) + r(X),$$

avec $r = 0$ ou $\deg(r) < \deg(\Psi_n)$. Cette égalité est en particulier valide dans $\mathbb{C}[X]$. Mais dans $\mathbb{C}[X]$ nous savons que

$$X^n - 1 = \Psi_n(X) \Phi_n(X).$$

Puisque la division avec reste dans $\mathbb{C}[X]$ détermine un unique quotient $q(X)$ et reste $r(X)$, il découle que $q(X) = \Phi_n(X)$ est bien un polynôme à coefficient entier. (Et aussi $r(X) = 0$.) ■

Puisque $\Phi_n(X)$ et donc aussi $\Psi_n(X)$ sont à coefficients entiers, on peut considérer ces polynômes dans $\mathbb{F}_p[X]$. Dans ce qui suit, nous supposons que p ne divise pas n et examinerons le polynôme

$$X^n - 1 = \Phi_n(X)\Psi_n(X) \in \mathbb{F}_p[X].$$

Lemme 3.15 Supposons que p ne divise pas n . Alors $X^n - 1$ n'a pas de zéros multiples dans \mathbb{F}_p . C'est-à-dire, il n'existe pas de $a \in \mathbb{F}_p$ tel que $X^n - 1 = (X - a)^2 q(X)$ pour un polynôme $q(X) \in \mathbb{F}_p[X]$.

Démonstration. Supposons que $X^n - 1 = (X - a)^2 q(X)$. La dérivée de cette expression donne

$$nX^{n-1} = (X - a)(2q(X) + (X - a)q'(X)).$$

L'évaluation de ceci en $X = a$ donne

$$na^{n-1} = 0 \in \mathbb{F}_p.$$

Puisque $n \neq 0 \in \mathbb{F}_p$ et que \mathbb{F}_p est intègre, ceci force $a = 0 \in \mathbb{F}_p$. Mais 0 n'est pas un zéro de $X^n - 1$. ■

Proposition 3.16 Supposons que p ne divise pas n . Soit $a \in \mathbb{F}_p \setminus \{0\}$. Alors l'ordre de a est n si et seulement si $\Phi_n(a) = 0$.

Démonstration. Induction sur n . Supposons $n = 1$ et rappelons que $\Phi_1(X) = X - 1$. L'ordre de a est 1 si et seulement si $a = 1$ si et seulement si $\Phi_1(a) = a - 1 = 0$.

Supposons la proposition valide pour des nombres $< n$ et montrons les deux implications.

\implies : Soit a un élément d'ordre n . Alors a est zéro de $X^n - 1 = \prod_{d|n} \Phi_d(X)$. En particulier il existe $d \mid n$ tel que $\Phi_d(a) = 0$. Si $d < n$, ceci implique par induction que a a ordre $d < n$, ce qui est exclu. Donc $d = n$ et $\Phi_n(a) = 0$.

\impliedby : Si $\Phi_n(a) = 0$ alors $a^n = 1$. L'ordre d de a divise donc n et $\Phi_d(a) = 0$. Si $d < n$, ceci impliquerait que $X^n - 1$ a un zéro multiple, ce qui est impossible par le Lemme 3.15. ■

Théorème 3.17 Soient $n, p \in \mathbb{N}$ tels que p est un premier ne divisant pas n . Sont équivalents :

1. $X^n - 1$ est un produit de polynômes de degré 1 dans $\mathbb{F}_p[X]$,
2. $p \equiv 1 \pmod{n}$,
3. il existe $k \in \mathbb{Z}$ tel que p divise $\Phi_n(k)$ dans \mathbb{Z} .

Démonstration. 2. \implies 1 : Supposons que $p \equiv 1 \pmod n$. Alors il existe $q \in \mathbb{Z}$ tel que $p - 1 = qn$. Soit $a \in \mathbb{F}_p$ un générateur du groupe cyclique \mathbb{F}_p^* . Alors

$$\mathbb{F}_p = \{0, 1, a, a^2, \dots, a^{p-2}\}$$

et les n éléments distincts

$$a^q, a^{2q}, \dots, a^{(n-1)q}, a^{nq} = 1$$

sont n racines de $X^n - 1$.

1. \implies 2 : Supposons que

$$X^n - 1 = (X - a_1) \cdot \dots \cdot (X - a_n)$$

avec $a_i \in \mathbb{F}_p^*$. En particulier, tous les facteurs $\Phi_d(X)$, pour $d \mid n$, se décomposent en produit de polynômes de degré 1. C'est en particulier le cas pour $\Phi_n(X)$, qui a donc un zéro, qui est par la Proposition 3.16 un élément d'ordre n . Cet ordre n doit diviser l'ordre du groupe $|\mathbb{F}_p^*| = p - 1$, ce qui revient à dire que $p \equiv 1 \pmod n$.

3. \implies 1 : Si il existe $k \in \mathbb{Z}$ tel que p divise $\Phi_n(k)$ alors $\Phi_n(\bar{k}) = 0 \in \mathbb{F}_p$. Par la Proposition 3.16, ceci implique que \bar{k} a ordre n . Les n éléments distincts

$$\bar{k}, \bar{k}^2, \dots, \bar{k}^n = 1$$

sont tous zéros de $X^n - 1$.

1. \implies 3 : Si $X^n - 1$ est un produit de polynômes de degré 1, c'est aussi le cas de $\Phi_n(X)$. En particulier, il existe $\bar{a} \in \mathbb{F}_p^*$ tel que $\Phi_n(\bar{a}) = 0 \in \mathbb{F}_p$, ce qui veut précisément dire que $\Phi_n(a) \in \mathbb{Z}$, pour tout représentant $a \in \mathbb{Z}$ de $\bar{a} \in \mathbb{F}_p$, est un multiple de p . ■

Lemme 3.18 Soient $m, n \in \mathbb{N}$ tels que $m, n \geq 2$. Alors $\Phi_n(m) \neq 0, \pm 1$.

Démonstration. On montre que le module de $\Phi_n(m)$ est strictement plus grand que 1 :

$$\begin{aligned} |\Phi_n(m)| &= \prod_{\substack{1 \leq k \leq n \\ \text{pgcd}(k,n)=1}} |m - \omega_n^k| \\ &\geq \prod_{\substack{1 \leq k \leq n \\ \text{pgcd}(k,n)=1}} |\text{Re}(m - \omega_n^k)| \\ &= \prod_{\substack{1 \leq k \leq n \\ \text{pgcd}(k,n)=1}} |m - \text{Re}(\omega_n^k)|, \end{aligned}$$

Mais $\text{Re}(\omega_n^k) \leq 1$ avec égalité si et seulement si $\omega_n^k = 1$, c'est-à-dire $k = n$, qui n'est pas considéré dans ce produit puisque $n \neq 1$. Nous avons donc une minoration stricte

$$|\Phi_n(m)| > \prod_{\substack{1 \leq k \leq n \\ \text{pgcd}(k,n)=1}} |m - 1| = |m - 1|^{\varphi(n)} \geq 1,$$

où pour la dernière inégalité nous avons utilisé que $m \geq 2$. ■

Théorème 3.19 — Théorème de Dirichlet faible. Pour tout $n \in \mathbb{N}^*$, il existe une infinité de p premiers tels que $p \equiv 1 \pmod{n}$.

Démonstration. Pour $n = 1$, il n'y a rien à montrer. Supposons $n \geq 2$. Supposons qu'il existe un nombre fini de premiers p_1, \dots, p_k tels que $p_i \equiv 1 \pmod{n}$. (Le cas $k = 0$ est autorisé.) Posons

$$h := p_1 \cdot \dots \cdot p_k.$$

On a

$$(nh)^n - 1 = \Phi_n(nh)\Psi_n(nh).$$

Puisque $n \geq 2$, on a aussi $nh \geq 2$ et on sait par le Lemme 3.18 que $\Phi_n(nh)$ admet un facteur premier p . Ce facteur divise aussi $(nh)^n - 1$ et ne peut donc pas diviser n . Nous pouvons donc appliquer le Théorème 3.17 pour déduire que $p \equiv 1 \pmod{n}$. Ce premier est un nouveau premier, puisque de nouveau, il divise $(nh)^n - 1$ et ne peut donc pas diviser h . Contradiction. ■

A. Annexe : Arithmétique

A.1 Division Euclidienne ou division avec reste

Théorème A.1 — Division Euclidienne. Soient $n, d \in \mathbb{Z}$ avec $d > 0$. Alors il existe $q, r \in \mathbb{Z}$ tels que

$$n = qd + r \quad \text{et} \quad 0 \leq r < d.$$

De plus, q et r sont uniquement déterminés par ces conditions.

Démonstration. Existence : Posons

$$\mathcal{S} := \{n - q'd \mid q' \in \mathbb{Z}\} \cap \mathbb{N}.$$

Observons que $\mathcal{S} \neq \emptyset$ puisque

- si $n \geq 0$ alors $n = n - 0 \cdot d \in \mathcal{S}$,
- si $n < 0$ alors $n - nd = (1 - d)n \geq 0$ appartient à \mathcal{S} puisque ça a bien la forme $n - q'd$ (pour $q' = n$) et que comme produit de deux nombres $1 - d \leq 0, n < 0$, plus petits ou égaux à 0, c'est un nombre plus grand ou égal à 0.

L'ensemble \mathcal{S} est de plus un sous-ensemble de \mathbb{Z} minoré, puisque il est minoré par 0. (En effet pour tout $x \in \mathcal{S}$, on a $x \geq 0$.) Or un sous-ensemble minoré et non vide de \mathbb{Z} admet un plus petit élément. Soit $r \in \mathcal{S}$ le plus petit élément.

Puisque $r \in \mathcal{S}$, par définition de \mathcal{S} , il existe $q \in \mathbb{Z}$ tel que $r = n - qd \geq 0$. Voyons de plus que $r < d$. Si ce n'était pas le cas, on aurait $r \geq d$ mais alors $r' := r - d \geq 0$ appartiendrait à \mathcal{S} puisque c'est un nombre plus grand ou égal à 0 et que

$$r' = r - d = n - qd - d = n - (q + 1)d.$$

Or $r' < r$ ce qui contredit la minimalité de r dans \mathcal{S} .

Unicité : Supposons

$$n = q_1d + r_1 = q_2d + r_2,$$

avec $0 \leq r_1, r_2 < d$. Si $q_1 \neq q_2$ on peut supposer par symétrie que $q_1 < q_2$. Mais alors

$$r_1 = \underbrace{r_2}_{\geq 0} + \underbrace{(q_2 - q_1)d}_{\substack{>0 \\ \geq d}} \geq d,$$

ce qui est impossible. Il en découle que $q_1 = q_2$ et aussi $r_1 = r_2$. ■

Basé sur la division Euclidienne, voyons un algorithme remontant à Euclide (ou vraisemblablement antérieur, mais énoncé dans les *Eléments* d'Euclide) pour calculer le plus grand commun diviseur de deux entiers. Rappelons au préalable quelques définitions.

Définition A.2 Soient $a, b \in \mathbb{Z}$

- On dit que a *divise* b , ou que b est *divisible* par a , qu'on notera $a \mid b$, s'il existe $q \in \mathbb{Z}$ tel que $aq = b$.
- Le *plus grand commun diviseur* de a et b est le nombre

$$\text{pgcd}(a, b) := \begin{cases} 0 & \text{si } a = b = 0, \\ \max\{n \in \mathbb{N} \mid n \mid a \text{ et } n \mid b\} & \text{sinon.} \end{cases}$$

- On dit que a et b sont *premiers entre eux* si $\text{pgcd}(a, b) = 1$.

Observons que par définition, tout nombre $n \in \mathbb{Z}$ divise 0 (en effet $n \cdot 0 = 0$), mais seul 0 est divisible par 0.

Lemme A.3 Si c divise a et b divise c alors c divise $ma + nb$ pour tous $m, n \in \mathbb{Z}$.

Démonstration. Exercice évident. ■

Nous appellerons un nombre de la forme $ma + nb$, pour $m, n \in \mathbb{Z}$, une *combinaison \mathbb{Z} -linéaire* de a et b .

Lemme A.4 Soient $n, d \in \mathbb{Z}$ et $q, r \in \mathbb{Z}$ tels que $n = qd + r$. Alors

$$\text{pgcd}(n, d) = \text{pgcd}(d, r).$$

Démonstration. Posons $p = \text{pgcd}(n, d)$ et $p' = \text{pgcd}(d, r)$. Montrons que $p' \mid p$ et $p \mid p'$, ce qui implique que $p = p'$.

$p' \mid p$: Par définition du pgcd, il faut montrer que p' divise n et d , or p' divise déjà d puisque par définition, c'est le plus grand diviseur commun de d et r . Mais puisqu'il divise d et r , il divise toute combinaison \mathbb{Z} -linéaire de d et r , et donc aussi $n = qd + r$.

$p \mid p'$: C'est quasiment identitique. Par définition du pgcd, il faut montrer que p divise d et r , or p divise déjà d puisque par définition, c'est le plus grand diviseur commun de n et d . Mais puisqu'il divise n et d , il divise toute combinaison \mathbb{Z} -linéaire de n et d , et donc aussi $r = n - qd$. ■

Théorème A.5 Soient $a, b \in \mathbb{Z}$. Alors il existe $m, n \in \mathbb{Z}$ tels que

$$am + bn = \text{pgcd}(a, b).$$

Inversément, tout entier de la forme $am + bn$ est un multiple de $\text{pgcd}(a, b)$.

Ce théorème est une formulation sensiblement différente mais complètement équivalente du Corollaire 1.53 que nous avons démontré à l'aide de la théorie des groupes dans le paragraphe 1.8. Nous proposons ici une preuve purement arithmétique. Notons que la deuxième assertion est triviale : Puisque $\text{pgcd}(a, b)$ divise a et b , il divise toute combinaison \mathbb{Z} -linéaire de a et b . La démonstration de la première assertion sera constructive : L'algorithme d'Euclide présenté ci-dessous pour le calcul du pgcd de deux nombres a et b permettra de trouver m et n dans \mathbb{Z} tels que $am + bn = \text{pgcd}(a, b)$.

Algorithme d'Euclide pour le calcul du pgcd

Soient $d_1 \geq d_2 > 0$ deux entiers.

1ère étape : Par division Euclidienne, $d_1 = q_1 d_2 + d_3$, pour $q_1 \in \mathbb{Z}$ et $0 \leq d_3 < d_2$. Si $d_3 = 0$ on passe à la dernière étape. Sinon, à la deuxième.

2ème étape : Par division Euclidienne, $d_2 = q_2 d_3 + d_4$, pour $q_2 \in \mathbb{Z}$ et $0 \leq d_4 < d_3$. Si $d_4 = 0$ on passe à la dernière étape. Sinon, à la troisième.

On continue ainsi pour obtenir une suite

$$d_2 > d_3 > d_4 > \dots \geq 0$$

qui est nécessairement finie. Soit d_k le plus petit entier de cette suite avec $d_k > 0$ de sorte que $d_{k+1} = 0$.

Dernière étape : $d_k = \text{pgcd}(d_1, d_2)$. En effet, par le Lemme A.4 on a

$$\text{pgcd}(d_1, d_2) = \text{pgcd}(d_2, d_3) = \dots = \text{pgcd}(d_{k-1}, d_k) = \text{pgcd}(d_k, \underbrace{d_{k+1}}_{=0}) = d_k.$$

Preuve constructive du Théorème A.5. On peut remonter cet algorithme pour trouver $n_1, n_2 \in \mathbb{Z}$ tels que $n_1 d_1 + n_2 d_2 = \text{pgcd}(d_1, d_2) = d_k$. En effet, montrons par induction décroissante sur $k \geq i \geq 1$ comment trouver $n_1, n_2 \in \mathbb{Z}$ tels que $n_1 d_i + n_2 d_{i+1} = d_k$.

Pour $i = k$ et puisque $d_{k+1} = 0$ il suffit de prendre $n_1 = 1$ et $n_2 = 0$, ce qui donne bien $1 \cdot d_k + 0 \cdot 0 = d_k$.

Supposons maintenant que l'on a $m_1, m_2 \in \mathbb{Z}$ tels que $m_1 d_{i+1} + m_2 d_{i+2} = d_k$ et montrons qu'il existe $n_1, n_2 \in \mathbb{Z}$ tels que $n_1 d_i + n_2 d_{i+1} = d_k$. On a

$$d_k = m_1 d_{i+1} + m_2 d_{i+2} = m_1 d_{i+1} + m_2 (d_i - q_i d_{i+1}) = m_2 d_i + (m_1 - m_2 q_i) d_{i+1},$$

ce qui démontre le théorème. ■

Illustrons ceci sur un exemple :

■ **Exemple A.6** Calcul du pgcd de 50 et 22 et comment trouver $m, n \in \mathbb{Z}$ tels que $m \cdot 50 + n \cdot 22 = \text{pgcd}(50, 22)$. On applique l'algorithme d'Euclide à $d_1 = 50, d_2 = 22$:

$$\begin{array}{llll} 50 & = & 2 \cdot 22 + 6 & \implies d_3 = 6, \\ 22 & = & 3 \cdot 6 + 4 & \implies d_4 = 4, \\ 6 & = & 1 \cdot 4 + 2 & \implies d_5 = 2, \\ 4 & = & 2 \cdot 2 + 0 & \implies d_6 = 0. \end{array}$$

Puisque $d_6 = 0$ on en déduit que $d_5 = 2 = \text{pgcd}(50, 22)$ (on peut espérer qu'on le savait déjà). Remontons maintenant l'algorithme :

$$\begin{aligned} 2 &= 6 - 1 \cdot 4 \\ &= 6 - 1 \cdot (22 - 3 \cdot 6) = -1 \cdot 22 + 4 \cdot 6 \\ &= -1 \cdot 22 + 4 \cdot (50 - 2 \cdot 22) = 4 \cdot 50 - 9 \cdot 22. \end{aligned}$$

A.2 Arithmétique modulaire

Définition A.7 Soient $n, a, b \in \mathbb{Z}$. On dit que a est congru à b modulo n ou a et b sont congrus modulo n si n divise $a - b$. On le note $a \equiv b \pmod{n}$.

Par exemple, 17 est congru à 5 modulo 4, $17 \equiv 5 \pmod{4}$, puisque 4 divise $17 - 5 = 12$. Observons que

$$a \equiv b \pmod{n} \iff \exists q \in \mathbb{Z} \text{ tel que } a = b + qn.$$

En particulier, deux nombres sont congrus modulo n si et seulement si ils sont congrus modulo $-n$. Donc quitte à remplacer n par $-n$, on peut toujours supposer que $n \geq 0$. De plus, si $n = 0$, puisque seul 0 est divisible par 0, la relation être congru modulo 0 n'est rien d'autre que l'égalité habituelle entre nombres entiers.

Congruence modulo 2 : Soit $a \in \mathbb{Z}$. Alors $a \equiv 0 \pmod{2}$ si et seulement si il existe $q \in \mathbb{Z}$ tel que $a = 2q$, autrement dit si et seulement si a est pair. Et $a \equiv 1 \pmod{2}$ si et seulement si il existe $q \in \mathbb{Z}$ tel que $a = 2q + 1$, autrement dit si et seulement si a est impair.

Proposition A.8 Soit $n \in \mathbb{Z}$. Être congru modulo n est une relation d'équivalence.

Démonstration. Exercice. ■

Dénotons par \bar{a} la classe d'équivalence de $a \in \mathbb{Z}$ pour la relation de congruence modulo n . (Le n sera clair du contexte.) Plus précisément,

$$\bar{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}.$$

Par exemple modulo 2 on a $\bar{1} = \bar{3} = \overline{2k+1}$ pour tout $k \in \mathbb{Z}$.

Théorème A.9 Soient $n, a \in \mathbb{Z}$ avec $n \geq 1$. Alors a est congru modulo n à un et un seul nombre parmi $0, 1, 2, \dots, n-1$. Autrement dit, il existe exactement n classes d'équivalences pour la relation de congruence modulo n : $\bar{0}, \bar{1}, \dots, \overline{n-1}$.

Démonstration. Par division Euclidienne, il existe des uniques $q, r \in \mathbb{Z}$ tels que $a = qn + r$ avec $0 \leq r < n$. En particulier, $a \equiv r \pmod{n}$. S'il existait un autre $r' \in \{0, 1, \dots, n-1\}$ tel que $a \equiv r' \pmod{n}$ alors il existerait $q' \in \mathbb{Z}$ tel que $a = q'n + r'$, ce qui contredit l'unicité de q et r dans la division Euclidienne. ■

Lemme A.10 Soient $a, a', b, b', n \in \mathbb{Z}$.

1. Si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$ alors $a + b \equiv a' + b' \pmod{n}$.
2. Si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$ alors $a \cdot b \equiv a' \cdot b' \pmod{n}$.

Démonstration. Exercice. ■

Il découle du Théorème A.9 et du Lemme A.10 qu'on peut définir l'addition et la multiplication modulo n comme des applications

$$\begin{aligned} + \pmod{n} : \{\overline{0}, \overline{1}, \dots, \overline{n-1}\} \times \{\overline{0}, \overline{1}, \dots, \overline{n-1}\} &\longrightarrow \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}, \\ \cdot \pmod{n} : \{\overline{0}, \overline{1}, \dots, \overline{n-1}\} \times \{\overline{0}, \overline{1}, \dots, \overline{n-1}\} &\longrightarrow \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}. \end{aligned}$$

En effet, pour $a, b \in \{0, 1, \dots, n-1\}$ représentant deux éléments arbitraires $\overline{a}, \overline{b}$ de $\{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$, la somme ou le produit modulo n de leurs classes d'équivalence est donnée par

$$\overline{a} + \overline{b} \pmod{n} := \overline{a+b} \quad \text{et} \quad \overline{a} \cdot \overline{b} \pmod{n} := \overline{a \cdot b}.$$

Le Lemme A.10 assure que ces opérations sont bien définies et le Théorème A.9 implique que les images $\overline{a+b}$ et $\overline{a \cdot b}$ appartiennent bien à $\{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$. Par exemple, l'addition et la multiplication modulo 4 sont données par les tables suivantes, où pour ne pas alourdir la notation, nous nous privons de surligner les chiffres 0, 1, 2, 3 :

$+ \pmod{4}$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot \pmod{4}$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Applications

Petit Théorème de Fermat

Nous avons démontré dans le paragraphe 1.8 le Petit Théorème de Fermat suivant, ainsi que sa généralisation à l'aide du Théorème de Lagrange 1.34. Nous proposons ici une preuve purement arithmétique.

Rappelons qu'un nombre $2 \leq p \in \mathbb{N}$ est dit *premier* si pour tous $a, b \in \mathbb{Z}$, si p divise le produit ab alors p divise a ou p divise b .

Théorème A.11 — Petit Théorème de Fermat. Soient p premier, $a \in \mathbb{Z}$ avec $\text{pgcd}(a, p) = 1$. Alors

$$a^{p-1} \equiv 1 \pmod{p}.$$

Pour la preuve, nous aurons besoin des deux énoncés suivants :

Lemme A.12 Soit p premier et i un entier tel que $0 < i < p$. Alors p divise le coefficient binomial $\binom{p}{i}$.

Démonstration. Exercice. ■

Proposition A.13 Soit p premier et $a, b \in \mathbb{Z}$. Alors

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

Démonstration. On a

$$(a + b)^p = \sum_{i=0}^p \binom{p}{i} a^i b^{p-i} \equiv a^p + b^p \pmod{p},$$

puisque pour $0 < i < p$ le coefficient binomial $\binom{p}{i}$ est 0 modulo p par le Lemme A.12. ■

Preuve du Petit Théorème de Fermat. Montrons d'abord par induction sur $k \in \mathbb{N}$ que

$$k^p \equiv k \pmod{p} \tag{A.1}$$

pour tout $k \in \mathbb{N}$. Pour $k = 0$, c'est trivialement vrai. Supposons l'assertion démontrée pour tout entier $< k$ et montrons-la pour k :

$$\begin{aligned} k^p &= ((k-1) + 1)^p \equiv (k-1)^p + 1^p \pmod{p} && \text{Proposition A.13,} \\ &\equiv (k-1) + 1 \pmod{p} && \text{Induction et } 1^p = 1, \\ &\equiv k \pmod{p}. \end{aligned}$$

Nous pouvons réécrire l'Equation (A.1) comme

$$k(k^{p-1} - 1) \equiv 0 \pmod{p}.$$

En particulier p divise le produit $k(k^{p-1} - 1)$. Pour $k = a \in \mathbb{Z}$ tel que $\text{pgcd}(a, p) = 1$, puisque p ne divise pas le facteur a , il doit diviser le facteur $a^{p-1} - 1$, ce qui équivaut à $a^{p-1} \equiv 1 \pmod{p}$. ■

Carrés

Un nombre entier $a \in \mathbb{Z}$ est un *carré* si et seulement si il existe $b \in \mathbb{Z}$ tel que $a = b^2$. De même, une classe $\bar{a} \in \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ est un *carré modulo n* si et seulement si il existe $\bar{b} \in \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ tel que $a \equiv b^2 \pmod{n}$.

Lemme A.14 Les seuls carrés modulo 4 sont $\bar{0}$ et $\bar{1}$.

Démonstration. Il suffit de calculer les carrés de 0, 1, 2, 3 modulo 4. On a

$$\begin{aligned} 0^2 &\equiv 0 \pmod{4}, & 1^2 &\equiv 1 \pmod{4}, \\ 2^2 &\equiv 4 \equiv 0 \pmod{4}, & 3^2 &\equiv (-1)^2 \equiv 1 \pmod{4}, \end{aligned}$$

ce qui montre bien que les seules valeurs possibles sont $\bar{0}$ et $\bar{1}$. ■

Lemme A.15 Un nombre de la forme $4k + 3$, pour $k \in \mathbb{Z}$ n'est jamais une somme de deux carrés. Plus précisément il n'existe pas de $a, b \in \mathbb{Z}$ tels que $4k + 3 = a^2 + b^2$.

Démonstration. Supposons qu'il existe $a, b \in \mathbb{Z}$ tels que $4k + 3 = a^2 + b^2$. Regardons cette équation modulo 4 :

$$4k + 3 \equiv 3 \equiv a^2 + b^2 \pmod{4}.$$

Par le Lemme A.14, a^2 et b^2 sont égaux à 0 ou 1 modulo 4. Et donc $a^2 + b^2$ est soit $0 + 0 = 0$, $0 + 1 = 1$, $1 + 0 = 1$ ou $1 + 1 = 2$ modulo 4, mais en aucun cas 3, ce qui démontre le lemme. ■

Dans le même esprit, vous pourrez démontrer en exercice qu'un nombre de la forme $8k + 7$ n'est jamais somme de trois carrés. Ou bien aussi que si un nombre est un carré alors son unité est 0, 1, 5, 6 et 9. Par exemple, 34'562 n'est pas un carré puisqu'il se termine par 2.

L'équation $x^3 + y^3 = z^3$

Nous démontrerons dans le Chapitre 2 sur les anneaux le premier cas ($p = 3$) de la fameuse conjecture de Fermat, depuis 1995 un théorème de Wiles : Soit $p > 2$ un nombre premier. S'il existe $x, y, z \in \mathbb{Z}$ tels que $x^p + y^p = z^p$, alors $xyz = 0$. Bien sûr pour $p = 2$ il existe une infinité de solutions non triviales. Pour $p = 3$, nous suivrons une preuve datant déjà d'Euler dont la première étape est la suivante :

Lemme A.16 Soient $x, y, z \in \mathbb{Z}$ tels que $x^3 + y^3 = z^3$. Alors 3 divise x, y ou z .

Démonstration. Supposons que 3 ne divise aucun des trois nombres x, y et z . Cherchons les valeurs possibles de a^3 modulo 9 si 3 ne divise pas a . Il suffit donc de calculer $a^3 \pmod{9}$ pour $a = 1, 2, 4, 5, 7, 8$, ou de façon équivalent pour $a = \pm 1, \pm 2, \pm 4$. On calcule

$$1^3 \equiv 1 \pmod{9}, \quad 2^3 = 8 \equiv -1 \pmod{9}, \quad 4^3 = 64 \equiv 1 \pmod{9}.$$

Puisque $(-a)^3 = -a^3$ on en déduit

$$(-1)^3 \equiv -1 \pmod{9}, \quad (-2)^3 = 1 \pmod{9}, \quad (-4)^3 \equiv -1 \pmod{9}.$$

En particulier $x^3, y^3, z^3 \equiv \pm 1 \pmod{9}$ et l'égalité $x^3 + y^3 - z^3 \equiv 0 \pmod{9}$ ne peut jamais être vérifiée. Contradiction. ■

Critères de divisibilité

Un nombre $n \in \mathbb{N}$ admet une unique écriture en base 10 comme

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_k \cdot 10^k,$$

avec $0 \leq a_i \leq 9$, où l'on choisit k tel que $a_k \neq 0$.

Critère de divisibilité par 2 : Un nombre

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_k \cdot 10^k$$

est divisible par 2 si et seulement si $a_0 \in \{0, 2, 4, 6, 8\}$.

Critère de divisibilité par 5 : Un nombre

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10 + \cdots + a_k \cdot 10^k$$

est divisible par 5 si et seulement si $a_0 \in \{0, 5\}$.

Critère de divisibilité par 10 : Un nombre

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10 + \cdots + a_k \cdot 10^k$$

est divisible par 10 si et seulement si $a_0 = 0$.

Critère de divisibilité par 9 : Un nombre

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10 + \cdots + a_k \cdot 10^k$$

est divisible par 9 si et seulement si

$$a_0 + a_1 + \cdots + a_k$$

est divisible par 9.

Par exemple,

2'345'678	n'est pas divisible par 9 car
2 + 3 + 4 + 5 + 6 + 7 + 8 = 35	n'est pas divisible par 9 car
3 + 5 = 8	n'est pas divisible par 9.

1'264'284	est divisible par 9 car
1 + 2 + 6 + 4 + 2 + 8 + 4 = 27	est divisible par 9 car
2 + 7 = 9	est divisible par 9.

Démonstration n'utilisant que de l'arithmétique de base (pas de modulo). On a

$$\begin{aligned}
 n &= a_0 + a_1 10 + a_2 10^2 + \cdots + a_k 10^k \\
 &= a_0 + a_1(10 - 1) + a_1 + a_2(10^2 - 1) + a_2 + \cdots + a_k(10^k - 1) + a_k \\
 &= (a_0 + a_1 + a_2 + \cdots + a_k) + \underbrace{a_1(10 - 1) + a_2(10^2 - 1) + \cdots + a_k(10^k - 1)}_{\text{divisible par 9}},
 \end{aligned}$$

puisque

$$10 - 1 = 9, \quad 10^2 - 1 = 99, \quad 10^3 - 1 = 999$$

et plus généralement, pour tout $m \geq 1$,

$$10^m - 1 = \underbrace{9 \dots 9}_{m-1 \text{ fois}} = 9 \cdot \underbrace{(1 \dots 1)}_{m-1 \text{ fois}}.$$

On conclut en utilisant le fait que pour tous $a, b, q \in \mathbb{Z}$,

$$9|a \iff 9|b + qp.$$



Le même critère est valide pour 3 :

Critère de divisibilité par 3 : Un nombre

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10 + \cdots + a_k \cdot 10^k$$

est divisible par 3 si et seulement si

$$a_0 + a_1 + \cdots + a_k$$

est divisible par 3.

Formalisation et généralisation : Soit $m \in \mathbb{N}$. La réduction modulo m que nous dénotons

$$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

est un homomorphisme d'anneau. Soit

$$n = a_0 + a_1 \cdot 10 + \cdots + a_k \cdot 10^k = \sum_{i=0}^k a_i 10^i \in \mathbb{N}.$$

Alors $m \mid n$ si et seulement si

$$0 = \pi(n) = \sum_{i=0}^k \pi(a_i) \pi(10)^i,$$

où l'on a utilisé crucialement que π est un homomorphisme d'anneau. Soient maintenant $r_i \in \mathbb{Z}$ tels que $\pi(10)^i = \pi(r_i)$. Le terme de gauche de la dernière équation s'écrit aussi comme

$$\sum_{i=0}^k \pi(a_i) \pi(r_i) = \pi \left(\sum_{i=0}^k a_i r_i \right).$$

Nous avons donc montré le critère de divisibilité général suivant :

Critère de divisibilité général : Soit $m \in \mathbb{N}$ et $r_i \in \mathbb{Z}$ tels que $10^i \equiv r_i \pmod{m}$. Alors

$$m \mid n = \sum_{i=0}^k a_i 10^i \iff m \mid \sum_{i=0}^k a_i r_i.$$

■ Exemples A.17

$n = 2$. Dans ce cas $\pi(10) = \bar{0}$ et donc $\pi(10^i) = \bar{0}$ pour tous i , de sorte que l'on peut prendre $r_0 = 1$ et $r_i = 0$ pour $i > 0$. Le critère se traduit en

$$2 \mid \sum_{i=0}^k a_i 10^i \iff 2 \mid a_0.$$

La même démarche fonctionne pour $n = 5$ ou 10 .

$n = 9$. Dans ce cas $\pi(10) = \bar{1}$ et donc $\pi(10^i) = \bar{1}$, de sorte que l'on peut prendre $r_i = 1$ pour tout $i \geq 0$. Le critère se traduit en

$$9 \mid \sum_{i=0}^k a_i 10^i \iff 9 \mid \sum_{i=0}^k a_i.$$

La même démarche fonctionne pour $n = 3$.

$n = 11$. Dans ce cas $\pi(10) = \overline{-1}$ et donc $\pi(10^2) = \overline{1}$ et $\pi(10^{2i}) = \overline{1}$ et $\pi(10^{2i+1}) = \overline{-1}$ pour tout $i \geq 0$, de sorte que l'on peut prendre $r_{2i} = 1$ et $r_{2i+1} = -1$ pour tout $i \geq 0$. Le critère se traduit en

$$11 \mid \sum_{i=0}^k a_i 10^i \iff 11 \mid \sum_{i=0}^k (-1)^i a_i.$$

$n = 7$. On calcule

$$\begin{array}{lll} \pi(10) = \overline{3} & \pi(10)^2 = \overline{2} & \pi(10)^3 = \overline{-1} \\ \pi(10)^4 = \overline{-3} & \pi(10)^5 = \overline{-2} & \pi(10)^6 = \overline{1}. \end{array}$$

Ceci implique que $\pi(10)^{6q+r} = \pi(10)^r$ de sorte que l'on peut prendre

$$\begin{array}{lll} r_{6i} = 1, & r_{6i+1} = 3, & r_{6i+2} = 2, \\ r_{6i+3} = -1, & r_{6i+4} = -3, & r_{6i+5} = -2. \end{array}$$

Le critère se traduit en

$$7 \mid \sum_{i=0}^k a_i 10^i \iff 7 \mid (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + \dots$$

Ce dernier critère n'est vraiment utile, pour le calcul mental, que pour des nombres n de relativement petite taille. Voyons un autre critère de divisibilité, n'utilisant que des additions pour se ramener à un n de petite taille. Supposons pour ceci que le diviseur $m = p$ est premier, différent de 2 ou 5 de sorte que $\text{pgcd}(p, 10) = 1$. Il existe donc $r \in \mathbb{N}^*$ tel que $\pi(10)^r = \overline{1}$. (Par exemple on peut toujours prendre $r = p - 1$.) Quitte à rajouter quelques coefficients $a_i = 0$ supposons que $k = r \cdot \ell + (r - 1)$ pour $\ell \in \mathbb{N}$. Observons que

$$\begin{aligned} n = \sum_{i=0}^k a_i 10^i &= (a_0 + a_1 10 + \dots + a_{r-1} 10^{r-1}) \\ &\quad + 10^r (a_r + a_{r+1} 10 + \dots + a_{2r-1} 10^{r-1}) + \dots \\ &\quad + 10^{r\ell} (a_{r\ell} + a_{r\ell+1} 10 + \dots + a_{r\ell+(r-1)} 10^{r-1}) \\ &= \sum_{i=0}^{\ell} 10^{r \cdot i} \left(\sum_{j=0}^{r-1} a_{ri+j} 10^j \right). \end{aligned}$$

Finalement, $p \mid n$ si et seulement si

$$p \mid \sum_{i=0}^{\ell} \left(\sum_{j=0}^{r-1} a_{ri+j} 10^j \right).$$

Pour $p = 7$ on peut prendre $r = 6$ et obtenir par exemple

$$7 \mid 123'456'789 \iff 7 \mid 123 + 456'789.$$

S'il existe $s \in \mathbb{N}^*$ tel que $\pi(10)^s = \overline{-1}$. Alors $p \mid m$ si et seulement si

$$p \mid \sum_{i=0}^{\ell} (-1)^i \left(\sum_{j=0}^{r-1} a_{ri+j} 10^j \right),$$

ce qui devient, pour $p = 7$ sensiblement plus agréable :

$$7 \mid 123'456'789 \iff 7 \mid 123 - 456 + 789.$$

A.3 Cryptographie RSA

Cet algorithme de cryptage dit à clé publique a été présenté par Rivest, Shamir et Adleman (d'où le nom RSA) en 1977. Avant de le décrire, précisons ce que nous entendons par cryptographie.

Le problème général est qu'Alice veut recevoir un message de Bob qu'aucun intermédiaire ne doit pouvoir déchiffrer. (C'est toujours une histoire entre Alice et Bob en cryptographie. Parfois s'y ajoutent Charlie, Dan, Eve etc.) Bob doit donc être en mesure d'encoder un message. On pense à un message comme à un nombre : Par exemple naïvement on peut associer aux 26 lettres de l'alphabet le nombre correspondant entre 01 et 26, rajouter éventuellement un 27 pour un espace, de sorte que toute phrase se transforme en un nombre, par concaténation. En pratique ce sera plutôt via le code ASCII. Mais ce n'est pas le point important de l'histoire. Donc Bob doit pouvoir encoder un nombre, et Alice, à l'arrivée le décrypter.

Un exemple datant de Jules César est de shifter l'alphabet par un certain nombre k , ce qui correspond à considérer l'opération $+k \bmod 26$ pour le cryptage, et $-k \bmod 26$ pour le décryptage : Par exemple pour $k = 2$,

$$\text{AVE CESAR} = 1, 22, 5 \quad 3, 5, 19, 1, 18,$$

qui après cryptage devient

$$3, 23, 7 \quad 5, 7, 21, 3, 20 = \text{CXG EGUCT}.$$

Cette méthode de cryptage pose des problèmes évidents : Dans un long texte, on reconnaîtra facilement les lettres apparaissant le plus souvent (comme le E en français), ce qui donnera la clé de décryptage. Plus problématique : Comment envoyer la clé de décryptage $-k \bmod 26$? Il faudrait pouvoir la coder, mais pour la coder, il faut une autre clé de décryptage. On ne s'en sort plus.

Le système RSA résout ce problème. C'est ce qu'on appelle un cryptage à clé publique : tout le monde a accès à la clé de cryptage (Bob, Charlie, Dan, Eve, etc), et peut donc encrypter un message avant de l'envoyer. Mais seule Alice a la clé de décryptage.

En pratique, le cryptage RSA est assez lent, et est typiquement encore utilisé aujourd'hui seulement pour obtenir des clés de cryptages dites privées (connues seulement des deux interlocuteurs), qu'on utilise ensuite pour la poursuite d'un échange confidentiel.

Description du codage RSA

Préparation par Alice :

- A=Alice choisit secrètement deux nombres premiers distincts p et q .
- A calcule $n = pq$ et $\varphi(n) = (p-1)(q-1)$.
- A choisit $e \in \{1, 2, \dots, \varphi(n) - 1\}$ tel que $\text{pgcd}(e, \varphi(n)) = 1$.
- A trouve $d \in \{1, 2, \dots, \varphi(n) - 1\}$ tel que $ed \equiv 1 \bmod \varphi(n)$.
- A publie n et e et conserve secrètement $p, q, \varphi(n)$ et d .

Cryptage par Bob : B=Bob souhaite envoyer secrètement un message à A. Le message est un nombre

$$x \in \{0, 1, 2, \dots, n-1\}.$$

- B calcule $y = x^e \bmod n$ et

— transmet (publiquement) y à A.

Déryptage par Alice : A reçoit y et calcule

$$y^d \pmod n.$$

C'est bien le message x de B : En effet montrons que

$$y^d \pmod n \equiv (x^e)^d \pmod n \equiv x \pmod n.$$

Commençons par montrer que cette égalité est valide modulo p (et donc par symétrie modulo q) : Si p divise x , il n'y rien à montrer $0 \equiv (x^e)^d \pmod p \equiv x \pmod p$. Supposons que ce n'est pas le cas :

$$\begin{aligned} y^d \pmod p &\equiv (x^e)^d \pmod p \\ &\equiv x^{ed} \pmod p \\ &\equiv x^{k\varphi(n)+1} \pmod p && \text{car } ed \equiv 1 \pmod{\varphi(n)} \\ &\equiv x^{k(p-1)(q-1)+1} \pmod p \\ &\equiv (x^{k(q-1)})^{p-1} x \pmod p \\ &\equiv x && \text{par le Petit Théorème de Fermat.} \end{aligned}$$

En particulier p divise $x^{ed} - x$ et par symétrie q aussi. Donc $n = pq$ divise $x^{ed} - x$ et $(x^e)^d \pmod n \equiv x \pmod n$.

Exemple

A choisit $p = 3$ et $q = 11$ et calcule $n = 3 \cdot 11 = 33$ et $\varphi(n) = 2 \cdot 10 = 20$. A choisit $e = 7$ (qui satisfait bien $\text{pgcd}(e, \varphi(n)) = \text{pgcd}(20, 7) = 1$). Pour trouver d tel que $ed \equiv 1 \pmod{20}$, on applique l'algorithme d'Euclide :

$$\begin{aligned} 20 &= 2 \cdot 7 + 6 \\ 7 &= 1 \cdot 6 + 1 \\ 6 &= 6 \cdot 1 + 0, \end{aligned}$$

ce qui implique que

$$1 = 7 - 1 \cdot 6 = 7 - (20 - 2 \cdot 7) = 3 \cdot 7 - 20.$$

Donc $d = 3$.

A publie $n = 33$ et $e = 7$ et garde secrètement tous les autres entiers. B veut envoyer le message $x = 6$. Il calcule

$$\begin{aligned} x^e = 6^7 &= 6^{3 \cdot 2 + 1} = 36^3 \cdot 6 \\ &\equiv 3^3 \cdot 2 \cdot 3 \pmod{33} \equiv 2 \cdot 81 \pmod{33} \\ &\equiv 2 \cdot 15 \pmod{33} \equiv 30 \pmod{33}. \end{aligned}$$

A réceptionne le message crypté $y = 30$ de B et le décrypte en calculant

$$\begin{aligned} y^d &= 30^3 = \\ &\equiv (-3)^3 \pmod{33} \equiv -27 \pmod{33} \\ &\equiv 6 \pmod{33}. \end{aligned}$$

En pratique, les nombres premiers p et q seront plutôt de l'ordre de 10^{100} . La fiabilité du système RSA repose sur le fait qu'il est, à ce jour, très difficile et surtout très long de factoriser un nombre de l'ordre de 10^{200} .