Christophe Mourougane

ALGÈBRE ET ARITHMÉTIQUE 3

Christophe Mourougane

Cours de l'Université de Rennes 1 (2009–2010).
Url : `http://perso.univ-rennes.fr/christophe.mourougane/`

Version du 25 mars 2010

ALGÈBRE ET ARITHMÉTIQUE 3

Christophe Mourougane

TABLE DES MATIÈRES

PARTIE I

STRUCTURES ARITHMÉTIQUES

Introduction

Le premier but de ce cours est de placer les résultats vus en “Algèbre et Arithmétique 1” ou “Algèbre et Arithmétique 2” dans une perspective générale. Les notions de divisibilité, de pgcd, de congruence, les lemmes de Gauss et d’Euclide, le théorème de Bezout, le théorème Chinois, le petit théorème de Fermat et le théorème d’Euler et le théorème de Gauss par exemple seront traduits dans un language abstrait puis généralisés. On pourra alors donner la définition de structures comme les anneaux et les groupes, puis de nouveaux exemples.

CHAPITRE 1

L'ANNEAU $(\mathbb{Z}, +, \times)$

1.1. Notions de groupes

Notre point de départ est l'arithmétique élémentaire sur $\mathbb{Z}$. On cherche à formaliser le concept d'ensemble muni d'opérations, c'est à dire à unifier par exemple l'addition et la multiplication des nombres, l'addition et la multiplication des polynômes.

1.1.1. Les définitions. —

Définition. — *Une loi de composition interne (ou opération) sur un ensemble E est une application*

$$\begin{array}{rccl} f & : & E \times E & \to E \\ & & (a,b) & \mapsto f(a,b) \text{ souvent noté } a \star b. \end{array}$$

On cherche à dégager quelques propriétés qui permettront de calculer comme avec les nombres.

Définition. — *Soit $\star$ une loi de composition interne sur un ensemble E*

- *Elle est dite associative si*

$$\forall (a,b,c) \in E^3,\ (a \star b) \star c = a \star (b \star c).$$

  On peut alors asans ambiguité écrire $a \star b \star c$ car le résultat est le même quelque soit l'ordre dans lequel on effectue ces deux opérations $\star$.
- *Elle admet x comme élément neutre si x est un élément de E et si*

$$\forall a \in E,\ x \star a = a \star x = a.$$

  (Vérifier qu'alors il n'y a pas d'autre élément neutre.)
- *Si elle admet un élément neutre e, le symétrique d'un élément a de E est un élément b de E tel que*

$$a \star b = b \star a = e.$$

Proposition. — *Si la loi interne $\star$ sur l'ensemble E est associative et admet un élément neutre e, alors chaque élement a de E admet au plus un symétrique.*

Démonstration. — Soit b et b' deux symétriques de a. Alors

$$b = b \star (a \star b') = (b \star a) \star b' = b'.$$

□

Définition. — *Un groupe est un ensemble E muni d'une loi de composition interne associative, avec un élément neutre et tel que tout élément admet un symétrique.*

Une propriété de calcul importante mais non requise dans la définition de groupe est

Définition. — *Une loi de composition interne est dite commutative si*

$$\forall (a,b) \in E^2,\ a \star b = b \star a.$$

Exercice. — *La table suivante définit-elle un groupe ?*

$\star$	a	b	c
a	a	b	c
b	b	a	b
c	c	b	a

1.1.2. Les notations. — Il y a trois façons principales de noter l'opération de groupes et ses attributs.

	générale	additive	multiplicative
opération	$\star$	$+$	$\times$
élément neutre	e	0	1
symétrique	symétrique	opposé	inverse
symétrique de a	a'	$-a$	a^{-1}
		$0a = 0$	$x^0 = 1$
puissance	$\underbrace{a \star a \star \cdots \star a}_{k \text{ fois}}$	ka	a^k
puissance négative	$\underbrace{a' \star a' \star \cdots \star a'}_{k \text{ fois}}$	$-ka$	a^{-k}

1.1.3. Morphismes de groupes. —

Définition. — *Un morphisme de groupes est une application $\varphi : (G, \star) \to (F, \otimes)$ entre deux groupes $(G, \star)$ et $(F, \otimes)$ telle que*

$$\forall (a, b) \in G^2,\ \varphi(a \star b) = \varphi(a) \otimes \varphi(b).$$

En d'autres termes, calculer le produit $a \star b$ dans G puis l'envoyer dans F ou envoyer les facteurs a et b dans F puis calculer le produit des images dans F mènent au même résultat.

Exercice. — *Vérifier que l'image de l'élément neutre de G par un tel morphisme de groupes est l'élément neutre de H et que l'image du symétrique d'un élément a de G est le symétrique dans F de $\varphi(a)$.*

1.1.4. Les premiers exemples. — L'ensemble $\mathbb{N}$ des nombres naturels muni de l'addition n'est pas un groupe. La construction de l'ensemble $\mathbb{Z}$ des nombres entiers (relatifs) a permis de donner à chaque entier un opposé. La multiplication dans $\mathbb{Z}$ n'en fait pas un groupe. La construction de l'ensemble $\mathbb{Q}$ des nombres rationels a permis de donner à chaque nombre entier non nul un inverse. En résumé , $(\mathbb{Z}, +)$ et $(\mathbb{Q} - \{0\}, \times)$ sont des groupes.

Exercice. — *La table*

$\star$	a	b
a	a	b
b	b	a

définit un groupe à deux éléments. (Vérifier l'associativité)

L'application

$$\begin{array}{rccc} \exp : (\mathbb{R}, +) & \to & (]0, +\infty[, \times) \\ x & \mapsto & \exp(x) \end{array}$$

est un morphisme de groupes. C'est une façon formelle de formuler la propriété

$$\forall (x, y) \in \mathbb{R}^2,\ \exp(x + y) = \exp(x) \times \exp(y).$$

1.1.5. Sous-groupes. —

Définition. — *Une partie H d'un groupe $(G, \star)$ est appelée sous-groupe de G si l'élément neutre e_G de G est dans H, si H est stable par l'opération $\star$, et si le symétrique calculé dans G de tout élément de H est en fait dans H.*

La loi $\star$ est alors interne dans H et fait de H un groupe.

Un des intérêts de la notion de sous-groupe est le fait que l'associativité (difficile à vérifier sur les tables par exemple) est héritée d'un groupe G sur un sous-groupe H. Elle n'est pas requise dans la définition de sous-groupe, mais provient automatiquement de l'associativité sur le groupe G.

Exercice. — *Le noyau d'un morphisme de groupes $\varphi : (G, \star) \to (F, \otimes)$ est l'image réciproque de e_F. Montrer que le noyau d'un morphisme de groupes $\varphi : (G, \star) \to (F, \otimes)$ est un sous-groupe de G.*

L'intersection de deux sous-groupes de G est encore un sous-groupe de G. Plus généralement, toute intersection de sous-groupes de G est un sous-groupe de G.

Soit P est une partie de G. On considère l'ensemble des sous-groupe de G qui contiennent P et on en cherche un plus petit élément (pour la relation d'ordre donnée par l'inclusion). Comme l'intersection de tous les sous-groupes de G qui contiennent P est un sous-groupe, c'est le plus petit sous-groupe de G qui contient P. On l'appelle *sous-groupe engendré par P* et on le note $< P >$.

Par exemple,

Lemme. — 1. *Le sous-groupe $< a >$ engendré par un élément a de G est l'ensemble de ses puissances positives et négatives*

$$\mathcal{P}(a) = \{g \in G,\ \exists k \in \mathbb{Z}, g = a^k\} = \{\cdots, a^{-2}, a^{-1}, e_G, a, a^2, \cdots\}.$$

2. *Le sous-groupe $< a >$ engendré par un élément a d'ordre fini k dans G est*

$$< a >= \{e_G, a, a^2, \cdots\cdots, a^{k-2}, a^{k-1}\}.$$

Il a exactement k éléments. L'ordre d'un élément (d'ordre fini) est donc le cardinal du sous-groupe engendré.

Démonstration. — 1. En effet, cet ensemble de puissances est un sous-groupe de G, qui contient a et qui est contenu dans tout sous-groupe H qui contient a. (un tel sous-groupe doit contenir par exemple a^2 ou a^{-1}.)

2. Comme $a^k = e_G$, $< a >= \mathcal{P}(a) = \{e_G, a, a^2, \cdots\cdots, a^{k-2}, a^{k-1}\}$. Comme k est la plus petite puissance p non nulle telle que $a^p = e_G$, les élements $e_G, a, a^2, \cdots\cdots, a^{k-2}, a^{k-1}$ sont deux à deux distincts. En effet si $a^i = a^j$ avec $j \geq i$, alors $a^{j-i} = e_G$ et $0 \geq j - i \leq k - 1$, ce qui implique que $i = j$.

□

Le sous-groupe engendré par deux éléments est en général délicat à décrire.

Exercice. — *Décrire le sous-groupe d'un groupe G engendré par deux éléments a et b qui commutent.*

Définition. — *Un groupe est dit monogène s'il admet un élément a tel que $G =< a >$. On dit alors que a est un générateur de G. Un groupe est dit cyclique s'il est monogène et fini.*

Le groupe $(\mathbb{Z}, +)$ est monogène mais pas cyclique. Ses générateurs sont 1 et -1. Le groupe $(\mathbb{R}[X], +)$ n'est pas monogène. Les groupes monogènes sont commutatifs.

1.2. Notions d'anneaux commutatifs

1.2.1. Les définitions. —

Définition. — *Un anneau est un ensemble A muni de deux lois de composition internes $+$ et $\times$ telles que*

- *$(A, +)$ est un groupe commutatif d'élément neutre noté 0_A.*
- *$\times$ est associative et admet un élément neutre noté 1_A.*
- *La multiplication $\times$ est distributive par rapport à l'addition $+$.*

$$\forall (x, y, z) \in A^3,\ (x + y) \times z = (x \times z) + (y \times z) \text{ et } z \times (x + y) = (z \times x) + (z \times y).$$

Si la multiplication est commutative, on dit que l'anneau $(A, +, \times)$ est commutatif. (L'addition est commutative par hypothèse).

La définition d'anneau commutatif contient toutes les règles de calcul nécessaires par exemple pour démontrer la formule du binôme.

Exercice. — *Vérifier que si A est un anneau commutatif,*

$$\forall (x, y) \in A^2,\ (x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3.$$

Ainsi à chaque fois que nous pourrons vérifier que deux opérations sur un ensemble en font un anneau commutatif, on pourra utiliser la formule du binôme.

1.2.2. Les notations et priorités de calcul. — Nous avons l'habitude dans une expression comme $x^3 + 3x^2y + 3xy^2 + y^3$ de reconnaître que les signes de multiplication sont omis et ce sont les multiplications qu'il faut effectuer avant les additions. Nous garderons ces conventions d'écriture pour tout anneau et nous écririons par exemple la distributivité comme

$$\forall (x, y, z) \in A^3,\ (x + y)z = xz + yz \text{ et } z(x + y) = zx + zy.$$

1.2.3. Morphismes d'anneaux. —

Définition. — *Un morphisme d'anneaux est une application $f : (A, +, \times) \to (B, \oplus, \otimes)$ entre deux anneaux $(A, +, \times)$ et $(B, \oplus, \otimes)$ telle que*

1. $\forall (a, b) \in A^2,\ f(a + b) = f(a) \oplus f(b)$ *(f est un morphisme de groupes)*
2. $\forall (a, b) \in A^2,\ f(a \times b) = f(a) \otimes f(b)$ *et* $f(1_A) = 1_B$.

Noter que la propriété $f(0_A) = 0_B$ n'est pas requise mais résulte de la première condition.

Un isomorphisme de groupes (resp. d'anneaux) est par définition un morphisme de groupes (resp. d'anneaux) qui est une bijection et dont la bijection réciproque est aussi un morphisme de groupes (resp. d'anneaux). On peut vérifier qu'un morphisme de groupes (resp. d'anneaux) qui est une bijection est un isomorphisme de groupes (resp. d'anneaux).

Un isomorphisme de groupes conserve les propriétés de base du groupe, comme la commutativité, l'ordre des éléments, la structure des sous-groupes...

1.2.4. Les premiers exemples. — Le triplet $(\mathbb{Z}, +, \times)$ sera pour nous le prototype d'un anneau commutatif.

Les tables

$+$	a	b
a	a	b
b	b	a

et

$\times$	a	b
a	a	a
b	a	b

font de $\{a, b\}$ un anneau commutatif.

Nous utiliserons aussi les anneaux $(k[X], +, \times)$ de polynômes à une indéterminée sur un corps k.

1.2.5. Idéaux des anneaux commutatifs. — La notion de sous-anneau ne nous sera pas utile. Par contre, il est important de connaître la définition d'idéal.

Définition. — *Une partie I d'un anneau commutatif $(A, +, \times)$ est appelée idéal de A si c'est un sous-groupe de $(A, +)$ et si*

$$\forall m \in I, \forall a \in A,\ m \times a \text{ calculé dans } A \text{ est dans } I.$$

On demande bien plus que le fait que I soit stable par la multiplication.

Exercice. — *Montrer qu'un idéal d'un anneau commutatif A qui contient l'élément 1_A est en fait égal à A tout entier.*

Exercice. — *Le noyau d'un morphisme d'anneaux $f : (A, +, \times) \to (B, \oplus, \otimes)$ est l'image réciproque de 0_B. Montrer que le noyau d'un morphisme d'anneau est un idéal.*

Comme toute intersection d'idéaux d'un anneau commutatif est un idéal, on peut introduire la notion d'idéal engendré par une partie. Dans $\mathbb{Z}$, l'idéal engendré par 2 est l'ensemble des entiers relatifs pairs, et plus généralement l'idéal engendré par un entier m est l'ensemble $m\mathbb{Z}$ des multiples de m.

1.3. La division euclidienne et les sous-groupes de $\mathbb{Z}$

1.3.1. Structure des sous-groupes de $\mathbb{Z}$. — Rappelons le

Théorème de la division euclidienne. — *Soit a et d deux entiers relatifs, avec $d \neq 0$. Il existe des entiers relatifs q et r, uniques, tels que $a = dq + r$ et $0 \leq r \leq |d| - 1$.*

Dans $\mathbb{Z}$, la notation na signifie vis-à-vis de l'addition $\underbrace{a + a + \cdots + a}_{n \text{ fois}}$ et vis à vis de la multiplication $n \times a$. Mais par construction de ces deux opérations à partir de la fonction successeur des axiomes de Peano ces deux quantités coïncident. La formalisation du théorème de la division euclidienne avec le language des groupes et anneaux est le

Théorème. — 1. *Les sous-groupes de $(\mathbb{Z}, +)$ sont monogènes. Chaque sous-groupe de $(\mathbb{Z}, +)$ est donc l'ensemble des multiples d'un entier m, et s'écrit donc de la forme $m\mathbb{Z}$.*
2. *Les sous-groupes de $(\mathbb{Z}, +)$ sont des idéaux de $(\mathbb{Z}, +, \times)$.*

Démonstration. — Soit A un sous-groupe de $(\mathbb{Z}, +)$. Si $A = \{0\}$ alors $A = 0\mathbb{Z}$. Sinon, si a est un élément non nul de A, soit a soit $-a$ est un élément de $(A - \{0\}) \cap \mathbb{N}$. Cet ensemble, sous ensemble non vide de $\mathbb{N}$ a un plus petit élément, noté m. Comme m est dans A, l'ensemble $m\mathbb{Z}$ de ses multiples est donc dans le sous-groupe A. Récirpoquement, soit a un élément de A. Effectuons la division euclidienne de a par m non nul. Il existe $(q, r) \in \mathbb{Z}^2$ tel que $a = qm + r$ et $0 \leq r < m$. Comme $r = a - qm$, r est dans le sous-groupe A. Comme m est le plus petit élément strictement positif de A et comme $0 \leq r < m$, r est nul et donc a est un multiple de m. □

1.3.2. Divisibilité et sous-groupes. — Le théorème de la dicision euclidienne et en particulier l'algorithme d'Euclide étendu nous ont permis de montrer que le pgcd de deux entiers a et b n'est pas simplement un diviseur commun plus grand que tous les diviseurs communs de a et b mais même un multiple de tous les diviseurs communs de a et b. La structure des idéaux de $\mathbb{Z}$ permet de donner une nouvelle caractérisation du pgcd, qui sera généralisable à tous les anneaux avec division euclidienne. Par définition,

$$a\mathbb{Z} + b\mathbb{Z} := \{n \in \mathbb{Z},\ \exists (u, v) \in \mathbb{Z}^2, n = au + bv\}.$$

Proposition. — *Soit a et b deux entiers.*

1. *a est un multiple de b $\iff$ $a\mathbb{Z} \subset b\mathbb{Z}$*
2. *$a\mathbb{Z} + b\mathbb{Z} = \text{pgcd}(a, b)\mathbb{Z}$.*
3. *$a\mathbb{Z} \cap b\mathbb{Z} = \text{ppcm}(a, b)\mathbb{Z}$.*

Démonstration. —

1. Si a est multiple de b, a est dans le sous-groupe $b\mathbb{Z}$ et donc le sous-groupe $a\mathbb{Z}$ engendré par a aussi. Réciproquement, si $a\mathbb{Z} \subset b\mathbb{Z}$, $a \times 1 = a$ est un multiple de b.
2. a est multiple de $\text{pgcd}(a, b)\mathbb{Z}$. Par la propriété précédente, $a\mathbb{Z} \subset \text{pgcd}(a, b)\mathbb{Z}$ et de même $b\mathbb{Z} \subset \text{pgcd}(a, b)\mathbb{Z}$. Comme $\text{pgcd}(a, b)\mathbb{Z}$ est stable par addition, $a\mathbb{Z} + b\mathbb{Z} \subset \text{pgcd}(a, b)\mathbb{Z}$. Réciproquement, par le théorème de Bezout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = \text{pgcd}(a, b)$. Par conséquent, $\text{pgcd}(a, b)$ est dans $a\mathbb{Z} + b\mathbb{Z}$. Par suite, tout le groupe engendré $\text{pgcd}(a, b)\mathbb{Z}$ est dans $a\mathbb{Z} + b\mathbb{Z}$.
3. Par la première propriété, $\text{ppcm}(a, b)\mathbb{Z} \subset a\mathbb{Z}$ et $\text{ppcm}(a, b)\mathbb{Z} \subset b\mathbb{Z}$, soit $\text{ppcm}(a, b)\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$.

□

CHAPITRE 2

LES ANNEAUX $\mathbb{Z}/n\mathbb{Z}$

2.1. Rappels sur les relations d'équivalence

Définition. — *Une relation $\mathcal{R}$ sur un ensemble E réflexive, symétrique et transitive est appelée* relation d'équivalence.

La classe d'équivalence (notée $cl(x)$ ou $[x]_{\mathcal{R}}$) d'un élément x de E est le sous-ensemble de E des éléments en relation avec x. Un élément x de E est dit représentant d'une classe C si x appartient à C. Les classes d'équivalence forment une partition de l'ensemble E. Réciproquement toute partition de E en sous-ensembles définit une relation d'équivalence sur E, en décrétant que deux éléments sont en relation si et seulementsi ils sont dans le même sous-ensemble.

Définition. — *Par définition, l'ensemble quotient de E par la relation d'équivalence $\mathcal{R}$ est l'ensemble de toutes les classes d'équivalence.*

C'est un ensemble dont les éléments sont des parties non vides de E, les classes d'équivalence. On le note souvent $E/\mathcal{R}$; Le passage à la classe d'équivalence définit une application π

$$\begin{array}{rccc} \pi & : & E & \to & E/\mathcal{R} \\ & & x & \mapsto & [x]_{\mathcal{R}} \end{array}$$

Cette application π est surjective et on l'appelle projection naturelle.

2.2. Classes modulo un sous-groupe

Soit $(G,+)$ un groupe et H un sous-groupe. On définit une relation $\mathcal{R}_H$ sur G en posant

$$y\mathcal{R}_H x \iff y - x \in H$$

autrement dit

$$y\mathcal{R}_H x \iff \exists h \in H,\ y = x + h.$$

Puisque H est un sous-groupe, c'est une relation d'équivalence. Soit x un élément du groupe G. La classe d'équivalence de l'élément x, appelée classe de x modulo H, est

$$[x]_H = \{y \in G,\ -x + y \in H\} = \{y \in G, \exists h \in H, y = x + h\} = x + H.$$

L'ensemble quotient $G/\mathcal{R}_H$ est simplement noté G/H. L'application $H \to x + H$, $h \mapsto x + h$ est une bijection. En particulier, si H est fini toutes les classes ont le même cardinal. Le cardinal d'un groupe est aussi appelé ordre du groupe. On obtient donc le

Théorème de Lagrange. — *Si G est un groupe fini et H un sous-groupe*

$$\operatorname{card} G = \operatorname{card}(G/H) \operatorname{card} H.$$

En particulier, dans un groupe fini l'ordre d'un élément divise l'ordre du groupe.

2.3. Groupe quotient

On suppose ici que le groupe G est commutatif.

Lemme. — *Soit $(G,+)$ un groupe commutatif et H un sous-groupe de G. Alors*

$$\begin{pmatrix} x\mathcal{R}_H x' \\ y\mathcal{R}_H y' \end{pmatrix} \Rightarrow (x+y)\mathcal{R}_H(x'+y')$$

autrement dit

$$\begin{pmatrix}[x]_H = [x']_H \\ [y]_H = [y']_H\end{pmatrix} \Rightarrow [x+y]_H = [x'+y']_H$$

Démonstration. — Si $x\mathcal{R}_H x'$ et $y\mathcal{R}_H y'$, il existe h et l dans H tels que $x' = x+h$ et $y' = y+l$. Par conséquent, $x'+y' = x+h+x'+l = x+x'+(h+l)$ car G est commutatif. Comme $h+l$ appartient à H, $x'+y'$ et $x+x'$ diffèrent d'un élément de H et donc $(x+y)\mathcal{R}_H(x'+y')$. □

Le lemme précédent permet de construire sur l'ensemble G/H des classes d'équivalence modulo le sous-groupe H une opération $\oplus$ qui en fait un groupe.

Opération sur le groupe quotient. — *La somme $X \oplus Y$ de deux classes d'équivalence modulo H est la classe d'équivalence modulo H qui contient toutes les sommes $x+y$ d'éléments x de X par un élément y de Y.*

Proposition. — *Soit $(G,+)$ un groupe commutatif et H un sous-groupe. L'ensemble G/H muni de l'opération précédente est un groupe et l'application naturelle $\pi : G \to G/H$ devient un morphisme de groupes $\pi : (G,+) \to (G/H, \oplus)$.*

Démonstration. — Pour montrer l'associativité de $\oplus$, on considère trois classes X, Y, Z et on choisit trois représentants respectifs x, y, z.

$$(X \oplus Y) \oplus Z = [x+y] \oplus Z = [(x+y)+z] = [x+(y+z)] = X \oplus (Y \oplus Z).$$

La classe $[e_G]$ de l'élément neutre de G est l'élément neutre de G/H car pour toute classe X, ayant choisi un représentant x, on a

$$X \oplus [e] = [x] \oplus [e] = [x+e] = [x] = X.$$

Le symétrique de la classe X de représentant x est la classe de $-x$ car

$$X \oplus [-x] = [x] \oplus [-x] = [x+(-x)] = [e] = e_{G/H}.$$

Pour montrer que π devient un morphisme de groupes, on considère deux éléments x et y de G,

$$\pi(x+y) = [x+y] = [x] \oplus [y] = \pi(x) \oplus \pi(y).$$

□

2.4. Anneau quotient

Nous reprenons les constructions d'opérations sur l'ensemble quotient en partant cette fois d'un anneau commutatif, plutôt que d'un groupe commutatif et d'un idéal plutôt que d'un sous-groupe.

Lemme. — *Soit $(A,+,\times)$ un anneau commutatif et I un idéal de A. Alors*

$$\begin{pmatrix}x\mathcal{R}_I x' \\ y\mathcal{R}_I y'\end{pmatrix} \Rightarrow (x+y)\mathcal{R}_I(x'+y')$$

autrement dit

$$\begin{pmatrix}[x]_I = [x']_I \\ [y]_I = [y']_I\end{pmatrix} \Rightarrow [x+y]_I = [x'+y']_I$$

et

$$\begin{pmatrix}x\mathcal{R}_I x' \\ y\mathcal{R}_I y'\end{pmatrix} \Rightarrow (x\times y)\mathcal{R}_I(x'\times y')$$

autrement dit

$$\begin{pmatrix}[x]_I = [x']_I \\ [y]_I = [y']_I\end{pmatrix} \Rightarrow [x \times y]_I = [x' \times y']_I$$

Démonstration. — La première partie résulte du fait qu'un idéal de $(A, +, \times)$ est en particulier un sous-groupe de $(A, +)$. Pour la seconde partie, soit $(x, x', y, y') \in A^4$ tel que $x\mathcal{R}_I x'$ et $y\mathcal{R}_I y'$. Il existe donc $i \in I$ et $j \in I$ tels que $x' = x + i$ et $y' = y + j$.

$$x' \times y' = (x + i) \times (y + j) = xx' + xj + iy + ij.$$

Comme I est un idéal, xj et iy et ij sont dans I et par suite leur somme aussi. Ainsi, $x' \times y'$ diffère de $x \times y$ par un élément de I. □

Opérations sur l'anneau quotient. — *La somme $X \oplus Y$ de deux classes d'équivalence modulo I est la classe d'équivalence modulo I qui contient toutes les sommes $x + y$ d'éléments x de X par un élément y de Y.*

Le produit $X \otimes Y$ de deux classes d'équivalence modulo I est la classe d'équivalence modulo I qui contient toutes les produits $x \times y$ d'éléments x de X par un élément y de Y.

On en déduit comme précédement

Proposition. — *Soit $(A, +, \times)$ un anneau commutatif et I un idéal de A. L'ensemble A/I muni des deux opérations précédentes est un anneau l'application naturelle $\pi : A \to A/I$ devient un morphisme d'anneaux $\pi : (A, +, \times) \to (G/H, \oplus, \otimes)$ dont le noyau est l'idéal I.*

2.5. Les relations de congruence et les anneaux $\mathbb{Z}/n\mathbb{Z}$

Dans tout ce paragraphe n désignera un entier relatif fixé.

Proposition. — *La relation de congruence modulo n dans l'ensemble $\mathbb{Z}$ coïncide avec la relation modulo l'idéal $n\mathbb{Z}$.*

Démonstration. — En effet, d'une part $y = x \pmod n \iff \exists k \in \mathbb{Z}, y = x + kn$ et d'autre part $y\mathcal{R}_{n\mathbb{Z}}x \iff y - x \in n\mathbb{Z}$. □

Les opérations sur l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ reflètent donc les propriétés que nous avions établies sur les congruences.

Les tables d'opérations sur $\mathbb{Z}/4\mathbb{Z}$ sont

$+$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

et

$+$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$

Les tables d'opérations sur $\mathbb{Z}/5\mathbb{Z}$ sont

$+$	$[0]_5$	$[1]_5$	$[2]_5$	$[-2]_5$	$[-1]_5$
$[0]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[-2]_5$	$[-1]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[-2]_5$	$[-1]_5$	$[0]_5$
$[2]_5$	$[2]_5$	$[-2]_5$	$[-1]_5$	$[0]_5$	$[1]_5$
$[-2]_5$	$[-2]_5$	$[-1]_5$	$[0]_5$	$[1]_5$	$[2]_5$
$[-1]_5$	$[-1]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[-2]_5$

et

$+$	$[0]_5$	$[1]_5$	$[2]_5$	$[-2]_5$	$[-1]_5$
$[0]$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$
$[1]$	$[0]_5$	$[1]_5$	$[2]_5$	$[-2]_5$	$[-1]_5$
$[2]$	$[0]_5$	$[2]_5$	$[-1]_5$	$[1]_5$	$[-2]_5$
$[-2]$	$[0]_5$	$[-2]_5$	$[1]_5$	$[-1]_5$	$[2]_5$
$[-1]$	$[0]_5$	$[-1]_5$	$[-2]_5$	$[2]_5$	$[1]_5$

2.6. Le lemme d'Euclide et la condition d'intégrité

La table de multiplication de $\mathbb{Z}/4\mathbb{Z}$ fait apparaître une pathologie : le carré de l'élément non nul $[2]_4$ est nul.

Définition. — – *Un élément a non nul d'un anneau commutatif A est appelé diviseur de zéro s'il existe un élément b non nul tel que $ab = 0$ dans A.*
– *Un élément a d'un anneau commutatif A est dit simplifiable si toute égalité $ab = ac$ dans A implique $b = c$.*
– *Un élément a d'un anneau commutatif est dit inversible dans A s'il existe b dans A tel que $ab = 1$.*

Lemme. — *Dans un anneau commutatif, tout élément inversible est simplifiable et tout élément diviseur de 0 est non simplifiable.*

Démonstration. — Si a est inversible et $ab = ac$ en multipliant par l'inverse a' de a, on obtient $b = c$. Si a est un diviseur de zéro, il existe tel que $a \times b = 0 = a \times 0$ mais $b \neq 0$. □

Définition. — – *Un anneau commutatif sans diviseur de zéro est dit intègre.*
– *Un anneau commutatif dont tous les éléments non nuls sont inversibles est appelé un corps commutatif.*

En particulier un corps commutatif est intègre.

Proposition. — *L'ensemble $(A^\times, \times)$ des inversibles d'un anneau A muni de la multiplication est un groupe.*

Démonstration. — Le produit de deux éléments inversibles a et b est inversible d'inverse $b^{-1}a^{-1}$. La multiplication fournit donc une opération interne sur $A^\times$. Son associativité résulte de l'associativité de la multiplication $\times$ sur A. L'élément 1_A neutre pour la multiplication sur A est neutre pour la multiplication sur $A^\times$. Si a est inversible a^{-1} l'est aussi. Tout élément de $A^\times$ admet donc un symétrique dans $(A^\times, \times)$. □

Si n n'est pas premier, $\mathbb{Z}/n\mathbb{Z}$ a des diviseurs de zéro. Si n est premier, si $[a]_n \neq 0$ et $[a]_n[b]_n = 0$, n divise ab mais n ne divise pas a donc par le lemme d'Euclide n divise b et $[b]_n = 0$. Par conséquent, la traduction du lemme d'Euclide est le fait que si n est premier $\mathbb{Z}/n\mathbb{Z}$ est intègre.

On rappelle que par définition un entier a de $\mathbb{Z}$ est inversible modulo n s'il existe un entier b de $\mathbb{Z}$ tel que $ab = 1 \pmod{n}$. Il est donc équivalent de dire que l'entier a de $\mathbb{Z}$ est inversible modulo n et de dire que la classe $[a]_n$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

On obtient donc comme traduction du théorème obtenu en première année, comme conséquence du théorème de Bezout.

Théorème. — *Une classe X de $\mathbb{Z}/n\mathbb{Z}$ est inversible (dans $\mathbb{Z}/n\mathbb{Z}$) si et seulement si elle est représentée par un entier premier avec n.*

Les conséquences sont nombreuses. On rappelle que la fonction φ d'Euler est définie par

$$\varphi(n) := \text{card}\{m \in \{1, 2, \cdots n\},\ n \wedge m = 1\}.$$

Il y a $\varphi(n)$ éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$. Plus précisément,

Théorème. — *L'ensemble* $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ *des inversibles de* $\mathbb{Z}/n\mathbb{Z}$ *muni de la multiplication est un groupe de cardinal* $\varphi(n)$. *En particulier, on retrouve le théorème d'Euler. Soit* a *un entier premier avec* n. *Alors* $a^\varphi \equiv 1 \pmod{n}$.

Démonstration. — Le théorème d'Euler provient avec le formalisme des groupes et anneaux du théorème de Lagrange. □

Exercice. — *Ecrire la liste des éléments de* $(\mathbb{Z}/10\mathbb{Z})^\times$ *et sa table de multiplication.*

Si n est premier tous les éléments non nuls de $\mathbb{Z}/n\mathbb{Z}$ sont inversibles, et $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Théorème. — *L'anneau* $\mathbb{Z}/n\mathbb{Z}$ *est un corps si et seulement si* n *est premier.*

Si p est un nombre premier, le corps $\mathbb{Z}/p\mathbb{Z}$ est noté $\mathbb{F}_p$.

2.7. Le théorème Chinois

Définition. — *Une application* $f : E \to F$ *entre deux ensembles* E *muni d'une relation* $\mathcal{R}$ *et* F *est dite* compatible à $\mathcal{R}$ *si*

$$\forall (x, x') \in E^2,\ x\mathcal{R}y \Rightarrow f(x) = f(y).$$

Par une application compatible f, tous les éléments d'une même classe d'équivalence C pour $\mathcal{R}$ ont la même image. On peut donc définir une application $\underline{f}$ de $E/\mathcal{R}$ dans F qui à une classe C associe l'image commune par f de ses éléments. On dit alors que $\underline{f}$ est bien définie sur l'ensemble quotient $E/\mathcal{R}$ et on a $f = \underline{f} \circ \pi$

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ \downarrow{\scriptstyle \pi} & \nearrow_{\underline{f}} & \\ E/\mathcal{R} & & \end{array}$$

Théorème de factorisation. — *Soit* $f : (A, +, \times) \to (B, \boxplus, \boxtimes)$ *un morphisme d'anneaux. Soit* I *un idéal de* A. *Soit* π *la projection naturelle de* A *dans* A/I. *Si* I *est inclus dans le noyau* $N(f)$ *de* f *alors il existe un morphisme d'anneaux* $\underline{f} : ((A/I, \oplus, \otimes) \to (B, \boxplus, \boxtimes)$ *tel que* $f = \underline{f} \circ \pi$.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle \pi} & \nearrow_{\underline{f}} & \\ A/I & & \end{array}$$

Démonstration. — Si I est inclus dans le noyau $N(f)$, tous les éléments d'une même classe $a+I$ modulo I ont même image par f car

$$f(a+i) = f(a) \boxplus f(i) = f(a) \boxplus 0_B = f(a).$$

On peut donc définir une application $\underline{f}$ de A/I dans B qui à une classe C associe l'image commune par f de ses éléments. Pour montrer que $\underline{f}$ est un morphisme d'anneaux, il suffit de prendre C et C' dans A/I deux représentants x et x' dans A et remarquer que

$$\underline{f}(C \oplus C') = f(x + x') = f(x) \boxplus f(x') \text{ et } \underline{f}(C \otimes C') = f(x \times x') = f(x) \boxtimes f(x')$$

et enfin

$$\underline{f}(1_{A/I}) = \underline{f}([1]_I) = \underline{f}(\pi(1_A)) = f(1_A) = 1_B.$$

□

Exercice. — *Énoncer un théorème de factorisation pour les morphismes de groupes.*

Comme conséquence, en remarquant que si l'entier n divise l'entier N alors l'ideal $N\mathbb{Z}$ est inclus dans $n\mathbb{Z}$ le noyau de la projection naturelle $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

Proposition. — *Si l'entier n divise l'entier N alors il existe un morphisme d'anneaux $\underline{f} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Ce morphisme est surjectif.*

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\pi_n} & \mathbb{Z}/n\mathbb{Z} \\ {\scriptstyle \pi_N}\downarrow & \nearrow_{\underline{f}} & \\ \mathbb{Z}/N\mathbb{Z} & & \end{array}$$

Soit m et n deux entiers. On munit le produit cartésien $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ des opérations coordonnées par coordonnées. On obtient ainsi un anneau $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, \boxplus, \boxtimes)$. L'application qui a un entier a associe le couple $([a]_n, [a]_m)$ de ses classes modulo n et m est ainsi un morphisme d'anneaux dont le noyau est

$$\{a \in \mathbb{Z}, [a]_m = 0 \text{ et } [a]_m = 0\} = m\mathbb{Z} \cap n\mathbb{Z} = \text{ppcm}(m,n)\mathbb{Z}.$$

On notera $N := \text{ppcm}(m,n)$. Par la proposition précédente, on peut donc construire un morphisme d'anneaux

$$\begin{array}{rccc} \underline{f} : & \mathbb{Z}/N\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & C = [a]_N & \mapsto & ([a]_n, [a]_m) \end{array}$$

Montrons que cette application est injective. Si $\underline{f}(C) = \underline{f}(C')$, avec $a \in C$ et $a' \in C'$ on obtient $[a]_m = [a']_m$ et $[a]_n = [a']_n$, soit m divise $a' - a$ et n divise $a' - a$. On en déduit que $N = \text{ppcm}(m,n)$ divise $a' - a$ et $C = [a]_N = [a']_N = C'$.

Théorème chinois. — *Si m et n sont deux entiers premiers entre eux, les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont isomorphes. En conséquence, si a et b sont deux entiers fixés, le système d'inconnue $x \in \mathbb{Z}$,*

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

a pour pour ensemble de solutions une classe et une seule modulo mn.

Démonstration. — Le produit $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est de cardinal mn. Comme une application injective entre ensembles finis de même cardinal est bijective, l'application $\underline{f} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ et une bijection qui est un morphisme d'anneaux. On peut alors vérifier que son inverse est un morphisme d'anneaux. Reprenons le diagramme

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\pi_m \times \pi_n} & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ {\scriptstyle \pi_N}\downarrow & \nearrow_{\underline{f}} & \\ \mathbb{Z}/N\mathbb{Z} & & \end{array}$$

Comme l'ensemble des solutions du système est l'image réciproque de $([a]_m, [b]_n)$ par $\pi_m \times \pi_n$, et comme $\underline{f}$ est une bijection, l'ensemble cherché est la classe de $\underline{f}^{-1}([a]_m, [b]_n)$ modulo N. □

Corollaire. — *Si m et n sont deux entiers premiers entre eux, $\varphi(mn) = \varphi(m)\varphi(n)$.*

Démonstration. — Il suffit de vérifier que le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est le produit cartésien $(\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$ de cardinal $\varphi(m)\varphi(n)$. □

CHAPITRE 3

LES ANNEAUX DE POLYNÔMES

3.1. Division euclidienne et structure des idéaux de $k[X]$

Rappelons le théorème de la division euclidienne sur les anneaux $k[X]$ de polynômes à une indéterminée à coefficients dans un corps commutatif k.

Théorème de la division euclidienne dans $k[X]$. — *Soit $D \in k[X]$ un polynôme non nul. Pour tout polynôme A de $k[X]$ il existe un unique couple $Q, R) \in (k[X])^2$ tel que*

$$A = DQ + R$$
$$\deg R < \deg D.$$

On peut ensuite tirer des conséquences sur la structure des idéaux de $k[X]$.

Théorème. — *Les idéaux de $k[X]$ sont exactement les ensembles des multiples d'un polynôme de $k[X]$.*

On notera $(D) = Dk[X]$ l'ensemble des multiples d'un polynôme D de $k[X]$. La démonstration est analogue à celle de la structure des sous-groupes de $\mathbb{Z}$. Le générateur D d'un idéal I non réduit à $\{0\}$ est choisi comme un polynôme de degré minimal dans $I - \{0\}$. Si a_d est le coefficient dominant de D, comme $a_d^{-1}D$ appartient à l'idéal I, on peut même supposer que D est unitaire.

3.2. Calculs dans $k[X]/(D)$

Soit $D = a_dX^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0$ un polynôme de $k[X]$. On suppose D unitaire, c'est à dire $a_d = 1$. On note $\alpha = [X]$ la classe du polynôme X dans $k[X]/(D)$. Comme la classe de D est nulle, on obtient la relation dans l'anneaux $k[X]/(D)$

$$\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_1\alpha + a_0 = [0] \text{ soit } \alpha^d = -a_{d-1}\alpha^{d-1} - \cdots - a_1\alpha - a_0.$$

Ainsi, en substituant cette relation dans tout polynôme on obtient que dans toute classe, il y a un représentant de degré strictement inférieur à d. Plus précisément, en effectuant la division euclidienne de P par D on vérifie que la classe d'équivalence de P modulo D contient un unique polynôme R de degré strictement inférieur au degré de D. Comme pour spécifier un polynôme de degré strictement inférieur à d il faut d coefficients dans k, on obtient en particulier,

Proposition. — *Soit k un corps commutatif fini et D un polynôme de degré $d = \deg D$ de $k[X]$. Alors l'anneau $k[X]/(D)$ est fini de cardinal p^d. (C'est même un espace vectoriel sur le corps k, de dimension d qui admet pour base $(1_k, \alpha, \alpha^2, \cdots \alpha^{d-1})$.)*

3.3. Théorème de Bezout et structure de $k[X]/(D)$

Pour préciser la structure des anneaux quotients $k[X]/(D)$, on introduit la définition

Définition. — *Un polynôme est dit constant s'il est de dégré nul. Un polynome D de $k[X]$ est dit réductible s'il existe deux polynômes non constants A et B tels que $D = AB$, et irréductible sinon.*

Si $D = AB$ est réductible (où A et B sont deux polynômes non constants), $k[X]/(D)$ n'est pas intègre car $[A][B] = [0]$ alors que A et B de degré strictement plus petit que $\deg D$ ne sont pas multiples de D et donc $[A] \neq [0]$ et $[B] \neq [0]$ dans $k[X]/(D)$.

Les diviseurs d'un polynôme irréductible sont les polynômes constants et ses multiples. On voit ici l'analogie entre polynômes irréductibles et nombres premiers. Ainsi, un polynôme irréductible

D est premier avec tous les polynômes non multiples de D. Comme conséquence du théorème de Bezout, on obtient

Théorème. — *L'anneau $k[X]/(D)$ est un corps si et seulement si D est irréductible.*

Proposition. — *Les seuls polynômes irréductibles de $\mathbb{F}_2[X]$ de degré 2 est X^2+X+1 et de degré 3 sont X^3+X+1 et X^3+X^2+1. Les seuls polynômes irréductibles de $\mathbb{F}_3[X]$ de degré 2 sont X^2+1 et X^2+X+2 et X^2+2X+2.*

Démonstration. — Comme les polynômes de degré 1 ont une racine, il en est de même pour les polynômes réductibles de degré 2 ou 3. Réciproquement, un polynôme de degré 2 ou 3 qui admet une racine r dans $\mathbb{F}_2$ est divisible par $(X-r)$ dans $\mathbb{F}_2[X]$ et donc réductible. Il suffit donc de déterminer parmi les 2^2 polynômes de degré 2 et 2^3 polynômes de degré 3 ceux qui n'ont ni $[0]_2$ ni $[1]_2$ comme racine. □

On obtient donc l'exemple de corps finis : $K=\mathbb{F}_2[X]/(X^2+X+1)$.
On note α la classe du polynôme X. Comme $1+1=2=0$ dans $\mathbb{F}_2$,

$$[X+X]=[2X]=\alpha+\alpha=0.$$

On retient aussi la relation

$$[X^2+X+1]=\alpha^2+\alpha+1=0$$

soit $\alpha^2=\alpha+1$.

Comme toute classe admet un représentant qui est un polynôme de degré inférieur à 1, le corps K a comme élément 0, 1, α $\alpha+1$. Enfin, le théorème de Lagrange montre que dans le groupe $\big(\mathbb{F}_2[X]/(X^2+X+1)\big)^\times$ des inversibles qui est d'ordre 3, l'élément inversible α par exemple vérifie

$$\alpha^3=1.$$

La table d'addition

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

La table de multiplication s'obtient par utilisation de la relation $\alpha^2=\alpha+1$.

$\times$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

On voit que la table du groupe des inversibles

$\times$	1	α	$\alpha+1$
1	1	α	$\alpha+1$
α	α	$\alpha+1$	1
$\alpha+1$	$\alpha+1$	1	α

est semblable à la table de $(\mathbb{Z}/3\mathbb{Z},+)$

$\times$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.

Le but des chapitres à venir est de montrer que ce phénomène est général.

PARTIE II

EXEMPLES DE GROUPES

CHAPITRE 4

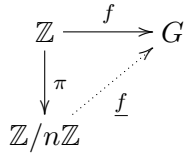
GROUPES CYCLIQUES

4.1. Propriétés des groupes cycliques

On rappelle qu'un groupe G est dit cyclique s'il est monogène et fini.

Proposition. — *Tout groupe cyclique d'ordre n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.*

Démonstration. — Soit G un groupe cyclique d'ordre n et g un générateur. On considère l'application $f : (\mathbb{Z}, +) \to (G, \star)$, $a \mapsto g^a$. C'est un morphisme de groupes. Son noyau $f^{-1}(e_G)$ contient l'ensemble $n\mathbb{Z}$ des multiples de n. Son image est le sous-groupe $< g >$ engendré par g et donc G. Par le théorème de factorisation des morphismes de groupes, il existe un morphisme $\underline{f} : \mathbb{Z}/n\mathbb{Z} \to G$



Le morphisme $\underline{f}$ est surjectif et comme $\mathbb{Z}/n\mathbb{Z}$ et G ont même cardinal, $\underline{f}$ est un isomorphisme de groupes. □

Même si ce théorème affirme que les groupes cycliques sont bien connus, leur richesse réside dans la difficulté de trouver un générateur. La démonstration précédente suppose connu un générateur.

Lemme. — *Soit G un groupe et a un élément d'ordre m. Alors, pour tout entier naturel k, l'ordre de a^k est $\frac{m}{\text{pgcd}(k,m)}$.*

Démonstration. — On note $d = \text{pgcd}(k, m)$. Il existe $(k', m') \in \mathbb{N}^2$, tel que $k = dk'$, $m = dm'$, et $k' \wedge m' = 1$. D'abord, $(a^k)^{m'} = (a^{dm'})^{k'} = (a^m)^{k'} = e_G$. L'ordre de a^k est donc diviseur de m'. Soit ensuite l tel que $(a^k)^l = e_G$. Alors, $a^{kl} = e_G$ et donc kl est multiple de l'ordre m de a. On en déduit que $k'l$ est multiple de m'. Or, m' est premier avec k'. Par le lemme de Gauss, m' divise l. Ainsi, m' est bien l'ordre de a^k. □

Lemme. — *Soit G un groupe cyclique d'ordre m. Alors G admet exactement $\varphi(m)$ générateurs.*

Démonstration. — Soit g un générateur de G. Les éléments de G sont donc les produits de la forme g^k avec k entre 0 et $m-1$. L'ordre de g^k est $\frac{m}{\text{pgcd}(k,m)}$ et il vaut m si et seulement si k est premier avec m. Il y a donc exactement $\varphi(m)$ générateurs. □

Structure des sous-groupes d'un groupe cyclique. — *Soit G un groupe cyclique d'ordre n. Soit d un diviseur de n. Soit*

$$U_d := \{g \in G,\ g^d = e_G\}.$$

Alors,

- *U_d est un sous-groupe de G, cyclique d'ordre d.*
- *C'est le seul sous-groupe d'ordre d de G.*
- *Il y a $\varphi(d)$ éléments d'ordre d dans G.*

Démonstration. — – D'abord e_G appartient à U_d. Comme G est monogène, il est commutatif. On vérifie alors que si x et y sont dans U_d, $(xy)^d = x^d y^d = e_G$. On a aussi $(x^{-1})^d = e_G$. Donc, U_d stable par produit et passage à l'inverse est un sous-groupe de G.

Il existe $n' \in \mathbb{N}$ tel que $n = dn'$. Soit g un générateur de G. Les éléments de G sont les produits de la forme g^k avec k entre 0 et $m-1$.

$$g^k \in U_d \iff g^{kd} = e_G \iff n \text{ divise } kd \iff n' \text{ divise } k.$$

Les éléments de U_d sont donc les d puissances, deux à deux différentes, $e_G, g^{n'}, g^{2n'}, \cdots, g^{(d-1)n'}$ de $g^{n'}$. L'élément $g^{n'}$ engendre donc U_d, qui est donc cyclique d'ordre d.

– Par le théorème de théorème de Lagrange, tous les éléments des sous-groupes d'ordre d de G sont dans U_d.
– Un élément d'ordre d de G est dans U_d et c'est un générateur de U_d. Comme U_d est cyclique, il y a exactement $\varphi(d)$ éléments d'ordre d dans G.

□

On obtient un résultat inattendu sur la fonction φ d'Euler.

Corollaire. — *Soit n un entier naturel non nul. Alors*

$$\sum_{d \text{ diviseur de } n} \varphi(d) = n.$$

Démonstration. — Il suffit de considérer la partition de G obtenue en regroupant les éléments de même ordre. □

Exercice. — *Considérons le groupe $(\mathbb{Z}/10\mathbb{Z}, +)$. Quels sont les ordres possibles d'un élément de ce groupe ? Combien d'éléments de chaque ordre ce groupe possède -t-il ? Déterminer tous les générateurs de ce groupe.*

4.2. Caractérisation des groupes cycliques

Proposition. — *Tout groupe fini d'ordre premier est cyclique.*

Démonstration. — Par le théorème de Lagrange tout élément autre que l'élément neutre dans un groupe d'ordre premier p engendre un sous-groupe d'ordre égal à l'ordre du groupe. C'est donc un générateur. (Remarquons qu'il y a alors $p-1 = \varphi(p)$ générateurs.) □

Critère de cyclicité. — *Soit G un groupe fini d'ordre n. Pour tout diviseur d de n, on considère $V_d := \{g \in G, g^d = e_G\}$ et $\alpha_G(d)$ le nombre d'éléments de G d'ordre d. Alors les assertions suivantes sont équivalentes*

1. *G est cyclique.*
2. *Pour tout diviseur d de n,* $\operatorname{card} V_d \leq d$.
3. *Pour tout diviseur d de n, $\alpha_G(d) \leq \varphi(d)$.*

Démonstration. —1⇒ 2 Si G est cyclique, pour tout diviseur d de n, $\operatorname{card} V_d = d$.

2⇒ 3 S'il n'y a pas d'élément d'ordre d dans G, l'implication est évidente. Sinon, supposons que $\operatorname{card} V_d \leq d$ et considérons un élément a d'ordre d dans G. Il est dans V_d ainsi que tout le groupe qu'il engendre. Comme $\operatorname{card} V_d \leq d$, V_d est exactement le groupe cyclique engendré par a. Les éléments d'ordre d dans G sont donc les $\varphi(d)$ générateurs de V_d.

3⇒ 1 Supposons que pour tout diviseur d de n, $\alpha_G(d) \leq \varphi(d)$. En considérant la partition de G obtenue en regroupant les éléments de même ordre on trouve $\sum_{d \text{ diviseur de } n} \alpha_G(d) = n$. Ainsi, aucune inégalité $\alpha_G(d) \leq \varphi(d)$ ne peut être stricte sans contredire l'égalité $\sum_{d \text{ diviseur de } n} \varphi(d) = n$. En particulier, $\alpha(n) = \varphi(n) \geq 1$ et G contient un élément d'ordre n donc générateur de G.

□

4.3. Théorème de Gauss et groupe multiplicatif d'un corps fini

Nous avons vu en arithmétique élémentaire

***Théorème* (Gauss).** — *Soit p un nombre premier. Il existe un élément $\omega \in \{1, \dots, p-1\}$ dont l'ordre multiplicatif modulo p est égal à $p-1$. De plus, tout élément de $\{1, \dots, p-1\}$ est congru à un unique élément de l'ensemble $\{1, \omega, \omega^2, \dots, \omega^{p-2}\}$.*

Un tel élément ω est appelé *générateur multiplicatif* modulo p. Cet énoncé est relatif au groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ des inversible du corps $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

Nous avons vu précédemment comment à partir d'un corps $\mathbb{F}_p$ et d'un polynôme P de $k[X]$ irréductible de degré d construire un nouveau corps $\mathbb{F}_p[X]/(P)$ de cardinal p^d.

Théorème. — *Soit $\mathbb{K}$ un corps commutatif fini. Alors le groupe multiplicatif $(K^\times, \times)$ de ses éléments inversibles est cyclique.*

Démonstration. — On considère pour tout diviseur d de $\mathrm{card}(K^\times)$ l'ensemble $V_d := \{x \in \mathbb{K},\ x^d = 1_K\}$. Comme c'est l'ensemble des solutions dans le corps $\mathbb{K}$ d'une équation polynômiale de degré d à coefficients dans $\mathbb{K}$, V_d a au plus d éléments. Par le critère de cyclicité, $(K^\times, \times)$ est donc cyclique. □

Noter ici que nous n'avons pas exhibé de générateur.

Exercice. — *Considérons le groupe $(\mathbb{F}_{13})^\times$. Quels sont les ordres possibles d'un élément de ce groupe ? Combien d'éléments de chaque ordre ce groupe possède -t-il ? Déterminer tous les générateurs de ce groupe.*

Exercice. — *Considérons le groupe $\big(\mathbb{F}_2[X]/(X^3+X+1)\big)^\times$. Quels sont les ordres possibles d'un élément de ce groupe ? Combien d'éléments de chaque ordre ce groupe possède -t-il ? Déterminer tous les générateurs de ce groupe.*

Exercice. — *Énoncer le théorème de Lagrange pour le groupe $(\mathbb{F}_p[X]/(P))^\times$.*

CHAPITRE 5

GROUPES DE PETIT ORDRE

5.1. Des exemples

5.1.1. Groupes cycliques. — Nous avons déjà vu les groupes cycliques. Rappelons qu'un groupe cyclique d'ordre n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$. En représentant les cycles (non inclus dans des plus grands cycles) on obtient par exemple pour $\mathbb{Z}/6\mathbb{Z}$, le diagramme des cycles  .

5.1.2. A partir de groupes cycliques. — Par produit, on peut construire des groupes plus compliqués comme $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Le diagramme des cycles de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ est  .

Exercice. — *Etablir le diagramme des cycles des groupes* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Ces diagrammes permettent de montrer que deux groupes ne sont pas isomorphes. Par contre, pour des groupes de grand ordre, ils ne suffisent pas pour montrer que deux groupes sont isomorphes. La table, qui contient toute l'information sur la loi d'opération, permet, elle, de le démontrer. Il est cependant parfois nécessaire de faire un changement dans l'ordre des éléments, pour que ces isomorphismes apparaissent.

5.1.3. Groupes de permutations. — Une bijection d'un ensemble E dans lui-même est appelée permutation. L'ensemble $\mathfrak{S}(E)$ des permutations d'un ensemble E muni de la loi de composition est un groupe. Si E est un ensemble fini de cardinal n, le groupe $\mathfrak{S}_n$ est d'ordre $n!$. Par exemple, le groupe $\mathfrak{S}_3 = \mathfrak{S}(\{1,2,3\})$ des permutations d'un ensemble à trois éléments est d'ordre 6. On appelle transposition une permutation qui échange deux éléments et laisse fixe les autres. Il y en a trois dans $\mathfrak{S}_3$, la transposition $(1,2)$ qui échange 1 et 2, (13) et $(2,3)$. On appelle 3-cycle une permutation qui envoie a sur b, b sur c et c sur a, sans bouger les autres éléments. Il y en a deux dans $\mathfrak{S}_3$, $c = (1,2,3)$ et $(1,3,2)$. Remarquons que $(1,3,2) = (1,2,3) \circ (1,2,3) = c^2$ Le groupe $\mathfrak{S}_3$ est donc composé de

$$\mathfrak{S}_3 = \{\mathrm{Id}, \tau = (1,2), (1,3), (2,3), c, c^2\}$$

La table de multiplication est

$\circ$	Id	$(1,2)$	$(1,3)$	$(2,3)$	c	c^2
Id	Id	$(1,2)$	$(1,3)$	$(2,3)$	c	c^2
$(1,2)$	$(1,2)$	Id	c^2	c	$(2,3)$	$(1,3)$
$(1,3)$	$(1,3)$	c	Id	c^2	$(1,2)$	$(2,3)$
$(2,3)$	$(2,3)$	c^2	c	Id	$(1,3)$	$(1,2)$
c	c	$(1,3)$	$(2,3)$	$(1,2)$	c^2	Id
c^2	c^2	$(2,3)$	$(1,2)$	$(1,3)$	Id	c

ou bien après permutation de la liste des éléments

$\circ$	Id	c	c^2	$(1,2)$	$(1,3)$	$(2,3)$
Id	Id	c	c^2	$(1,2)$	$(1,3)$	$(2,3)$
c	c	c^2	Id	$(1,3)$	$(2,3)$	$(1,2)$
c^2	c^2	Id	c	$(2,3)$	$(1,2)$	$(1,3)$
$(1,2)$	$(1,2)$	$(2,3)$	$(1,3)$	Id	c^2	c
$(1,3)$	$(1,3)$	$(1,2)$	$(2,3)$	c	Id	c^2
$(2,3)$	$(2,3)$	$(1,3)$	$(1,2)$	c^2	c	Id

Le premier cadran exhibe maintenant un sous-groupe. La table d'un groupe est toujours un carré latin, car sur la ligne de a, si $b \neq c$, $ab \neq ac$. La réciproque est fausse. Un carré latin n'est pas toujours associé à un groupe (voir TD). L'associativité ne se lit pas facilement sur la table, par exemple.

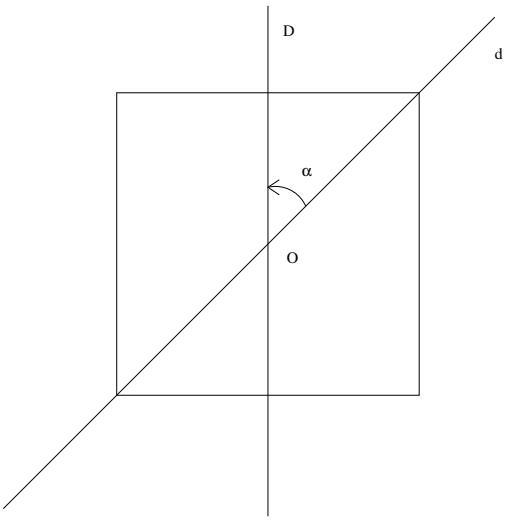
Exercice. — *(Cet exercice est difficile) Montrer que la table suivante*

$\star$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	1	5	3
3	3	5	4	2	1
4	4	1	5	3	2
5	5	3	2	1	4

est un carré latin, mais ne représente pas un groupe.

Le diagramme des cycles de $\mathfrak{S}_6$ est 

5.1.4. Groupes d'isométries. — On étudie par exemple le groupe D_8 des isométries d'un carré dans un plan euclidien.



Une isométrie du carré est par définition une isométrie du plan qui conserve globalement le carré. Parmi ces isométries, il y a l'identité, les trois rotations r , r^2 et r^3 de centre O d'angle $2\alpha = +\pi/2$, $4\alpha = \pi$ et $6\alpha = +3\pi/2$, et les quatre symétries axiales (par exemple la symétrie $s = s_d$ par rapport à la droite d). Pour la liste, on utilise les relations

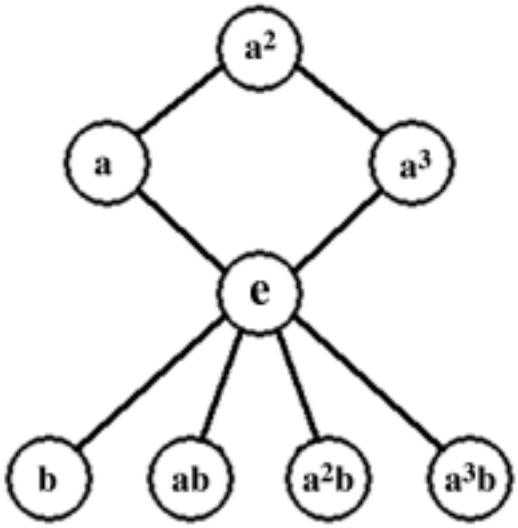
$$s^2 = \mathrm{Id}, r^4 = \mathrm{Id}, \text{ et } s_D \circ s_d = r \text{ ou encore } s_D = r \circ s.$$

Les symétries sont donc s, $r \circ s$, $r^2 \circ s$ $r^3 \circ s$ Pour établir la table de multiplication, il suffit de la relation supplémentaire

$$s \circ r = s_d \circ (s_D \circ s_d) = (s_d \circ s_D) \circ s_d = r^{-1} \circ s_d = r^3 \circ s$$

$\circ$	Id	r	r^2	r^3	s	rs	r^2s	r^3s
Id	Id	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	Id	rs	r^2s	r^3s	s
r^2	r^2	r^3	Id	r	r^2s	r^3s	s	rs
r^3	r^3	Id	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	Id	r^3	r^2	r
rs	rs	s	r^3s	r^2s	r	Id	r^3	r^2
r^2s	r^2s	rs	s	r^3s	r^2	r	Id	r^3
r^3s	r^3s	r^2s	rs	s	r^3	r^2	r	Id

Le diagramme des cycles est

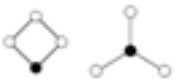


Exercice. — *Etablir le diagramme des cycles du groupe D_6 des isométries d'un triangle équilatéral. Prédire et démontrer un isomorphisme entre ce groupe et "autre" groupe.*

5.2. Classification des groupes de petit ordre

Nous cherchons à déterminer tous les groupes d'ordre petit, à isomorphisme près. Cette précision "à isomorphisme près" indique que nous ne différencierons pas par exemple $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ou encore $\mathbb{Z}/6\mathbb{Z}$. La démarche est de trouver la liste des éléments et les tables d'opération possibles. Ensuite, on vérifie que ces tables fournissent bien une structure de groupe (associativité, existence d'un élément neutre et d'un symétrique pour chaque élément). Pour cette seconde partie, il suffit de réaliser les tables obtenues comme tables de groupes connus.

5.2.1. Groupes d'ordre premier. — Nous avons montré que les groupes d'ordre premier p sont cycliques et donc isomorphes à $\mathbb{Z}/p\mathbb{Z}$. Ceci détermine donc, à isomorphisme près, tous les groupes d'ordre 2, 3, 5, 7 et 11.

5.2.2. Groupes d'ordre 4. — Nous avons déjà vu deux types de groupes d'ordre 4, $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ dont les diagrammes sont respectivement  . Ces deux groupes ne sont donc pas isomorphes.

Montrons maintenant qu'à isomorphisme près, il n'y a pas d'autres groupes d'ordre 4. Soit G un groupe d'ordre 4. S'il a un élément d'ordre 4, le groupe est isomorphe à $\mathbb{Z}/4\mathbb{Z}$. Sinon par le théorème de Lagrange, tous les éléments autres que l'identité sont d'ordre 2. Le diagramme est donc  .

Si a et b sont deux tels éléments, noter que comme $b \neq e$, $ab \neq a$. De même $ab \neq b$. La liste est donc $\{e, a, b, ab\}$. Comme $ba \neq a$ et $ba \neq b$, $ba = ab$. La table est donc

$\star$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

et on retrouve la table de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ en ayant ordonné ses éléments dans l'ordre $(0,0), (1,0), (0,1), (1,1)$.

5.2.3. Groupes d'ordre 6. — Nous avons déjà rencontré deux groupes d'ordre 6, le groupe cyclique $\mathbb{Z}/6\mathbb{Z}$ (isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$)  et le groupe non commutatif $\mathfrak{S}_3$ (isomorphe au groupe D_6 des isométries du triangle équilatéral)  ..

Nous allons montrer qu'à isomorphisme près, il n'y en a pas d'autres. Soit donc G un groupe d'ordre 6. S'il a un élément d'ordre 6, il est cyclique isomorphe à $\mathbb{Z}/6\mathbb{Z}$. Sinon, il a n_2 sous-groupes d'ordre 2 et n_3 sous-groupes d'ordre 3.

Lemme. — 1. *Dans un groupe, l'intersection de deux sous-groupes distincts de même ordre premier est réduite au singleton $\{e\}$.*
2. *Dans un groupe, l'intersection de deux sous-groupes d'ordre premier entre eux est réduite au singleton $\{e\}$.*

Démonstration. — 1. L'intersection de deux sous-groupes H et L est en particulier un sous-groupe de H. Comme H est supposé d'ordre premier, par le théorème de Lagrange, ses seuls sous-groupes sont H ou $\{e\}$.
2. Tout élément dans l'intersection de deux sous-groupes H et L d'ordre premier entre eux, est d'ordre un diviseur commun de l'ordre de H et de l'ordre de L. C'est donc un élément d'ordre 1, donc l"élément neutre.

□

Les sous-groupes d'ordre 2 et 3 ne se rencontrent donc qu'en e. Ainsi, on obtient une partition de $G - \{e\}$ et donc

$$n_2(2-1) + n_3(3-1) = 6 - 1, \text{ soit } n_2 + 2n_3 = 5.$$

Il y a donc nécessairement un élément s d'ordre 2.

Lemme. — *Dans un groupe, si a, b sont deux éléments distincts d'ordre 2 qui commutent, alors $\{e, a, b, ab\}$ est un sous-groupe d'ordre 4.*

Démonstration. — Si a, b sont deux éléments distincts d'ordre 2 qui commutent, $(ab)^2 = a^2b^2 = e$. Par conséquent, $\{e, a, b, ab\}$ contient l'élément neutre et est stable par passage à l'inverse car tous ses éléments sont d'ordre 1 ou 2. De plus, comme $a^2 = e, b^2 = e, ba = ab$, cette partie est stable par produit. □

Si a et b sont deux éléments distincts de G d'ordre 2 dont le produit est d'ordre 2, $ab = (ab)^{-1} = ba$, on aurait un sous-groupe d'ordre 4 ; ce qui contredit le théorème de Lagrange. Il y a donc nécessairement un élément r d'ordre 3.

La liste des éléments de G est $\{e, r, r^2, s, rs, r^2s\}$. En effet, par simplification, ces éléments sont deux à deux distincts. Par exemple, comme $r \neq s$, $r^2s \neq r$.

$\circ$	Id	r	r^2	s	rs	r^2s
Id	Id	r	r^2	s	rs	r^2s
r	r	r^2	Id	rs	r^2s	s
r^2	r^2	Id	r	r^2s	s	rs
s	s			Id		
rs	rs			r		
r^2s	r^2s			r^2		

Pour terminer la table, il suffit de déterminer la valeur de sr dans la liste $\{e, r, r^2, s, rs, r^2s\}$. Les éléments $\{e, r, r^2, s\}$ sont exclus par simplification. Comme généralisation du théorème chinois, nous avons le

Lemme. — *Dans un groupe, si a, b sont deux éléments d'ordre premier entre eux qui commutent, alors $ord(ab) = ord(a) \times ord(b)$.*

Démonstration. — Si a, b sont deux éléments qui commutent d'ordre premier entre eux , alors avec $m = \text{ppcm}(ord(a), ord(b)) = ord(a) \times ord(b)$, $(ab)^m = a^m b^m = ee = e$. Maintenant, si $(ab)^k = e$ alors $a^k = b^{-k}$ est dans l'intersection des sous-groupes engendrés par a et par b. Par le théorème de Lagrange, son ordre est donc diviseur de $ord(a)$ et de $ord(b)$. Comme ces deux nombres sont premiers entre eux, $a^k = e$ et $b^k = e$. Donc, k est un multiple de $\text{ppcm}(ord(a), ord(b)) = m$. □

Si $sr = rs$, l'élément sr est d'ordre 6. Comme nous avons déjà traité le cas d'existence d'un élément d'ordre 6, la seule valeur possible pour sr est $sr = r^2s$.

$\circ$	Id	r	r^2	s	rs	r^2s
Id	Id	r	r^2	s	rs	r^2s
r	r	r^2	Id	rs	r^2s	s
r^2	r^2	Id	Id	r^2s	s	rs
s	s	r^2s	rs	Id	r^2	r
rs	rs	s	r^2s	r	Id	r^2
r^2s	r^2s	rs	s	r^2	r	Id

On trouve le groupe D_6 des isométries du triangle équilatéral.

5.2.4. Groupes d'ordre 8. —

Lemme. — *Un groupe d'ordre pair a toujours un nombre impair d'éléments d'ordre* 2.

Démonstration. — En effet, si on regroupe un élément et son inverse, on obtient une partition du groupe. Pour un élément d'ordre différent de 1 et 2, le sous-ensemble qui le contient a deux éléments distincts. Comme le groupe est de cardinal pair, il y a un nombre pair de sous-ensembles avec un seul élement qui est donc d'ordre 1 ou 2. Comme le seul élément d'ordre 1 est e, on conclut qu'il y a un nombre impair d'éléments d'ordre 2. □

Nous donnerons ici la liste des groupes d'ordre 8 à isomorphisme près, sans démontrer que cette liste est exhaustive.

Parmi les groupes commutatifs, il y a

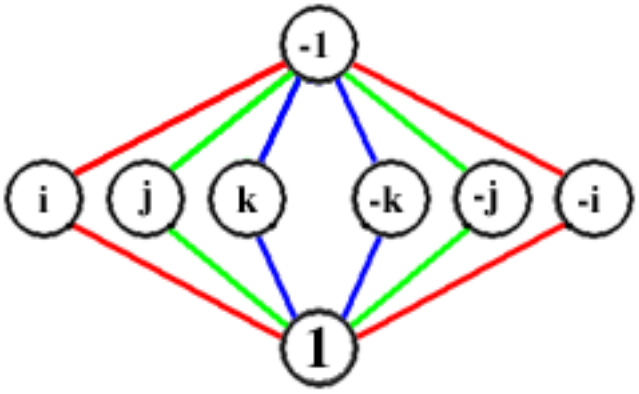
$$\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z},\ \text{ et }\ \mathbb{Z}/2\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}.$$

Exercice. — *Montrer que ces groupes ne sont pas isomorphes, en traçant le graphe de leurs cycles.*

Parmi les groupes non commutatifs, nous avons déjà vu le groupe D_8 des isométries du carré.

Reste le groupe des quaternions

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1



dont le graphe des cycles est

5.2.5. Groupes d'ordre 9. — Nous allons montrer ici qu'à isomorphisme près, les seuls groupes d'ordre 9 sont le groupe cyclique $\mathbb{Z}/9\mathbb{Z}$  et $\mathbb{Z}/3 \times \mathbb{Z}/3\mathbb{Z}$  .

Soit G un groupe d'ordre 9 non cyclique. Ses éléments autres que l'élément neutre sont donc tous d'ordre 3. Deux sous-groupes distincts d'ordre 3 se rencontrent seulement en l'élément neutre. Il y a donc exactement quatre sous-groupes d'ordre 3. Le diagramme des cycles est donc

Soit a et b deux éléments d'ordre 3 qui sont dans des sous-groupes distincts. Par simplification, on montre que ab n'est dans aucun de ces deux sous-groupes. Ainsi, $\{e, a, a^2, b, b^2, ab, a^2b^2, a^2b, ab^2\}$ sont neuf éléments distincts.

Comme $b \neq e$, $(ab)2 \neq a^2b$. Comme $a \neq e$, $(ab)2 \neq ab2$. Par conséquent, $(ab)^2 = a^2b^2$ et donc $ba = ab$.

On peut donc établir la table de G et vérifier que G est isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

5.2.6. Groupes d'ordre 10. — Nous avons deux exemples de sous-groupes d'ordre 10, $\mathbb{Z}/10\mathbb{Z}$  et le groupe D_{10}  des isométries d'un pentagone régulier.

Nous allons montrer qu'à isomorphisme près, il n'y en a pas d'autres. Soit G un groupe d'ordre 10. On raisonne comme dans le cas des groupes d'ordre 6. On suppose que G n'est pas cyclique, et n'a donc pas d'éléments d'ordre 10. Soit n_2 (resp. n_5) le nombre de sous-groupes d'ordre 2 (resp. 5). On a $n_2 + 4n_5 = 9$.

Il y a donc un élément s d'ordre 2. Comme G d'ordre 10 n'a pas de sous-groupe d'ordre 4, il a nécessairement un élément r d'ordre 5. On peut alors établir la liste d'éléments deux à deux distincts

$$\{e, r, r^2, r^3, r^4, s, rs, r^2s, r^3s, r^4s\}$$

et commencer la table.

$\circ$	Id	r	r^2	r^3	r^4	s	rs	r^2s	r^3s	r^4s
Id	Id	r	r^2	r^3	r^4	s	rs	r^2s	r^3s	r^4s
r	r	r^2	r^3	r^4	Id	rs	r^2s	r^3s	r^4s	s
r^2	r^2	r^3	r^4	Id	r	r^2s	r^3s	r^4s	s	rs
r^3	r^3	r^4	Id	r	r^2	r^3s	r^4s	s	rs	r^2s
r^4	r^4	Id	r	r^2	r^3	r^4s	s	rs	r^2s	r^3s
s	s					Id				
rs	rs					r				
r^2s	r^2s					r^2				
r^3s	r^3s					r^3				
r^4s	r^4s					r^4				

Reste à déterminer le produit sr, dans $\{e, r, r^2, r^3, r^4, s, rs, r^2s, r^3s, r^4s\}$ mais en fait dans $\{rs, r^2s, r^3s, r^4s\}$. Le cas $sr = rs$ mène au groupe cyclique car rs serait d'ordre 5×2. Le cas $sr = r^{-1}s = r^4s$ même au groupe D_{10}. Il faut vérifier que les autres cas sont impossibles. Par exemple, si $sr = r^2s$

$$r = s(sr) = sr^2s = (sr)rs = r^2(sr)s = r^2r^2ss = r^4s^2 = r^4.$$

et si $sr = r^3 s$

$$r = s(sr) = sr^3 s = (sr)r^2 s = r^3(sr)rs = r^3 r^3 (sr)s = r^3 r^3 r^3 ss = r^9 = r^4.$$

Noter que ceci donne des carrés latins qui ne correspondent pas à des groupes.

PARTIE III

EXEMPLES D'ANNEAUX

CHAPITRE 6

L'ANNEAU DES ENTIERS DE GAUSS

Le but de ce chapitre est de déterminer les nombres premiers p qui peuvent s'écrire comme somme $p = a^2 + b^2$ de deux carrés (de nombres entiers relatifs).

6.1. Expérimentation

Parmi les premiers nombres premiers, certains peuvent s'écrire comme somme de deux carrés.

$$\begin{aligned} 2 &= 1^2 + 1^2 \\ 5 &= 1^2 + 2^2 \\ 13 &= 2^2 + 3^2 \\ 17 &= 1^2 + 4^2 \\ 29 &= 2^2 + 5^2. \end{aligned}$$

Outre 2, ils sont tous congrus à 1 modulo 4.

Les autres $3, 7, 11, 19$ et 23 ne le peuvent pas. Par exemple, pour 23, les quantités $23-1^2 = 22$, $23 - 2^2 = 19$, $23 - 3^2 = 14$ et $23 - 4^2 = 7$ ne sont pas des carrés. Et pour les entiers naturels n strictement plus grands que 4, $23 - n^5$ est stritement négatif. Ils sont tous congrus à 3 modulo 4.

C'est en fait un théorème

Théorème des deux carrés. — *Un nombre premier est somme de deux carrés si et seulement s'il vaut* 2 *ou s'il est congru à* 1 *modulo* 4.

Exercice. — *Le nombre* 37 *est-il premier ? Peut-il s'écrire comme somme de deux carrés. Si oui, faites-le.*

6.2. Le sens direct par les congruences

Comme

$a[4]$	0	1	2	-1
$a^2[4]$	0	1	0	1

les carrés sont congrus à 0 ou 1 modulo 4. Comme

$a^2 + b^2[4]$	$a^2[4] = 0$	$a^2[4] = 1$
$b^2[4] = 0$	0	1
$b^2[4] = 1$	1	2

les sommes de deux carrés sont congrues à $0, 1$ ou 2 modulo 4. Comme le seul nombre premier pair est 2, un nombre premier différent de 2 et somme de deux carrés est congru à 1 modulo 4.

6.3. Le sens direct par le théorème de Lagrange

Soit p un nombre premier différent de 2 et somme de deux carrés

$$p = a^2 + b^2.$$

Comme p n'est pas un carré, ni a ni b n'est nul. Comme $p^2 > p$, on a les ingégalités $0 < a < p$ et $0 < b < p$. En particulier, a et b sont premiers avec p, donc inversibles dans $\mathbb{F}_p$. On obtient

$$a^2 + b^2 = 0[p], \quad \left(ab^{-1}\right)^2 + 1 = 0[p], \quad \left(ab^{-1}\right)^2 = -1[p].$$

Par conséquent, ab^{-1} est un élément d'ordre 4 du groupe $\mathbb{F}_p^\times$ d'ordre $p - 1$. Le théorème de Lagrange permet donc de conclure que 4 divise $p - 1$, soit $p = 1[4]$.

6.4. La réciproque par le théorème de Minkowski

Soit p un nombre premier congru à 1 modulo 4. Nous cherchons à l'écrire comme somme de deux carrés.

6.4.1. Un élément d'ordre 4 de $\mathbb{F}_p^\times$. — On cherche d'abord un élément d'ordre 4 de $\mathbb{F}_p^\times$.

6.4.1.1. En théorie. — L'hypothèse sur p peut se traduire par le fait que $p-1$ est divisible par 2 et $\frac{p-1}{2}$ est pair. Comme $(-1)^{\frac{p-1}{2}} = 1[p]$, l'entier -1 est un carré modulo p. Il existe donc un entier c tel que $c^2 = -1[p]$. Ainsi c est d'ordre 4 dans $\mathbb{F}_p^\times$.

6.4.1.2. En pratique. — On écrit $p-1 = 2^n m$ où m est un entier impair. Si x est un élément de $\mathbb{F}_p^\times$, $(x^m)^{2^n} = x^{p-1} = 1[p]$ par le petit théorème de Fermat. Par conséquent l'ordre de $y = x^m$ divise 2^n. Si cet ordre 2^k n'est pas 2, $y^{2^{k-2}} = y^{\frac{2^k}{4}}$ est un élément d'ordre 4. En pratique, on choisi un x au hasard, on calcule $y = x^m$ et si $y \neq 1[p]$ et $y \neq -1[p]$, on pose

$$\begin{aligned} y_1 &= y^2 \\ y_2 &= y_1^2 \\ &\vdots \\ y_{k-1} &= (y_{k-2})^2 = y^{2^{k-1}} = -1 \\ y_k &= (y_{k-1})^2 = y^{2^k} = 1 \end{aligned}$$

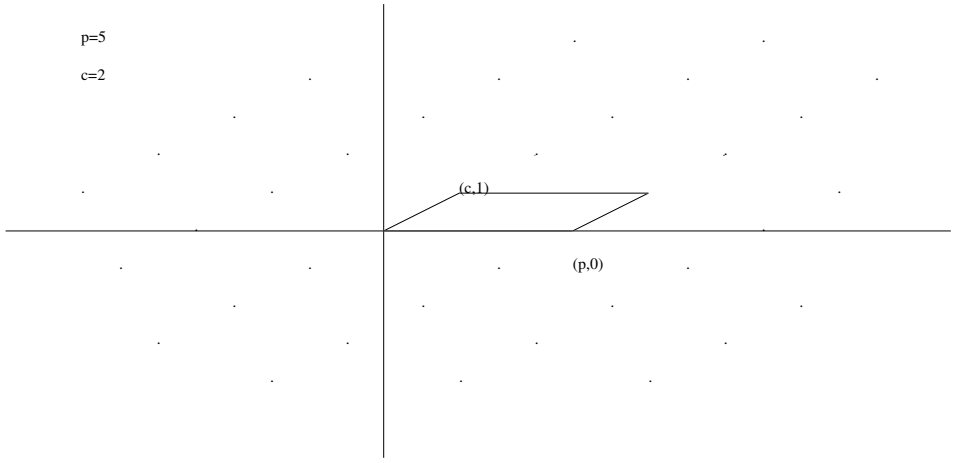
L'entier c d'ordre 4 cherché peut être choisi comme y_{k-2}.

Exercice. — *Déterminer une racine de* -1 *modulo* 97.

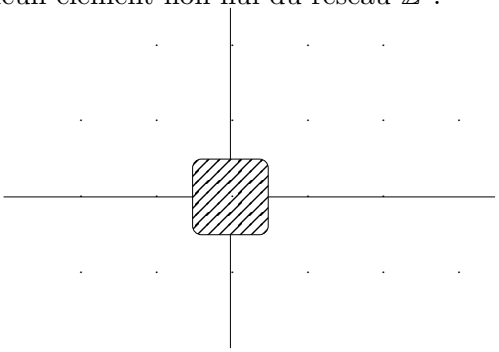
6.4.2. Application du théorème de Minkowski. — Un couple (a,b) cherché vérifie $ab^{-1} = c[p]$. On considère donc l'ensemble

$$\mathcal{R} := \{(a,b) \in \mathbb{Z}^2, a = bc[p]\}.$$

Un couple dans $\mathcal{R}$ s'écrit avec $k \in \mathbb{Z}$ tel que $a - bc = kp$, $(a,b) = (a-bc,0) + b(c,1) = k(p,0) + b(c,1)$. Tous les couples de la forme $\lambda(p,0) + \mu(c,1)$ avec $(\lambda,\mu) \in \mathbb{Z}^2$, sont dans $\mathcal{R}$, car $\lambda p + \mu c = \mu c[p]$. Par conséquent, $\mathcal{R}$ est un $\mathbb{Z}$-module engendré par les deux vecteurs $\mathbb{R}$-indépendants $(p,0)$ et $(c,1)$. On dit que $\mathcal{R}$ est un réseau de $\mathbb{R}^2$. Son volume est défini comme le volume de la maille élémentaire, ici $\left|\det \begin{pmatrix} p & c \\ 0 & 1 \end{pmatrix}\right| = p$



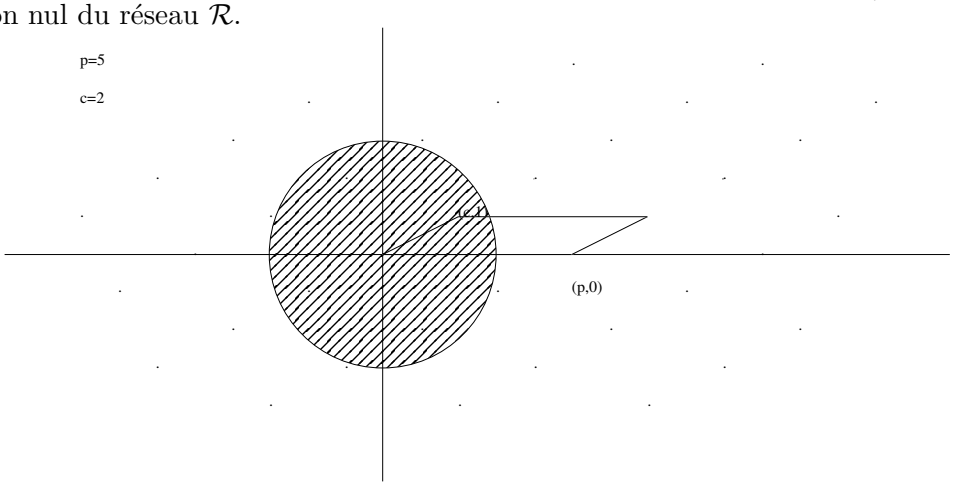
Le réseau le plus familier de $\mathbb{R}^2$ est $\mathbb{Z}^2$ engendré par la base canonique $(1,0)$ et $(0,1)$, de volume 1. On peut construire un convexe fermé de $\mathbb{R}^2$ de volume proche de 4 qui ne contient aucun élément non nul du réseau $\mathbb{Z}^2$.



Le théorème de Minkowski affirme que

Théorème de Minkowski. — *Les ensembles convexes fermés de volume supérieur à* 4 *de* $\mathbb{R}^2$ *contiennent un élément non nul du réseau* $\mathbb{Z}^2$*. Plus généralement, les ensembles convexes fermés de volume supérieur à* $4v$ *contiennent un élément non nul de tout réseau de volume* v*.*

Dans notre cas, la boule convexe fermée de volume $4p$, donc de rayon $\sqrt{\frac{4p}{\pi}}$, contient un élément non nul du réseau $\mathcal{R}$.



Un tel élément (a,b) vérifie $a \in \mathbb{Z}, b \in \mathbb{Z}, a = bc[p]$ et $0 < a^2 + b^2 < \frac{4p}{\pi} < 2p$. Par conséquent, $a^2 + b^2 = (bc)^2 + b^2 = b^2(c^2+1) = 0[p]$. Ainsi, $a^2 + b^2$ est un multiple de p strictement positif et strictement plus petit que $2p$: c'est donc p. On trouve $a^2 + b^2 = p$.

Exercice. — *Le nombre* 41 *est-il premier ? Peut-on l'écrire comme somme de deux carré ? Déterminer une racine* c *de* -1 *modulo* 41*. Représenter graphiquement le réseau* $\mathcal{R} := \{(a,b) \in \mathbb{Z}^2, a = bc[41]\}$*. Déterminer un élément du réseau de plus petite norme. Ecrire* 41 *comme somme de deux carrés.*

6.5. La réciproque avec les entiers de Gauss

6.5.1. L'anneau des entiers de Gauss. — Le sous-ensemble de $\mathbb{C}$ défini par

$$\mathbb{Z}[i] := \{(a+ib) \in \mathbb{C}, a \in \mathbb{Z}, b \in \mathbb{Z}\}$$

est un sous-anneau de $\mathbb{C}$. (On vérifie simplement qu'il contient 0, qu'il est stable par somme, qu'il contient 1 et qu'il est stable par produit car $i^2 = -1$.) On définit une conjuguaison $\mathbb{Z}[i] \to \mathbb{Z}[i], (a+ib) \mapsto (a-ib)$ et une norme $N(a+ib) = a^2+b^2$. Comme $N(A) = A\overline{A}$, la fonction N est multiplicative $N(AB) = N(A)N(B)$. En particulier, si D divise A, alors $N(D)$ divise $N(A)$. On montre que les éléments inversibles de $\mathbb{Z}[i]$ sont exactement les éléments de norme 1, c'est à dire 1, -1, i et $-i$. Deux éléments de $\mathbb{Z}[i]$ sont dits associés s'ils diffèrent par multiplication par un élément inversible.

Un point fondamental de l'arithmétique de cet anneau est la possibilité d'effectuer des divisions euclidiennes.

Théorème de la division euclidenne dans $\mathbb{Z}[i]$. — *Soit A et B deux entiers de Gauss avec $B \neq 0$. Alors il existe deux entiers de Gauss Q et R tels que $A = BQ + R$ et $N(R) < N(B)$.*

Noter qu'il n'y a pas unicité. Un quotient Q possible est l'entier de Gauss le plus proche du nombre complexe $\frac{A}{B} = \frac{A\overline{B}}{N(A)}$ déterminé par les divisions euclidiennes dans $\mathbb{Z}$ des parties réelles et imaginaires de $A\overline{B}$ par $N(A)$.

Exercice. — *Effectuer la division euclidenne de $154+i$ par $25-4i$ dans $\mathbb{Z}[i]$. Effectuer la division euclidenne de $640+639i$ par $25-4i$ dans $\mathbb{Z}[i]$. Effectuer la division euclidienne de 641 par $154+i$ dans $\mathbb{Z}[i]$.*

Ce théorème permet de montrer en particulier le théorème de structure des idéaux de $\mathbb{Z}[i]$ de façon analogue à la description des idéaux de $\mathbb{Z}$ ou de $k[X]$.

Théorème. — *Tout idéal de $\mathbb{Z}[i]$ est l'ensemble des multiples d'un entier de Gauss.*

En particulier, l'idéal (A, B) engendré par deux entiers de Gauss est engendré par un entier, appelé $\text{pgcd}(A, B)$ (bien défini à multiplication par 1, -1, i ou $-i$ près) qui se calcule par division euclidienne.

6.5.2. Une solution par calcul de *pgcd*. — Soit p un nombre premier congru à 1 modulo 4. Nous cherchons à l'écrire comme somme de deux carrés, c'est à dire comme la norme d'un entier de Gauss.

Supposons d'abord que $p = a_0^2 + b_0^2$. Alors,

$$p = a_0^2 + b_0^2 = N(a_0 + ib_0) = (a_0 + ib_0)(a_0 - ib_0).$$

En reprenant c une racine carré de -1 modulo p, on constate que toute solution $(a_0 + ib_0)$ satisfait $(a_0 + cb_0)(a_0 - cb_0) = a_0^2 - c^2b_0^2 = a_0^2 + b_0^2 = p = 0[p]$ et donc

$$[a_0 + cb_0]_p = 0 \quad \text{ou} \quad [a_0 - cb_0]_p = 0.$$

Il est donc naturel de considérer l'application

$$\begin{array}{rcl} \Phi \ : \ \mathbb{Z}[i] & \to & \mathbb{F}_p \\ (a+ib) & \mapsto & [a-cb]_p \end{array}$$

C'est un morphisme d'anneaux. L'un des deux entiers de Gauss $(a_0 + ib_0)$ ou $(a_0 - ib_0)$ cherchés sera un élément du noyau de Φ. Comme Φ est un morphisme d'anneaux, tout élément A dans son noyau a une norme $A\overline{A}$ dans le noyau, c'est à dire multiple de p. Ainsi, l'un des deux entiers de Gauss $(a_0 + ib_0)$ ou $(a_0 - ib_0)$ cherchés sera un élément non nul de plus petite norme du noyau. Comme le noyau est un idéal, cet élément sera un générateur de l'idéal.

Nous ne supposons désormais plus l'existence d'une écriture $p = a_0^2 + b_0^2$. En reprenant l'application

$$\begin{array}{rcl} \Phi \ : \ \mathbb{Z}[i] & \to & \mathbb{F}_p \\ (a+ib) & \mapsto & [a-cb]_p \end{array}$$

on constate que $\Phi(p) = 0$ et $\Phi(c+i) = 0$. Tout élément $(a+ib)$ dans le noyau de cette application (c'est à dire avec $a - bc = 0[p]$, $a - bc = kp$) s'écrit $a + ib = (a - bc) + b(c + i) = kp + b(c + i)$. On en déduit que le noyau de Φ est l'idéal de $\mathbb{Z}[i]$ engendré par p et $c+i$. C'est donc l'idéal engendré par le $D = \text{pgcd}(p, c+i)$. Par la multiplicativité des normes, la norme du pgcd D est un diviseur de $N(p) = p^2$. Ce n'est pas 1 car 1 n'est pas dans le noyau de Φ. Si $N(D) = p^2 = N(p)$, c'est que D est associé à p. On peut choisir pour D (bien défini à multiplication par 1, -1, i ou $-i$ près) $D = p$. Mais p ne divise pas $c + i$ car il n'existe pas d'entier de Gauss $(a + ib)$ tel que $c + i = p(a + i)$. Ainsi $N(D) = N(\text{pgcd}(p, c + i))$ est un diviseur propre de $N(p) = p^2$, c'est à dire p. Nous trouvons que D est un entier de Gauss cherché, dont la norme est p.

6.5.3. Un exemple. — Pour $p = 97$, on écrit $p-1 = 2^5 \times 3$. Avec $x = 2$ on trouve $y = x^3 = 8$. En calculant $y_3 = y^{2^3}$ on trouve que $c = 22$ est une racine de -1 modulo 97.

Pour déterminer le $\text{pgcd}(p, c + i) = \text{pgcd}(97, 22 + i)$ on effectue la division euclidienne dans $\mathbb{Z}[i]$ de 97 par $22 + i$.

$$\frac{97}{22+i} = \frac{97 \times (22-i)}{22^2+1} = \frac{97 \times (22-i)}{485} = \frac{2134}{485} - i\frac{97}{485}.$$

L'entier de Gauss le plus proche de ce nombre complexe est 4. Ainsi $97 = 4(22 + i) + 9 - 4i$. De plus, $22 + i = (9 - 4i)(2 + i)$. Le $\text{pgcd}(97, 22 + i) = \text{pgcd}(22 + i, 9 - 4i)$ est donc $9 - 4i$ de norme

$$9^4 + 4^2 = 97.$$

Exercice. — *Le nombre* 641 *est-il premier ? Peut-on l'écrire comme somme de deux carrés. Si oui, faites-les.*

PARTIE IV

CODAGE ET CRYPTHOGRAPHIE