MAT 2260
Théorie des anneaux

François Bergeron et Christophe Reutenauer
exercices par Nathan Chapelier

9 juin 2026

UQÀM | Département de mathématiques
FACULTÉ DES SCIENCES
Université du Québec à Montréal

Table des matières

Page

1 Anneaux et corps **7**
- 1.1 Introduction . . . 7
- 1.2 Définitions . . . 7
- 1.3 Exemples . . . 8
- 1.4 Calculs dans un anneau . . . 11
- 1.5 Sous-anneaux . . . 13
- 1.6 Produits et homomorphismes . . . 15
- 1.7 Idéaux et quotients . . . 17
- 1.8 Anneaux $\mathbb{Z}/n\mathbb{Z}$ . . . 19
- 1.9 Corps . . . 21
- 1.10 Algèbre d'un monoïde . . . 25
- 1.11 Polynômes en plusieurs variables . . . 26
- 1.12 (∗) Autres exemples d'anneaux . . . 27
- 1.13 Exercices . . . 30

2 Anneaux euclidiens **35**
- 2.1 Définitions de base . . . 35
- 2.2 Théorèmes principaux . . . 38
- 2.3 Algorithme d'Euclide . . . 40
- 2.4 Le cas des polynômes . . . 41
- 2.5 Entiers de Gauss . . . 42
- 2.6 Théorème des restes chinois . . . 47
- 2.7 (∗) Codes polynomiaux . . . 48
- 2.8 Exercices . . . 51

3 Anneaux de Polynômes **55**
- 3.1 Introduction . . . 55
- 3.2 Factorialité . . . 56
- 3.3 Théorème de Hilbert . . . 59
- 3.4 Polynômes cyclotomiques . . . 60
- 3.5 (∗) Bases de Gröbner . . . 62
- 3.6 (∗) Polynômes symétriques . . . 63
- 3.7 Exercices . . . 69

4 Corps finis, Galois **73**
- 4.1 Cardinal des corps finis . . . 74
- 4.2 Théorème de Wedderburn . . . 76
- 4.3 Classification des corps finis . . . 78
- 4.4 Un peu de théorie de Galois . . . 81
- 4.5 Exercices . . . 85

5 Algèbres de Lie **87**

6 Solutionnaire **89**

Bibliographie commentée **96**

Rappels ensembles, fonctions **99**

Rappels groupes **103**

Introduction

Un des objectifs fondamentaux de la théorie des anneaux est d'organiser la réflexion autour de la résolution de systèmes d'équations algébriques en plusieurs variables. C'est là un problème central en mathématiques. Déjà, le cas particulier des solutions dans $\mathbb{C}$ d'une seule équation à une inconnue correspond au théorème fondamental de l'algèbre, et c'est l'objet d'étude de la théorie de Galois. Comme autre cas spécial, on a les systèmes où toutes les équations sont de degré 1, qui donne sa raison d'être à l'algèbre linéaire. Il est aussi inévitable de mentionner le lien avec la théorie (algébrique) des nombres et le célèbre théorème de Fermat [1], prouvé par Wiles [2], sur l'existence de solutions (ou non) de l'équation

$$x^n + y^n = z^n, \qquad n \in \mathbb{N}.$$

Enfin, les solutions de systèmes d'équations polynomiales correspondent aux variétés algébriques, l'objet d'étude de la géométrie algébrique ; et ce n'est pas tout.

On s'intéresse par exemple à la résolution d'un système d'équations, comme

$$\begin{aligned} x^3 + 4y^3 - 3y &= 0, \\ x^2 + y^2 - 1 &= 0. \end{aligned}$$

Les équations polynomiales jouent un rôle dans de nombreux domaines d'applications de la mathématique. Elles apparaissent naturellement en robotique, théorie des codes, biologie mathématique, théorie des jeux, intelligence artificielle, sciences économiques, statistiques, et de nombreux autres contextes. Cela est entre autres rendu possible par l'introduction d'outils de calcul symbolique performant, et la théorie joue un rôle important dans l'élaboration de ces outils. Pour s'initier à leur utilisation, le chapitre 9 du livre *Calcul mathématique avec Sage* [3], est une excellente référence.

Les notions de la théorie des anneaux jouent un rôle prépondérant dans de nombreux domaines des mathématiques, comme : la théorie de la représentation des groupes et des algèbres, la topologie algébrique, l'analyse fonctionnelle, les λ-anneaux ; de même qu'en physique mathématique.

1. Pierre de Fermat (1601–1665).
2. Andrew John Wiles (1953–).
3. Disponible gratuitement sur le web : http ://sagebook.gforge.inria.fr.

Chapitre 1

Anneaux et corps

1.1 Introduction

La notion d'anneau est l'une des plus importantes de l'algèbre abstraite. Pour en savoir plus sur son origine, voir

- mathshistory.st-andrews.ac.uk/HistTopics/Ring_theory.html, ou
- wikipedia.org/wiki/Théorie_des_anneaux

1.2 Définitions de base

Définition 1. Un **anneau** $(\mathcal{A}, +, \cdot)$ est la donnée d'un ensemble $\mathcal{A}$ muni de deux opérations [1], la **somme** (ou addition) et le **produit** (ou multiplication), telles que :

(i) le couple $(\mathcal{A}, +)$ est un groupe abélien, dont l'élément neutre est noté 0 (ou parfois $0_{\mathcal{A}}$), et l'**inverse additif** (l'opposé) de $a \in \mathcal{A}$ est noté $-a$, c'est donc dire que

$$a + (-a) = 0 = (-a) + a;$$

(ii) le produit est **distributif** à droite et à gauche par rapport à la somme, c.-à-d. pour tout $a, b, c \in \mathcal{A}$ on a

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c), && \text{distributivité à gauche,} \\ (b + c) \cdot a &= (b \cdot a) + (c \cdot a), && \text{distributivité à droite;} \end{aligned}$$

(iii) le produit est **associatif**, et il a un élément neutre noté 1 (ou parfois $1_{\mathcal{A}}$). ∎

Il est habituel de simplifier l'écriture d'expressions dans un anneau d'une manière analogue à ce que l'ont fait pour les nombres. On omet certaines parenthèses, avec la convention que le produit a « priorité » sur la somme. Ainsi, $a \cdot b + c$ s'interprète comme $(a \cdot b) + c$, plutôt que comme $a \cdot (b + c)$. On omet aussi souvent le symbole de produit, pour écrire ab à la place de $a \cdot b$. On écrira aussi $-ab$ au

1. **Attention**, ces opérations prennent souvent un sens très différent du sens traditionnel de somme et produit pour les nombres, et elles n'ont que les propriétés explicitement mentionnées ici.

lieu de $-(ab)$ (priorité de la multiplication sur le moins). Enfin, l'associativité permet d'interpréter sans ambiguïté une somme de plusieurs éléments (ou un produit de plusieurs éléments), c.-à-d.

$$a+b+c=(a+b)+c=a+(b+c), \qquad \text{et} \qquad abc=(ab)c=a(bc).$$

Plus généralement, pour des $a_i \in \mathcal{A}$, avec $1 \leq i \leq n$, on pose

$$\sum_{i=1}^{n} a_i := a_1 + a_2 + \ldots + a_n, \qquad \text{et} \qquad \prod_{i=1}^{n} a_i := a_1\, a_2 \cdots a_n.$$

On dit qu'un anneau est **commutatif** si sa multiplication est commutative [2] :

$$\forall (a, b \in A) \qquad ab = ba.$$

La notion d'anneau permet de généraliser à d'autres contexte certains des calculs habituels sur les nombres, en prenant garde de ne pas utiliser d'autres propriétés que celles explicitement décrites dans la définition ci-dessus. On a donc les exemples suivants d'anneaux, pour les ensembles de nombres.

1.3 Exemples fondamentaux d'anneaux

Les exemples les plus simples d'anneaux correspondent à des ensembles de nombres classiques, avec les opérations usuelles.

Ainsi, on a des structures d'anneaux sur les nombres entiers $\mathbb{Z}$, les nombres rationnels $\mathbb{Q}$, les nombres réels $\mathbb{R}$, et les nombres complexes $\mathbb{C}$. On a aussi l'anneau **Trivial** 0, dans lequel il n'y a qu'un élément qui est à la fois le neutre additif et multiplicatif (c.-à-d. $0 = 1$). Tous ces anneaux sont commutatifs. Cependant, ces anneaux sont loin d'être les seuls qu'il est nécessaire d'avoir en tête pour pouvoir comprendre la théorie. Parmi d'autres qui sont importants [3], on compte certainement les suivants :

1.3.1 Entiers modulo n

Parmi les anneaux commutatifs finis, un exemple incontournable est certainement l'**anneau des entiers modulo** n : dénoté $\mathbb{Z}/n\mathbb{Z}$. Rappelons (voir l'annexe des rappels) que les éléments de l'ensemble $\mathbb{Z}/n\mathbb{Z}$, peuvent être décrits comme classe d'équivalence modulo n. Ce sont donc les ensembles $[a] := \{a + kn \mid k \in \mathbb{Z}\}$, pour $a \in \mathbb{Z}$, avec l'égalité $[a] = [a']$ si et seulement si $a - a'$ se divise par n. En particulier, on conclut (grâce à Euclide) que

$$\mathbb{Z}/n\mathbb{Z} = \{[a] \mid 0 \leq a \leq n-1\}.$$

On montre alors qu'il est possible de poser $[a] + [b] := [a+b]$ et $[a] \cdot [b] = [ab]$ (autrement dit, on montre que ces opérations sont bien définies, c.-à-d. qu'elles ne dépendent pas du choix du représentant de la classe). On vérifie enfin que ces opérations satisfont toutes les conditions pour que $\mathbb{Z}/n\mathbb{Z}$ soit ainsi munies d'une structure d'anneau qui est commutatif (car c'est le cas dans $\mathbb{Z}$).

2. L'addition est toujours commutative.
3. D'autres viendront plus tard.

1.3.2 Matrices à coefficients dans un anneau

De façon analogue au cas habituel, pour chaque anneau $\mathcal{A}$, on a la notion de **matrice** $(a_{ij})_{1\le i,j\le n}$ de taille $n\times n$ sur $\mathcal{A}$ (plus simplement on dénote aussi la matrice par (a_{ij})) :

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix},$$

où les **coefficients** (ou entrées) sont des éléments a_{ij} de $\mathcal{A}$. Pour deux matrices (a_{ij}) et (b_{ij}) de taille $n\times n$ sur $\mathcal{A}$, on définit la **somme** $(a_{ij})+(b_{ij})$ comme étant la matrice $(a_{ij}+b_{ij})$; et le **produit** $(a_{ij})(b_{ij})$ comme étant la matrice (c_{ij}), où

$$c_{ij} := \sum_{k=1}^{n} a_{ik}b_{kj}.$$

On a alors la proposition suivante (voir Exercice **??**) :

Proposition 1.1. *L'ensemble $\mathcal{A}^{n\times n}$, des matrices de taille $n\times n$ sur $\mathcal{A}$, muni des opérations de somme et de produit est un anneau. Cet anneau n'est pas commutatif si $n\ge 2$.*

1.3.3 Polynômes à coefficients dans un anneau

Pour tout anneau $\mathcal{A}$, un **monôme**, est une expression de la forme $a\,x^n$. On dit que x est une **variable**, et que a est le **coefficient** du monôme.

Définition 2. Un **polynôme** à coefficients dans un anneau $\mathcal{A}$, de degré $n\in\mathbb{N}$, est une somme finie de monômes :

$$p = \sum_{k=0}^{n} a_k x^k = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \qquad a_n \neq 0.$$

On a aussi le polynôme **nul**, noté 0, qu'on considère comme ayant degré $-\infty$. ∎

Attention, il ne faut pas considérer qu'un polynôme p est simplement une fonction de x de $\mathcal{A}$ vers $\mathcal{A}$. Par exemple, avec $\mathcal{A}=\mathbb{Z}/3\mathbb{Z}$, on a les deux polynômes distincts :

$$p = x^2 + x + 1 \qquad \text{et} \qquad q = x^4 + x + 1,$$

qui coïncident comme fonction sur $\mathbb{Z}/3\mathbb{Z} = \{[0],[1],[2]\}$, puisque

$$p([0]) = [1] = q([0]), \quad p([1]) = [0] = q([1]), \quad \text{et} \quad p([2]) = [1] = q([2]).$$

De fait, il y a une infinité de polynômes à coefficients dans $\mathbb{Z}/n\mathbb{Z}$, mais seulement un nombre fini de fonctions de $\mathbb{Z}/n\mathbb{Z}$ ver $\mathbb{Z}/n\mathbb{Z}$.

On dénote par $\deg(p)$ le **degré** de p, et par $\mathcal{A}[x]$ l'ensemble des polynômes à coefficients dans $\mathcal{A}$. Deux polynômes sont égaux, $p=q$, si et seulement si ils ont même degré et leurs coefficients sont tous égaux. Les polynômes **constants** non nuls, sont les éléments de $\mathcal{A}\setminus\{0\}$. Ils ont degré 0.

La **somme de polynômes** $p = \sum_{i=0}^{n} a_k x^k$ et $q = \sum_{j=0}^{m} b_j x^j$ est le polynôme

$$p + q = \sum_{k=0}^{\max m,n} (a_k + b_k)\, x^k,$$

où on convient au besoin de poser $b_k = 0$, si $k \geq m$, et a_k, si $k \geq n$. Cette somme est un polynôme de degré au plus égal à $\max(\deg(p), \deg(q))$. On pose aussi $-p = \sum_{k=0}^{n}(-a_k)x^k$. On définit enfin le **produit** de p et q comme étant

$$p \cdot q := \sum_{k=0}^{n+m} c_k x^k. \qquad \text{où} \qquad c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0 = \sum_{i+j=k} a_i b_j.$$

Proposition 1.2. *Avec la somme et le produit défini ci-haut, l'ensemble des polynômes $\mathcal{A}[x]$ est un anneau. Si $\mathcal{A}$ est commutatif, alors $\mathcal{A}[x]$ l'est aussi.*

Preuve. La vérification est laissée en exercice au lecteur (voir exercice). ∎

1.3.4 Exercices

Exercice 1.1 (**Caractérisation des racines**). Soit $\mathcal{A}$ un anneau commutatif et $f \in A[x]$ un polynôme non nul. Soit $a \in A$. En utilisant l'identité $x^n - a^n = (x-a)(x^{n-1} + \cdots + a^{n-1})$, montrer que $f(x) - f(a) = (x-a)g(x)$. Montrer que l'on a équivalence entre :

i) $f(a) = 0$.
ii) $x - a$ divise f dans $\mathcal{A}[x]$.

Exercice 1.2. Soit $\mathcal{A}$ un anneau commutatif.

1) Montrer que $\mathcal{A}[x]$ admet une structure d'anneau.
2) Montrer que $\mathcal{A}[x]$ est intègre si et seulement si $\mathcal{A}$ est intègre.
3) Soient $f, g \in \mathcal{A}[x]$ non nuls. On suppose que soit $\mathcal{A}$ est intègre soit le coefficient dominant de f est inversible. Montrer alors qu'on a la formule des degrés $\deg(fg) = \deg(f) + \deg(g)$. Montrer de plus que, si f divise g alors $\deg(f) \leq \deg(g)$.
4) Montrer que si $\mathcal{A}$ est intègre alors les inversibles de $\mathcal{A}[x]$ sont ceux de $\mathcal{A}$, c'est-à-dire $\mathcal{A}[x]^* = \mathcal{A}^*$.

Exercice 1.3 (**Division euclidienne**).
Soit $\mathcal{A}$ un anneau commutatif et soient $f, g \in \mathcal{A}[x]$ tels que le coefficient dominant de g soit inversible dans $\mathcal{A}$. Montrer alors qu'on peut faire la division euclidienne de f par g, c'est-à-dire qu'il existe un unique couple $(q, r) \in \mathcal{A}[x] \times \mathcal{A}[x]$ tels que $f = gq + r$ et $\deg(r) < \deg(g)$.

Exercice 1.4 (**Racine simple et multiplicité**). Soient $\mathcal{A}$ un anneau commutatif, $f \in A[x]$ non nul et $a \in A$ une racine de f. On appelle multiplicité de a dans f l'entier m tel que $(x-a)^m$ divise f mais $(x-a)^{m+1}$ ne divise pas f. On dit que a est une racine simple si sa multiplicité est 1.

1) Montrer que a est une racine simple si et seulement si $f'(a) \neq 0$.
2) Si a est de multiplicité m, montrer que $f(a) = f'(a) = \ldots = f^{(m-1)} = 0$. Si de plus $\mathcal{A}$ est de caractéristique nulle montrer que $f^{(m)}(a) \neq 0$.
3) Montrer que le polynôme $f(x) = x^{12} - 239 \in \mathbb{R}[x]$ n'a que des racines simples.
4) Montrer que le même raisonnement s'applique pour ce polynôme sur un corps de caractéristique 5.

1.3.5 Fonctions à valeurs dans un anneau

Pour tout ensemble X et tout anneau $\mathcal{A}$, on muni l'ensemble $\mathcal{A}^X$, des fonctions de X vers $\mathcal{A}$, de la somme et du produit suivant. Soit $f : X \longrightarrow \mathcal{A}$ et $g : X \longrightarrow \mathcal{A}$ dans $\mathcal{A}^X$, alors

a) La **somme** $f + g : X \longrightarrow \mathcal{A}$ est la fonction dont la valeur pour $x \in X$ est $f(x) + g(x)$. En formule, $(f + g)(x) := f(x) + g(x)$.

b) Le **produit** $(f \cdot g) : X \longrightarrow \mathcal{A}$ est la fonction dont la valeur pour $x \in X$ est $f(x) \cdot g(x)$. En formule, $(f \cdot g)(x) := f(x) \cdot g(x)$.

Les fonctions $0 := X \longrightarrow \mathcal{A}$ et $1 := X \longrightarrow \mathcal{A}$, sont définies en posant $0(x) := 0$ et $1(x) = 1$ pour tout x dans X. Ce sont des fonctions **constantes**.

Proposition 1.3. *Si $\mathcal{A}$ est un anneau, l'ensemble $\mathcal{A}^X$, des fonctions de X vers $\mathcal{A}$, avec la somme et le produit défini ci-haut, est un anneau dont les éléments neutres additif et multiplicatif sont respectivement les fonctions constantes 0 et 1. Si $\mathcal{A}$ est commutatif, alors $\mathcal{A}^X$ l'est aussi.*

Preuve. La vérification est laissée en exercice au lecteur (voir exercice). ∎

1.4 Calculs dans un anneau

Plusieurs identités usuelles sont valables dans les anneaux quelconques. Ainsi, on a

Proposition 1.4. *Dans tout anneau $\mathcal{A}$, avec a et b dans $\mathcal{A}$, on a*

(i) $a \cdot 0 = 0 = 0 \cdot a$,

(ii) $(-a)\,b = a\,(-b) = -ab$, *et* $(-a)(-b) = ab$, (règle des signes)

(iii) $-(a + b) = (-a) + (-b)$.

La propriété (i) exprime que 0 est **absorbant**.

Preuve. Faite en cours. ∎

On écrit $a - b$ pour $a + (-b)$.

Proposition 1.5 (Distributivité généralisée)**.** *Pour tout a_i et b_j dans $\mathcal{A}$, avec $1 \le i \le p$ et $1 \le j \le q$, on a*

$$\begin{aligned}(a_1 + a_2 + \ldots + a_p)(b_1 + b_2 + \ldots + b_q) &= \sum_{1\le i\le p}\sum_{1\le j\le q} a_i\,b_j \\ &= (a_1b_1 + a_1b_2 + \ldots a_1b_q) \\ &\quad + (a_2b_1 + a_2b_2 + \ldots a_2b_q) + \\ &\qquad \vdots \\ &\quad + (a_pb_1 + a_pb_2 + \ldots a_pb_q).\end{aligned} \tag{1.4.1}$$

Preuve. Par double récurrence sur p et q. Faite en cours. ∎

La **puissance n-ième** d'un élément a de $\mathcal{A}$ se définit par récurrence comme

$$a^n := \begin{cases} 1 & \text{si } n = 0, \\ a\,(a^{n-1}) & \text{si } n > 0. \end{cases}$$

Ceci a aussi un sens dans un semi-anneau.

Proposition 1.6. *Pour tout i et j dans $\mathbb{N}$, on a*

(i) $a^i a^j = a^{i+j}$,

(ii) $(a^i)^j = a^{ij}$.

Preuve. Faite en théorie des groupes. ∎

Rappelons que dans un groupe abélien (ici $(\mathcal{A}, +)$), pour $n \in \mathbb{Z}$ et $a \in \mathcal{A}$, on dénote[4] par $n \cdot a$ l'élément de $\mathcal{A}$ défini par récurrence comme suit

$$n \cdot a := \begin{cases} 0 & \text{si } n = 0, \\ a + ((n-1) \cdot a) & \text{si } n > 0. \\ -((-n)\,a) & \text{si } n < 0, \qquad (\text{donc } (-n) > 0). \end{cases}$$

Autrement dit, lorsque $n > 0$, on a

$$n \cdot a := \underbrace{a + a + \cdots + a}_{n \text{ fois}},$$

et on dit de $n \cdot a$ que c'est un **multiple entier** de a. On a les propriétés : $-(-a) = a$, et $(n + k) \cdot a = n \cdot a + k \cdot a$ pour tout entiers n et k. De plus, $(n \cdot a) \cdot (k \cdot b) = (nk) \cdot (ab)$.

Pour prouver la dernière égalité, on commence par le cas $n, k \geq 0$, en utilisant la Proposition la disstributivité généralisée, 1.5 ; puis on utilise la règle des signes pour le cas général.

Proposition 1.7. *Soit $\mathcal{A}$ un anneau commutatif, et a et b des éléments de $\mathcal{A}$. Alors, pour tout $n \in \mathbb{N}$, on a*[5]

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}. \tag{1.4.2}$$

Preuve. Comparer $(a + b)^n$ et $(a + b)\,(a + b)^{n-1}$, et utiliser la récurrence classique du triangle de Pascal. ∎

Observez que lorsque $\mathcal{A}$ n'est pas commutatif, la formule (1.4.2) n'est pas valable. En effet, si $ab \neq ba$, on a

$$(a + b) = a^2 + ab + ba + b^2 \neq a^2 + 2ab + b^2.$$

4. **Attention**, n n'est pas un élément de $\mathcal{A}$, et donc $n \cdot a$ n'est pas un produit dans $\mathcal{A}$ mais seulement une abréviation pour une somme.

5. Rappelons que $\binom{n}{k} = n!/(k!(n-k)!)$.

Exercice 1.5. Définir, par récurrence[6] sur le cardinal de I, la **sommation** $\sum_{i\in I} a_i$, pour des éléments a_i de $\mathcal{A}$ indicés par un ensemble fini quelconque I. Montrer que si I et J sont des ensembles disjoints, avec des $a_j \in \mathcal{A}$ pour chaque $j \in J$, alors

$$\Big(\sum_{i\in I} a_i\Big) + \Big(\sum_{j\in J} a_i\Big) = \sum_{k\in I\cup J} a_k.$$

Remarquez qu'il est donc (!) naturel de poser $\sum_{i\in I} a_i = 0$ si I est l'ensemble vide.

Exercice 1.6. Pour un anneau commutatif, définir le **produit** $\prod_{i\in I} a_i$, pour des éléments a_i de $\mathcal{A}$ indicés par un ensemble fini quelconque I. Montrer que si I et J sont des ensembles disjoints, avec des $a_j \in \mathcal{A}$ pour chaque $j \in J$, alors

$$\Big(\prod_{i\in I} a_i\Big) \cdot \Big(\prod_{j\in J} a_i\Big) = \prod_{k\in I\cup J} a_k.$$

Remarquez qu'il est naturel de poser $\prod_{i\in I} a_i = 1$ si I est l'ensemble vide. Pourquoi n'est-il pas clair d'étendre directement cette définition au cas non commutatif ?

Exercice 1.7 (**Identités remarquables**).

1) Montrer que dans un anneau commutatif on a l'identité :

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

2) Dans un anneau quelconque calculer :

i) $(a+b)^2 + (a-b)^2$

ii) $(1+a)(a+b-1)+1$

iii) $1 + (a+b-1)(2+a+b+ab)(a+b-1) + 3(a+b-1)$

1.5 Sous-anneaux, éléments inversibles et diviseurs de zéro

Définition 3. Un **sous-anneau** $\mathcal{B}$ d'un anneau $\mathcal{A}$, est un sous-groupe additif[7] de $(\mathcal{A}, +)$, tel que

- l'élément neutre de $\mathcal{A}$ appartient à $\mathcal{B}$: $1 \in \mathcal{B}$.
- pour tout a et b dans $\mathcal{B}$, on a $ab \in \mathcal{B}$. ■

Proposition 1.8. *L'intersection d'une famille de sous-anneaux est un sous-anneau. C'est le plus grand sous-anneau qui est contenu dans tous les sous-anneaux de la famille.*

Preuve. Soit $\{\mathcal{B}_k\}_{k\in K}$ une famille de sous-anneaux de $\mathcal{A}$. Puisque 0 et 1 sont des éléments de chacun des $\mathcal{B}_k$ (puisque les $\mathcal{B}_k$ sont des sous-anneaux), ils sont aussi des éléments de $\mathcal{C} := \bigcap_{k\in K} \mathcal{B}_k$. Pour a et b dans $\mathcal{C}$, par définition, a et b sont dans chacun des $\mathcal{B}_k$, et donc on a que $a+b$ et ab sont dans chacun des $\mathcal{B}_k$. Il s'ensuit que $a+b$ et ab sont dans $\mathcal{C}$, ce qui montre que $\mathcal{C}$ est bien un sous-anneau. ■

Corollaire 1.9. *L'intersection de tous les sous-anneaux de $\mathcal{A}$ est l'ensemble $\{n\cdot 1 \mid n \in \mathbb{Z}\}$, des multiples entiers de l'élément neutre de $\mathcal{A}$. C'est le plus petit sous-anneau de $\mathcal{A}$.*

6. Pourquoi la commutativité de la somme permet-elle de faire cela sans problème ?
7. Donc, $0 \in \mathcal{B}$, si $a, b \in \mathcal{B}$ alors $(a+b) \in \mathcal{B}$, et si $a \in \mathcal{B}$ alors $-a \in \mathcal{B}$.

On dit de ce sous-anneau, que c'est le **sous-anneau premier** de $\mathcal{A}$. Lorsqu'il existe $n \geq 1$ tel que $n \cdot 1 = 0$, on dit du plus petit tel entier que c'est la **caractéristique** de $\mathcal{A}$. S'il n'y a pas de tel entier, on dit que $\mathcal{A}$ est de caractéristique 0. Par exemple, les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, et $\mathbb{C}$ sont tous de caractéristique 0 ; tandis que $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n. Lorsque le contexte s'y prête, on dénote simplement par n l'élément $n \cdot 1$ de $\mathcal{A}$. Il s'agit là d'un abus de notation qu'il faut savoir manipuler avec soin.

Définition 4. On dit d'un élément a de A qu'il admet un **inverse à droite** (resp. **inverse à gauche**), s'il existe $d \in \mathcal{A}$ tel que $a\,d = 1$ (rep. s'il existe $g \in \mathcal{A}$ tel que $g\,a = 1$). ■

On vérifie que, si a admet à la fois un inverse à droite et un inverse à gauche, alors ces deux inverses sont uniques et égaux. On désigne par a^{-1} cet inverse. On dit alors que a est **inversible**, et on désigne par $U(\mathcal{A})$ l'ensemble des éléments inversibles de $\mathcal{A}$.

Proposition 1.10. *L'ensemble $U(\mathcal{A})$ des éléments inversibles de $\mathcal{A}$, avec comme opération la multiplication dans $\mathcal{A}$, forme un groupe.*

Preuve. On constate d'abord que 1 est évidemment dans $U(\mathcal{A})$. Comme $b^{-1}a^{-1}$ est inverse de ab, on trouve que $U(\mathcal{A})$ est fermé par multiplication. De plus, a est l'inverse de a^{-1} (c.-à-d. $(a^{-1})^{-1} = a$), d'où a^{-1} est aussi dans $U(\mathcal{A})$ pour tout $a \in U(\mathcal{A})$. Enfin, la multiplication de $U(\mathcal{A})$ est associative, puisque c'est le cas dans $\mathcal{A}$. On a donc montré que $(U(\mathcal{A}), \cdot)$ est un groupe. ■

Exemples. Le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$ lui-même, et il en est de même pour $\mathbb{Z}/n\mathbb{Z}$. Le groupe des éléments inversibles de $\mathbb{Z}$ est $\{1, -1\}$. Pour $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$, ou $\mathbb{C}$, le groupe des éléments inversibles de $\mathbb{K}^{n\times n}$ est l'ensemble des matrices dont le déterminant est non nul :

$$U((\mathbb{K}^{n\times n})) = \{M \mid M \in \mathbb{K}^{n\times n},\ \det M \neq 0\}.$$

On dit que c'est le **groupe général linéaire**, et on le dénote habituellement par $\mathrm{GL}_n(\mathbb{K})$.

Définition 5. Dans un anneau $\mathcal{A}$, un **diviseur de zéro** à gauche (resp. à droite) est un élément $a \neq 0$ de $\mathcal{A}$, tel qu'il existe $b \neq 0$ avec $ab = 0$ (resp. $ba = 0$). Un **diviseur de zéro** (sans autre mention), est un diviseur de zéro à gauche ou à droite. ■

Exemple. Dans l'anneau $\mathbb{Z}/12\mathbb{Z}$, les diviseurs de zéro sont : 2, 3, 4, 6, 8, 9, et 12.

Définition 6. Un anneau est dit **intègre** (on dit aussi que c'est un domaine d'intégrité) s'il n'a pas de diviseur de zéro. ■

Proposition 1.11. *Tout sous-anneau d'un anneau intègre est intègre.*

Démonstration. Si $ab = 0$, où a, b sont deux éléments du sous-anneau, alors, l'anneau étant intègre, on doit avoir $a = 0$ ou $b = 0$. Donc le sous-anneau est intègre. ■

Proposition 1.12. *Soit $\mathcal{A}$ intègre, et a, b, c des éléments de $\mathcal{A}$. Alors*

$$ab = 0 \quad \Longrightarrow \quad a = 0 \text{ ou } b = 0.$$

De plus, si $a \neq 0$, alors

$$ab = ac \ \Rightarrow\ b = c; \qquad \text{et} \qquad ba = ca \ \Rightarrow\ b = c. \qquad \text{(Loi de simplification)}$$

Preuve. En cours. ∎

Exercice 1.8. Soit $(\mathcal{A}, +, \cdot)$ un anneau.

1) Montrer que $|\mathcal{A}| \geq 2$ si et seulement si $0 \neq 1$.

2) Soient $x, y \in \mathcal{A}$. Montrer que si $x \cdot y$ est inversible alors x est inversible à droite et y est inversible à gauche.

3) Montrer qu'un élément inversible n'est pas un diviseur de zéro et qu'un diviseur de zéro n'est pas inversible.

Exercice 1.9 (Éléments nilpotents). Soit $\mathcal{A}$ un anneau. On dit qu'un élément $a \in A$ qu'il est **nilpotent** s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$. Soient $a, b \in A$ deux éléments nilpotents.

1) Si $\mathcal{A}$ est commutatif montrer que ab est nilpotent.

2) Si $\mathcal{A}$ est commutatif montrer que $a + b$ est nilpotent

3) Si $\mathcal{A}$ est commutatif montrer que $1 - a$ est inversible.

4)) On suppose que ab est nilpotent. Montrer que ba l'est aussi.

1.6 Produits et homomorphismes d'anneaux

Pour $\mathcal{A}$ et $\mathcal{B}$ deux anneaux, on munit l'ensemble $\mathcal{A} \times \mathcal{B}$ d'une somme et d'un produit en posant, pour (a, b) et (a', b') des éléments de $\mathcal{A} \times \mathcal{B}$, que

- $(a, b) + (a', b') := (a + a', b + b')$, et
- $(a, b) \cdot (a', b') := (aa', bb')$.

On dit aussi que cet anneau est la **somme directe**[8] de $\mathcal{A}$ et de $\mathcal{B}$, et on écrit $\mathcal{A} \oplus \mathcal{B}$.

Proposition 1.13. *Avec les opérations ci-haut, l'ensemble $\mathcal{A} \times \mathcal{B}$ constitue un anneau, dont l'élément neutre additif est $0_{\mathcal{A}\times\mathcal{B}} := (0_{\mathcal{A}}, 0_{\mathcal{B}})$, et le neutre multiplicatif est $1_{\mathcal{A}\times\mathcal{B}} := (1_{\mathcal{A}}, 1_{\mathcal{B}})$. C'est un anneau commutatif si et seulement si $\mathcal{A}$ et $\mathcal{B}$ le sont. Il n'est pas intègre en général.*

Preuve. En cours. ∎

L'anneau dont il est question ci-dessus est l'**anneau produit** de $\mathcal{A}$ et $\mathcal{B}$. On peut généraliser cette définition (voir exercice) pour obtenir le produit de plusieurs anneaux : $\mathcal{A}_1 \times \mathcal{A}_2 \times \cdots \times \mathcal{A}_k$.

Proposition 1.14. *Pour $\mathcal{A}$ et $\mathcal{B}$ des anneaux, on a la relation suivante*[9] *pour le groupe des inverses :*

$$U((\mathcal{A} \times \mathcal{B})) = U(\mathcal{A}) \times U(\mathcal{B}). \tag{1.6.1}$$

Preuve. En cours. ∎

Comme c'est le cas pour de nombreuses structures algébriques (groupes, espaces vectoriels, etc.), la notion d'homomorphisme joue un rôle crucial dans l'étude des anneaux.

Définition 7. Pour $\mathcal{A}$ et $\mathcal{B}$ des anneaux, un **homomorphisme d'anneaux** de $\mathcal{A}$ vers $\mathcal{B}$ est une fonction $f : \mathcal{A} \longrightarrow \mathcal{B}$ telle que

8. Entres autres raisons, à cause de la similitude avec la construction de la somme directe d'espaces vectoriels.
9. Voir le cours de théorie des groupes pour la notion de produit de groupes.

(i) f est un homomorphisme[10] de groupe additif ;

(ii) $f(1_{\mathcal{A}}) = 1_{\mathcal{B}}$;

(iii) pour tout éléments a et a' de $\mathcal{A}$, on a $f(aa') = f(a)f(a')$.

On vérifie directement que la fonction identité $\mathrm{Id}_{\mathcal{A}}$ (d'un anneau $\mathcal{A}$ vers lui-même) est un homomorphisme, et que le composé de deux homomorphismes est un homomorphisme.

On appelle **noyau** de $f : \mathcal{A} \longrightarrow \mathcal{B}$, l'ensemble

$$f^{-1}(0) := \{a \in \mathcal{A} \mid f(a) = 0\},$$

et on le dénote $\mathrm{Ker}(f)$. L'**image** de $f : \mathcal{A} \longrightarrow \mathcal{B}$, dénotée $\mathrm{Im}(f)$ ou $f(\mathcal{A})$, est l'ensemble

$$f(\mathcal{A}) := \{f(a) \mid a \in \mathcal{A}\}.$$

C'est un sous-anneau de l'anneau $\mathcal{B}$. ■

Définition 8. On dit qu'un homomorphisme d'anneaux $f : \mathcal{A} \longrightarrow \mathcal{B}$ est un **isomorphisme** si la fonction f est bijective. La fonction inverse f^{-1} est dans ce cas aussi un homomorphisme d'anneaux. Un **endomorphisme** d'un anneau $\mathcal{A}$, est un homomorphisme de $\mathcal{A}$ vers $\mathcal{A}$. Un **automorphisme** d'un anneau $\mathcal{A}$, est un isomorphisme de $\mathcal{A}$ vers $\mathcal{A}$. Un **monomorphisme** est un homomorphisme pour lequel la fonction f est injective, et c'est un **epimorphisme** si la fonction f est surjective. On dénote avec la forme spéciale de flèche $\mathcal{A} \hookrightarrow \mathcal{B}$ un monomorphisme, $\mathcal{A} \twoheadrightarrow \mathcal{B}$ un épimorphisme, et $\mathcal{A} \xrightarrow{\sim} \mathcal{B}$ les isomorphismes. ■

Proposition 1.15. *Un homomorphisme d'anneaux $f : \mathcal{A} \longrightarrow \mathcal{B}$ est un monomorphisme si et seulement si* $\mathrm{Ker}(f) = \{0\}$.

Preuve. En cours. ■

Proposition 1.16. *Pour des sous-anneaux $\mathcal{A}'$ et $\mathcal{B}'$, respectivement de $\mathcal{A}$ et $\mathcal{B}$, et $f : \mathcal{A} \longrightarrow \mathcal{B}$ un homomorphisme d'anneaux, l'image $f(\mathcal{A}') := \{f(a) \mid a \in \mathcal{A}'\}$ est un sous-anneau de $\mathcal{A}$, et l'image réciproque $f^{-1}(\mathcal{B}') := \{a \in \mathcal{A} \mid f(a) \in \mathcal{B}'\}$ est un sous-anneau de $\mathcal{B}$.*

Preuve. En cours. ■

Proposition 1.17. *Si $\mathcal{A}$ est intègre et $\mathcal{B}$ est isomorphe à A, alors $\mathcal{B}$ est intègre.*

Exercice 1.10. On suppose que les anneaux B et $B_1 \times \cdots \times B_k$ sont isomorphes. Montrer que les anneaux $B \times C$ et $B_1 \times \cdots \times B_k \times C$ sont isomorphes

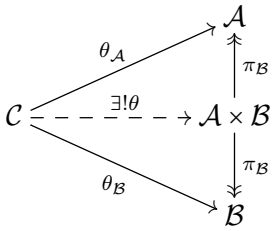
1.6.1 Exemples d'homomorphismes

Voici une petite liste d'homomorphismes d'anneaux typiques.

- Les inclusions de $\mathbb{Z}$ dans $\mathbb{Q}$, de $\mathbb{Q}$ dans $\mathbb{R}$, et de $\mathbb{R}$ dans $\mathbb{C}$, sont des monomorphismes d'anneaux.

10. c.-à-d. $f(a+b) = f(a) + f(b)$.

- La **projection** $\pi_{\mathcal{A}} : \mathcal{A} \times \mathcal{B} \longrightarrow \mathcal{A}$, définie en posant $\pi_{\mathcal{A}}(a, b) := a$, est un epimorphisme d'anneau. Son noyau est $\{0_{\mathcal{A}}\} \times \mathcal{B}$. On a le diagramme :



- Pour tout entier $n \geq 0$, la fonction de $\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$ qui envoie $a \in \mathbb{Z}$ sur la classe $[a]$ des entiers congrus à a modulo n : c.-à-d. $[a] := \{a + k\,n \mid k \in \mathbb{Z}\}$, est un epimorphisme d'anneau. Son noyau est $n\mathbb{Z} := \{kn \mid k \in \mathbb{Z}\}$.
- Pour tout anneau $\mathcal{A}$, la fonction $a \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ de $\mathcal{A}$ vers $\mathcal{A}^{2\times 2}$ est un homomorphisme d'anneaux.
- Pour tout anneau $\mathcal{A}$, si $a \in U(\mathcal{A})$, alors $x \mapsto axa^{-1}$ est un automorphisme de l'anneau $\mathcal{A}$.
- Soit $\mathcal{A}$ un anneau commutatif, et a est un élément fixé de $\mathcal{A}$. On a un homomorphisme de l'anneau des polynômes $\mathcal{A}[x]$ vers $\mathcal{A}$, qui envoie un polynômes p sur $p(a)$.
- Pour tout élément fixé c de X, on a la fonction $\mathrm{ev}_c : \mathcal{A}^X \longrightarrow \mathcal{A}$ qui associe à une fonction $f : X \longrightarrow \mathcal{A}$, sa valeur en c : c.-à-d. $ev_c(f) := f(c)$. On dit que c'est l'homomorphisme d'**évaluation** en c.
- L'anneau $\mathcal{A}^{\mathbb{N}}$ des suites à coefficients dans $\mathcal{A}$ est naturellement [11] isomorphe à l'anneau des séries formelles $\mathcal{A}[[x]]$.

1.7 Idéaux et anneaux quotients

La notion d'idéal joue en rôle fondamental pour la compréhension des homomorphismes d'anneaux.

Définition 9. Un **idéal** I, dans un anneau $\mathcal{A}$, est un sous-ensemble de $\mathcal{A}$ tel que

(i) I est un sous-groupe additif de $(\mathcal{A}, +)$;

(ii) pour tout $a \in \mathcal{A}$ et tout $x \in I$, on a ax et xa dans I.

Comme cas particuliers d'idéaux de $\mathcal{A}$, il y a $\{0\}$ et $\mathcal{A}$. Les idéaux autres que $\mathcal{A}$ sont dits **propres**. ■

Proposition 1.18. *Le noyau d'un homomorphisme est toujours un idéal.*

Preuve. En cours. ■

Définition 10. Pour tout idéal I dans un anneau $\mathcal{A}$, le groupe additif quotient $\mathcal{A}/I$ est muni d'opérations de somme et de produit (ceci est justifié à la proposition suivante) :

- $[a]_I + [b]_I := [a + b]_I$, (rappel)
- $[a]_I \cdot [b]_I := [a \cdot b]_I$.

Rappelons que les éléments du quotient $\mathcal{A}/I$ sont les classes d'équivalences $[a]_I := \{a + x \mid x \in I\}$. ■

11. Il y a une notion mathématique précise de naturalité, qui exprime qu'une construction "s'impose".

Proposition 1.19. *Avec ces définitions, on a une structure d'anneau bien définie sur $\mathcal{A}/I$, dont l'élément neutre multiplicatif est la classe $[1_{\mathcal{A}}]_I$. L'homomorphisme de groupe canonique*[12]

$$\pi : A \twoheadrightarrow A/I , \qquad a \mapsto [a]_I$$

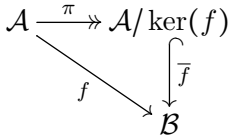
est un homomorphisme d'anneaux, dont le noyau est I. Il est surjectif (c'est un epimorphisme).

Preuve. En cours. ∎

Définition 11. L'anneau $\mathcal{A}/I$ ainsi obtenu est l'**anneau quotient** de $\mathcal{A}$ par I. ▪

Le théorème suivant décrit l'interaction entre homomorphismes et idéaux. On le nomme *propriété universelle du quotient*

Théorème 1.20. *Soit $f : \mathcal{A} \longrightarrow \mathcal{B}$ un homomorphisme d'anneaux. Il existe alors un seul homomorphisme d'anneaux $\overline{f} : A/\ker(f) \longrightarrow \mathcal{B}$, tel que le diagramme suivant commute :*



De plus, $\overline{f}$ est injectif (c'est un monomorphisme). Si f est un épimorphisme, alors $\overline{f}$ l'est aussi, et donc $\overline{f} : \mathcal{B} \xrightarrow{\sim} \mathcal{A}/\operatorname{Ker}(f)$ est un isomorphisme (c'est une bijection).

Preuve. En cours. ∎

Corollaire 1.21. *Si $f : \mathcal{A} \xrightarrow{\sim} \mathcal{B}$ est un homomorphisme d'anneaux, alors on a toujours l'isomorphisme d'anneaux $\mathcal{A}/\operatorname{Ker} f \xrightarrow{\sim} f(A)$.*

Proposition 1.22. *L'image réciproque d'un idéal par un homomorphisme est toujours un idéal. L'image par un épimorphisme d'un idéal est un idéal.*

Proposition 1.23. *L'intersection d'une famille d'idéaux est un idéal. C'est le plus grand idéal qui est contenu dans chacun des idéaux de la famille.*

Définition 12. Si X est un sous-ensemble d'un anneau A, alors $\langle X \rangle$ est l'idéal obtenu comme intersection de tous les idéaux qui contiennent les éléments de X. On dit que c'est l'**idéal engendré** par X. C'est le plus petit idéal qui contient X. Si X ne contient qu'un élément $a \in \mathcal{A}$, alors $\langle a \rangle = \{x\,a \mid x \in \mathcal{A}\} = \mathcal{A}\,a$ est l'ensemble des "multiples" de a. ▪

Définition 13. Un idéal I d'un anneau $\mathcal{A}$ est dit **maximal**, si et seulement si, pour tout idéal J de $\mathcal{A}$ tel que $I \subseteq J$, on a forcément $J = I$ ou $J = \mathcal{A}$. ▪

Définition 14. Un idéal I d'un anneau commutatif $\mathcal{A}$ est dit **premier**, si et seulement si c'est un idéal propre et, pour tout a et b dans $\mathcal{A}$, on a

$$(a\,b \in I) \qquad \Longrightarrow \qquad (a \in I \text{ ou } b \in I).$$

▪

12. Rappelons qu'il est défini en posant $\pi(a) := [a]_I$.

Proposition 1.24. *Un idéal I d'un anneau commutatif $\mathcal{A}$ est premier si et seulement si $\mathcal{A}/I$ est intègre.*

Proposition 1.25. *Tout idéal maximal d'un anneau commutatif est premier.*

Définition 15. Un idéal I d'un anneau commutatif $\mathcal{A}$ est dit **irréductible**, si et seulement si on ne peut pas l'écrire comme intersection de deux idéaux strictement plus grands. ∎

Définition 16. Pour I et J des idéaux d'un anneau commutatif $\mathcal{A}$, on a la **somme** et le **produit** :

$$I + J := \{a + b \mid a \in I \text{ et } b \in J\}, \qquad \text{et} \qquad I\,J := \langle ab \mid a \in I \text{ et } b \in J\rangle.$$

∎

1.7.1 Exemples d'idéaux et d'anneaux quotients

Parmi les exemples d'idéaux et de quotients associées on retrouve les suivants. D'autres seront décrits par la suite.

- On a les quotients triviaux $\mathcal{A}/\{0\} \simeq \mathcal{A}$, et $\mathcal{A}/\mathcal{A} \simeq 0$.
- Dans $\mathbb{Z}$, les idéaux sont de la forme $n\mathbb{Z}$ (l'ensemble des multiples de n dans $\mathbb{Z}$), voir plus loin. Le quotient associé $\mathbb{Z}/n\mathbb{Z}$ est l'anneau des entiers modulo n. La notion de quotient d'anneau généralise donc la construction de $\mathbb{Z}/n\mathbb{Z}$.
- Si a est un élément fixé d'un anneau commutatif $\mathcal{A}$, alors $\langle a\rangle := \{a \cdot b \mid b \in \mathcal{A}\}$ (des multiples de a) est un idéal dans $\mathcal{A}$.
- Comme cas spécial de l'exemple précédent, on considère le polynôme $a = x^2 + 1$ dans $\mathcal{A} = \mathbb{R}[x]$. Grâce au Théorème 1.20 on peut voir que le quotient $\mathbb{R}[x]/\langle x^2 + 1\rangle$ est isomorphe à $\mathbb{C}$.

1.7.2 Exercices

Exercice 1.11. Soit $\mathcal{A}$ un anneau commutatif. Calculer les quotients suivants :

1) $\mathcal{A}[x]/\langle x\rangle$,
2) $\mathcal{A}[x, y]/\langle x\rangle$,
3) $\mathcal{A}[x_1, x_2, ..., x_n]/\langle x_1, ..., x_n\rangle$,
4) $\mathbb{R}[x]/\langle x^2 + 1\rangle$,
5) $\mathbb{Z}[x]/\langle x^2 - d\rangle$ avec $d \in \mathbb{N}$,
6) $\mathbb{Q}[x]/\langle x^2 - 2\rangle$,
7) $\mathcal{A}[x, y]/\langle xy - 1\rangle$.

1.8 Anneaux $\mathbb{Z}/n\mathbb{Z}$

Commençons par caractériser les idéaux de $\mathbb{Z}$.

Proposition 1.26. *1) Un sous-ensemble de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un idéal si et seulement si c'est un sous-groupe additif. 2) Dans $\mathbb{Z}$, les idéaux sont de la forme $n\mathbb{Z}$ (l'ensemble des multiples de n dans $\mathbb{Z}$).*

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est l'anneau dont les éléments sont les classes modulo n. Il a n éléments si $n \geq 1$. On dit aussi que c'est l'anneau des *entiers modulo n*. Comme chaque entier a est congru à exactement un entier r dans $\{0, 1, \ldots, n-1\}$ (qui est le reste de la division euclidienne de a par n, on écrit souvent, par abus, $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$.

Proposition 1.27. *Soit $n \geq 2$. $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement n est un nombre premier.*

Preuve. Supposons que n est premier. Si $x = [a]$ et $y = [b]$ dans $\mathbb{Z}/n\mathbb{Z}$ sont tels que $xy = 0$, alors on a $ab \equiv 0 \mod n$, et donc n divise ab. Mais alors n divise a ou n divise b, ce qui correspond à dire que $x = 0$ ou $y = 0$. On donc montré l'une des implications nécessaires.

Pour montrer l'autre implication, on suppose par contradiction que n n'est pas premier et que $\mathbb{Z}/n\mathbb{Z}$ intègre. Mais alors il existe des entiers a et b tels que $n = ab$, avec ni a ni b qui se divisent par n. On a donc $[a] \neq 0$ et $[b] \neq 0$ dans $\mathbb{Z}/n\mathbb{Z}$. D'autre part $[a][b] = [ab] = [n] = 0$, ce qui contredit l'intégralité de $\mathbb{Z}/n\mathbb{Z}$. Ceci achève la démonstration. ∎

Proposition 1.28. *Les éléments inversibles $[a]$ de $\mathbb{Z}/n\mathbb{Z}$ sont ceux pour lesquels a et n sont* **relativement premiers**, *et on écrit $a \perp n$.*

Preuve. Si $a \perp n$, le théorème de Bézout assure qu'il existe des entiers b et k tels que $ab + nk = 1$. On a donc $[ab] = [a][b] = 1$ dans $\mathbb{Z}/n\mathbb{Z}$, et $[a]$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Réciproquement, si $[a]$ est inversible, il existe $[b]$ tel que $1 = [a][b] = [ab]$. Il existe donc k tel que $ab = 1 + nk$. Autrement dit $ab - nk = 1$, et $a \perp n$. ∎

Corollaire 1.29. *Le groupe $U(\mathbb{Z}/n\mathbb{Z})$ est en bijection avec l'ensemble $\{a \mid 0 \leq a \leq n-1,\ a \perp n\}$. En conséquence, son cardinal est $|U(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$.*

Rappelons que la **fonction φ d'Euler**[13] (aussi appelée l'**indicateur d'Euler**) est justement définie comme

$$\varphi(n) = \mathrm{card}\{a \mid 0 \leq a \leq n-1,\ a \perp n\}.$$

L'une des propriétés classiques de la fonction φ se déduit directement de la Proposition 1.14, et du fait qu'on ai un isomorphisme $\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$, lorsque $m = nk$ avec $n \perp k$.

Proposition 1.30. *Si n et k sont premiers entre eux, alors $\varphi(nk) = \varphi(n)\varphi(k)$.*

Preuve. Pour $m = nk$, an a $\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$, donc $U((\mathbb{Z}/m\mathbb{Z})) \simeq U((\mathbb{Z}/n\mathbb{Z})) \times U((\mathbb{Z}/k\mathbb{Z}))$ par la Proposition 1.14. D'où $\varphi(nk) = \varphi(n)\varphi(k)$ comme annoncé. ∎

Il s'ensuit qu'on a la formule classique suivante pour $\varphi(n)$.

Corollaire 1.31. *Si $n \in \mathbb{N}$ admet le développement $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ avec les p_i des nombres premiers distincts et des $m_i \geq 1$, alors*

$$\varphi(n) = n \prod_{i=1}^{k} \Big(1 - \frac{1}{p_i}\Big). \tag{1.8.1}$$

13. Leonhard Euler, 1707-1783.

Preuve. Pour p premier et $a \geq 1$, on a la formule

$$\begin{aligned}\varphi(p^a) &= \operatorname{card}\{x \mid 0 \leq x \leq p^a - 1,\ x \perp p\} \\ &= \operatorname{card}\big(\{x \mid 0 \leq x \leq p^a - 1\} \setminus \{0, p, 2p, 3p, \ldots, (p^{a-1} - 1)\, p\}\big) \\ &= p^a - p^{a-1} \\ &= p^a\Big(1 - \frac{1}{p}\Big).\end{aligned}$$

Le corollaire se déduit alors de la Proposition 1.30 appliquée successivement pour $p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$. ■

Proposition 1.32. *Soit $\mathcal{A}$ un anneau de caractéristique $n \geq 1$.*

1. *$\mathbb{Z}/n\mathbb{Z}$ s'injecte canoniquement dans $\mathcal{A}$, et l'image est le sous-anneau premier de A.*
2. *Si $\mathcal{A}$ est intègre, alors n est un nombre premier.*

Preuve. Par définition, la caractéristique de $\mathcal{A}$ est l'entier n tel que $n\mathbb{Z}$ soit le noyau de l'homomorphisme $\mathbb{Z} \longrightarrow \mathcal{A}$ qui envoie $1_\mathbb{Z}$ dans $1_\mathcal{A}$. Son image est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ par le Théorème 1.20. Par la Proposition 1.11, il s'ensuit que $\mathbb{Z}/n\mathbb{Z}$ est intègre, et donc que n est premier (voir prop. 1.27). ■

Proposition 1.33. *Si $\mathcal{A}$ est un anneau commutatif de caractéristique p, un nombre premier, alors l'application $F : \mathcal{A} \longrightarrow \mathcal{A}$ telle que $F(x) = x^p$ est un homorphisme d'anneau. On l'appelle l'homomorphisme de* **Frobenius**[14].

Preuve. Évidemment $0^p = 0$ et $1^p = 1$. On utilise ensuite l'identité (1.4.2), avec le fait que p divise $\binom{p}{k}$ lorsque $1 \leq k \leq n-1$, pour conclure que $(a+b)^p = a^p + b^p$. Ceci, avec la propriété usuelle $(a\cdot)^p = a^p \cdot b^p$, montre que F est bien un homomorphisme. ■

1.9 Corps

Un **corps** est un anneau dans lequel tout élément non nul est inversible. Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps, mais $\mathbb{Z}$ ne l'est pas.

Proposition 1.34. *Un corps est un anneau intègre.*

Preuve. Si $xy = 0$, et $x \neq 0$, alors x est inversible. Son inverse est x^{-1}, et on calcule alors que

$$0 = x^{-1}0 = x^{-1}xy = y.$$

d'où l'intégralité. ■

Proposition 1.35. *Si A est un anneau intègre fini, alors $\mathcal{A}$ est un corps.*

Preuve. Pour tout $x \neq 0$, on considère la fonction $\mathcal{A} \longrightarrow \mathcal{A}$, telle que $a \mapsto ax$. Cette fonction est bijective, car elle admet comme inverse la fonction $a \mapsto ax^{-1}$. En particulier la fonction est surjective, et il y a donc une valeur de a pour laquelle $ax = 1$, ce qui montre que x est inversible. ■

14. Ferdinand Georg Frobenius (1849-1917)

Bien entendu la condition pour $\mathcal{A}$ d'être fini est essentielle. En effet l'anneau $\mathbb{Z}$ est intègre, mais ce n'est pas un corps.

Définition 17. Un **sous-corps** d'un corps, est un sous-anneau qui contient l'inverse (multiplicatif) de chacun des éléments non nuls qu'il contient. C'est donc bien aussi un corps. ■

On a par exemple que $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, et $\mathbb{R}$ est un sous-corps de $\mathbb{C}$.

Proposition 1.36. *Si $\mathcal{A}$ est un anneau commutatif, alors $\mathcal{A}$ est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et $\mathcal{A}$.*

Preuve. En cours ■

Proposition 1.37. *$\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier.*

Preuve. En cours ■

On verra au chapitre 4 que les corps finis sont de cardinalité p^n, pour p premier et $n \geq 1$. Pour $n = 1$, ce sont les $\mathbb{Z}/p\mathbb{Z}$ (il n'y en a pas d'autres). Pour $n \geq 2$, ce ne sont pas les anneaux $\mathbb{Z}/p^n\mathbb{Z}$ (qui ne sont pas intègre).

Pour calculer explicitement l'inverse de $[a]$ dans le corps $\mathbb{Z}/p\mathbb{Z}$, on applique l'algorithme d'Euclide au couple (a, n), pour trouver des entiers b et k tels que $ab + nk = 1$. Alors, l'inverse de $[a]$ est $[b]$. Par exemple, pour $p = 137$ et $a = 21$, on calcule que

$$\begin{aligned} 137 &= 6 \cdot 21 + 11 && \Longrightarrow 11 = 137 - 6 \cdot 21 \\ 21 &= 1 \cdot 11 + 10 && \Longrightarrow 10 = 21 - 1 \cdot 11 \\ 11 &= 1 \cdot 10 + 1 && \Longrightarrow 1 = 11 - 1 \cdot 10. \end{aligned}$$

Remontant ces égalités, on trouve

$$\begin{aligned} 1 &= 11 - 1 \cdot 10 \\ &= 11 - 1 \cdot (21 - 1 \cdot 11) = 2 \cdot 11 - 1 \cdot 21 \\ &= 2 \cdot (137 - 6 \cdot 21) - 1 \cdot 21 \\ &= 2 \cdot 137 + (-13) \cdot 21, \end{aligned}$$

donc $[-13] = [124]$ est l'inverse de $[21]$ dans $\mathbb{Z}/137\mathbb{Z}$.

Nous verrons plus tard (voir chapitre 3) que l'anneau $\mathbb{Q}[x]/\langle x^4 - x^2 - 2\rangle$ donné comme exemple à la section 1.9.1 est un corps, tout simplement parce que le polynôme $x^4 - x^2 - 2$ est irréductible dans $\mathbb{Q}[x]$.

Proposition 1.38. *Soit $\mathcal{A}$ un anneau commutatif, et I un idéal de A. Alors $\mathcal{A}/I$ est un corps si et seulement si l'idéal I est maximal.*

Preuve. En cours. ■

Corollaire 1.39. *Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$, pour p premier.*

Proposition 1.40. *Si un corps $\mathbb{K}$ est de caractéristique non nulle, celle-ci est un nombre premier p, et $\mathbb{K}$ contient un sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$, à savoir son sous-corps premier.*

Preuve. En cours. ∎

Proposition 1.41. *Soit $\mathcal{A}$ un anneau différent de l'anneau $\{0\}$ et $\mathbb{K}$ un corps, alors tout homomorphisme d'anneaux $f : \mathbb{K} \longrightarrow \mathcal{A}$ est injectif.*

Preuve. En cours. ∎

Proposition 1.42. *L'ensemble $\{a + bi \mid a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$, dont les éléments inversibles sont 1, -1, i et $-i$. C'est l'anneau des* **entiers de Gauss**, *dénoté $\mathbb{Z}[i]$, et il est intègre. L'ensemble $\{a + bi \mid a, b \in \mathbb{Q}\}$ forme un sous-corps de $\mathbb{C}$. C'est le corps des* **rationnels de Gauss**, *dénoté $\mathbb{Q}[i]$.*

Preuve. En exercice. ∎

1.9.1 Anneau $\mathbb{K}[x]/\langle f(x)\rangle$

Dans cette partie, $\mathbb{K}$ est un corps commutatif. Pour un polynôme fixé $f(x)$ dans $\mathbb{K}[x]$, on considère le quotient de $\mathbb{K}[x]$ par l'idéal

$$\langle f(x)\rangle = \{f(x)g(x) \mid g(x) \in \mathbb{Q}[x]\},$$

des multiples de $f(x)$. Pour simplifier la présentation, on suppose que le terme de degré maximal dans $f(x)$ est de la forme x^n. C'est donc dire que

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0.$$

On dit alors que $f(x)$ est **unitaire** (ou aussi **monique**). L'algorithme d'Euclide pour les polynômes (voir chapitre 2 pour une généralisation de ces notions) permet de calculer un représentant canonique pour les éléments de l'anneau quotient $\mathbb{K}[x]/\langle f(x)\rangle$. En effet, la classe d'équivalence $[p(x)]$ de tout polynôme $p(x)$ dans $\mathbb{K}[x]$, contient un unique polynôme qui est :

- soit 0, si $p(x)$ est un multiple de $f(x)$,
- soit un polynôme $r(x)$, dont le degré est plus petit que celui de $f(x)$, dans les autres cas.

Ce polynôme $r(x)$ est obtenu comme le reste $r(x)$ de la division euclidienne de $p(x)$ par $f(x)$:

$$p(x) = f(x)\,q(x) + r(x),$$

où, soit $r(x) = 0$, soit $\deg(r(x)) < \deg(f(x))$. Ces polynômes $q(x)$ et $r(x)$ sont uniquement caractérisés par ces propriétés. On peut ainsi "identifier" $\mathbb{K}[x]/\langle f(x)\rangle$ avec l'ensemble des polynômes de la forme :

$$r(x) = c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \ldots + c_1x + c_0,$$

avec la somme habituelle. Pour calculer le produit de deux polynômes $r(x)$ et $r'(x)$ de cette forme, on calcule le reste de la division de $r(x)r'(x)$ par $f(x)$. On dit que c'est le calcul **modulo** $f(x)$, et on écrit $(r(x)r'(x) \mod f(x))$ pour le reste en question. On observe qu'on peut organiser le calcul

du produit modulo $f(x)$ en exploitant la bilinéarité du produit, pour le réduire à de simples produits de la forme $x^k x^l = x^{k+l}$. Il suffit alors de calculer (une fois pour toute) les valeurs de $(x^k \mod f(x))$, pour les valeurs de k se situant entre n et $2n-2$, et on écrit $x^k \equiv (x^k \mod f(x))$. On observe qu'on obtient facilement ces valeurs récursivement en exploitant l'identité

$$x^{k+n} \equiv -(a_{n-1}x^{k+n-1} + a_{n-2}x^{k+n-2} + \ldots + a_1 x^{k+1} + a_0 x^k), \tag{1.9.1}$$

pour réduire le calcul à des puissance plus petites.

De ceci on peut déduire le théorème suivant.

Théorème 1.43. *Soit $f(x) \in \mathbb{K}[x]$, $\mathbb{K}$ un corps commutatif. On suppose f non nul. Soit $\mathcal{A} = \mathbb{K}[x]/\langle f(x)\rangle$.*

1. $\mathcal{A} = 0$ si et seulement si f est constant. Supposons f non constant.

2. $\mathbb{K}$ s'injecte canoniquement dans $\mathcal{A}$ comme sous-corps et $\mathcal{A}$ devient ainsi un espace vectoriel sur $\mathbb{K}$. La dimension de $\mathcal{A}$ sur $\mathbb{K}$ est égale au degré de f.

Illustrons ceci par un exemple, avec $\mathbb{K} = \mathbb{Q}$. . Soit $f(x) = x^4 - x^2 - 2$. Par le processus décrit plus haut, les classes d'équivalences du quotient correspondent bijectivement aux polynômes de la forme $a + bx + cx^2 + dx^3$, avec a, b, c, d dans $\mathbb{Q}$. Les règles de calcul de base issues de (1.9.1) sont alors les suivantes :

$$\begin{aligned} x^4 &\equiv x^2 + 2, \\ x^5 &\equiv x^3 + 2x, \\ x^6 &\equiv 3x^2 + 2; \end{aligned}$$

d'où on déduit la règle de calcul suivante dans l'anneau $\mathbb{Q}[x]/\langle x^4 - x^2 - 2\rangle$:

$$\begin{aligned} (a_1 + b_1 x + c_1 x^2 + d_1 x^3)(a_2 + b_2 x + c_2 x^2 + d_2 x^3) \\ &\equiv (a_1 a_2 + 2\,b_1 d_2 + 2\,b_2 d_1 + 2\,c_1 c_2 + 2\,d_1 d_2) \\ &\quad + (a_1 b_2 + a_2 b_1 + 2\,c_1 d_2 + 2\,c_2 d_1)\,x \\ &\quad + (a_1 c_2 + a_2 c_1 + b_1 b_2 + b_1 d_2 + b_2 d_1 + c_1 c_2 + 3\,d_1 d_2)\,x^2 \\ &\quad + (a_1 d_2 + a_2 d_1 + b_1 c_2 + b_2 c_1 + c_1 d_2 + c_2 d_1)\,x^3. \end{aligned}$$

On observe que x est inversible dans $\mathbb{Q}[x]/\langle x^4 - x^2 - 2\rangle$. Son inverse est $(-1/2)x^3 + (1/2)x$, car on a

$$x\left(\frac{-1}{2}x^3 + \frac{1}{2}x\right) = \frac{1}{2}(x^4 - x^2) \equiv 1,$$

puisque $x^4 - x \equiv 2$.

1.9.2 Corps de fractions

Parmi les exemples importants de corps, on a certainement les corps de fractions associés aux anneaux intègres. Nous allons nous restreindre au cas commutatif.

Définition 18. Soit $\mathcal{A}$ un anneau commutatif intègre. Sur l'ensemble $\{(a,b) \mid b \neq 0\}$, on considère la relation d'équivalence :

$$(a,b) \simeq (a',b') \text{ si et seulement si } ab' = a'b.$$

La classe d'équivalence de (a,b) pour cette relation est dénotée a/b, et $\mathrm{Frac}(\mathcal{A})$ désigne l'ensemble de ces **fractions**. On obtient le **corps de fractions** de $\mathcal{A}$, en munissant l'ensemble $\mathrm{Frac}(\mathcal{A})$ de la somme et du produit définis comme :

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1b_2 + a_2b_1}{a_1b_1}, \qquad \text{et} \qquad \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1a_2}{b_1b_2},$$

avec $0/1$ comme neutre additif, et $1/1$ comme neutre multiplicatif. C'est un corps commutatif qui contient (une copie [15] de) $\mathcal{A}$ comme sous-anneau. ∎

Par exemple, on a le corps de fractions associé à l'anneau des polynômes [16] $\mathbb{K}[x]$, sur un corps commutatif, qui est habituellement dénoté $\mathbb{K}(x)$. Le corps de fraction de l'anneau des entiers de Gauss est isomorphe au corps des rationnels de Gauss $\mathbb{Q}[i]$.

Proposition 1.44. *(propriété universelle du corps des fractions) Si $\mathcal{A}$ est un anneau commutatif intègre et si $\mathcal{A} \to K$ est un homomorphismes d'anneau injectif, alors il se prolonge de manière unique à un homomorphisme d,anneaux injectif* $\mathrm{Frac}(\mathcal{A}) \to K$.

1.10 Algèbre d'un monoïde

Un **monoïde** est un ensemble $\mathcal{M}$ muni d'une opération $(a,b) \mapsto a \cdot b$ qui est associative, avec un élément neutre 1. Il est **commutatif** si de plus $a \cdot b = b \cdot a$, pour tout $a, b \in \mathcal{M}$.

La notation $a \cdot b$ pour la multiplication s'appelle la **notation multiplicative**. On peut aussi noter l'opération $a + b$, ce qu'on appelle **notation additive**. Le plus souvent, lorsqu'on est en notation additive, il est sous-entendu que le monoïde est commutatif.

Pour un anneau $\mathcal{A}$, on considère l'ensemble $\mathcal{A}[\mathcal{M}]$ des fonctions de $\mathcal{M}$ vers $\mathcal{A}$, dont le "support" est fini. Le **support** d'une fonction f est l'ensemble

$$\mathrm{supp}(f) := \{m \in \mathcal{M} \mid f(x) \neq 0\}.$$

Pour f et g deux fonction de $\mathcal{M}$ vers $\mathcal{A}$ de support fini, on défini

- la **somme** $f + g$, en posant $(f+g)(m) := f(m) + g(m)$,
- le **produit** $f \cdot g$, en posant $(f \cdot g)(m) := \sum_{pq=m} f(p) \cdot g(q)$.

On vérifie (en exercice) que $\mathrm{supp}(f+g) \subset \mathrm{supp}(f) \cup \mathrm{supp}(g)$, et que

$$\mathrm{supp}(f \cdot g) \subset \mathrm{supp}(f) \cdot \mathrm{supp}(g) = \{pq| \mid p \in \mathrm{supp}(f) \text{ et } q \in \mathrm{supp}(g)\}.$$

Ceci montre que $f + g$ et $f \cdot g$ sont bien des éléments de $\mathcal{A}[M]$. L'ensemble $\mathcal{A}[\mathcal{M}]$, munit de ces opérations est un anneau. On l'appelle la $\mathcal{A}$-**algèbre** de $\mathcal{M}$.

15. Les éléments a de $\mathcal{A}$ sont identifiées aux fractions $a/1$.
16. Qui est intègre.

Définition 19. Pour $m \in \mathcal{M}$, la fonction caractéristique de $\{m\}$ est la fonction $\chi_m : \mathcal{M} \longrightarrow \mathcal{A}$ définie en posant

$$\chi_m(p) := \begin{cases} 1_{\mathcal{A}} & \text{si } p = m, \\ 0_{\mathcal{A}} & \text{sinon.} \end{cases}$$

On vérifie (en exercice) que la fonction $m \mapsto \chi_m$ est un monomorphisme de monoïde de $\mathcal{M}$ ver $\mathcal{A}[\mathcal{M}]$. Par abus de notation, on désignera par m la fonction χ_m. ∎

Définition 20. Pour $a \in \mathcal{A}$, on a la fonction $\varphi_a : \mathcal{M} \longrightarrow \mathcal{A}$ définie en posant

$$\varphi_a(m) := \begin{cases} a & \text{si } m = 1_{\mathcal{M}}, \\ 0_{\mathcal{A}} & \text{sinon.} \end{cases}$$

On vérifie (en exercice) que la fonction $a \mapsto \varphi_a$ est un monomorphisme d'anneau $\mathcal{A}$ ver $\mathcal{A}[\mathcal{M}]$. Par abus de notation, on désignera par a la fonction φ_a. ∎

Avec ces définitions, et les abus de notations correspondants, on vérifie qu'on peut écrire tout élément f de $\mathcal{A}[\mathcal{M}]$ comme :

$$f = \sum_{m \in \mathcal{M}} f(m)\, m \qquad \text{(Sans les abus, cela s'écrirait } f = \sum_{m \in \mathcal{M}} \varphi_{f(m)}\, \chi_m\text{).} \tag{1.10.1}$$

Dans un langage moins formel, on peut dire que les éléments de $\mathcal{A}[\mathcal{M}]$ sont les combinaisons linéaires d'éléments de $\mathcal{M}$, c.-à-d. des expressions de la forme $\sum_{m \in \mathcal{M}} a_m\, m$, avec seulement un nombre fini des **coefficients** $a_m \in \mathcal{A}$ étant non-nuls. La somme et le produit s'expriment alors respectivement comme

$$\Big(\sum a_m\, m\Big) + \Big(\sum b_m\, m\Big) = \sum (a_m + b_m)\, m, \tag{1.10.2}$$

$$\Big(\sum a_m\, m\Big) \cdot \Big(\sum b_m\, m\Big) = \sum_m \Big(\sum_{pq=m} a_p \cdot b_q\Big)\, m. \tag{1.10.3}$$

1.11 Polynômes en plusieurs variables

D'un point de vue formel (dans la lignée de la section précédente), on considère le monoïde des **monômes**

$$\mathbb{M} := \{x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k} \mid (n_1, n_2 \ldots, n_k) \in \mathbb{N}^k\},$$

avec la multiplication

$$(x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}) \cdot (x_1^{m_1} x_2^{m_2} \cdots x_k^{m_k}) := (x_1^{n_1+m_1} x_2^{n_2+m_2} \cdots x_k^{n_k+m_k}).$$

Une notation, souvent dite "vectorielle", est souvent avantageuse dans ce cas. Ainsi, pour un "vecteur" de degrés $\boldsymbol{n} = (n_1, n_2, \ldots, n_k)$ dans $\mathbb{N}^k$ (qui est considéré ici comme monoïde pour l'addition), on pose

$$\boldsymbol{x}^{\boldsymbol{n}} := x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k},$$

où $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ est un "vecteur" de variables. On a alors

$$\begin{aligned} \boldsymbol{x}^{\boldsymbol{0}} &= 1, \\ \boldsymbol{x}^{\boldsymbol{n}} \cdot \boldsymbol{x}^{\boldsymbol{m}} &= \boldsymbol{x}^{\boldsymbol{n}+\boldsymbol{m}}, \\ (\boldsymbol{x}^{\boldsymbol{n}})^a &= \boldsymbol{x}^{a\,\boldsymbol{n}}. \end{aligned}$$

La $\mathcal{A}$-algèbre du monoïde $\mathbb{M}$, est la $\mathcal{A}$-algèbre des polynômes en les variables $x_1, x_2, \ldots, x_n$, et on la dénote $\mathcal{A}[\boldsymbol{x}] = \mathcal{A}[x_1, x_2, \ldots, x_n]$. Dans un langage moins formel, on peut dire que les éléments de $\mathcal{A}[\boldsymbol{x}]$ sont simplement les combinaisons linéaires de monômes avec coefficients dans $\mathcal{A}$, c.-à-d. des expressions de la forme

$$P = \sum_{\boldsymbol{n}\in\mathbb{N}^k} a_{\boldsymbol{n}}\, \boldsymbol{x}^{\boldsymbol{n}},$$

où seulement un nombre fini des **coefficients** $a_n \in \mathcal{A}$ sont non nuls. La somme et le produit s'expriment alors respectivement comme

$$\Big(\sum_{\boldsymbol{n}} a_{\boldsymbol{n}}\, \boldsymbol{x}^{\boldsymbol{n}}\Big) + \Big(\sum_{\boldsymbol{n}} b_{\boldsymbol{n}}\, \boldsymbol{x}^{\boldsymbol{n}}\Big) = \sum_{\boldsymbol{n}} (a_{\boldsymbol{n}} + b_{\boldsymbol{n}})\, \boldsymbol{x}^{\boldsymbol{n}}, \tag{1.11.1}$$

$$\Big(\sum_{\boldsymbol{n}} a_{\boldsymbol{n}}\, \boldsymbol{x}^{\boldsymbol{n}}\Big) \cdot \Big(\sum_{\boldsymbol{n}} b_{\boldsymbol{n}}\, \boldsymbol{x}^{\boldsymbol{n}}\Big) = \sum_{\boldsymbol{n}} \Big(\sum_{\boldsymbol{p}+\boldsymbol{q}=\boldsymbol{n}} a_{\boldsymbol{p}} \cdot b_{\boldsymbol{q}}\Big)\, \boldsymbol{x}^{\boldsymbol{n}}. \tag{1.11.2}$$

Par définition, le **degré** $\deg(P)$ d'un polynôme P non nul est :

$$\deg(P) := \max_{a_{\boldsymbol{n}}\neq 0} |\boldsymbol{n}|, \qquad \text{où} \qquad |\boldsymbol{n}| := n_1 + \ldots + n_k,$$

et il est pratique [17] de poser $\deg(0) := -\infty$. Dans ce cas, les règles de calcul de la somme sur $\mathbb{N}$ sont étendues à $\mathbb{N} \cup \{-\infty\}$ en posant pour tout $n \in \mathbb{N}$ que : $n - \infty = -\infty + n = -\infty$.

1.12 (*) Autres exemples d'anneaux

1.12.1 (*) L'anneau des suites à coefficients dans un anneau commutatif $\mathcal{A}$

Sur l'ensemble des fonctions de $\mathbb{N}$ dans un anneau commutatif $\mathcal{A}$, on considère une autre structure d'anneau en changeant le produit de l'exemple précédent par le **produit de convolution**. Pour souligner la différence, on dit dans ce cas que les éléments de $\mathcal{A}^{\mathbb{N}}$ sont des **suites** à coefficients dans $\mathcal{A}$, et on les dénote $\alpha = (a_n)_{n\in\mathbb{N}} = (a_0, a_1, a_2, \ldots)$. Deux suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont égales si et seulement si on a $a_n = b_n$ pour tout n dans $\mathbb{N}$.

On écrit aussi plus simplement (a_n) pour $(a_n)_{n\in\mathbb{N}}$. On a la somme $(a_n) + (b_n) := (a_n + b_n)$. Autrement dit,

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots),$$

et l'élément neutre additif est la suite constante $(0) := (0, 0, \ldots)$. Le produit de convolution se définit comme

$$(a_n) * (b_n) := \Big(\sum_{k=0}^{n} a_k b_{n-k}\Big).$$

Autrement dit,

$$(a_0, a_1, a_2, \ldots) * (b_0, b_1, b_2, \ldots) = (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \ldots).$$

C'est un produit associatif, avec comme neutre l'élément $(1, 0, 0, \ldots)$.

Proposition 1.45. *L'ensemble des suites $\mathcal{A}^{\mathbb{N}}$ à coefficient dans un anneau commutatif $\mathcal{A}$, muni de la somme et le produit défini ci-haut, est un anneau commutatif.*

Preuve. Les vérifications nécessaires sont laissées en exercice au lecteur. ∎

17. Pour avoir la formule $\deg(PQ) = \deg(P) + deg(Q)$ pour tout P et Q.

1.12.2 (∗) L'anneau des séries formelles à coefficient dans $\mathcal{A}$

Pour toute suite $\alpha = (a_n)$ dans $\mathcal{A}^{\mathbb{N}}$, et x un variable abstraite, on considère la **série formelle**[18] associée à α :

$$\alpha(x) = \sum_{n=0}^{\infty} a_n\, x^n.$$

L'ensemble de ces séries formelles est dénoté $\mathcal{A}[[x]]$ (**attention** au double crochet, qui distingue cet ensemble de celui des polynômes $\mathcal{A}[x]$). On fait de $\mathcal{A}[[x]]$ un anneau, en considérant pour $\alpha(x) = \sum_{n=0}^{\infty} a_n\, x^n$ et $\beta(x) = \sum_{n=0}^{\infty} b_n\, x^n$ que :

(i) la somme $\alpha(x) + \beta(x)$ est la série

$$\alpha(x) + \beta(x) := \sum_{n=0}^{\infty} (a_n + b_n)\, x^n.$$

Autrement dit, c'est la série associée à la suite $\alpha + \beta$; et

(ii) la produit $\alpha(x)\beta(x)$ est la série

$$\alpha(x)\beta(x) := \sum_{n=0}^{\infty} \Big(\sum_{k=0}^{n} a_k b_{n-k} \Big)\, x^n.$$

Autrement dit, c'est la série associée à la suite $\alpha * \beta$.

Il est utile de souligner que deux séries formelles sont égales

$$\sum_{n=0}^{\infty} a_n\, x^n = \sum_{n=0}^{\infty} b_n\, x^n \qquad \text{ssi} \qquad \forall (n \in \mathbb{N})\ a_n = b_n. \tag{1.12.1}$$

Proposition 1.46. *L'ensemble des séries $\mathcal{A}[[x]]$ à coefficient dans un anneau commutatif $\mathcal{A}$, muni de la somme et le produit défini ci-haut, est un anneau commutatif.*

Preuve. Les vérifications nécessaires sont laissées en exercice au lecteur. ∎

Proposition 1.47. *L'ensemble des séries formelle de la forme $1 + \sum_{n\geq 1} a_n\, x^n$, avec la multiplication dans $\mathcal{A}[[x]]$, forme un groupe.*

Preuve. Il s'agit principalement de vérifier que toutes ces séries sont inversibles. L'inverse de $\alpha(x) = 1 + \sum_{n\geq 1} a_n\, x^n$ est la série $\beta(x) = 1 + \sum_{n\geq 1} b_n\, x^n$, où les b_n (pour $n \geq 1$)se calculent récursivement au moyen de la formule

$$b_n = -a_1 b_{n-1} - a_2 b_{n-2} - \ldots - a_n,$$

obtenue en comparant les coefficients respectifs de x^n dans l'identité $\alpha(x)\beta(x) = 1 + 0\,x + 0\,x^2 + \ldots$ en vertu de (1.12.1). On trouve ainsi que l'inverse de $\alpha(x)$ est

$$\begin{aligned}\beta(x) = 1 &- a_1 x + (a_1^2 - a_2)\, x^2 + (-a_1^3 + 2\,a_1 a_2 - a_3)\, x^3 \\ &+ (a_1^4 - 3\,a_1^2 a_2 + 2\,a_1 a_3 + a_2^2 - a_4)\, x^4 \\ &+ (-a_1^5 + 4\,a_1^3 a_2 - 3\,a_1^2 a_3 - 3\,a_1 a_2^2 + 2\,a_1 a_4 + 2\,a_2 a_3 - a_5)\, x^5 + \ldots\end{aligned}$$

ce qui achève la démonstration. ∎

18. Il n'y a pas question de convergence ici, ceci est un objet algébrique abstrait.

Les calculs avec les séries formelles, à coefficients dans $\mathbb{Z}$ ou $\mathbb{Q}$, permettent de simplifier plusieurs questions de combinatoire énumérative. La théorie des espèces de structures, développée à l'UQAM, permet de structurer cette approche. Voir

- bergeron.math.uqam.ca/especes-combinatoires, ou
- wikipedia.org/wiki/Combinatorial_species

1.12.3 (*) Semi-anneau tropical

Un **semi-anneau** est comme un anneau, mais sans la condition d'avoir toujours un inverse pour l'addition. Ainsi $\mathbb{N}$, avec la somme et le produit usuel est un semi-anneau. Un exemple qui a de plus en plus été considéré ces dernières années est le suivant. Pour un peu d'histoire, voir wikipedia.org/wiki/Mathématiques_tropicales, où est correctement expliquée l'origine de l'adjectif "tropical".

Définition 21. Sur l'ensemble $\mathbb{R} \cup \{\infty\}$, on considère les opérations[19] de **somme tropicale** et **produit tropical**

- $x \oplus y := \min(x, y)$, et
- $x \odot y := x + y$,

avec ∞ comme neutre tropical additif, et 0 comme neutre tropical multiplicatif. Cela donne une structure de semi-anneau, qu'on appelle le **semi-anneau tropical**. ∎

Observons que dans le semi-anneau tropical, on a

$$x^n := \underbrace{x \odot x \odot \cdots \odot x}_{n\text{–fois}} = n \cdot x,$$

avec ce dernier $n \cdot x$ calculé au sens usuel, c.-à-d. $x + x + \ldots + x$.

Le calcul des puissances des matrices $n \times n$, à coefficients dans l'anneau semi-tropical, donne un algorithme de calcul pour les chemins de coût minimal dans un graphe (qui est une forme de l'algorithme de Dijkstra).

Toute une branche récente de la géométrie algébrique est basée sur le semi-anneau tropical : c'est la géométrie tropicale. On y considère des analogues tropicaux des polynômes. Par exemple, $(a \odot x) \oplus (b \odot y) \oplus c$ est un analogue tropical du polynôme $ax+by+c$, qui correspond à $\min(a+x, b+y, c)$. Voir arxiv.org/pdf/math/0408099.pdf pour une bonne présentation, assez accessible. On y discute entres autres de liens avec la biologie computationnelle.

19. Au début, il faut s'habituer à penser à la somme usuelle comme un produit.

1.13 Exercices du chapitre 1

Exercice 1.12 (**Anneau de Boole**). Soit $\mathcal{A}$ un anneau tel que pour tout $a \in A$ on ait $a^2 = a$. On appelle un tel anneau un anneau de Boole.

1) Montrer que $\forall a \in \mathcal{A}, a = -a$.
2) Montrer que $\mathcal{A}$ est commutatif.
3) Montrer qu'un anneau de Boole est intègre si et seulement s'il contient exactement deux éléments.
4) Est-ce qu'un anneau de Boole peut contenir exactement trois éléments ?
5) Montrer que la relation $\leq$ définie sur $\mathcal{A}$ par : $x \leq y \Leftrightarrow xy = x$ est une relation d'ordre sur $\mathcal{A}$, pour laquelle $\mathcal{A}$ possède un plus petit et un plus grand élément.

Exercice 1.13. On considère $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}, a, b \in \mathbb{Z}\}$

1) Montrer que $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ est un anneau.
2) On note $N(a+b\sqrt{2}) = a^2 - 2b^2$. Montrer que pour tout $x, y \in \mathbb{Z}[\sqrt{2}]$ on a $N(xy) = N(x)N(y)$.
3) En déduire la forme des éléments inversibles.

Exercice 1.14 (**Entiers de Gauss**).
On considère $\mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}\}$

1) Montrer $\mathbb{Z}[i]$ est un anneau commutatif pour l'addition et la multiplication complexe. On appelle cet anneau, anneau des **entiers de Gauss**.
2) Pour $z \in \mathbb{Z}[i]$ on pose $N(z) = |z|^2$. Montrer que pour tout $z, z' \in \mathbb{Z}[i]$ on a $N(zz') = N(z)N(z')$ et $N(z) \in \mathbb{Z}$.
3) Déterminer les éléments inversibles de cet anneau.

Exercice 1.15. Soient $\mathcal{A} = \{n/m \mid n \in \mathbb{Z}, m \in \mathbb{Z}^* \text{ impair}\}$ et $\mathcal{B} = \{n/2^m \mid n \in \mathbb{Z}, m \in \mathbb{N}\}$.

1) Montrer que $\mathcal{A}$ et $\mathcal{B}$ sont des sous anneaux de $(\mathbb{Q}, +, \cdot)$.
2) Montrer que 6 n'est pas inversible dans $\mathcal{B}$, mais qu'il y est irréductible.
3) Calculer les inversibles de $\mathcal{A}$ et de $\mathcal{B}$.

Exercice 1.16. Soit $d \in \mathbb{N}$. On pose $\mathcal{A}_d = \{(x, y) \in \mathbb{Z}^2 \text{ tel que } x - y \in d\mathbb{Z}\}$.

1) Montrer que $\mathcal{A}_d$ est un sous anneaux de $\mathbb{Z}^2$.
2) Soit $\mathcal{A}$ un sous anneau de $\mathbb{Z}^2$. Montrer que $H = \{x \in \mathbb{Z} \mid (x, 0) \in A\}$ est un sous groupe de $\mathbb{Z}$.
3) En déduire qu'il existe $d' \in \mathbb{N}$ tel que $\mathcal{A} = \mathcal{A}_{d'}$.

Exercice 1.17.

1) Déterminer les inversibles, les nilpotents et les diviseurs de zéros des anneaux $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/360\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$.
2) Calculer toutes les puissances des éléments de $\mathbb{Z}/12\mathbb{Z}$.
3) Calculer le groupe des inversibles $(\mathbb{Z}/12\mathbb{Z})^*$ de $\mathbb{Z}/12\mathbb{Z}$.
4) $(U(\mathbb{Z}/12\mathbb{Z}))$ est-il un groupe cyclique ?
5) À quelle condition sur n existe-t-il un élément nilpotent non nul dans $\mathbb{Z}/n\mathbb{Z}$?

Exercice 1.18. Soit $(A, +, \times)$ un anneau. On note 0_A le neutre pour la loi $+$ et 1_A le neutre pour la loi $\times$ (habituellement s'il n'y a pas de confusion on note 0 et 1 ces deux éléments).

1) Soient $x, y \in A$. Montrer que si $x \times y$ est inversible, alors x est inversible à droite et y est inversible à gauche
2) Montrer qu'un élément inversible n'est pas un diviseur de zéro et qu'un diviseur de zéro n'est pas inversible.

Exercice 1.19. Montrer que l'ensemble $Aut(\mathcal{A})$ des automorphismes de $\mathcal{A}$ est un groupe sous la composition. On note $f_a \in Aut(\mathcal{A})$, défini par $f_a(x) = axa^{-1}$, si $a \in U(\mathcal{A})$. Montrer que l'automorphisme réciproque est $f_{a^{-1}}$. Montrer que $f_a \circ f_b = f_{ab}$. En déduire que la fonction $U(\mathcal{A}) \to Aut(\mathcal{A})$, $a \mapsto f_a$ est un homomorphisme de groupes. Quel est son noyau ?

Exercice 1.20. Soit $\mathcal{A}$ l'anneau des matrices carrées d'ordre n. Soit $M \in \mathcal{A}$, non nulle. Montrer que M est un diviseur de 0 si et seulement si M n'est pas inversible.

Exercices à propos des idéaux et des corps

Exercice 1.21 (**Produits de corps**).
On suppose que $\mathbb{K}$ et $\mathbb{L}$ sont des corps.

2) Trouver tous les éléments nilpotents et tous les éléments idempotents de l'anneau produit $\mathbb{K} \times \mathbb{L}$. Trouver de plus tous les diviseurs de zéro $\mathbb{K} \times \mathbb{L}$.

3) Quels sont les idéaux maximaux de $\mathbb{K} \times \mathbb{L}$?

4) Soient $\mathbb{K}$, $\mathbb{L}$, $\mathbb{A}$, $\mathbb{B}$ quatre corps tels que $\mathbb{K} \times \mathbb{L}$ est isomorphe à $\mathbb{A} \times \mathbb{B}$. Montrer alors que $\mathbb{K}$ est isomorphe à $\mathbb{A}$ ou à $\mathbb{B}$. Indication : il y a un homomorphisme surjectif de $\mathbb{A} \times \mathbb{B}$ vers $\mathbb{K}$; utiliser 3.

Exercice 1.22 (**Idéaux engendrés**).
Soit $\mathcal{A}$ un anneau commutatif.

1) Pour $a \in A$, rappelons que $\langle a \rangle = \{ab \mid b \in A\} = aA$. Montrer que $\langle a \rangle$ est un idéal de $\mathcal{A}$.

2) Plus généralement, pour $a_1, ..., a_n \in A$, on pose $\langle a_1, ..., a_n \rangle = a_1A + ... + a_nA$. Montrer que $\langle a_1, ..., a_n \rangle$ est un idéal de $\mathcal{A}$.

Exercice 1.23 (**Opérations sur les idéaux**).
Soit $(A, +, .)$ un anneau commutatif. Pour I et J deux idéaux de $\mathcal{A}$,

$$I + J = \Big\{ a + b \mid a \in I, b \in J \Big\} \qquad \text{et} \qquad I \cdot J = \Big\{ \sum_{\text{fini}} ab \mid a \in I, b \in J \Big\}$$

1) Montrer que $I + J$ et $I \cdot J$ sont des idéaux de $\mathcal{A}$.

2) Montrer que $I + J$ est le plus petit idéal de $\mathcal{A}$ contenant I et J.

3) Montrer que $I \cdot J \subset I \cap J$.

4) Montrer que $(I + J) \cdot (I \cap J) \subset I \cdot J$.

5) Soit $I_1 \subset I_2 \subset ... \subset I_k \subset ...$ une suite croissante infinie d'idéaux de $\mathcal{A}$. Montrer que $J = \sum_{i=1}^{\infty} I_i$ est un idéal de $\mathcal{A}$. Si tous les I_i sont des idéaux propres montrer que J est aussi un idéal propre.

6) On dit que I et J sont premiers entre eux si $I + J = A$. Montrer que I et J sont premiers entre eux si et seulement s'il existe $a \in I$ et $b \in J$ tels que $a + b = 1$.

7) Montrer que si I et J sont premiers entre eux alors pour tout $k, n \in \mathbb{N}^*$, les idéaux I^k et J^n sont aussi premiers entre eux.

8) Montrer que si I et J sont premiers entre eux alors $I \cdot J = I \cap J$.

9) Soient K un troisième idéal de $\mathcal{A}$, tel que I et J soient premiers entre eux ainsi que I et K. Montrer alors que I et $J \cdot K$ sont premiers entre ainsi que I et $J \cap K$.

10) On pose $A = \mathbb{Z}$, $I = \langle n \rangle$, $J = \langle m \rangle$. Calculer $I \cap J$ et $I + J$.

11) On pose $I = \langle x_1, ..., x_p \rangle$ et $J = \langle y_1, ..., y_q \rangle$ deux idéaux de $\mathcal{A}$. Décrire en fonction des x_i et y_j les idéaux $I + J$, $I \cdot J$ et I^2.

Exercice 1.24. Soient $\mathcal{A}$ un anneau commutatif, I un idéal de $\mathcal{A}$ et $a \in \mathcal{A}$. Montrer que :

1) $I = \mathcal{A}$ si et seulement si I contient un inversible.

2) $\langle a \rangle = \mathcal{A}$ si et seulement si a est inversible.

3) $\mathcal{A}$ est intègre si et seulement si $\langle 0 \rangle$ est un idéal premier de $\mathcal{A}$.

4) $\mathcal{A}$ est un corps si et seulement si $\langle 0 \rangle$ est le seul idéal propre de $\mathcal{A}$.

Exercice 1.25.

1) Un idéal n'est pas un sous anneau en général. Donner un contre exemple dans $\mathbb{Z}$.

2) Un sous anneau n'est pas un idéal en général. Montrer que $\mathbb{Z}$ est un sous anneau de $\mathbb{Q}$ mais pas un idéal de $\mathbb{Q}$.

3) En général l'union d'idéaux n'est pas un idéal. Donner un exemple dans $\mathbb{Z}$ de l'union de deux idéaux dont l'union n'est pas un idéal.

Exercice 1.26. Soit I un idéal de $\mathbb{Z}^2$.

1) On pose $I_1 = \{a \in \mathbb{Z} \mid (a,0) \in I\}$ et $I_2 = \{b \in \mathbb{Z} \mid (0,b) \in I\}$. Montrer que I_1 et I_2 sont des idéaux de $\mathbb{Z}^2$.

2) Montrer que $I = I_1 \times I_2$.

3) Quelle est la forme des idéaux de $\mathbb{Z}^2$.

Exercice 1.27. Soit $\mathcal{A}$ un anneau commutatif. Soit B un sous ensemble de $\mathcal{A}$. On appelle **annulateur** de B l'ensemble :

$$\mathrm{Ann}(B) = \{a \in \mathcal{A} \mid ab = 0 \quad \forall b \in B\}$$

1) Montrer que $\mathrm{Ann}(B)$ est un idéal de $\mathcal{A}$.

2) On suppose que $\mathcal{A}$ est intègre et que toute suite décroissante d'idéaux est *stationnaire* (de manière équivalente : toute suite strictement décroissante d'idéaux est finie). Montrer que $\mathcal{A}$ est un corps. Indication : soit $a \in A^*$; considérer la suite décroissante d'idéaux $(a) \supset (a^2) \supset (a^3) \ldots$.

3) On suppose que $\mathcal{A}$ est intègre et qu'il admet un nombre fini d'idéaux. Montrer que $\mathcal{A}$ est un corps.

4) Monter que si $\mathcal{A}$ est fini, tout idéal premier est maximal. Indication : utiliser les propositions 1.24,1.35 et 1.38.

5) On suppose que tout idéal de $\mathcal{A}$ est premier. Montrer que $\mathcal{A}$ est un corps. Indication : montrer que A est intègre ; montrer que si $a \in A^*$, alors $a \in (a^2)$.

Exercice 1.28. Soit $\mathcal{A}$ un anneau commutatif.

1) Soit I un idéal propre de $\mathcal{A}$. Montrer que I est premier si et seulement si, lorsque le produit de deux idéaux est contenu dans I alors l'un des deux est contenu dans I. Indication : montrer que si $I_1 I_2 \subset I$, et si I_1 n'est pas contenu dans I_2, alors $I_2 \subset I$.

2) Déduire que si $\mathcal{M}$ est un idéal maximal de $\mathcal{A}$, alors le seul idéal premier de $\mathcal{A}$ qui contient $\mathcal{M}^n$ est $\mathcal{M}$ pour tout $n \in \mathbb{N}$.

Exercices à propos des anneaux quotients

Exercice 1.29 (Anneaux quotients).
Soient $\mathcal{A}$ un anneau commutatif et I un idéal de $\mathcal{A}$. Rappelons que les éléments de l'ensemble quotient $\mathcal{A}/I$ sont les classes d'équivalence $[a] = [a]_I$ pour la relation d'équivalence $a \simeq b$ si et seulement si $a - b \in I$. De plus, la structure d'anneau quotient $\mathcal{A}/I$ est définie par :

$$[a] + [b] := [x + y] \quad \text{et} \quad [a].[b] := [xy],$$

avec

$$0_{\mathcal{A}/I} := [0_{\mathcal{A}}] \quad \text{et} \quad 1_{\mathcal{A}/I} := [1_{\mathcal{A}}].$$

1) Montrer que la façon de définir ces opérations ne dépend pas des représentants.
2) Que représente l'ensemble $0_{\mathcal{A}/I}$?
3) Montrer que $\mathcal{A}/I$ est intègre si et seulement si I est premier.
4) Montrer que $\mathcal{A}/I$ est un corps si et seulement si I est maximal.

Exercice 1.30 (**Caractérisation des anneaux quotients**).
Soit $\mathcal{A}$ un anneau commutatif et I un sous groupe additif propre de $\mathcal{A}$. Montrer l'équivalence entre les deux assertions suivantes :
i) $\mathcal{A}/I$ est un anneau (pour la structure vue dans l'exercice précédent).
ii) I est un idéal.

Exercice 1.31 ((∗) **Correspondance des idéaux d'un anneau et de ceux de son quotient**).
Soient $\mathcal{A}$ un anneau commutatif et I et J deux idéaux de $\mathcal{A}$. Soit $\pi : \mathcal{A} \to \mathcal{A}/I$ la projection canonique et $\pi(J)$ l'image de l'idéal J selon cette projection.
1) Montrer que $\pi(J)$ est un idéal de $\mathcal{A}/I$.
2) Montrer que l'on a un isomorphisme $(\mathcal{A}/I)/\pi(J) \simeq \mathcal{A}/(I+J)$.
3) Que se passe-t-il si I et J sont premiers entre eux ?
4) On note $\mathcal{I}(\mathcal{A}, I)$ l'ensemble des idéaux de $\mathcal{A}$ contenant I et $\mathcal{I}(\mathcal{A}/I)$ l'ensemble des idéaux de $\mathcal{A}/I$. Montrer que la fonction $\mathcal{I}(A, I) \longrightarrow \mathcal{I}(A/I)$ telle que $K \mapsto \pi(K)$ est une bijection.

Exercices à propos des homomorphismes d'anneaux

Exercice 1.32.
1) Calculer le nombre d'éléments de $\mathbb{Z}[\sqrt{d}]/\langle m\rangle$ où $m \in \mathbb{Z}$ et $m \neq 0$.
2) L'idéal $\langle 2\rangle$ est-il premier dans $\mathbb{Z}[\sqrt{d}]$?

Exercice 1.33. Soit G un groupe abélien. On note $\mathcal{F}(G)$ l'ensemble des fonctions de G dans G. Cet ensemble est naturellement muni d'une addition définie par : $(f+g)(x) := f(x) + g(x)$,où le second "+" est la loi du groupe.
1) En notant $\circ$ la composition naturelle, montrer que $\circ$ est distributive à droite par rapport à +.
2) Montrer qu'en général $\circ$ n'est pas distributive à gauche par rapport à + (Prendre $G = \mathbb{Z}$, $f(x) = x^2$, $g(x) = h(x) = x$ et considérer $f \circ (g+h)$ et $f \circ g + f \circ h$).
3) Montrer que si l'on se restreint au sous ensemble $\mathrm{End}(G)$ des endomorphismes de G, alors $\circ$ est distributive à gauche par rapport à +. Montrer ensuite $\mathrm{End}(G)$ est un anneau.

Exercice 1.34. Soit $f : \mathbb{C} \longrightarrow \mathbb{C}$ un homomorphisme d'anneaux tel que pour tout $x \in \mathbb{R}$ on ait $f(x) = x$. Montrer que f est soit l'identité, soit la conjugaison complexe. Indication : montrer que $f(i) = i$ ou $-i$.

Exercice 1.35. Soit X un ensemble et $x \in X$. Montrer que la fonction $e_x : \mathcal{F}(X, \mathbb{R}) \to \mathbb{R}$ définie par $e_x(f) = f(x)$ est un homomorphisme d'anneaux.

Exercice 1.36. Soient $\mathcal{A}$ et $\mathcal{B}$ deux anneaux commutatifs et $f : \mathcal{A} \to \mathcal{B}$ un homomorphisme d'anneaux. Montrer que :
1) L'image réciproque par f d'un idéal premier de $\mathcal{B}$ et un idéal premier de $\mathcal{A}$.
2) L'image réciproque par f d'un idéal maximal de $\mathcal{B}$ n'est pas forcément un idéal maximal de $\mathcal{A}$. Montrer par contre que si f est un épimorphisme, alors ceci est vrai.

Exercice 1.37. Soient $\mathcal{A}$ et $\mathcal{B}$ deux anneaux et $f : \mathcal{A} \to \mathcal{B}$ un homomorphisme d'anneaux. Soit $x \in A$ un inversible. Montrer que $f(x)$ est inversible dans B.

Exercice 1.38 (**Caractérisation des monomorphismes**)**.**

1) Soit $\mathcal{A}$ un anneau commutatif. Déterminer tous les homomorphismes d'anneaux de $\mathbb{Z}[X]$ dans $\mathcal{A}$.

2) Pour ce qui suit les anneaux sont commutatifs. Soit $f : \mathcal{A} \longrightarrow \mathcal{B}$ un homomorphisme d'anneaux tels que la propriété suivante soit satisfaite :

$$\forall g, h : \mathcal{B} \to \mathcal{C} \text{ homorphismes}, \qquad (f \circ g = f \circ h) \implies (g = h) \qquad (*).$$

Montrer qu'alors f est un monomorphisme.

3) Montrer qu'un monomorphisme entre anneaux commutatifs vérifie la propriété $(*)$.

4) Déterminer les automorphismes de $\mathbb{Z}[X]$.

Chapitre 2

Anneaux euclidiens, principaux, et factoriels

Nous allons maintenant étendre certaines des propriétés habituelles de l'anneau des entiers $\mathbb{Z}$, à d'autres anneaux importants (souvent commutatifs).

2.1 Définitions de base

Définition 22. Dans un anneau commutatif $\mathcal{A}$, pour $a, b \in \mathcal{A}$ on dit que a **divise** b, et on écrit $a \mid b$, s'il existe $c \in \mathcal{A}$ tel que $ac = b$. Alors b est dit **multiple** de a, et a est un **diviseur** [1] de b. ▪

Par exemple, on a

- 2 divise 12 dans $\mathbb{Z}$;
- $x+1$ divise x^2+3x+2 dans $\mathbb{Q}[x]$, car $x^2+3x+2 = (x+1)(x+2)$;
- $1+\sqrt{7}$ divise 6 dans le sous-anneau $\{a+b\sqrt{7} |\ a, b \in \mathbb{Z}\}$ de $\mathbb{R}$, car $6 = (1+\sqrt{7})(-1+\sqrt{7})$.
- si a est inversible dans $\mathcal{A}$, alors a divise tout $b \in \mathcal{A}$, car $b = a\,(a^{-1}b)$.
- si a divise b et u est inversible, alors au divise aussi b, car on a $b = ac$ et donc $b = (au)(u^{-1}c)$.

Définition 23. Deux éléments a, b d'un anneau commutatif $\mathcal{A}$ sont dits **associés**, s'il existe un élément inversible u de $\mathcal{A}$, tel que $b = au$. ▪

- n et $-n$ sont associés dans $\mathbb{Z}$;
- $a+b\,i$ et $-b+a\,i$ sont associés dans le sous-anneau $\{a+b\,i \mid a, b \in \mathbb{Z}\}$ de $\mathbb{C}$;
- si a et b sont deux éléments non nuls d'un corps, alors a et b sont associés.

Proposition 2.1. *Soit $\mathcal{A}$ un anneau intègre, alors la relation "a et b sont associés" est une relation d'équivalence. De plus* [2]*, $\langle a \rangle = \langle b \rangle$ si et seulement a et b sont associés.*

1. **Attention**, notre notion préalable de diviseur de 0 est un peu en conflit avec celle-ci. À proprement parler, on aurait peut-être dû dire diviseur non trivial de 0, mais la terminologie standard est celle que nous avons donnée.
2. Rappelons que $\langle a \rangle := \{x\,a \mid x \in \mathcal{A}\}$.

Preuve. Si $b = au$, alors $\langle b\rangle = \langle u\,a\rangle = \langle a\rangle$, puisque $\langle u\rangle = \mathcal{A}$. En effet, pour tout $x \in \mathcal{A}$, on a $x = (xu^{-1})u \in \mathcal{A}\,u$. Inversement, supposons que $\langle a\rangle = \langle b\rangle$. Alors, il existe c tel que $b = ac$, et d tel $a = bd$. On trouve donc que $a = bd = acd$. Si $a \neq 0$, comme l'anneau est intègre, on trouve $1 = cd$. Les éléments c et d sont donc inversibles, ce qui montre que a et b sont associés. ■

Définition 24. Un élément a non nul et non inversible, d'un anneau commutatif $\mathcal{A}$, est dit **irréductible**, si pour tout b et c tels que $a = bc$, on a forcément b ou c inversible. Un élément qui n'est pas irréductible est dit **réductible**. ■

Par exemple, on a

- si p est un nombre premier, alors p et $-p$ sont irréductibles dans $\mathbb{Z}$;
- $x^2 - 7$ est irréductible [3] dans $\mathbb{Q}[x]$;
- $x^2 - 7$ est réductible dans $\mathbb{R}[x]$, car $x^2 - 7 = (x + \sqrt{7})(x - \sqrt{7})$;
- $x^2 + 1$ est irréductible dans $\mathbb{R}[x]$;
- $x^2 + 1$ est irréductible dans $\mathbb{C}[x]$, car $x^2 + 1 = (x + i)(x - i)$.

On peut montrer facilement que si deux éléments sont associés, alors ils sont simultanément irréductibles ou non (resp. inversibles).

Définition 25. Pour deux éléments a et b d'un anneau commutatif, un **diviseur commun** de a et de b, est un élément d qui divise à la fois a et b.

Si un diviseur commun $d \in \mathcal{A}$ de a et b est multiple de tout diviseur commun de a et de b, on dit que d est un **plus grand diviseur commun** de a et de b. ■

Attention, il peut y avoir plusieurs plus grands diviseurs communs de a et de b. On écrit souvent "pgdc" pour "plus grand diviseur commun".

Lemme 2.2. *Si $\mathcal{A}$ est intègre, alors deux pgdc de a et de b sont nécessairement associés.*

Preuve. Soient e et d deux pgdc de a et b. Alors d est un diviseur commun de a et b, et comme e est un pgdc, e est un multiple de d. Symétriquement, d est un multiple de e. Donc $eA = dA$ et par la Proposition 2.1, e et d sont associés. ■

Définition 26. Un idéal d'un anneau commutatif $\mathcal{A}$ est dit **principal**, s'il est de la forme

$$\langle a\rangle = \{x\,a \mid x \in \mathcal{A}\},$$

pour un certain a dans $\mathcal{A}$. L'anneau $\mathcal{A}$ est lui-même dit **principal**, si tout ses idéaux sont principaux. ■

Définition 27. Deux éléments a, b d'un anneau commutatif intègre $\mathcal{A}$ sont dits **premiers entre eux**, si pour tout x dans $\mathcal{A}$,

$$(x \,|\, a \quad \text{et} \quad x \,|\, b) \qquad \Longrightarrow \qquad x \text{ inversible.}$$

On écrit alors $a \perp b$. ■

3. Notons que, pour $\mathbb{K}$ un corps, les éléments inversibles de $\mathbb{K}[x]$ sont les polynômes constants non nuls,c.-à-d. éléments de $\mathbb{K} \setminus \{0\}$.

Lemme 2.3. *Soit $\mathcal{A}$ un anneau principal intègre, et a, b dans $\mathcal{A}$. Alors*

$$(a \perp b) \qquad \text{ssi} \qquad \exists (x, y \in \mathcal{A})\ a\,x + b\,y = 1.$$

Autrement dit, $\mathcal{A} = \{a\,x + b\,y \mid x, y \in \mathcal{A}\}$.

Preuve. Supposons que a et b sont premiers entre eux, et soit

$$I := \langle a \rangle + \langle b \rangle = \{ax + by \mid x, y \in \mathcal{A}\}.$$

On vérifie (en exercice) que I est un idéal qui contient a et b. Comme $\mathcal{A}$ est principal, il existe $c \in \mathcal{A}$, tel que $I = \langle c \rangle$. On a donc que c divise a et c divise b, car a et b sont dans $I = \langle c \rangle$. Comme $a \perp b$, cela force c à être inversible. D'où $\mathcal{A} = \langle c \rangle = I$, et donc il existe x, y dans $\mathcal{A}$ tels que $1 = ax + by$.

Inversement, supposons que $1 = ax + by$. Soit c qui divise a et b. On a donc $a = c\,a'$ et $b = c\,b'$, pour certains a', b' dans $\mathcal{A}$. Donc $1 = ax + by = ca'x + cb'y = c(a'x + b'y)$, ce qui montre que c est inversible. On conclut que a et b sont premiers entre eux. ■

Lemme 2.4. *Soit $\mathcal{A}$ un anneau principal, et a, b dans $\mathcal{A}$. Si $a \perp b$ et si a divise $b\,c$, alors a divise c. De plus, si p est irréductible, et p divise $a_1 a_2 \dots a_n$, alors p divise l'un des a_i.*

Preuve. Pour le premier énoncé, par hypothèse il existe x et y tels que $ax + by = 1$ (grâce au lemme 2.3), et il existe d tel que $ad = bc$. On calcule donc que

$$\begin{aligned} c &= c\,(ax + by) \\ &= acx + (bc)y \\ &= acx + (ad)y \\ &= a\,(cx + dy) \end{aligned}$$

d'où a divise c.

Pour le second, on procède par récurrence sur n. On considère la situation où p irréductible divise ba_n, avec $b = a_1 \cdots a_{n-1}$. Si p est premier avec a_n, alors on a le résultat par récurrence, puisque la première partie assure que p divise b. Sinon, si p et a_n ne sont pas premiers entre eux, alors il existe c qui n'est pas inversible et qui divise p et a_n. On a donc $p = cx$, mais p étant irréductible on a que x est forcément inversible, puisque c ne l'est pas. Il s'ensuit que $c = px^{-1}$, d'où p divise c, qui lui divise a_n, d'où l'énoncé. ■

Définition 28. Une **valuation** sur un anneau commutatif intègre $\mathcal{A}$, est une fonction $v : \mathcal{A} \setminus \{0\} \longrightarrow \mathbb{N}$. L'anneau $\mathcal{A}$ est dit **euclidien** s'il existe une valuation v sur $\mathcal{A}$, telle que : pour tout $a, b \in \mathcal{A}$, avec $b \neq 0$, il existe q et r dans $\mathcal{A}$ pour lesquels

$$a = b\,q + r, \qquad \text{et} \qquad r = 0 \quad \text{ou} \quad v(r) < v(b). \tag{2.1.1}$$

On dit que q est le **quotient** et r le **reste** de la division de a par b. ■

Par exemple, on a

- $\mathbb{Z}$ est euclidien, avec $v(a) = |a|$;
- $\mathbb{K}[x]$ est euclidien avec $v(p) = \deg(p)$ (voir la section 2.4).

Proposition 2.5. *Si $\mathcal{A}$ est principal et intègre, alors deux éléments a et de b non nuls de $\mathcal{A}$ ont nécessairement un pgdc d. Il est unique à un facteur inversible près, et $\langle d\rangle = \{a\,x + b\,y \mid x, y \in \mathcal{A}\}$.*

Preuve. On considère l'idéal $I = \{a\,x + b\,y \mid x, y \in \mathcal{A}\}$. Comme $\mathcal{A}$ est principal, on a $I = \langle d\rangle$ pour un certain d. Comme a et b sont dans I, d est un diviseur commun de a et de b. D'autre part, si c divise a et b, alors c divise tout élément de la forme $a\,x + b\,y$. On a donc que c divise d, ce qui montre l'assertion. L'unicité à un facteur inversible près est assurée par le lemme 2.2. ∎

Définition 29. Un anneau commutatif intègre $\mathcal{A}$ est dit **factoriel** si

(i) tout élément de $\mathcal{A}$, qui n'est ni nul ni inversible, est un produit (fini) d'éléments irréductibles ;

(ii) si $p_1p_2\cdots p_r = q_1q_2\cdots q_s$, avec les p_i et q_i irréductibles ; alors $r = s$ et il existe une permutation σ de l'ensemble $\{1, 2, \ldots, r\}$, telle que p_i et $q_{\sigma(i)}$ soient associés, pour $1 \le i \le r$. ∎

Définition 30. Un anneau commutatif $\mathcal{A}$ est dit **noethérien**[4] s'il satisfait la condition de chaîne ascendante pour les idéaux, c.-à-d. que pour toute suite croissante d'idéaux $\{I_n\}_{n\in\mathbb{N}}$:

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots \tag{2.1.2}$$

il existe un r tel que $I_s = I_r$ pour tout $s \ge r$. ∎

2.1.1 Exercices

Exercice 2.1 (**Exemples d'idéaux non principaux**).
Soit $\mathcal{A}$ un anneau commutatif.

1) Montrer que 2 et x sont premiers entre eux dans $\mathbb{Z}[x]$ mais que 1 n'est pas dans l'idéal $\langle 2, x\rangle$.
2) Montrer que $\langle 2, x\rangle$ n'est pas un idéal principal de $\mathbb{Z}[x]$.
3) Montrer $\langle x, y\rangle$ n'est pas un idéal principal de $\mathcal{A}[x, y]$.
4) Soit $\mathbb{K}$ un corps. Montrer que $\langle x\rangle$ est un idéal premier de $\mathbb{K}[x, y]$. Quel est le quotient ?
5) Parmi les idéaux $\langle 2, x\rangle$, $\langle x, y\rangle$, et $\langle 2, x, y\rangle$ de $\mathbb{Z}[x, y]$ lesquels sont premiers ? maximaux ?
6) Soit $a \in \mathcal{A}$. Montrer que $\mathcal{A}[x]/\langle x - a\rangle \simeq \mathcal{A}$.

2.2 Théorèmes principaux

Les théorèmes suivants sont fondamentaux.

Théorème 2.6. *Tout anneau euclidien est principal.*

Preuve. Soit $\mathcal{A}$ euclidien et I un idéal dans $\mathcal{A}$, qu'on peut supposer non nul (le cas nul correspondant à $\langle a\rangle$ avec $a = 0$). L'ensemble $\{v(a) \mid a \in I, et\, a \neq 0\}$ est un sous-ensemble de $\mathbb{N}$. Soit m son élément minimal[5]. Il existe $b \in I$ tel que $v(b) = m$, et $b \neq 0$. On vérifie comme suit que $I = \langle b\rangle$. Comme on sait déjà que $\langle b\rangle \subseteq I$, il suffit de voir que $I \subseteq \langle b\rangle$. Autrement dit, on veut vérifier que chaque a dans I est un multiple de b. Mais, $a = b\,q + r$ pour certains q et r, avec $r = 0$ ou $v(r) < v(b)$. Comme $r = a - bq$ est dans I, car a et b le sont, on doit avoir $r = 0$. Sinon, on a $r \in I$ avec $v(r) < v(b)$, ce qui contredit le fait que $v(b)$ est minimal. D'où $r = 0$ et $a \in \langle b\rangle$, ce qui montre que $I \subseteq \langle b\rangle$. ∎

4. En l'honneur de la mathématicienne Emmy Noether, 1882-1935.
5. Une des propriétés fondamentales de $\mathbb{N}$ est que chacun de ses sous-ensembles admet un élément minimal.

Théorème 2.7. *Tout anneau principal est noethérien.*

Preuve. Soit une famille $\{I_n\}_{n\in\mathbb{N}}$ une chaîne ascendante comme en (2.1.2). On considère $I = \bigcup_{n\in\mathbb{N}} I_n$. C'est un idéal (voir en exercice), et il est donc principal, car $\mathcal{A}$ l'est. Soit donc $a \in \mathcal{A}$ tel que $I = \langle a\rangle$. Comme $a \in I = \bigcup_{n\in\mathbb{N}} I_n$, il existe r tel que $a \in I_n$. Mais alors, les inclusions (2.1.2) font que $a \in I_s$ pour tout $s \geq r$. Il s'ensuit que $I = \langle a\rangle \subseteq I_s \subseteq I$, et donc $I_s = I$ pour tout $s \geq r$. ∎

Théorème 2.8. *Tout anneau commutatif intègre principal est factoriel.*

Comme $\mathbb{Z}$ est un anneau eulidien, on obtient le

Corollaire 2.9. *$\mathbb{Z}$ est principal, factoriel et noetherien.*

Preuve. [du théorème 2.8]

1) On montre d'abord que tout élément $a \in \mathcal{A}$, non nul et non inversible de l'anneau, a un diviseur irréductible. Si a lui-même est irréductible, il n'y a rien à montrer. Sinon, soit $a = a_1b_1$, avec a_1 et b_1 non inversibles. On observe que $\langle a\rangle$ est un sous-ensemble strict de $\langle a_1\rangle$. En effet, si $\langle a\rangle = \langle a_1\rangle$ on aurait $a_1 = ac$, et alors $a = a_1b_1 = acb_1$. Comme $\mathcal{A}$ est intègre, on trouve $1 = cb_1$, d'où b_1 est inversible, ce qui contredit l'hypothèse sur b_1. Si a_1 est irréductible, on a terminé. Sinon, il existe a_2 et b_2 tels que $a_1 = a_2b_2$, avec a_2 et b_2 non inversibles. On continue ainsi à construire des a_i et b_i non inversibles, tels que $a_{i-1} = a_ib_i$ tant que a_i est non irréductible, jusqu'à ce qu'on trouve un a_i irréductible, qui divise alors clairement a. Comme on a une suite ascendante d'idéaux $\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \langle a_3\rangle\cdots$, ce processus ne peut continuer sans que cela contredise le théorème 2.7.

2) Si a n'est pas irréductible, on peut supposer que $a = p_1c_1$ avec p_1 irréductible et c_1 non-inversible (sinon a est irréductible et nous avons la factorisation cherchée). Si c_1 n'est pas irréductible, on a $c_1 = p_2c_2$ avec p_2 irréductible et c_2 non inversible, et $a = p_1p_2c_2$. On continue ainsi, pour obtenir $a = p_1p_2\cdots p_kc_k$, avec les p_i irréductibles. Comme l'inclusion des idéaux $\langle c_i\rangle \subseteq \langle c_{i+1}\rangle$ est stricte, le processus ne peut continuer indéfiniment sans contredire le fait que $\mathcal{A}$ est noethérien. On trouve donc un factorisation de $\mathcal{A}$ en éléments irréductibles.

3) Pour montrer l'unicité, on procède comme suit. Soit $p_1p_2\cdots p_r = q_1q_2\cdots q_s$, avec $s \geq r$ (sinon on échange les termes de l'égalité). Par le lemme 2.4, p_1 divise l'un des q_i. Quitte à permuter les q_i, on peut supposer que $i = 1$. Donc, $q_1 = p_1\varepsilon_1$, avec p_1 et q_1 irréductibles. Cela force ε_1 à être inversible, et donc p_1 et q_1 sont donc associés. On a donc $p_1p_2\cdots p_r = p_1\varepsilon_1q_2\cdots q_s$ qui implique $p_2\cdots p_r = \varepsilon_1q_2\cdots q_s$. En répétant le processus, on trouve $1 = \varepsilon_1\varepsilon_2\cdots\varepsilon_rq_{r+1}\cdots q_s$. Mais alors, $q_{r+1}\cdots q_s$ doit être le produit vide, ce qui montre que $r = s$, ce qui achève la démonstration. ∎

2.2.1 Formulation de propriétés en termes d'idéaux

Dans un anneau principal (en particulier commutatif) intègre $\mathcal{A}$, plusieurs des notions définies plus haut pour des éléments de $\mathcal{A}$ se reformule naturellement en termes d'idéal. Certains de ces énoncés ont déjà été vus. Ainsi, on a

- $\langle a\rangle = \langle b\rangle$ si et seulement si a et b sont associés ;
- $\langle a\cdot b\rangle = \langle a\rangle\langle b\rangle$;
- $\langle a\rangle \subseteq \langle b\rangle$ si et seulement si b divise a ;

- si $\langle b\,c\rangle \subseteq \langle a\rangle$ et $\langle a, b\rangle = \mathcal{A}$, alors $\langle c\rangle \subseteq \langle a\rangle$ (lemme de Gauss) ;
- $\langle a, b\rangle = \langle 1\rangle$ si et seulement si a et b sont premiers entre eux, $a \perp b$;
- $\langle d\rangle = \langle a_1\rangle + \ldots + \langle a_k\rangle$ si et seulement si d est un plus grand commun diviseur des a_i ;
- $\langle m\rangle = \langle a_1\rangle \cap \cdots \cap \langle a_k\rangle$ si et seulement si m est un plus petit commun multiple des a_i ;
- $\langle a\rangle$ irréductible propre si et seulement a est irréductible ;
- Si $\langle a\rangle$ est propre, alors

$$\langle a\rangle \text{ est premier} \Leftrightarrow \langle a\rangle \text{ est maximal} \Leftrightarrow \langle a\rangle \text{ est irréductible.}$$

2.3 Algorithme d'Euclide

Pour un anneau euclidien $\mathcal{A}$, la division euclidienne est dite **effective** si, pour tout a et b dans $\mathcal{A}$, il existe un algorithme pour calculer le quotient q et le reste r, tel que $a = b\,q + r$ satisfaisant la propriété (2.1.1). On peut alors "calculer" le plus grand commun diviseur $d = \text{pgdc}(a, b)$ de deux éléments a et b, avec l'**algorithme d'Euclide** et donner une expression explicite de la forme $a\,x + b\,y$ pour d. On dit parfois que c'est l'algorithme d'Euclide étendu.

Algorithme d'Euclide étendu. Pour le calcul de $d = \text{pgdc}(a, b)$, posons $a_0 = a$ et $a_1 = b$. On utilise alors récursivement la relation :

$$\text{pgdc}(a_i, a_{i+1}) = \text{pgdc}(a_{i+1}, a_{i+2}), \qquad \text{avec} \qquad a_i = a_{i+1}\,q_i + a_{i+2}$$

où, soit $a_{i+2} = 0$ soit $v(a_{i+2}) < v(a_{i+1})$. On observe que, si on a déjà une expression pour d de la forme $d = a_{i+1}\,x_{i+1} + a_{i+2}\,y_{i+1}$ (pour certains x_{i+1} et y_{i+1}), alors on en déduit

$$\begin{aligned} d &= a_{i+1}\,x_{i+1} + (a_i - b\,q)\,y_{i+1} \\ &= a_i\,y_{i+1} + a_{i+1}\,(x_{i+1} - q_i\,y_{i+1}), \end{aligned}$$

car $a_{i+2} = a_i - a_{i+1}\,q_i$. On posera donc

$$x_i = y_{i+1} \qquad y_i = x_{i+1} - q_i\,y_{i+1},$$

ce qui permet de remonter jusqu'à $d = a_0\,x_0 + a_1\,y_0 = a\,x_0 + b\,y_0$. Observons que, si $a_{i+2} = 0$, avec $a_{i+1} \neq 0$, alors on a trouvé $d = a_{i+1}$, le pgdc cherché. Ce cas se produit forcément pour un certain i, car la division euclidienne assure que $v(a_1) > v(a_2) > \ldots > v(a_i)$, et il est impossible d'avoir une suite infinie (strictement) décroissante d'entiers positifs. ∎

Il est clair qu'on peut calculer le pgdc de plusieurs éléments $a_1, a_2, \ldots, a_k$, utilisant le fait que

$$\text{pgdc}(a_1, a_2, \ldots, a_k) = \text{pgdc}(a_1, \text{pgdc}(a_2, \ldots, a_k)).$$

2.4 Le cas des polynômes

Théorème 2.10. *Pour tout corps commutatif $\mathbb{K}$, l'anneau des polynômes $\mathbb{K}[x]$ est euclidien.*

Preuve. Pour f et g dans $\mathbb{K}[x]$, on cherche donc à construire des polynômes q et r, tels que

$$f = g\,q + r,$$

avec soit $r = 0$, soit $\deg(r) < \deg(g)$. Cette construction est récursive (et explicite, en autant que les calculs dans $\mathbb{K}$ le soient), en termes de $n = \deg(f)$, le degré de f. Soit

$$f = a_0 + a_1 x + \ldots + a_n x^n, \qquad \text{et} \qquad g = b_0 + b_1 x + \ldots + b_k x^k,$$

avec $a_n \neq 0$ et $b_k \neq 0$. Si $k > n$, alors on a déjà terminé le calcul, avec $q = 0$ et $r = f$.

Sinon, on calcule que

$$\begin{aligned} f' = f - \frac{a_n}{b_k} x^{n-k} g &= (a_0 + a_1 x + \ldots + a_n x^n) - \frac{a_n}{b_k} x^{n-k}(b_0 + b_1 x + \ldots + b_k x^k) \\ &= a_0 + a_1 x + \ldots + a_{n-k-1} x^{n-k-1} + \sum_{j=n-k}^{n-1} (a_j - \frac{a_n}{b_k} b_j)\, x^j \end{aligned}$$

est un polynôme de degré au plus $n-1$. Récursivement on sait calculer q' et r' avec soit $r' = 0$ soit $\deg(r') < \deg g$, tels que $f' = g\,q' + r'$. Il suffit donc de poser $q := \frac{a_n}{b_k} x^{n-k} + q'$, pour avoir

$$\begin{aligned} f - g\,q &= f - g\left(\frac{a_n}{b_k} x^{n-k} + q'\right) \\ &= f' - g\,q' \\ &= r' \end{aligned}$$

on trouve donc aussi le polynôme $r = r'$ désiré. ∎

Corollaire 2.11. *Pour tout corps commutatif $\mathbb{K}$, l'anneau des polynômes $\mathbb{K}[x]$ est factoriel.*

En vertu de la section 2.3, on a un algorithme de calcul pour le plus grand commun diviseur de polynômes $f_1, f_2, \ldots, f_k$ dans $\mathbb{K}[x]$. De cette façon, on trouve explicitement un polynôme d tel que $\langle f_1, f_2, \ldots, f_k\rangle = \langle d\rangle$. On observe que cela donne une description canonique pour l'idéal. Ainsi, on peut déterminer explicitement si deux idéaux $\langle f_1, f_2, \ldots, f_k\rangle$ et $\langle g_1, g_2, \ldots, g_j\rangle$ sont égaux.

2.4.1 Facteurs multiples de polynômes

Lorsqu'on cherche à factoriser un polynôme $f = a_0 + a_1 x + \ldots + a_n x^n$ dans $\mathbb{K}[x]$, pour $\mathbb{K}$ un corps commutatif, une première partie du calcul consiste à détecter s'il contient des **facteurs multiples**. On dit que g (de degré ≥ 1) est un facteur de multiplicité k dans f, si $f = g^k \cdot h$, avec g et h premiers entre eux. Pour détecter et trouver les facteurs multiples (c.-à-d. $k \geq 2$) d'un polynôme f, on exploite la notion de **dérivée** définie[6] comme

$$D(f) := \sum_{i=1}^{n} i a_i x^{i-1}. \tag{2.4.1}$$

6. **Attention**, ici on ne travaille pas avec la définition usuelle du calcul différentiel. Pas de limites, pas de continuité, c'est une définition "algébrique".

On vérifie par calcul direct qu'on a les identités usuelles $D(f_1 + f_2) = D(f_1) + D(f_2)$, et que $D(f_1 \cdot f_2) = D(f_1)f_2 + f_1 D(f_2)$. Un argument récursif permet de déduire de cette dernière égalité qu'on a aussi la règle classique

$$D(f^k) = k\, D(f)\, f^{k-1}.$$

pour tout entier k. On voit aussi que $D(f) \neq 0$ si $\deg(f) \geq 1$.

Proposition 2.12. *Tout facteur multiple d'un polynôme f dans $\mathbb{K}[x]$ est un diviseur de* $\operatorname{pgdc}(f, D(f))$.

Preuve. Supposons que $f = g^k \cdot h$, avec $k \geq 2$ et $\deg(g) \geq 1$, alors

$$\begin{aligned} D(f) &= D(g^k \cdot h) \\ &= D(g^k)\, h + g^k D(h) \\ &= k\, g^{k-1} D(g)\, h + g^k D(h) \\ &= g^{k-1}(k\, D(g)\, h + g D(h)) \end{aligned}$$

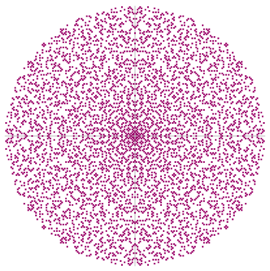
On constate donc que g^{k-1} divise à la fois f et $D(f)$, donc aussi $\operatorname{pgdc}(f, D(f))$. On peut donc trouver, via l'algorithme d'Euclide, les facteurs communs de f. ∎

Par exemple, pour $f = x^3 - x^2 - x + 1$ (dans $\mathbb{Q}[x]$), on a $D(f) = 3x^2 - 2x - 1$, et alors l'algorithme donne

$$\begin{aligned} x^3 - x^2 - x + 1 &= \frac{1}{3}x\,(3x^2 - 2x - 1) + \Big(-\frac{1}{3}x^2 - \frac{2}{3}x + 1\Big) \\ 3x^2 - 2x - 1 &= -9\Big(-\frac{1}{3}x^2 - \frac{2}{3}x + 1\Big) + (-8x + 8) \\ \Big(-\frac{1}{3}x^2 - \frac{2}{3}x + 1\Big) &= \frac{1}{24}(-8x + 8) + (-x + 1) \\ (-8x + 8) &= 8\,(-x + 1) + 0 \end{aligned}$$

d'où $x - 1 = \operatorname{pgdc}(f, D(f))$ (on a "normalisé" en multipliant par un élément de $\mathbb{Q}$ pour avoir un coefficient dominant égal à 1). On conclut que f se divise par $(x-1)^2$. En fait, $f = (x-1)^2(x+1)$.

2.5 L'anneau des entiers de Gauss, et sommes de deux carrés



Un des problèmes classiques de la théorie des nombres est de déterminer quels sont les nombres $n \in \mathbb{N}$ qui s'écrivent comme une somme de deux carrés $n = a^2 + b^2$ (avec a, b dans $\mathbb{N}$). On cherche

aussi à trouver toutes les façons de le faire, quand c'est possible. Ainsi, parmi les nombres ≤ 200, ceux (les seuls) qui s'expriment comme somme de deux carrés sont les suivants [7] :

$$0,1,2,4,5,8,9,10,13,16,17,18,20,25,26,29,32,34,36,37,40,41,45,49,50,$$
$$52,53,58,61,64,65,68,72,73,74,80,81,82,85,89,90,97,98,100,101,104,$$
$$106,109,113,116,117,121,122,125,128,130,136,137,144,145,146,148,149,$$
$$153,157,160,162,164,169,170,173,178,180,181,185,193,194,196,197,200$$

Par exemple, on a

$$1105 = 32^2 + 9^2 = 33^2 + 4^2 = 31^2 + 12^2 = 24^2 + 23^2. \tag{2.5.1}$$

La solution du problème est agréablement organisée dans le contexte de l'anneau des entiers de Gauss. L'histoire se déroule comme suit. On observe d'abord que l'anneau $\mathbb{Z}[i]$ est euclidien.

Proposition 2.13. *L'anneau $\mathbb{Z}[i]$, des entiers de Gauss, est euclidien avec la valuation $N(a+bi) = a^2+b^2$, et la division euclidienne y est effective. La fonction N est multiplicative (on dit que c'est une* **norme***), et les seuls éléments inversibles de $\mathbb{Z}[i]$ sont ceux pour lesquels $N(a+bi) = 1$.*

Preuve. On vérifie par calcul direct que N est multiplicative. La dernière assertion est facile à vérifier, sachant que les seuls éléments inversibles de $\mathbb{Z}[i]$ sont 1, -1, i, et $-i$, qui correspondent au 4 solutions dans $\mathbb{Z}$ de l'équation $a^2+b^2 = 1$.

Il suffit ensuite de montrer que pour $\alpha = a+bi$ et $\beta = c+di \neq 0$ dans $\mathbb{Z}[i]$, il existe q et r dans $\mathbb{Z}[i]$ tels que

$$\alpha = \beta q + r, \qquad \text{avec } r = 0 \text{ ou } N(r) < N(\beta).$$

On observe d'abord que, dans le corps $\mathbb{Q}[i]$ des rationnels de Gauss, l'inverse de $c+di$ est

$$\frac{c}{c^2+d^2} - \frac{d}{c^2+d^2}\,i, \qquad \text{puisque} \qquad (c+di)(c-di) = c^2+d^2.$$

Il s'ensuit que dans $\mathbb{Q}[i]$, on a des nombres rationnels x, y tels que

$$\alpha\beta^{-1} = (a+bi)(c+di)^{-1} = x+yi, \qquad \text{avec} \qquad x = \frac{ac+bd}{c^2+d^2} \quad \text{et} \quad y = \frac{-ad+bc}{c^2+d^2}.$$

On pose $q = n+ki$ et $r = \alpha - \beta q$, où n et k sont des entiers tels que

$$-\frac{1}{2} \leq x-n \leq \frac{1}{2} \quad \text{et} \quad -\frac{1}{2} \leq y-k \leq \frac{1}{2}.$$

Montrons que $N(r) \leq N(\beta)/2$. Calculant dans $\mathbb{Q}[i]$, on a $r = \beta\,(\alpha/\beta - q)$. De plus,

$$\begin{aligned}\frac{\alpha}{\beta} - q &= (x+yi) - (n+ki)\\ &= (x-n) + (y-k)\,i,\end{aligned}$$

donc

$$\begin{aligned}N\Big(\frac{\alpha}{\beta} - q\Big) &= (x-n)^2 + (y-k)^2\\ &\leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}.\end{aligned}$$

7. Tel que répertoriés par Euler, en 1758.

On a donc

$$N(r) = N(\beta)N\Big(\frac{\alpha}{\beta} - q\Big) \leq \frac{1}{2}N(\beta).$$

■

On a une proposition analogue pour l'anneau des **entiers d'Eisenstein** [8] $\mathbb{Z}[\omega] := \{a+b\omega \mid a, b \in \mathbb{Z}\}$, où ω est une racine primitive cubique de l'unité [9], avec la valuation $N(a+b\omega) = a^2 - ab + b^2$. Pour la suite de notre histoire, nous allons exploiter le fait suivant, qui découle de la proposition 2.13 en vertu du théorème 2.8.

Corollaire 2.14. *L'anneau $\mathbb{Z}[i]$ est principal et factoriel.*

Pour poursuivre, une observation clé est que :

Proposition 2.15. *Soit p un nombre entier premier distinct de 2. Alors, les conditions suivantes sont équivalentes :*

(i) $p \equiv 1 \mod 4$;

(ii) -1 *est un carré dans* $\mathbb{Z}/p\mathbb{Z}$;

(iii) p *n'est pas irréductible dans* $\mathbb{Z}[i]$;

(iv) *il existe* a *et* b *dans* $\mathbb{Z}$, *tels que* $p = a^2 + b^2$.

Dans ce cas, avec les notations de (iv), $a + bi$ est irréductible dans $\mathbb{Z}[i]$; et de plus, a et b sont uniques à l'ordre et au signe près.

Preuve.

(i) ⇒ (ii) : Par hypothèse p est premier et de la forme $4k+1$. Rappelons d'abord que, par le théorème de Wilson, on a $(p-1)! \equiv -1 \mod p$. Posons $t = (2k)!$, et montrons que $t^2 = -1 \mod p$, ce qui montrera l'assertion (ii). On a :

$$\begin{aligned} t &= 1 \cdot 2 \cdot 3 \cdots (2k) \\ &= (-1)(-2)(-3)\cdots(-2k), \qquad \text{(car il y a un nombre pair de facteurs).} \end{aligned} \tag{2.5.2}$$

D'où,

$$\begin{aligned} -1 &\equiv p-1 \,(\mathrm{mod}\ p) = 4k \\ -2 &\equiv p-2 \,(\mathrm{mod}\ p) = 4k-1 \\ &\vdots \\ -2k &\equiv p-2\,k \,(\mathrm{mod}\ p) = 2k+1 \end{aligned}$$

et donc $t \equiv (2k+1)\cdots(4k-1)(4k) \mod p$. Utilisant cette expression d'une part, et (2.5.2) d'autre part, on trouve que

$$t^2 \equiv \underbrace{1 \cdot 2 \cdot 3 \cdots (2k)}_{t} \cdot \underbrace{(2k+1)\cdots(4k-1)(4k)}_{t \mod p} = (4k)! = (p-1)! \equiv -1 \mod p.$$

8. Ferdinand Gotthold Max Eisenstein (1823–1852).
9. $w = \exp(2\pi i/3)$.

(ii) ⇒ (iii) : Si $t^2+1 \equiv 0 \mod p$, alors on a $pq = t^2+1$ pour un certain q. Donc, p divise $(t+i)(t-i)$ dans $\mathbb{Z}[i]$. Si p était irréductible dans $\mathbb{Z}[i]$, alors puisque $\mathbb{Z}[i]$ est factoriel, p diviserait soit $t+i$ soit $t-i$. Si par exemple p divise $t+i$, on obtient $t+i = p(a+bi) = pa+pbi$; et alors $pb = 1$ dans $\mathbb{Z}$, ce qui est impossible étant donné que p est premier. Donc p n'est pas irréductible.

(iii) ⇒ (iv) : Si p n'est pas irréductible dans $\mathbb{Z}[i]$, alors $p = (a+bi)(c+di)$, avec $(a+bi)$ et $(c+di)$ non inversibles. En particulier, $N(a+bi) \geq 2$ et $N(c+di) \geq 2$. Mais alors, on a

$$p^2 = N(p) = N(a+bi)N(c+di) = (a^2+b^2)(c^2+d^2) \qquad \text{(dans } \mathbb{N}\text{)}.$$

Comme p est premier, il découle de l'unicité de la factorisation en nombre premier dans $\mathbb{N}$, que $p = a^2+b^2 = c^2+d^2$.

(iv) ⇒ (i) : Soit $p = a^2+b^2$ dans $\mathbb{N}$. Modulo 4, tous les carrés sont congrus soit à 0 (le carré des nombres pairs), soit à 1 (le carré de nombres impairs). Comme p n'est pas pair, l'un des nombres a^2 ou b^2 est congru à 1, et l'autre à 0. Donc $p \equiv 1 \mod 4$.

L'égalité $p = a^2+b^2$ implique que $p = N(a+bi)$, et donc $a+bi$ doit être irréductible (sinon p se factorise, puisque N est multiplicatif).

Supposons maintenant que $p = a^2+b^2 = c^2+d^2$. Alors $(a+bi)(a-bi) = (c+di)(c-di)$, et ces quatre nombres sont irréductibles dans $\mathbb{Z}[i]$. Par factorialité de $\mathbb{Z}[i]$, on a (par exemple) $a+bi = \varepsilon(c+di)$ pour $\varepsilon = 1, -1, i$ ou $-i$. Donc a, b et c, d son égaux à l'ordre et au signe près. ∎

Nous pouvons donc maintenant donner une liste complète des éléments irréductibles de $\mathbb{Z}[i]$.

Corollaire 2.16. *Les éléments irréductibles de $\mathbb{Z}[i]$ sont :*

(i) $1+i$;

(ii) *les nombres premiers p dans $\mathbb{N}$, tels que $p \equiv 3 \mod 4$;*

(iii) *les nombres $a+bi$ et $a-bi$ tels que a^2+b^2 est premier dans $\mathbb{N}$;*

et leurs associés (par exemple $1-i = (1+i)\,i$).

Preuve. Montrons d'abord que les nombres de (i), (ii), (iii) sont irréductibles dans $\mathbb{Z}[i]$.

Pour (i), c'est direct, puisque $N(1+i) = 2$ ce qui force $1+i$ à être irréductible. Pour (ii), on applique la proposition 2.15, et de même pour (iii).

Il reste à prouver qu'il n'y a pas d'autres éléments irréductibles dans $\mathbb{Z}]i]$. Observons d'abord que tout irréductible π de $\mathbb{Z}[i]$ divise un nombre premier p dans $\mathbb{N}$. À cette fin, considérons l'idéal $(\pi\mathbb{Z}[i]) \cap \mathbb{Z}$ de $\mathbb{Z}$. Comme $\mathbb{Z}$ est principal, il existe $p \in \mathbb{Z}$ tel que $(\pi\mathbb{Z}[i]) \cap \mathbb{Z} = p\mathbb{Z}$. Si $p = ab$, alors $ab \in \pi\mathbb{Z}[i]$ et soit π divise a soit π divise b. On a donc, soit a ou b dans $p\mathbb{Z}$, donc p divise a ou p divise b. Ceci force p à être premier.

Soit maintenant π irréductible dans $\mathbb{Z}[i]$. Il existe un nombre premier p (dans $\mathbb{N}$), tel que π divise p. Si $p \equiv 3 \mod 4$, alors p est irréductible dans $\mathbb{Z}[i]$, donc π est associé à p, donc de la forme (ii). Si $p \equiv 1 \mod 4$, alors $p = a^2+b^2$, et π divise $(a+bi)(a-bi)$, avec ces deux nombres irréductibles dans $\mathbb{Z}[i]$. Il s'ensuit que $\pi = x+yi$ est associé à $a+bi$ (ou à $a-bi$), et alors $x^2+y^2 = a^2+b^2 = p$. On a donc que π est de la forme (iii). Enfin, si $p = 2$, on raisonne de même pour voir que π divise $(1+i)(1-i)$ et donc que π est de la forme (i). ∎

Notre premier résultat global concernant les entiers qui peuvent s'écrire comme somme de deux carrés est le suivant. Soulignons que $n \in \mathbb{N}$ peut s'écrire comme somme de deux carrés $n = a^2 + b^2$, si et seulement si n est la norme d'un élément de $\mathbb{Z}[i]$, à savoir $a + b\,i$.

Corollaire 2.17. *Soit $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, avec les p_i distincts deux à deux. Alors, n peut s'écrire comme somme de deux carrés si et seulement si les exposants n_i correspondant à des premiers $p_i \equiv 3 \mod 4$ sont tous des nombres pairs.*

Preuve. On observe d'abord que, si n et n' peuvent s'écrire comme somme de deux carrés, alors c'est aussi le cas de $n\,n'$. C'est là essentiellement la multiplicativité de N, puisque si $n = N(z)$ et $n' = N(z')$ alors $nn' = N(zz')$. Donc, la condition du corollaire est suffisante.

Pour voir qu'elle est nécessaire, on suppose $n = a^2 + b^2$, on a donc la factorisation $n = (a+b\,i)(a-b\,i)$ dans $\mathbb{Z}[i]$. On décompose $a + b\,i$ en irréductibles dans $\mathbb{Z}[i]$, pour obtenir

$$a + b\,i = \prod_j \pi_j. \tag{2.5.3}$$

Comme $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$, la conjugaison [10] y est multiplicative. On a donc

$$a - b\,i = \prod_j \overline{\pi_j}.$$

qui est aussi un produit d'irréductibles. En regroupant les irréductibles de $a + b\,i$ avec ceux $a - b\,i$ conformément au corollaire 2.16 (ceux de la forme $(c + d\,i)$ avec $d > 0$, avec $(c - d\,i)$, et les $p \in \mathbb{N}$ congrus à $(3 \mod 4)$ avec eux-mêmes), on achève la démonstration. ∎

Les diverses façons d'écrire n comme somme de deux carrés correspondent aux choix possibles dans la répartition des facteurs de n dans l'expression (2.5.3). Ainsi, la décomposition en facteur dans $\mathbb{Z}[i]$ de 1105 est :

$$1105 = 5 \cdot 13 \cdot 17 = \underbrace{(2+i)(2-i)}_{5} \cdot \underbrace{(3+2\,i)(3-2\,i)}_{13} \cdot \underbrace{(4+i)(4-i)}_{17}.$$

On trouve les diverses façons d'écrire 1105 énumérées en (2.5.1), comme suit. Dans chaque cas on ne prend qu'un des deux facteurs du nombre premier congru à $(1 \mod 4)$. On trouve (au moins)

$$\begin{aligned}
(2+i)\cdot(3+2\,i)\cdot(4+i) &= 9 + 32\,i \\
(2-i)\cdot(3+2\,i)\cdot(4+i) &= 31 + 12\,i \\
(2+i)\cdot(3-2\,i)\cdot(4+i) &= 33 + 4\,i \\
(2+i)\cdot(3+2\,i)\cdot(4-i) &= 23 + 24\,i
\end{aligned}$$

ce qui correspond aux 4 façons d'écrire 1105 comme somme de deux carrés données en (2.5.1). Toutes les autres répartitions des facteurs et leurs associés donne une de ces 4 possibilités, la liste est donc complète.

On peut comparer cette approche à celle d'Euler (d'avant la théorie des anneaux) en consultant une traduction anglaise (très lisible) de son article : eulerarchive.maa.org/docs/translations/E228en.pdf. En passant, il y a en Sage tous les outils nécessaires pour travailler dans $\mathbb{Z}[i]$.

10. $\overline{x + y\,i} = x - y\,i$.

2.5.1 Exercices

Exercice 2.2. Déterminer les entiers de 1 à 100 qui sont somme de deux carrés, et les exprimer comme une telle somme.

Exercice 2.3. Montrer que pour p premier impair, et $\mathcal{F}_p = \mathbb{Z}/p\mathbb{Z}$, l'idéal de $\mathcal{F}_p[x]$ engendré par x^2+1 est maximal si et seulement si p est de la forme $4k+3$. Dans ce cas, montrer que le corps quotient est engendré par $\mathcal{F}_p$ et un élément i tel que $i^2 = -1$.

Exercice 2.4. Montrer que si $p = 4k+1$ est un nombre premier, alors il existe un entier i, $1 \le i \le k$, tel que le nombre entier $-1+ip$ soit un carré dans $\mathbb{N}$. Indications : montrer qu'il existe $x \in \{1, 2, \dots, 2k\}$ tel que $x^2 \equiv -1 \mod p$.

Exercice 2.5. Dans $\mathbb{Z}[i]$, à quelle condition un élément $a+bi$ est-il associé à son conjugué $a-bi$?

2.6 Théorème du reste chinois

Le théorème de théorie des nombres dit "des restes chinois" donne la solution d'un problème célèbre qu'on retrouve déjà au 4e-siècle dans le livre du mathématicien Sun Zi (~400–460). Il se généralise de la façon suivante.

Théorème 2.18. *Soient $a_1, a_2, \dots, a_k$ des éléments deux à deux relativement premiers dans un anneau principal intègre $\mathcal{A}$. On a un isomorphisme d'anneaux naturel*

$$\varphi : \mathcal{A}/\langle a_1 \cdots a_k\rangle \xrightarrow{\sim} \mathcal{A}/\langle a_1\rangle \times \mathcal{A}/\langle a_2\rangle \times \cdots \times \mathcal{A}/\langle a_k\rangle .$$

Preuve. Commençons par $k = 2$. On considère le morphisme $\pi : \mathcal{A} \longrightarrow \mathcal{A}/\langle a_1\rangle \times \mathcal{A}/\langle a_2\rangle$ défini par

$$\pi(b) = (b_1, b_2), \qquad \text{avec} \qquad b_i = \pi_i(b),$$

où $\pi := \mathcal{A} \twoheadrightarrow \mathcal{A}/\langle a_i\rangle$ est l'épimorphisme canonique.

Montrons que π est surjectif. Il suffit de montrer que si b_1, b_2 sont deux éléments de $\mathcal{A}$, alors il existe $b \in \mathcal{A}$ tel que $b \equiv b_i \mod a_i$ pour $i = 1, 2$. Par le théorème de Bezout pour les anneaux principaux, il existe $c_1, c_2 \in \mathcal{A}$ tels que $1 = -c_1a_1 + c_2a_2$. On a donc $b_1 - b_2 = -(b_1-b_2)c_1a_1 + (b_1-b_2)c_2a_2$. Donc $b_1 + (b_1-b_2)c_1a_1 = b_2 + (b_1-b_2)c_2a_2$ et on note b cet élément, qui résout la question.

Le noyau de π est l'ensemble des b qui sont divisibles à la fois par a_1 et par a_2, c'est-à-dire par leur ppmc. Celui-ci est a_1a_2, car l'anneau est factoriel. On obtient donc par la propriété universelle (corollaire 1.21) un épimorphisme $\mathcal{A}/\langle b\rangle \longrightarrow \mathcal{A}/\langle a_1\rangle \times \mathcal{A}/\langle a_2\rangle$.

Soit maintenant $k \ge 2$. Soient $a_1, \dots, a_{k+1}$ des éléments deux à deux premiers entre eux. Par hypothèse de récurrence on a un isomorphisme $\mathcal{A}/\langle a_1 \cdots a_k\rangle$ vers $\mathcal{A}/\langle a_1\rangle \times \mathcal{A}/\langle a_2\rangle \times \cdots \times \mathcal{A}/\langle a_k\rangle$. Par le cas $k = 2$, on a un isomorphisme $\mathcal{A}/\langle a_1 \cdots a_k a_{k+1}\rangle$ vers $\mathcal{A}/\langle a_1 \cdots a_{k+1}\rangle \times \mathcal{A}/\langle a_{k+1}\rangle$, car $a_1 \cdots a_k$ et a_{k+1} sont premiers entre eux. Mais ce dernier anneau produit est isomorphe à $\mathcal{A}/\langle a_1\rangle \times \mathcal{A}/\langle a_2\rangle \times \cdots \times \mathcal{A}/\langle a_k\rangle \times \mathcal{A}/\langle a_{k+1}\rangle$. ∎

2.6.1 Formule d'interpolation de Lagrange

Un cas particulier du théorème chinois est le suivant. Dans l'anneau des polynômes à coefficients réels (ou n'importe quel autre corps), $\mathcal{A} = \mathbb{R}[x]$, on considère comme a_i les polynômes $x - c_i$, pour $1 \leq i \leq n$, avec les $c_i \in \mathbb{R}$ des réels deux à deux distincts. Le polynôme b est donc

$$b = (x - c_1)(x - c_2)\cdots(x - c_n).$$

Parce que l'anneau $\mathcal{A}$ est euclidien, et que les polynômes $x - c_i$ sont de degré 1, on peut "identifier" les éléments (ce sont des classes d'équivalence) de $\mathcal{A}/\langle x - c_i\rangle$ avec des constantes d_i. Un élément du produit $\mathcal{A}/\langle a_1\rangle \times \mathcal{A}/\langle a_2\rangle \times \cdots \times \mathcal{A}/\langle a_k\rangle$ correspond donc à un "vecteur" $(d_1, d_2, \ldots, d_n)$ de réels. La situation du théorème se résume ainsi à choisir n points (c_i, d_i) dans dans $\mathbb{R}^2$, pour $1 \leq k \leq n$, avec les c_i deux à deux distincts, et l'énoncé du théorème affirme alors qu'ils correspondent à ces n points, un et un seul élément du quotient, $\mathcal{A}/\langle b\rangle$. Encore parce que $\mathcal{A}$ est euclidien, les éléments de $\mathcal{A}/\langle b\rangle$ s'identifient à des polynômes de degré au plus $n - 1$ (des restes modulo $(x - c_1)(x - c_2)\cdots(x - c_n)$).

La **formule d'interpolation de Lagrange**[11] donne un polynôme p, de degré au plus $n - 1$, tel $p(c_i) = d_i$ pour tout k. Autrement dit, c'est un polynôme dont le graphe passe par les points (c_i, d_i). Ce polynôme est exactement $\varphi^{-1}(d_1, d_2, \ldots, d_n)$. Le cas $n = 2$ correspond au fait que par deux points (d'abscisses distinctes) passe une et une seule droite, et pour $n = 3$ qu'il passe une et une seule parabole par trois points (d'abscisses distintes).

Les **interpolateurs** de Lagrange sont les polynômes $\ell_j(x)$ défini comme :

$$\ell_j(x) := \prod_{\substack{i \neq j \\ 1 \leq i \leq n}} \frac{x - c_i}{c_j - c_i}.$$

On constate que

$$\ell_j(c_i) = \begin{cases} 1, & \text{si } k = j, \\ 0, & \text{sinon.} \end{cases} \tag{2.6.1}$$

Ceci permet de définir le polynôme cherché en posant simplement

$$p(x) := \sum_{j=1}^{n} \ell_j(x)\, d_j. \qquad \text{(Formule d'interpolation de Lagrange)} \tag{2.6.2}$$

C'est manifestement un polynôme de degré au plus $n - 1$, et la propriété (2.6.1) donne directement que $p(c_i) = d_i$ pour tout k.

Exercice 2.6. Calculer le polynôme d'interpolation de Lagrange qui vaut 0 pour $x = 0, \ldots, n - 1$ et 1 pour n. Quel est le rapport avec les coefficients binomiaux ?

2.7 (∗) Codes polynomiaux

Comme son nom l'indique, le but de la théorie des codes correcteurs d'erreurs est de construire des protocoles de transmission de données de façon à pouvoir détecter/corriger les erreurs qui peuvent se glisser pendant la transmission, à cause d'interférences. Un cas bien connu est l'alphabet phonétique de l'OTAN, utilisé dans les communications radio en aviation et par divers services d'urgence. On

11. Joseph-Louis Lagrange (1736–1813).

remplace la lettre “a” par le vocable “alpha”, la lettre “b” par le vocable “bravo”, et ainsi de suite jusqu'à la lettre “z” par le vocable “zoulou”. S'il y a interférence lors de la transmission, celui qui n'entend que “...lou alpha brav...” décode malgré tout le message comme étant (très probablement) “zoulou alpha bravo”, ce qui signifie “zab”. Les codes polynomiaux sont l'une des constructions classiques de la théorie, qui reprend de façon plus efficace ce genre d'idée.

On considère l'anneau des polynômes $\mathbb{K}[x]$, pour $\mathbb{K}$ un corps fini qu'on supposera égal à $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ dans ce qui suit. Un vecteur $(a_0, a_1, \ldots, a_{n-1})$ dans l'espace vectoriel $\mathbb{F}_p^n$ est identifié au polynôme

$$f(x) = a_0\, x^{n-1} + \ldots + a_{n-2}\, x + a_{n-1},$$

de degré au plus $n-1$. Pour construire un **code polynomial**, on choisit un polynôme unitaire fixé $g(x)$ de degré m, qu'on appelle **polynôme générateur** du code, et un entier $n \geq m$. Les **mots de code** sont les polynômes de degré au plus $n-1$ qui sont divisibles par $g(x)$.

Par exemple, pour $\mathbb{F}_2$, on peut choisir $g(x) = x^2 + x + 1$ et $n = 5$. On vérifie que les mots de code possibles sont alors exactement les suivants

$$\{0 \cdot g(x), 1 \cdot g(x), x \cdot g(x), (x+1) \cdot g(x), x^2 \cdot g(x), (x^2+1) \cdot g(x), (x^2+x) \cdot g(x), g(x)^2\},$$

qui correspondent aux 8 vecteurs dans $\mathbb{F}_2^5$

0	$x^2 + x + 1$	$x^3 + x^2 + x$	$x^3 + 1$
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
00000	00111	001110	001001
$x^4 + x^3 + x^2$	$x^4 + x^3 + x + 1$	$x^4 + x$	$x^4 + x^2 + 1$
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
11100	11011	100100	10101

Afin de le coder, on commence par décrire comme ci-haut un vecteur $(b_i)_i$ dans $\mathbb{F}_p^{n-m}$ comme un polynôme $h(x)$ de degré au plus $n-m-1$. Puis, on calcule le reste $r(x)$ de la division de $x^m\, h(x)$ par $g(x)$. Le **code** de $h(x)$ est alors défini comme étant $x^m h(x) - r(x)$, qui est bien un multiple de $g(x)$. Via la bijection entre vecteurs dans $\mathbb{F}_2^5$ et polynômes de degré au plus 4, on trouve ainsi les codages suivants pour les huit éléments de $\mathbb{F}_2^3$

000	001	010	011
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
<u>00</u>000	<u>00</u>111	<u>01</u>001	<u>01</u>110
100	101	110	111
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
<u>10</u>010	<u>10</u>101	<u>11</u>011	<u>11</u>100

Par construction, les $n-m$ premiers coefficients de ces vecteurs codes correspondent au vecteur codé, puisque le reste calculé pour obtenir $x^m h(x) - r(x)$ est de degré au plus égal à $m-1$ (ou est nul). On détecte qu'il y a eu erreur de transmission si le reste du polynôme associé à un message (un élément de $\mathbb{F}_p^n$) par $g(x)$ n'est pas nul. On peut “corriger” les erreurs (s'il n'y en a pas trop) en prenant le vecteur de code le plus proche du message reçu.

Il est direct de voir que le sous-ensemble $\mathcal{C}$ des mot de codes est un sous-espace vectoriel de $\mathbb{F}_p^n$. Voilà pourquoi un dit que c'est un code **linéaire**. Le cas où on considère $g(x)$ un diviseur de $x^n - 1$ de degré m, est souvent considéré. Ce sont les codes **cycliques**. L'identification entre $\mathbb{F}_p^n$ et les polynômes de degré au plus $n-1$, correspond à calculer dans l'anneau $\mathbb{F}_p[x]/\langle x^n - 1\rangle$. Il est pratique de considérer le cas où $g(x)$ est irréductible, et alors le code est dit **irréductible**.

2.8 Exercices du chapitre 2

Exercice 2.7 (**Divisibilité**).
Soit $\mathcal{A}$ un anneau commutatif. Montrer que les propriétés suivantes sont équivalentes

i) Il existe $c \in \mathcal{A}$ tel que $ac = b$.
ii) $b \in \langle a \rangle$.
iii) $\langle b \rangle \subset \langle a \rangle$.

Exercice 2.8. Soit $\mathcal{A}$ un anneau commutatif principal et I un idéal de $\mathcal{A}$. Montrer que $\mathcal{A}/I$ est principal.

Exercice 2.9. Soit $\mathcal{A}$ un anneau commutatif principal et soit $a \in A$. Montrer que $\langle a \rangle$ est maximal si et seulement si a un élément irréductible.

Exercice 2.10 (**pgdc, ppcm**).
Soit $\mathcal{A}$ un anneau factoriel, et $\mathcal{P}$ l'ensemble de ses éléments irréductibles. Soient $x, y \in A$ non nuls tels que

$$x = u \prod_{p \in \mathcal{P}} p^{a_p}, \qquad \text{et} \qquad y = u' \prod_{p \in \mathcal{P}} p^{b_p},$$

où u et u' sont des inversibles de $\mathcal{A}$, et a_p, $b_p \in \mathbb{N}$. Montrer que :

1) $x \,|\, y$ si et seulement si $a_p \leq b_p$ pour tout $p \in \mathcal{P}$;
2) $d := \prod_{p \in \mathcal{P}} p^{min(a_p, b_p)}$ est un pgdc de x et y ;
3) $m := \prod_{p \in \mathcal{P}} p^{max(a_p, b_p)}$ est un ppcm de x et y ;
4) $\text{pgdc}(x, y)\text{ppcm}(x, y)$ et xy sont associés.
5) si de plus $\mathcal{A}$ est principal, alors

$$\langle \text{pgdc}(a_1, ..., a_n) \rangle = \langle a_1 \rangle + ... + \langle a_n \rangle, \qquad \text{et} \qquad \langle \text{ppcm}(a_1, ..., a_n) \rangle = \langle a_1 \rangle \cap ... \cap \langle a_n \rangle;$$

6) si $\mathcal{A}$ est seulement commutatif, alors les éléments $a_1, ..., a_n \in \mathcal{A}$ admettent un ppcm si et seulement si l'idéal $\langle a_1 \rangle \cap ... \cap \langle a_n \rangle$ est principal ;
7) si $\mathcal{A}$ est seulement commutatif et l'idéal $\langle a_1, ...a_n \rangle$ est principal, alors les éléments $a_1, ..., a_n$ admettent un pgdc.

Exercice 2.11 (**Lemme de Gauss**).
Soit $\mathcal{A}$ un anneau factoriel. Montrer que pour $a, b, c \in A$ tels que $a \,|\, bc$ et a premier avec b, on a forcément $a \,|\, c$;

Exercice 2.12. Soit $\mathcal{A}$ un anneau principal. Montrer que tout idéal premier non nul de $\mathcal{A}$ est maximal.

Exercice 2.13 (**Exemples d'anneaux intègres non factoriels**).

1) Soit $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$.
i) Montrer que $\mathbb{Z}[i\sqrt{5}]$ est un sous-anneau de $\mathbb{C}$.
ii) Montrer qu'il est intègre et noethérien.
iii) Calculer le groupe des éléments inversibles de $\mathbb{Z}[i\sqrt{5}]$. La notion de **norme** $N(a+ib\sqrt{5}) := a^2 + 5b^2$, pour les éléments de $\mathcal{A}$ pourra vous être utile.
iv) Montrer que $p = 2 + i\sqrt{5}$ est irréductible et $\langle p \rangle$ n'est pas premier. En déduire que $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.
v) Montrer que 3 et $2 + i\sqrt{5}$ n'ont pas de ppcm et que 9 et $3(2 + i\sqrt{5})$ n'ont pas de pgdc dans $\mathbb{Z}[i\sqrt{5}]$.

2) Soit $\mathbb{K}$ un corps.
   i) Montrer que $\mathcal{A} = \{f \in \mathbb{K}[t] \mid f'(0) = 0\}$ est un sous-anneau de $\mathbb{K}[t]$ et qu'il est intègre.
   ii) Montrer que $\mathcal{A} = \mathbb{K}[t^2, t^3]$ et que $\mathcal{A} \simeq \mathbb{K}[x, y]/\langle x^3 - y^2\rangle$. En déduire que $\mathcal{A}$ est noethérien.
   iii) Montrer que t^2 et t^3 sont irréductibles dans $\mathcal{A}$. Sont-ils premiers dans $\mathcal{A}$? En déduire que $\mathcal{A}$ n'est pas factoriel.
   iv) Donner deux factorisations en irréductibles de t^6 dans $\mathcal{A}$. Retrouver le fait que $\mathcal{A}$ n'est pas factoriel.
   v) Exhiber un idéal non principal de $\mathcal{A}$.

3) Montrer que $\mathbb{R}[x, y, z]/\langle z^2 - xy\rangle$ est intègre mais pas factoriel.

4) Soit $\mathbb{R}[\sin(x), \cos(x)]$ l'ensemble des polynômes en $\sin(x)$ et $\cos(x)$ à coefficients réels. Montrer que $\mathbb{R}[\sin(x), \cos(x)] \simeq \mathbb{R}[x, y]/\langle x^2 + y^2 - 1\rangle$. En déduire que $\mathbb{R}[\sin(x), \cos(x)]$ est intègre mais pas factoriel.

Exercice 2.14 (**Exemple d'anneaux factoriels non principaux**).
Soit $\mathbb{K}$ un corps. Montrer que $\mathbb{Z}[x]$ et $\mathbb{K}[x, y]$ sont factoriels mais non principaux.

Exercice 2.15 (**Condition nécessaire sur anneau pour qu'il soit euclidien**).
Soit $\mathcal{A}$ un anneau euclidien. Montrer qu'il existe $a \in \mathcal{A}$, non inversible, tel que la restriction de la surjection naturelle $\pi : \mathcal{A} \to \mathcal{A}/\langle a\rangle$ à $\mathcal{A}^\times \cup 0$ est surjective ($\mathcal{A}^\times$ désigne l'ensemble des éléments inversibles de $\mathcal{A}$, aussi noté $U(\mathcal{A})$). Montrer qu'alors $\mathcal{A}/(\langle a\rangle$ est un corps.

Exercice 2.16 (**Exemple d'anneau principal non euclidien**).
Ce genre d'anneau n'est pas facile à trouver. Dans Perrin, cours d'algèbres Ellipses 1996, il est montré que les anneaux $\mathbb{Z}[(1 + \sqrt{-19})/2]$ et $\mathbb{R}[x, y]/(x^2 + y^2 + 1)$ sont principaux sans être euclidiens. Dans cet exercice nous étudions $\mathbb{Z}[(1 + \sqrt{-19})/2]$. Posons $\alpha = (1 + \sqrt{-19})/2$ et $\mathcal{A} = \{f(\alpha) \mid f \in \mathbb{Z}[x]\}$.

1) Montrer que $\alpha^2 - \alpha + 5 = 0$. Montrer aussi que $A = \{a + b\alpha \mid a, b \in \mathbb{Z}\} = \mathbb{Z}[\alpha]$.

2) Montrer que $\mathcal{A}$ est stable par conjugaison. On définit $N(z) := z\overline{z}$ pour tout $z \in \mathcal{A}$. En utilisant cette norme décrire les éléments inversibles de $\mathcal{A}$.

3) Montrer que $\mathcal{A}$ n'est pas euclidien (utilisez l'exercice précédent).

4) Soient $z, z' \in \mathcal{A}$ non nuls. Montrer qu'il existe $q, r \in \mathcal{A}$ vérifiant les deux conditions suivantes :
   i) $N(r) < N(z')$
   ii) $z = z'q + r$ ou $2z = z'q + r$

5) Montrer que $\langle 2\rangle$ est un idéal maximal de $\mathcal{A}$ (Pensez à montrer que $\mathcal{A} \simeq \mathbb{Z}[x]/\langle x^2 - x + 5\rangle$).

6) Montrer que $\mathcal{A}$ est principal.

Exercice 2.17 (**L'anneau $\mathbb{Z}[\sqrt{n}]$**).
Soit $n \in \mathbb{Z}$ un entier qui n'est pas un carré. Soit ζ une racine du polynôme $x^2 - n$, et posons $\mathbb{Q}[\zeta] := \{a + b\zeta \mid a, b \in \mathbb{Q}\}$.

1) Montrer que $\mathbb{Q}[\zeta]$ est un sous corps de $\mathbb{C}$ de dimension 2 sur $\mathbb{Q}$

2) Montrer que $\mathbb{Q}[\zeta]$ est isomorphe à $\mathbb{Q}[x]/\langle x^2 - n\rangle$. Qu'en déduisez-vous sur $x^2 - n$?

3) Montrer que $\mathbb{Q}[\zeta]$ est le plus petit corps contenu dans $\mathbb{C}$, à isomorphisme près, contenant ζ et $\mathbb{Q}$.

4) Montrer que la fonction $\sigma : \mathbb{Q}[\zeta] \longrightarrow \mathbb{Q}[\zeta]$, telle que $a + b\zeta \mapsto a - b\zeta$, est un automorphisme de $\mathbb{Q}$-algèbre et calculer son inverse.

5) Posons $\mathbb{Z}[\zeta] := \{a + b\zeta \mid a, b \in \mathbb{Z}\}$. Montrer que c'est un sous-anneaux de $\mathbb{Q}[\zeta]$ et que σ induit par restriction un ismorphisme de $\mathbb{Z}[\zeta]$.

6) Soit $z = a + b\zeta \in \mathbb{Q}[\zeta]$. On pose $N(z) := z\sigma(z) = a^2 - nb^2$. Montrer que cette norme est multiplicative, c'est à dire que $N(zz') = N(z)N(z')$ pour tous $z, z' \in \mathbb{Q}[\zeta]$.

7) Montrer que $N(z) = 0$ si et seulement si $z = 0$.

8) Montrer que si $z \in \mathbb{Z}[\zeta]$ alors $N(z) \in \mathbb{Z}$.
9) Soit $z \in \mathbb{Z}[\zeta]$. Montrer que z est inversible dans $\mathbb{Z}[\zeta]$ si et seulement si $N(z) \in \{-1, 1\}$.
10) Montrer qu'il existe une décomposition en irréductibles de $\mathbb{Z}[\zeta]$.
11) Pour la suite, on suppose que $n = -5$.
i) Montrer que $\mathbb{Z}[\zeta]$ n'est pas factoriel, donc on retrouve en particulier que $\mathbb{Z}[i\sqrt{5}]$ ne l'est pas (on pourra remarquer que 6 admet plusieurs décompositions).
ii) Calculer les inversibles de $\mathbb{Z}[\zeta]$.
iii) Trouver un idéal non principal de $\mathbb{Z}[\zeta]$.

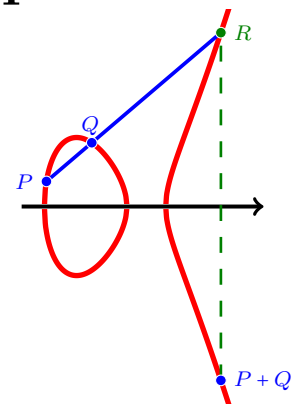
Exercice 2.18. Soit $\mathcal{A}$ l'anneau de toutes les fonctions $f : \mathbb{Z} \longrightarrow \mathbb{Z}$. Pour tout $n \in \mathbb{Z}$ on pose $I_n = \{f \in \mathcal{A} \mid f(x) = 0, \ \forall x > n\}$. Montrer que I_n est un idéal de $\mathcal{A}$ et que la suite d'idéaux (I_n) est strictement croissante.

Exercice 2.19 (**Exemples d'anneau non noethérien**).
Soit $A = \{f \in \mathbb{Q}[x] \mid f(0) \in \mathbb{Z}\}$.
1) Montrer que $\mathcal{A}$ n'est pas factoriel.
2) Montrer que $\mathcal{A}$ n'est pas noethérien.
3) Montrer que tout idéal de type fini de $\mathcal{A}$ est principal.

Exercice 2.20 (**Idéal primaire**).
Soit $\mathcal{A}$ un anneau commutatif. Un idéal I de $\mathcal{A}$ est dit **primaire** si pour tout $a, b \in \mathcal{A}$ tels que $ab \in A$ et $a \notin I$ il existe $n \in \mathbb{N}$ tel que $b^n \in I$.
1) Montrer qu'un idéal premier est primaire. Soit p un nombre premier. Montrer que $\langle p^2 \rangle$ est primaire mais pas premier.
2) Montrer que le radical d'un idéal primaire est un idéal premier.
3) Montrer que si $\mathcal{M}$ est un idéal maximal alors $\mathcal{M}^k$ est un idéal primaire pour tout $k \in \mathbb{N}^*$. Calculer ensuite $\sqrt{\mathcal{M}^k}$.

Chapitre 3

Anneaux de polynômes, et un peu de géométrie algébrique



3.1 Introduction

Pour revenir aux sujets abordés dans l'introduction de ces notes, qu'on peut maintenant mieux formuler avec les notions développées dans les chapitres précédents, un système (fini) d'équations polynomiales en les variables $\boldsymbol{x} = x_1, \ldots, x_j$ est la donnée de polynômes $f_1, \ldots, f_n$ dans $\mathbb{K}[\boldsymbol{x}]$, et on considère les équations

$$\begin{aligned} f_1(x_1, \ldots, x_j) &= 0, \\ &\vdots \\ f_n(x_1, \ldots, x_j) &= 0. \end{aligned} \qquad (*)$$

qu'on cherche à résoudre. Une solution [1] est un élément $\boldsymbol{a} = (a_1, \ldots, a_j) \in \mathbb{K}^j$, tel que $f_i(\boldsymbol{a})$ pour chaque $1 \leq i \leq n$. On peut considérer que l'idéal $\langle f_1, \ldots, f_n \rangle$ est l'ensemble des "conséquences" de ces équations. En effet, comme tout $h \in \langle f_1, \ldots, f_n \rangle$ s'écrit comme $h = f_1\, g_1 + f_2\, g_2 + \ldots + f_k g_k$ pour certains $g_i \in \mathbb{K}[x]$, on a $h(\boldsymbol{a}) = 0$ pour toute solution du système $(*)$. On peut donc interpréter $h(x_1, \ldots, x_j) = 0$ comme une formule qui est satisfaite par toutes les solutions de $(*)$.

Dans le cas où tous les polynômes f_i sont tous de degré 1, on montre en algèbre linéaire que résoudre le système $(*)$ passe par l'algorithme d'élimination de Gauss-Jordan. D'autre part, s'il n'y a qu'une variable, le calcul du pgdc des polynômes f_i donne un unique polynôme dont les racines sont exactement les solutions du système. L'algorithme d'Euclide, décrit dans ce qui suit, précise comment procéder à ce calcul. Nous allons voir plus loin une généralisation commune de ces deux algorithmes : le calcul des bases de Gröbner.

1. Il y a ici des subtilités que nous allons ignorer.

3.2 Factorialité d'anneaux des polynômes

Théorème 3.1. *Si $\mathcal{A}$ est un anneau factoriel, alors $\mathcal{A}[x]$ est aussi factoriel.*

Nous n'allons le montrer (un peu plus loin) que dans le cas $\mathbb{Z}$. Cependant, le cas général est très similaire, seulement un peu plus technique. En préparatif de cette preuve, on a les notions et lemmes suivants. Un polynôme

$$f(x) = \sum_{k=0}^{n} a_k x^k,$$

est dit **primitif**, si $\operatorname{pgdc}(a_0, \ldots, a_k) = 1$. En particulier, il est non nul.

Lemme 3.2 (de Gauss[2])**.** *Si f et g sont des polynômes primitifs, alors $f\,g$ l'est aussi.*

Preuve. Soit $\pi : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$ l'épimorphisme canonique, pour p un nombre premier. Il se prolonge (voir en exercice) en un épimorphisme d'anneau $\Theta : \mathbb{Z}[x] \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}[x]$, par la formule

$$\Theta\Big(\sum_{k=0}^{n} a_k x^k\Big) := \sum_{k=0}^{n} \theta(a_k) x^k.$$

Par contradiction, supposons que $f\,g$ ne soit pas primitif. Il existe alors un nombre premier p qui divise tous ses coefficients. Donc, $\Theta(f\,g) = 0$, ce qui entraîne que $\Theta(f)\Theta(g) = 0$. Mais $\mathbb{Z}/p\mathbb{Z}[x]$ est intègre, puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps. Il s'ensuit que, soit $\Theta(f) = 0$ ou $\Theta(g) = 0$, ce qui entraîne que soit f ou g n'est pas primitif, contredisant ainsi nos hypothèses. ∎

Appelons **dénominateur commun** d'une famille de nombres rationnels $r_1, r_2, \ldots, r_n$, un nombre $d \in \mathbb{Z}$ tel que tous les nombres $dr_1, dr_2, \ldots, dr_n$ soient dans $\mathbb{Z}$. Le **plus petit dénominateur commun** de $r_1, r_2, \ldots, r_n$ est le plus petit dénominateur commun > 0. Comme l'ensemble des dénominateurs communs d'une famille $(r_i)_i$ forme un idéal de $\mathbb{Z}$ (qui est principal), le plus petit d'entre eux les divise tous. On le dénote par $\operatorname{ppdc}(r_1, \ldots, r_n)$. Pour des $a_i \in \mathbb{Z} \setminus \{0\}$ (des entiers non nuls), avec $1 \le i \le n$, on dénote par $\operatorname{pgdc}(a_1, \ldots, a_n)$ le plus grand commun diviseur des a_i, obtenu de façon analogue.

Lemme 3.3. *Soient $r_1, r_2, \ldots, r_n$ des nombres rationnels non nuls. Il existe un unique rationnel $c > 0$, tel que les nombres $r_1/c, r_2/c, \ldots, r_n/c$ soient des entiers premiers entre eux. De fait, on a*

$$c = \frac{1}{d} \operatorname{pgdc}(dr_1, dr_2, \ldots, dr_n),$$

où $d = \operatorname{ppdc}(r_1, \ldots, r_n)$.

Exemple : $(r_1, r_2, r_3) = (4/3, 6, -2)$, $d = 3$, $pgdc(4, 18, -6) = 2$, $c = 2/3$, $(r_1/c, r_2/c, r_3/c) = (2, 9, -3)$, $pgdc(2, 9, -3) = 1$.

2. Johann Carl Friedrich Gauss (1777–1855).

Preuve. Soit $e := \text{pgdc}(dr_1, dr_2, \ldots, dr_n)$. Alors les nombres

$$\frac{dr_1}{e}, \ldots, \frac{dr_n}{e},$$

sont des entiers premiers entre eux. Ceci prouve l'existence de $c := e/d$.

On montre l'unicité de comme suit, avec c et d tel qu'obtenu ci-haut. Soit $c' = u/v > 0$ un nombre rationnel, avec u, v dans $\mathbb{N}^+$ et tels que $u \perp v$. Supposons que les nombres $r_1/c', r_2/c', \ldots, r_n/c'$ soient des entiers premiers entre eux, et montrons que $c = c'$. Posons $a_i := r_i/c'$. Par construction, on a

$$u\, a_i = u r_i \frac{v}{u} = r_i\, v \in \mathbb{Z},$$

d'où v est un dénominateur commun des r_i. Il s'ensuit que $v = d\, w$, pour un certain entier $w > 0$, et donc $d\, w\, r_i = v r_i = u\, a_i$. De plus, comme $u \perp v$, on a aussi $u \perp w$. Comme w divise $u\, a_i$, cela force que w divise a_i. Les a_i étant premiers entre eux, on trouve $w = 1$, et on conclu que $v = d$. Toujours parce que les a_i sont premiers entre eux, on a

$$u = \text{pgdc}(u\, a_1, \ldots, u\, a_n) = \text{pgdc}(d\, r_1, \ldots, d\, r_n) = e,$$

Finalement, $c' = u/v = e/d = c$. ∎

Observons que, tous les r_i sont des entiers si et seulement si $d = 1$, et si et seulement si $c \in \mathbb{N}^+$. Dans ce cas, $\text{pgdc}(r_1, r_2, \ldots, r_n) = 1$ si et seulement $c = 1$.

Définition 31. Pour un polynôme $f \in \mathbb{Q}[x]$, non nul, on dénote par $c(f)$ l'unique nombre rationnel positif, tel que le polynôme $f(x)/c(f)$ soit dans $\mathbb{Z}[x]$ et primitif. On pose $\overline{f} := f/c(f)$, qui est donc primitif. ∎

Le nombre $c(f)$ existe, et il est unique, par le lemme précédent. Exemple : $P = \frac{4}{3} + 6x - 2x^2$, $c(P) = \frac{2}{3}$, car $\frac{3}{2}P = 2 + 9x - 3x^2$, primitif.

Lemme 3.4. *Pour f, g dans $\mathbb{Q}[x]$, non nuls, on a $c(f\, g) = c(f)\, c(g)$; et $\overline{f\, g} = \overline{f}\, \overline{g}$.*

Preuve. On a $f = c(f)\, \overline{f}$, et $g = c(g)\, \overline{g}$. D'une part, on a

$$f\, g = c(f) c(g)\, \overline{f}\, \overline{g},$$

avec $\overline{f}\, \overline{g}$ primitif par le lemme 3.2. D'autre part, on a

$$f\, g = c(f\, g)\, h,$$

par définition, avec un certain polynôme h primitif. L'unicité de $c(f\, g)$ force son égalité avec $c(f)\, c(f)$, et donc aussi l'égalité $\overline{f\, g} = \overline{f}\, \overline{g}$. ∎

Preuve. [du théorème 3.1] Comme annoncé, nous montrons maintenant que $\mathbb{Z}[x]$ est factoriel. De plus, ses éléments irréductibles sont les polynômes de la forme :

- $f \in \mathbb{Z}[x]$, de degré plus grand où égal à 1, qui sont primitifs et irréductibles dans $\mathbb{Q}[x]$;
- $\pm p \in \mathbb{Z}$, pour p un nombre premier.

Démontrons d'abord la première assertion. Si $f \in \mathbb{Z}[x]$ est primitif et irréductible dans $\mathbb{Q}[x]$, alors supposons que $f = g\,h$, avec g et h dans $\mathbb{Z}[x]$. Comme f est irréductible dans $\mathbb{Q}[x]$, l'un des polynômes g ou h doit être inversible dans $\mathbb{Q}]x]$, et donc constant. Supposons que c'est g. Donc g est dans $\mathbb{Z}[x]$, et constant, à savoir $g \in \mathbb{Z}$. C'est un nombre qui divise tous les coefficients de f, qui est primitif, d'où $g = \pm 1$, donc g est inversible dans $\mathbb{Z}$. Ceci prouve que f est irréductible dans $\mathbb{Z}[x]$.

Supposons maintenant que $f = p$ est un nombre premier. Une égalité $f = g\,h$ dans $\mathbb{Z}[x]$ force g et h à être constant, donc dans $\mathbb{Z}$. Il s'ensuit que g ou h est égal à ± 1, ce qui montre l'assertion.

Réciproquement, soit $f \in \mathbb{Z}[x]$ un élément irréductible. Si $f \in \mathbb{Z}$, c'est forcément parce que $f = \pm p$ pour un nombre premier. Autrement, le degré de f est plus grand ou égal à 1. On a alors $f = c(f)\,\overline{f}$, avec $c(f) = 1$, sinon f est réductible. Autrement dit, f est primitif. Si f est réductible dans $\mathbb{Q}[x]$, on a $f = g\,h$ avec g et h dans $\mathbb{Q}[x]$ tous deux de degré plus grand où égal à 1 (car les éléments non nuls de $\mathbb{Q}$ sont tous inversibles). Mais alors $f = \overline{f} = \overline{g}\overline{h}$ dans $\mathbb{Z}[x]$, avec $\deg(\overline{g}) \geq 1$ et $\deg(\overline{h}) \geq 1$, ce qui contredit le fait que f est irréductible. On a donc terminé cette partie de la démonstration.

Reste à voir que $\mathbb{Z}[x]$ est factoriel. Soit f non nul dans $\mathbb{Z}[x]$, avec $f = g_1 \cdots g_n$ des polynômes irréductibles dans $\mathbb{Q}[x]$. Les polynômes g_i et $\overline{g_i}$ sont associés dans $\mathbb{Q}[x]$, puisque $g_i = c(g_i)\,\overline{g_i}$, avec $c(g_i) \in \mathbb{Q}^+$; le polynôme $\overline{g_i}$ est irréductible dans $\mathbb{Q}[x]$, et donc dans $\mathbb{Z}[x]$ d'après la première partie de la preuve. Il s'ensuit que

$$f = c(f)\bar{f} = c(f)\,\overline{g_1 \cdots g_n} = c(f)\,\overline{g_1} \cdots \overline{g_n},$$

et $c(f) \in N^+$, car $f \in \mathbb{Z}[x]$. On peut alors écrire $c(f)$ comme produit de nombres premiers, c.-à-d. $c(f) = p_1 \cdots p_k$. D'où $f = p_1 \cdots p_k\,\overline{g_1} \ldots \overline{g_n}$, ce qui est un produit d'éléments irréductibles dans $\mathbb{Z}[x]$.

L'unicité de la décomposition en éléments irréductibles suit de l'argument suivant. Tout produit d'éléments irréductibles dans $\mathbb{Z}[x]$ peut se mettre sous la forme $q_1 \cdots q_l\,h_1 \cdots h_m$, avec les q_i des nombres premiers, et les h_j des polynômes primitifs et irréductibles dans $\mathbb{Q}[x]$ de degré > 0 (quitte à remplacer des polynômes par leur opposé). Soit alors deux décompositions en irréductibles pour f :

$$f = p_1 \cdots p_k g_1 \cdots g_n = q_1 \cdots q_l\,h_1 \cdots h_m.$$

Par le lemme de Gauss, $g_1 \cdots g_n$ et $h_1 \cdots h_m$ sont primitifs. Donc $\overline{f} = g_1 \cdots g_n = h_1 \cdots h_m$, et $c(f) = p_1 \cdots p_k = q_1 \cdots q_l$, par unicité de la factorisation $f = c(f)\overline{f}$. L'unicité de la factorisation en nombres premiers dans $\mathbb{Z}$ entraîne alors que $k = l$ et qu'on a $p_i = q_{\sigma(i)}$ pour une permutation dans $\mathbb{S}_k$. De plus, interprétant l'égalité $g_1 \cdots g_n = h_1 \cdots h_m$ dans $\mathbb{Q}[x]$, qui est factoriel, on trouve que $n = m$, et que $g_j = r_j h_{\tau(j)}$ pour une permutation dans $\mathbb{S}_n$ et des rationnels non nuls r_j ; alors par unicité de $c(g_j)$, on a $r_j = \pm c(g_j) = \pm 1$. On a donc terminé la démonstration. ∎

Corollaire 3.5. *Si $\mathcal{A}$ est factoriel, alors $\mathcal{A}[x_1, x_2, \ldots, x_n]$ est factoriel.*

Preuve. Cela suit du fait que $\mathcal{A}[x_1, x_2, \ldots, x_n] \simeq \mathcal{B}[x_n]$, où $\mathcal{B} = \mathcal{A}[x_1, x_2, \ldots, x_{n-1}]$. Les détails seront faits au cours. ∎

Exercice 3.1. Soit p/q un nombre rationnel avec p, q entiers premiers entre eux, $q > 0$. Montrer que $c(x - p/q) = 1/q$. Montrer qu'un polynôme dans $\mathbb{Z}[x]$ a toutes ses racines dans $\mathbb{Q}$ (c'est-à-dire qu'il s'écrit $a \prod_i (x - p_i/q_i)$, $a, p_i, q_i \in \mathbb{Q}$) si et seulement s'il est un produit de facteurs linéaires $bx + c$, $b, c \in \mathbb{Z}$.

Exercice 3.2 (**Critère d'Eisenstein**).

1) Soit p un nombre premier et $f(x) = a_n x^n + \ldots + a_1 x + a_0$ un polynôme à coefficients dans $\mathbb{Z}$ tels que p ne divise pas a_n, p divise $a_{n-1}, \ldots, a_0$ et p^2 ne divise pas a_0. Montrer que $f(x)$ est irréductible dans $\mathbb{Q}[x]$.

2) En utilisant le critère d'Eisenstein, montrer que $x^n - 2$ est irréductible dans $\mathbb{Q}[x]$.

3.3 Théorème de Hilbert [3]

Les anneaux noethériens sont définis dans la Définition 30.

Proposition 3.6. *Un anneau commutatif est noetherien si et seulement si tout ideal est finiment engendré.*

Démonstration. Soit I un idéal de $\mathcal{A}$. S'il n'est pas finiment engendré, on peut trouver par récurrence une suite x_n d'éléments de I tels que $\forall n$, x_{n+1} n'est pas dans l'idéal I_n engendré par $x_0, \ldots, x_n$. Alors la suite (I_n) des idéaux de $\mathcal{A}$ est strictement croissante. Donc A n'est pas noetherien.

Réciproquement, supposons que tout idéal de $\mathcal{A}$ est finiment engendré. Soit (I_n) une suite croissante d'idéaux de $\mathcal{A}$. Alors $I = \bigcup I_n$ est un idéal. Il est finiment engendré, par des éléments $a_1, \ldots, a_k$ de I. il existe n tel que I_n contienne tous ces éléments. Alors $I_p = I_n$ pour tout $p \geq n$. ∎

Théorème 3.7. *Si $\mathcal{A}$ est un anneau noethérien, alors $\mathcal{A}[x]$ est un anneau noethérien.*

Corollaire 3.8. *Si $\mathbb{K}$ est un corps, l'anneaux des polynômes $\mathbb{K}[x_1, \ldots, x_k]$ est noethérien.*

Le corollaire se prouve, à partir du théorème, par récurrence sur k, de manière analogue à la preuve du corollaire 3.5. Nous donnons une preuve directe du corollaire ; le lecteur intéressé peut lire une preuve du théorème dans [4] (Theorem 3, Chapter 15).

Démonstration. On ordonne de deux manières les monômes $x_1^{n_1} \cdots x_n^{n_k}$. Le premier ordre, noté $<$ est un ordre partiel : $x_1^{n_1} \cdots x_n^{n_k} \leq x_1^{m_1} \cdots x_n^{m_k}$ si et seulement si $n_i \leq m_i$ pour tout $i = 1, \ldots, k$.

Le deuxième ordre est noté $<_l$: cet ordre ordonne les monômes d'abord par le degré $n_1 + \cdots + n_k$; ensuite, pour les monômes d'égal degré, on ordonne lexicographiquement les k-uplets $(n_1, \ldots, n_k)$, en commençant par la dernière composante. Par exemple, avec $k = 2$, $x_1^2 <_l x_1 x_2 <_l x_2^2 <_l x_1^2 x_2$, car les trois premiers monômes sont tous de degré 2, le dernier est de degré 3, et qu'on a, lexicographiquement, $(2,0) < (1,1) < (0,2)$. L'ordre $<_l$ est total.

Dans un polynôme non nul P, appelons *monôme dominant* le plus grand monôme de son support, pour l'ordre $<_l$ précédemment défini.

On considère un idéal I de $\mathbb{K}[x_1, \ldots, x_k]$, qu'on peut supposer non nul. On considère l'ensemble E des monômes dominants des polynômes non nul de I. Puis l'ensemble M des éléments minimaux de E pour l'ordre $<$; par le lemme ci-après, M est fini.

Pour tout monôme m dans M, soit f_m un polynôme dans I dont m est le monôme dominant ; on peut supposer que le coefficient de m dans f_m est 1.

3. David Hilbert (1862–1943).

Nous montrons que les f_m engendrent I, ce qui finira la preuve. Par l'absurde, supposons qu'il existe un polynôme dans I qui ne soit pas dans l'idéal engendré par les f_m ; choisissons ce f avec monôme dominant le plus petit possible pour l'ordre $<_l$: c'est possible car il n'y a pas de chaîne infinie strictement décroissante pour l'ordre $<_l$. Notons m' ce monôme, avec coefficient a. On a $m' \in E$, donc il existe $m \in M$ tel que $m \leq m'$. Alors $m' = mm_1$ pour un certain monôme m_1. Alors le polynôme $g = f - f_m m_1$ est dans I ; tous les monômes apparaissant dans g sont $<_l m'$ (car tous les monômes dans f_m sont $\leq_l m$, dons ceux dans $f_m m_1$ sont $\leq mm_1 = m'$). Donc par minimalité de m', on doit avoir $g = 0$. Donc $f \in I$. ∎

Lemme 3.9. *On considère l'ordre naturel dans $\mathbb{N}^k$, noté $<$.*

1. De toute suite infinie d'éléments de $\mathbb{N}^k$, on peut extraire une suite croissante.

2. ("lemme de Dickson") Tout sous-ensemble d'éléments deux à deux incomparables de $\mathbb{N}^k$ est fini.

Démonstration. 1. Pour $k = 1$, c'est clair : on peut extraire soit une suite constante, soit une suite strictement croissante ; dans les deux cas, une suite croissante.

Pour $k \geq 2$, on commence par extraire une suite, dont les premières composantes forment une suite croissante. De la suite dans $\mathbb{N}^{k-1}$ obtenue par projection sur les composantes de 2 à k, on peut extraire une suite croissante, par récurrence sur k. La suite obtenue ainsi dans $\mathbb{N}^k$ est croissante.

2. S'il était infini, il existerait une suite infinie d'éléments deux à deux incomparables, et ça contredirait 1. ∎

3.3.1 Exercices

Exercice 3.3 (**Caractérisation des anneaux noethériens**). Soit $\mathcal{A}$ un anneau commutatif. Montrer que l'on a équivalence entre

i) Toute suite croissante d'idéaux est stationnaire.
ii) Tout ensemble non vide d'idéaux de $\mathcal{A}$ admet un élément maximal (pour l'inclusion).
iii) Tout idéal de $\mathcal{A}$ est de type fini.

3.4 Polynômes cyclotomiques

On dit d'un nombre complexe que c'est une **racine n^{e} de l'unité**, si $\omega^n = 1$. Les racines n-èmes de l'unité sont donc les racines du polynôme $x^n - 1$.

L'**ordre** d'une racine de l'unité ω est le plus petit entier $k > 0$, tel que $\omega^k = 1$. Forcément, l'ordre d'une racine n^{e} de l'unité divise n. Si l'ordre d'une racine n^{e} de l'unité ω est égal à n, on dit que ω est une racine **primitive** d'ordre n. Ce sont exactement les nombres complexes de la forme $\exp(k\,i\,\pi/n)$, avec $1 \leq k \leq n-1$ où k et n sont premiers entre eux. Il y a donc $\varphi(n)$ racines primitive d'ordre n.

On appelle n-ème **polynôme cyclotomique** le polynôme dont les racines sont les racines

primitives d'ordre n. On le note $\varphi_n(x)$. On a donc

$$\varphi_n(x) = \prod_{\substack{k \perp n \\ 1 \le k \le n}} (x - \omega^k), \qquad \text{où} \qquad \omega = \exp(2i\pi/n). \tag{3.4.1}$$

Notons que ceci implique que le degré de $\varphi_n(x)$ est $\varphi(n)$.

Comme l'ordre de toute racine n-ème de l'unité est un entier d divisant n, et qu'elle est donc une racine primitive d'ordre d, on obtient

$$x^n - 1 = \prod_{d \mid n} \varphi_d(x). \tag{3.4.2}$$

On peut donc calculer récursivement $\varphi_d(x)$ comme

$$\varphi_n(x) = \frac{x^n - 1}{\prod_{d \mid n,\, d \neq n} \varphi_d(x)}. \tag{3.4.3}$$

On trouve les valeurs suivantes :

$$\begin{aligned}
&\varphi_1(x) = x - 1, && \varphi_2(x) = x + 1,\\
&\varphi_3(x) = x^2 + x + 1, && \varphi_4(x) = x^2 + 1,\\
&\varphi_5(x) = x^4 + x^3 + x^2 + x + 1, && \varphi_6(x) = x^2 - x + 1,\\
&\varphi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, && \varphi_8(x) = x^4 + 1,\\
&\varphi_9(x) = x^6 + x^3 + 1, && \varphi_{10}(x) = x^4 - x^3 + x^2 - x + 1.
\end{aligned}$$

Proposition 3.10. *Les polynômes cyclotomiques sont à coefficients entiers ; leurs termes constants sont* ± 1.

Démonstration. On a $\varphi_1(x) = x - 1$. Soit $n \ge 2$. Alors $x^n - 1 = \varphi_n(x)\psi(x)$, où $\psi(x) = \prod_{d \mid n, d \neq n} \varphi_d(x)$; ce dernier polynôme est à coefficients entiers, et son terme constant est ± 1, par hypothèse de récurrence. On démontre alors par récurrence que le coefficient de x^i dans $\varphi_n(x)$ est entier, pour $i = 2, \ldots, \deg(\varphi_n(x))$. ∎

Les racines de l'unité sont des nombres algébriques. Rappelons qu'un nombre complexe α est dit **algébrique** s'il existe un polynôme $f(x)$ dans $\mathbb{Q}[x]$, tel que $f(\alpha) = 0$. Comme l'ensemble des polynômes dans $\mathbb{C}[x]$ tels que $f(\alpha) = 0$ est un idéal, il existe un unique polynôme unitaire (non nul) $m_\alpha(x)$ qui est de degré minimal et tel que $m_\alpha(\alpha) = 0$ (car $\mathbb{C}[x]$ est principal). On dit que c'est le **polynôme minimal** pour α. Un **entier algébrique** est un nombre algébrique α pour lequel il existe un polynôme unitaire $f(x)$ dans $\mathbb{Z}[x]$, tel $f(\alpha) = 0$. Si α est un entier algébrique, on désigne par $\mathbb{Z}[\alpha]$ le plus petit sous-anneau de $\mathbb{C}$ qui contient $\mathbb{Z}$ et α.

Proposition 3.11. *Le polynôme minimal d'une racine primitive* n^{e} *de l'unité est le polynôme cyclotomique* $\varphi_n(x)$. *Il est à coefficients entiers et unitaire. Il s'ensuit que les racines de l'unité sont des entiers algébriques.*

Proposition 3.12. *L'ensemble des nombres algébriques forme un sous-corps de* $\mathbb{C}$, *dénoté* $\overline{\mathbb{Q}}$ (*ou parfois* $\mathbb{A}$). *C'est le plus petit sous-corps de* $\mathbb{C}$ *algébriquement clos qui contienne* $\mathbb{Q}$. *L'ensemble des entiers algébriques forme un sous-anneau de* $\overline{\mathbb{Q}}$.

Les polynômes cyclotomiques permettent d'éclairer les propriétés des formules qui font intervenir divers termes de la forme $x^n - 1$.

Proposition 3.13. *Soient k et n deux entiers non nuls dans $\mathbb{N}$. Alors on a les propriétés suivante.*

(i) *k divise n si et seulement si $x^k - 1$ divise $x^n - 1$. On a alors*

$$\frac{x^n - 1}{x^k - 1} = \prod_{\substack{d \mid n \\ d \nmid k}} \varphi_d(x). \tag{3.4.4}$$

(ii) *$d = \mathrm{pgdc}(n, k)$ dans $\mathbb{Z}$ si et seulement si $x^d - 1 = \mathrm{pgdc}(x^n - 1, x^k - 1)$ dans $\mathbb{Z}[x]$;*

Exercice 3.4 (Polynômes cyclotomiques).

1) Montrer que, pour $n = p^k$, avec $k \geq 1$ et p premier, on a

$$\varphi_n(x) = 1 + u + \ldots + u^{p-1}, \qquad \text{pour} \qquad u = x^{(p^{k-1})}.$$

2) Calculer les polynômes cyclotomiques pour $11 \leq n \leq 16$.

3.5 (*) Bases de Gröbner d'idéaux

La notion de base de Gröbner est due à Buchberger, qui les a nommées ainsi (dans sa thèse de doctorat de 1965) en l'honneur de son directeur de thèse Gröbner. En fait, la notion est déjà essentiellement présente dans les travaux de Gordan [4] dès 1900 [5].

Afin de définir les bases de Gröbner pour les idéaux d'un anneau de polynômes $\mathbb{K}[\boldsymbol{x}]$ en n variables $\boldsymbol{x} = x_1, \ldots, x_k$, il faut d'abord introduire une ordre sur les monômes $\boldsymbol{x}^{\boldsymbol{a}}$, pour $\boldsymbol{a} \in \mathbb{N}^k$, avec des propriétés adéquates. On dit avoir un **ordre monomial** $\boldsymbol{x}^{\boldsymbol{a}} \preceq \boldsymbol{x}^{\boldsymbol{b}}$ sur $\{\boldsymbol{x}^{\boldsymbol{n}} \mid \boldsymbol{n} \in \mathbb{N}^k\}$, si

(i) $1 \preceq \boldsymbol{x}^{\boldsymbol{a}}$ pour tout $\boldsymbol{a} \in \mathbb{N}^k$;

(ii) pour tout $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ dans $\mathbb{N}^k$, on a $\boldsymbol{x}^{\boldsymbol{a}} \preceq \boldsymbol{x}^{\boldsymbol{b}}$ implique $\boldsymbol{x}^{\boldsymbol{a}+\boldsymbol{c}} \preceq \boldsymbol{x}^{\boldsymbol{b}+\boldsymbol{c}}$.

Il y a plusieurs ordres de ce genre. Un exemple est l'ordre "Grlex", pour lequel $\boldsymbol{x}^{\boldsymbol{a}} \preceq \boldsymbol{x}^{\boldsymbol{b}}$ si et seulement si $|\boldsymbol{a}| < |\boldsymbol{b}|$, ou $|\boldsymbol{a}| = |\boldsymbol{b}|$ et le premier coefficient non nul de $\boldsymbol{b} - \boldsymbol{a}$ est positif. On écrit $x_{\boldsymbol{b}} \prec x_{\boldsymbol{a}}$ si $x_{\boldsymbol{b}}$ est **strictement plus petit** que $x_{\boldsymbol{a}}$ dans l'ordre "$\preceq$". Par exemple, si $k = 2$, on a

$$1 \prec x_1 \prec x_2 \prec x_1^2 \prec x_1 x_2 \prec x_2^2 \prec x_1^3 \prec x_1^2 x_2 \prec x_1 x_2^2 \prec x_2^3 \prec \ldots$$

Pour un ordre monomial fixé, on présente les termes d'un polynôme dans l'ordre décroissant. Le **monôme dominant** d'un polynôme f est le plus grand qui apparaît avec un coefficient non nul dans f. Ainsi, le monôme dominant de

$$f = c_{\boldsymbol{a}}\, \boldsymbol{x}^{\boldsymbol{a}} + \sum_{x_{\boldsymbol{b}} < x_{\boldsymbol{a}}} c_{\boldsymbol{b}}\, \boldsymbol{x}^{\boldsymbol{b}},$$

avec $c_{\boldsymbol{a}} \neq 0$, est $\boldsymbol{x}^{\boldsymbol{a}}$. On écrit alors $\mathrm{Dom}(f) := \boldsymbol{x}^{\boldsymbol{a}}$.

4. Paul Albert Gordan (1837–1912)
5. Voir l'article de Sturmfels dans les Notices de l'AMS, novembre 2005.

3.6 (∗) L'anneau des polynômes symétriques

Soit $\mathbb{K}$ un corps commutatif[6]. On désigne par $\mathcal{R}$ l'anneau des polynômes $\mathbb{K}[\boldsymbol{x}]$ en les n variables $\boldsymbol{x} = x_1, x_2, \ldots, x_n$, à coefficients dans $\mathbb{K}$. Le sous-espace vectoriel de $\mathcal{R}$ engendré par les monômes $\boldsymbol{x}^{\boldsymbol{a}}$ de degré d, est dénoté $\mathcal{R}_d$. On dit que c'est la **composante homogène** de degré d de $\mathcal{R}$. On a la décomposition en somme directe

$$\mathcal{R} = \mathcal{R}_1 \oplus \mathcal{R}_1 \oplus \ldots \oplus \mathcal{R}_d \oplus \ldots$$

de l'espace vectoriel $\mathcal{R}$. On observe que $\mathcal{R}_k \mathcal{R}_j \subseteq \mathcal{R}_{k+j}$. On dit alors que $\mathcal{R}$ est un **anneau gradué** par le degré.

Pour σ une permutation dans le groupe $\mathbb{S}_n$, et $f(\mathbf{x}) \in \mathcal{R}$, on pose :

$$\sigma \cdot f(x_1, x_2, \ldots, x_n) := f(x_{\sigma_1}, x_{\sigma_2}, \ldots, x_{\sigma_n}).$$

Cette action du groupe symétrique respecte le degré, c.-à-d. $\sigma \cdot \mathcal{R}_d \subseteq \mathcal{R}_d$. Par exemple, pour $\sigma = 21354$, on a

$$\sigma \cdot (3\, x_2^3 x_4^2 x_5^6 - 2\, x_1^3 x_4^7 + 6\, x_3^2) = 3\, x_1^3 x_5^2 x_4^6 - 2\, x_2^3 x_5^7 + 6\, x_3^2 .$$

Un polynôme $f(\mathbf{x})$ est dit **symétrique**, si et seulement si $\sigma \cdot f(\mathbf{x}) = f(\mathbf{x})$, pour toute permutation σ dans $\mathbb{S}_n$. On désigne par $\Lambda = \Lambda_{\mathbb{K}}$ l'ensemble des polynômes symétriques à coefficients dans $\mathbb{K}$. C'est un sous-anneau de $\mathcal{R}$, puisque la somme et le produit de polynômes symétrique donne un polynôme symétrique. Chaque composante homogène d'un polynôme symétrique est forcément symétrique. Il s'ensuit que Λ est un sous-anneau gradué de $\mathcal{R}$:

$$\Lambda = \Lambda_0 \oplus \Lambda_1 \oplus \Lambda_2 \oplus \cdots \oplus \Lambda_d \oplus \cdots ,$$

où $\Lambda_d := \Lambda \cap \mathcal{R}_d$ désigne la composante homogène de degré d de Λ, constituée des polynômes homogènes symétriques de degré d.

Ainsi, les polynômes constants sont tous symétriques. Donc, $\{m_0(\boldsymbol{x})\}$, avec $m_0(\boldsymbol{x}) := 1$, forme une base Λ_0. Les seuls polynômes homogènes symétriques de degré $d = 1$ sont les polynômes

$$a\,(x_1 + x_2 + \ldots + x_n) \qquad \text{avec} \qquad a \in \mathbb{K}.$$

6. Ici supposé de caractéristique 0, pour faciliter certains calculs. Cependant, la majorité de la présentation s'étend au cas plus général d'un corps quelconque

Donc, l'ensemble $\{m_1(\boldsymbol{x})\}$, avec $m_1(\boldsymbol{x}) := x_1 + x_2 + \ldots + x_n$, forme une base de Λ_1. Les polynômes symétriques homogènes de degré $d = 2$, avec $n > 1$, sont les combinaisons linéaires des polynômes [7]

$$m_2(\boldsymbol{x}) := x_1^2 + x_2^2 + \ldots + x_n^2, \qquad \text{et}$$
$$m_{11}(\boldsymbol{x}) := x_1\,x_2 + x_1\,x_3 + \ldots + x_i\,x_j + \ldots x_{n-1}\,x_n,$$

où, dans la dernière somme, les termes correspondent au $i < j$. Plus généralement, on définit comme suit les **polynômes symétriques monomiaux**. Pour ce faire, convenons de dénoter $\lambda(\mathbf{a})$ la liste décroissante [8] des entrées (non nulles) d'un vecteur $\mathbf{a} \in \mathbb{N}^n$. Ainsi, $\lambda(5103450012) = 5543211$. On dit alors que $\lambda(\mathbf{a})$ est le **partage** sous-jacent au monôme $\mathbf{x}^{\mathbf{a}}$. Pour chaque partage $\mu = \mu_1\,\mu_2 \cdots \mu_\ell$ de d (c.-à-d. $d = |\mu| := \mu_1 + \mu_2 + \ldots + \mu_k$), on pose

$$m_\mu(\boldsymbol{x}) := \sum_{\lambda(\mathbf{a})=\mu} \boldsymbol{x}^{\boldsymbol{a}},$$

où la somme a lieu sur l'ensemble des permutations distinctes $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ du vecteur μ (complété par des 0 pour le rendre de longueur n). En particulier $m_\mu(\mathbf{x}) = 0$ si le nombre de parts de μ est supérieur à n, car la somme est vide. Il est clair que chaque m_μ est un polynôme homogène symétrique de degré $d = |\mu|$. On a, par exemple,

$$m_{32}(x_1, x_2, x_3, x_4) = x_1^3\,x_2^2 + x_1^3\,x_3^2 + x_1^3\,x_4^2 + x_1^2\,x_2^3 + x_1^2\,x_3^3 + x_1^2\,x_4^3 + x_2^3\,x_3^2 + x_2^3\,x_4^2 + x_2^2\,x_3^3 + x_2^2\,x_4^3 + x_3^3\,x_4^2 + x_3^2\,x_4^3$$

Tout polynôme symétrique $f(\mathbf{x})$ s'écrit comme combinaison linéaire de polynômes monomiaux. On a donc le résultat suivant

Proposition 3.14. *L'espace Λ_d, des polynômes symétriques homogènes de degré d, admet comme base la famille des polynômes symétriques monomiaux m_μ, avec μ variant dans l'ensemble des partages de d ayant au plus n parts.*

Preuve. Le seul élément qui reste à prouver est que cet ensemble est linéairement indépendant. Cela découle du théorème fondamental de l'algèbre. ∎

Lien entre racines et coefficients de polynômes.

L'étude des racines d'un polynôme, à une variable t, nécessite d'établir un lien explicite entre les coefficients $((-1)^k e_k$ du polynôme [9]

$$f(t) = t^n - e_1\,t^{n-1} + e_2\,t^{n-2} + \ldots + (-1)^n e_n, \qquad = (t - x_1)(t - x_2)\cdots(t - x_n)$$

et les racines x_i de ce polynôme. Ainsi, le polynôme $t^3 - e_1\,t^2 + e_2\,t - e_3$ a trois les racines x_1, x_2 et x_3, et on a

$$\begin{aligned} t^3 - e_1\,t^2 + e_2\,t - e_3 &= (t - x_1)(t - x_2)(t - x_3) \\ &= t^3 - (x_1 + x_2 + x_3)\,t^2 + (x_1\,x_2 + x_1\,x_3 + x_2\,x_3)\,t - x_1\,x_2\,x_3 \end{aligned}$$

7. **Attention** : Lorsque $n = 1$, on a que $m_{11}(\boldsymbol{x}) = 0$.

8. Nous allons souvent éviter les parenthèses et les virgules dans ce qui suit (avec des exemples qui ne font intervenir que les nombres de 0 à 9).

9. Les signes qui apparaissent ici vont faciliter la suite de la présentation. Ils n'enlèvent rien à la généralité.

avec $e_1 = x_1+x_2+x_3$, $e_2 = x_1x_2+x_1x_3+x_2x_3$ et $e_3 = x_1x_2x_3$. En général, si l'on considère les racines x_i de $f(t)$ comme des variables, les coefficients de $f(t)$ deviennent des polynômes en ces variables :

$$\begin{aligned} e_1(x_1,x_2,\dots,x_n) &= x_1 + x_2 + \dots + x_n \\ e_2(x_1,x_2,\dots,x_n) &= x_1x_2 + x_1x_3 + \dots + x_ix_j + \dots + x_{n-1}x_n \\ &\vdots \\ e_n(x_1,x_2,\dots,x_n) &= x_1x_2\cdots x_n \end{aligned}$$

Chacun de ces polynômes est symétrique. Ce sont les polynômes symétriques **élémentaires**

$$e_k(\boldsymbol{x}) := \sum_{i_1<i_2<\cdots<i_k} x_{i_1}x_{i_2}\cdots x_{i_k}. \tag{3.6.1}$$

Autrement dit $e_k(\boldsymbol{x}) = m_{\underbrace{11\cdots1}_{n-\text{fois}}}(\boldsymbol{x})$. Pour chaque partage μ de d, on pose ensuite $e_\mu := e_{\mu_1}e_{\mu_2}\cdots e_{\mu_\ell}$. Ainsi,

$$e_{3211} = e_3\,e_2\,e_1\,e_1.$$

Une des raisons fondamentales pour l'introduction de ces polynômes est que

Théorème 3.15 (Newton). *L'ensemble*

$$\{e_\mu \mid \mu \text{ partage de } d \text{ avec plus grande part } \le n\},$$

est une base[10] *de Λ_d. De manière équivalente, Tout polynôme symétrique en n variables s'exprime uniquement comme polynôme en les e_k, $1 \le k \le n$.*

Preuve. Aux fins de cette preuve, on ordonne lexicographiquement les termes des polynômes. On constate que le terme dominant[11] de e_μ est

$$\begin{aligned} e_\mu &= e_{\mu_1}e_{\mu_2}\cdots e_{\mu_\ell} \\ &= (x_1x_2\cdots x_{\mu_1} + \dots)\,(x_1x_2\cdots x_{\mu_2} + \dots)\cdots(x_1x_2\cdots x_{\mu_\ell} + \dots) \\ &= x_1^{\mu'_1}x_2^{\mu'_2}\cdots + \dots \\ &= \mathbf{x}^{\mu'} + \dots \end{aligned}$$

On a donc

$$e_\mu = m_{\mu'} + \dots$$

où les termes manquants font intervenir des polynômes monomiaux $m_{\nu'}$ pour lesquels $\nu > \mu$ dans l'ordre lexicographique. La matrice de passage entre les e_μ et les $m_{\mu'}$ est donc triangulaire supérieure, ce qui montre le résultat. ∎

10. Indirectement ce résultat fait appel au fait qu'il y a autant de partages de d en au plus n parts, qu'il y a de partages de d en parts toutes $\le n$.

11. Le premier dans l'ordre lexicographique.

Ainsi, on a

$$\begin{aligned}
e_{1111} &= m_4 + 4\,m_{31} + 6\,m_{22} + 12\,m_{211} + 24\,m_{1111}\\
e_{211} &= m_{31} + 2\,m_{22} + 5\,m_{211} + 12\,m_{1111}\\
e_{22} &= m_{22} + 2\,m_{211} + 6\,m_{1111}\\
e_{31} &= m_{21} + 4\,m_{1111}\\
e_4 &= m_{1111}
\end{aligned}$$

Un polynôme $f(t)$ à des facteurs multiples si et seulement si, il a des racines multiples (dans un sur-corps de $\mathbb{K}$ algébriquement clos). On peut tester cette propriété en calculant son **discriminant** :

$$\mathrm{Disc}(f(t)) := \prod_{i<j}(x_i - x_j)^2\,,$$

où les x_i sont les n racines de $f(t)$ (avec multiplicités). On observe que le discriminant est un polynôme symétrique (en les racines). Le théorème de Newton affirme que « tout polynôme symétrique en n variables s'exprime uniquement en termes de $e_1, e_2, \ldots, e_n$ ». Comme les valeurs des e_k sont données par les coefficients du polynôme. On peut donc calculer $\mathrm{Disc}(f(t))$ sans connaître les racines de $f(t)$ Ainsi, le discriminant de $f(t) = t^3 - e_1\,t^2 + e_2\,t - e_3$, est donné par la formule

$$\mathrm{Disc}(f) = -4\,e_1^3e_3 + e_1^2e_2^2 + 18\,e_1e_2e_3 - 4\,e_2^3 - 27\,e_3^2.$$

Autres bases de Λ_d.

D'autres bases de Λ_d permettent de faciliter la recherche de formules, comme par exemple celle du discriminant. Ainsi, on a les **sommes de puissances**

$$p_k := x_1^k + x_2^k + x_3^k + \ldots,$$

et on pose $p_\mu := \prod_i p_{\mu_i}$. On a la formule suivante [12]

$$\sum_{n=0}^{\infty} e_n\,t^n = \exp\left(\sum_{j\geq 1}(-1)^{j-1}\,p_j\,\frac{t^j}{j}\right), \tag{3.6.2}$$

qui contient une infinité d'identités, obtenues en comparant les coefficients de t^n de chaque terme (ils sont égaux). De cette façon, on peut aussi reformuler la définition des polynômes symétriques élémentaires sour la forme de l'identité

$$\sum_{n=0}^{\infty} e_n\,t^n = \prod_{m=1}^{\infty}(1 + x_i\,t). \tag{3.6.3}$$

On démontre alors l'identité (3.6.2) comme suit. Utilisant la formule classique

$$\log(1 + x\,t) = \sum_{j=1}^{\infty}(-1)^{j-1}x^j\,\frac{t^j}{j}, \tag{3.6.4}$$

12. Exprimé en termes de séries génératrices.

on réécrit le membre de droite de (3.6.3) de la façon suivante

$$\begin{aligned}\prod_{m=1}^{\infty}(1+x_i\,t) &= \prod \exp\left(\sum_{j=1}^{\infty}(-1)^{j-1}x_i^j\,\frac{t^j}{j}\right)\\ &= \exp\left(\sum_{i=1}^{\infty}\sum_{j=1}^{\infty}(-1)^{j-1}x_i^j\,\frac{t^j}{j}\right)\end{aligned}$$

On échange alors les sommations, dans cette dernière expression, pour obtenir

$$\prod_{m=1}^{\infty}(1+x_i\,t) = \exp\left(\sum_{j\geq 1}(-1)^{j-1}\,p_j\,\frac{t^j}{j}\right) \tag{3.6.5}$$

ce qui donne exactement la formule annoncée.

Comparant les coefficients de t^n dans (3.6.2), on obtient l'identité

$$e_n = \sum_{\mu\vdash n}(-1)^{n-\ell(\mu)}\,\frac{p_\mu}{z_\mu}, \tag{3.6.6}$$

où z_μ est donné par la formule :

$$z_\mu = 1^{d_1}\,d_1!\,2^{d_2}\,d_2!\cdots k^{d_k}\,d_k!, \tag{3.6.7}$$

pour $\mu = 1^{d_1}\,2^{d_2}\cdots k^{d_k}$. On peut donc écrire chaque e_λ en termes des p_μ (et inversement, puisque p_μ est symétrique). Par exemple,

$$\begin{aligned}
e_4 &= -\tfrac{1}{4}\,p_4 + \tfrac{1}{3}\,p_{31} + \tfrac{1}{8}\,p_{22} - \tfrac{1}{4}\,p_{211} + \tfrac{1}{24}\,p_{1111}\\
e_{31} &= \tfrac{1}{3}\,p_{31} - \tfrac{1}{2}\,p_{211} + \tfrac{1}{6}\,p_{1111}\\
e_{22} &= \tfrac{1}{4}\,p_{22} - \tfrac{1}{2}\,p_{211} + \tfrac{1}{4}\,p_{1111}\\
e_{211} &= -\tfrac{1}{2}\,p_{211} + \tfrac{1}{2}\,p_{1111}\\
e_{1111} &= {p_1}^4
\end{aligned}$$

On observe que cette matrice est triangulaire, ce qui est un phénomène général. On peut donc exprimer les polynômes somme de puissances en termes des polynômes élémentaires, et obtenir

$$p_k = \text{dét}\begin{vmatrix} e_1 & 1 & 0 & \dots & 0\\ 2\,e_2 & e_1 & 1 & \dots & 0\\ 3\,e_3 & e_2 & e_1 & \dots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ k\,e_k & e_{k-1} & e_{k-2} & \dots & e_1 \end{vmatrix} \tag{3.6.8}$$

Les polynômes de **Schur** [13] sont, de loin, celles qui interviennent de la façon la plus profonde dans les applications des polynômes symétriques. Elles ont été introduites par Schur de la façon suivante. Un polynôme $f(\mathbf{x})$ est dit **antisymétrique** si et seulement si on a

$$\sigma\cdot f(\mathbf{x}) = (-1)^{\ell(\sigma)}f(\mathbf{x}),$$

13. Issai Schur (1875–1941).

pour toute permutation σ dans $\mathbb{S}_n$. Pour se construire des exemples, on considère les déterminants de matrices

$$M_{\mathbf{a}} := \begin{pmatrix} x_1^{a_1} & x_1^{a_2} & \cdots & x_1^{a_n} \\ x_2^{a_1} & x_2^{a_2} & \cdots & x_2^{a_n} \\ \vdots & \vdots & \ddots & \vdots \\ x_n^{a_1} & x_n^{a_2} & \cdots & x_n^{a_n} \end{pmatrix} \tag{3.6.9}$$

pour des entiers a_i, qu'on peut supposer décroissants, c.-à-d. que $a_1 \geq a_2 \geq \ldots \geq a_n$. On dénote par $\Delta_{\mathbf{a}} = \Delta_{\mathbf{a}}(\mathbf{x})$ le déterminant de la matrice $M_{\mathbf{a}}$. Comme une permutation des variables correspond à une permutation des lignes de la matrice $M_{\mathbf{a}}$, les polynômes $\Delta_{\mathbf{a}}(\mathbf{x})$ sont antisymétriques pour tout $\mathbf{a} \in \mathbb{N}^n$. Bien entendu, $\Delta_{\mathbf{a}}$ n'est non nul que si les a_i sont deux-à-deux distincts, puisque sinon il y a deux colones égales dans la matrice.

Le cas particulier de $a_i = n - i$ donne le **déterminant de Vandermonde** $\Delta_n = \Delta_n(\mathbf{x})$. On montre (voir exercice) que ce polynôme se factorise tout simplement de la façon suivante

$$\Delta_n(\mathbf{x}) = \prod_{j>i} (x_j - x_i). \tag{3.6.10}$$

En particulier, on a que $\deg \Delta_n(\mathbf{x}) = \binom{n}{2}$. Pour tout le quotient $\Delta_{\mathbf{a}}$ est un polynôme symétrique. Pour un partage μ, on pose $a_i := \mu_i + (n-1)$, et le **polynôme de Schur** est alors défini comme

$$s_\mu(\mathbf{x}) := \frac{\Delta_{\mathbf{a}}(\mathbf{x})}{\Delta_n(\mathbf{x}}.$$

On a les expressions suivantes en termes des polynômes symétriques monomiales :

$$\begin{array}{lcccccccccc} s_{1111} & = & m_{1111} & & & & & & & & \\ s_{211} & = & 3\,m_{1111} & + & m_{211} & & & & & & \\ s_{22} & = & 2\,m_{1111} & + & m_{211} & + & m_{22} & & & & \\ s_{31} & = & 3\,m_{1111} & + & 2\,m_{211} & + & m_{22} & + & m_{31} & & \\ s_{31} & = & m_{1111} & + & m_{211} & + & m_{22} & + & m_{31} & + & m_4 \end{array}$$

En général, $s_\lambda = \sum_\lambda K_{\lambda\mu}\, m_\mu$, où les $K_{\lambda\mu}$ sont les nombres de **Kostka**[14] qui sont des entiers positifs.

14. Pour lesquels il existe une jolie formule combinatoire. Pour plus de détails, voir les notes de combinatoire algébrique de François Bergeron, ou le texte plus avancé : Symmetric functions and combinatorics.

3.7 Exercices du chapitre 3

Exercice 3.5 (**Caractéristique et dérivée formelle**). Soit $\mathcal{A}$ un anneau commutatif de caractéristique nulle et $f \in A[x]$. On écrit ici f' pour $D(f)$ (voir définition (2.4.1))

1) Montrer que $\deg(f') = \deg(P) - 1$.

2) Que constatez-vous pour le polynôme $f(x) = x^p \in \mathbb{F}_p[x]$? Qu'en déduisez-vous ?

Exercice 3.6 (**Décomposition d'un polynôme**).
Soit $\mathcal{A}$ un anneau commutatif intègre et $f \in A[x]$ un polynôme de degré $n \geq 1$. Montrer que :

1) f a au plus n racines dans $\mathcal{A}$.

2) si $\alpha_1, ..., \alpha_k$ sont les racines distinctes de P dans $\mathcal{A}$ et $m_1, ..., m_k$ leurs multiplicités respectives alors f se décompose comme :

$$f(X) = \prod_{i=1}^{k} (x - \alpha_i)^{m_i} Q(x)$$

où $Q(x) \in A[x]$ n'a aucune racine dans $\mathcal{A}$.

3) En déduire une majoration sur le nombre de racines de f dans $\mathcal{A}$.

4) Considérer ce qu'il se passe pour le polynôme $2x \in \mathbb{F}_2[x]$. Qu'en concluez-vous sur les hypothèses ?

5) Considérer ce qu'il se passe pour le polynôme $x^2 + 1 \in \mathbb{H}[x]$, où $\mathbb{H}$ est le corps des **quaternions** [15]. Qu'en concluez-vous sur les hypothèses ?

Exercice 3.7 (**Localiser les racines d'un polynôme**).
Soit $\mathcal{A}$ un anneau commutatif et $f(X) = \sum_{k=0}^{n} a_k x^k \in A[x]$ un polynôme non nul.

1) Soit a une racine non nulle de f. Montrer que $a \,|\, a_0$.

2) On suppose ici que $\mathcal{A}$ est factoriel. Soit a/b une racine de f dans $\mathrm{Frac}(\mathcal{A})$ le corps de fraction de $\mathcal{A}$, avec a et b premiers entre eux. Montrer alors que $a \,|\, a_0$ et $b \,|\, a_n$. Qu'en déduisez vous si le coefficient dominant de f est 1 ? Où avons-nous utilisé l'hypothèse de factorialité ?

3) Montrer que le polynôme $x^{12} + x^9 + 4x^8 - 2x^6 - 7x^3 + 2 \in \mathbb{Z}[x]$ n'a pas de racines dans $\mathbb{Q}$.

4) Décomposer le polynôme $2x^4 - 3x^3 + 4x^2 - 4x - 3 \in \mathbb{Z}[x]$ en produit d'irréductibles dans $\mathbb{Q}[x]$.

Exercice 3.8.

1) Soit $\mathcal{A}$ un anneau commutatif intègre et $f \in A[x]$ un polynôme unitaire de degré 3. Montrer que soit f est irréductible dans $\mathcal{A}[x]$, soit f a une racine dans $\mathcal{A}$.

2) Déterminer tous les polynômes irréductibles de degré 3 dans $\mathbb{F}_2[x]$.

Exercice 3.9 (**Formule pour le discriminant**).

1) Utilisant le fait le déterminant d'une matrice est égal à celui de la matrice transposée, montrer que le discriminant $\mathrm{Disc}(f)$ du polynôme $f(t) = (t - x_1)(t - x_2) \cdots (t - x_n)$ est donné la

15. Voir fr.wikipedia.org/wiki/Quaternion pour la définition.

formule

$$\begin{aligned}\mathrm{Disc}(f) &= \det\left(\begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{pmatrix}\begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{pmatrix}\right) \\ &= \det\begin{pmatrix} n & p_1 & p_2 & \dots & p_{n-1} \\ p_1 & p_2 & p_3 & \dots & p_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{n-1} & p_n & p_{n+1} & \dots & p_{2n-1} \end{pmatrix}\end{aligned}$$

2) Montrer que, pour $n = 3$, on obtient

$$\begin{aligned}D(f) &= \det\begin{pmatrix} 3 & p_1 & p_2 \\ p_1 & p_2 & p_3 \\ p_2 & p_3 & p_4 \end{pmatrix} \\ &= 3p_2p_4 + 2p_1p_2p_3 - p_2^3 - p_1^2p_4 - 3p_3^2\end{aligned}$$

3) Exploiter la formule (3.6.8), pour calculer $\mathrm{Disc}(f)$ en termes des coefficients de f.

Exercice 3.10 ((∗) **Radical d'un idéal**).
Soient $\mathcal{A}$ un anneau commutatif et I et J deux idéaux de $\mathcal{A}$. On appelle **radical** de I l'ensemble :

$$\sqrt{I} := \{x \in \mathcal{A} \mid \exists n \in \mathbb{N} \text{ avec } x^n \in I\}.$$

1) Montrer que $\sqrt{I}$ est un idéal de $\mathcal{A}$.
2) Montrer que $\sqrt{I} \subseteq I$.
3) Montrer que $\sqrt{I \cdot J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.
4) Montrer que $\sqrt{I} + \sqrt{J} \subseteq \sqrt{I + J}$.
5) Montrer que $\sqrt{\sqrt{I}} = \sqrt{I}$.
6) Montrer que $\sqrt{I^n} = \sqrt{I}$ où $n \in \mathbb{N}^*$
7) On pose $\mathcal{A} = \mathbb{Z}$ et $I = n\mathbb{Z}$. Calculer $\sqrt{I}$.
8) On dit qu'un idéal est **radical** si $\sqrt{I} = I$. Montrer que I est radical si et seulement si $\mathcal{A}/I$ est sans nilpotent. En déduire que si I est premier alors I est radical.
9) Montrer que $\sqrt{I}$ est le plus petit idéal contenant I.

Exercice 3.11. Soit $\mathcal{A}$ un anneau commutatif.
1) Montrer que pour tout $f \in A[x]$ on a $f(x) - x | f(f(x)) - x$ dans $\mathcal{A}[x]$ et décrire le quotient.
2) Soient $a, b \in \mathbb{N}^*$ tels que $a \,|\, b$. Montrer que $x^a - 1 \,|\, x^b - 1$ dans $\mathcal{A}[x]$ et décrire le quotient.
3) Soient $a, b \in \mathbb{N}^*$ tels que a ne divise pas b. Montrer que $x^a - 1$ ne divise par $x^b - 1$ dans $\mathcal{A}[x]$.
4) Soient $a, b \in \mathbb{N}^*$ et $d = \mathrm{pgdc}(a, b)$. Montrer que $x^d - 1 = \mathrm{pgdc}(x^a - 1, x^b - 1)$ et décrire une relation de Bézout explicite.
5) Soient $m, n, q \in \mathbb{N}^*$. Montrer que $x^{q^m} - x | x^{q^n} - x$ si et seulement si $m \,|, n$.

Exercice 3.12. **1)** Montrer que $x^4 + 1$ est irréductible dans $\mathbb{Q}[x]$. Décomposez le en facteurs irréductibles dans $\mathbb{R}[x]$.
2) Est-ce que $x^3 - 5x^2 + 1$ est irréductible dans $\mathbb{Q}[x]$?
3) Montrer que $x^2 + y^2 + 2x + 1$ est irréductible dans $\mathbb{R}[x, y]$ et réductible dans $\mathbb{C}[x, y]$.
4) Montrer que $x^2 + y^2$ et $x^2 + y$ sont irréductibles dans $\mathbb{R}[x, y]$.

5) Montrer que dans $\mathbb{C}[x,y]$ le polynôme x^2+y^2 est réductible tandis que x^2+y ne l'est pas.
6) Décomposer en facteurs irréductibles x^n-y^n et x^n+y^n dans $\mathbb{C}[x,y]$ et dans $\mathbb{R}[x,y]$.

Exercice 3.13. Trouver tous les polynômes de $\mathbb{C}[x]$ vérifiant la relation :

$$f(x^2) = f(x)f(x+1)$$

Exercice 3.14 ((∗) **Radical de Jacobson**)**.**
Soit $\mathcal{A}$ un anneau commutatif. On note $J(\mathcal{A})$ l'intersection de tous les idéaux maximaux de $\mathcal{A}$ et on l'appelle le **radical de Jacobson**. On note U l'ensemble des éléments x de $\mathcal{A}$ tels que $1+xa$ est inversible pour tout $a \in \mathcal{A}$. Montrer que $J(\mathcal{A}) = U$.

Exercice 3.15 (**Propriétés des anneaux noethériens**)**.** Montrer les propriétés suivantes :
1) Si $\mathcal{A}$ est noethérien et I est un idéal de $\mathcal{A}$ alors $\mathcal{A}/I$ est noethérien.
2) Si $\mathcal{A}$ est noethérien alors $A[x_1,...,x_n]$ est noethérien (c'est le théorème de Hilbert).
3) Si $\mathcal{A}$ est noethérien alors $A[[x]]$ l'est aussi.
4) Un anneau principal est noethérien.
5) Si k est un corps alors il est noethérien.
6) Soit $\mathcal{A}$ un anneau tel que $A[x]$ soit noethérien. Montrer que $\mathcal{A}$ est noethérien.

Exercice 3.16. Soit $\mathcal{A}$ un anneau commutatif. Montrer que $\mathbb{Z}[x,y]/(x^2+y^2)$ est noethérien et que $\mathcal{A}[x,y]/(xy-1)$ est principal.

Exercice 3.17 (**Anneau local**)**.** Soit $\mathcal{A}$ un anneau commutatif. On dit que $\mathcal{A}$ est un **anneau local** si $\mathcal{A}$ possède un seul idéal maximal $\mathfrak{m}$. On note traditionnellement un tel anneau par $(A,\mathfrak{m})$. Ces anneaux ont un rôle fondamental en géométrie algébrique, ils permettent de comprendre la nature des fonctions rationnelles au voisinage d'un point d'une variété algébrique. On appelle **corps résiduel** d'un anneau local le quotient $A/\mathfrak{m}$.
1) Soit I un idéal de $\mathcal{A}$ tel que $\mathcal{A}-I = \mathcal{A}^*$. Montrer que $(\mathcal{A},I)$ est local.
2) Soit $(\mathcal{A},\mathfrak{m})$ un anneau local. Montrer que les éléments de la forme $1+x$, où $x \in \mathfrak{m}$, sont inversibles.
3) Inversement soit $\mathcal{A}$ un anneau et $\mathfrak{m}$ un idéal maximal de $\mathcal{A}$ tel que $1+\mathfrak{m} \subset \mathcal{A}^*$. Montrer alors que $\mathfrak{m}$ est le seul idéal maximal de $\mathcal{A}$.
4) Montrer que $\mathcal{A}$ est local si et seulement si l'ensemble des éléments inversibles de $\mathcal{A}$ est un idéal de $\mathcal{A}$.
5) Quels sont les premiers anneaux locaux auxquels l'on pense ?
6) Soit p un nombre premier et $\mathbb{Z}_p = \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z}^*,\ p \text{ ne divise pas } b\}$.
i) Montrer que $\mathbb{Z}_p$ est un sous-anneau de $\mathbb{Q}$ qui contient $\mathbb{Z}$.
ii) Montrer que $\mathbb{Z}_p$ est un anneau local et calculer son unique idéal maximal $\mathfrak{m}$.
iii) Calculer le corps résiduel de $\mathbb{Z}_p$.
7) Soit $f : A \to B$ un homomorphisme d'anneaux locaux. Que peut-on dire de cet homomorphisme ?

Chapitre 4

Corps finis, et un peu de théorie de Galois

Evariste Galois

Introduction

Nous allons essentiellement voir dans ce chapitre qu'il est possible de caractériser et construire tous les corps finis. En résumé, la démarche est constituée des étapes suivantes.

- On souligne d'abord que, pour p premier, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ (avec sa structure d'anneau déjà vue) est le seul corps ayant p éléments (à isomorphisme près).
- On rappelle qu'un corps fini a nécessairement un nombre d'éléments égal à p^n, pour p premier et $n \geq 1$.
- On montre que les corps finis sont tous commutatifs (théorème de Wedderburn). Rappelons que ceci n'est pas nécessairement le cas pour les corps infinis.
- On étudie ensuite (rappel) une construction de corps finis, via le quotient de l'anneau des polynômes $\mathbb{F}_p[x]$ par un idéal $\langle f(x) \rangle$ engendré par un polynôme irréductible.
- On termine la démarche en montrant que ce sont là, toujours à isomorphisme près, les seuls corps commutatifs finis possibles. De plus, pour tout nombre premier p et tout $n \geq 1$, on montre qu'il y a un seul corps à p^n éléments.

Le chapitre se termine avec une introduction à la théorie de Galois, dans laquelle les corps jouent un rôle fondamental.

Exemple. Illustrons d'abord par un exemple le genre de mécanisme qui force l'unicité d'un corps commutatif ayant un nombre d'éléments donné. S'il existe un corps à 4 élément :

$$\mathbb{F}_4 := \{0, 1, a, b\},$$

comme la caractéristique de $\mathbb{F}_4$ est 2, on doit avoir $x + x = 0$ pour tout élément de $\mathbb{F}_4$. Observons aussi que, pour tout $y \in \mathbb{F}_4$ fixé, la fonction $x \mapsto x + y$ est une bijection de $\mathbb{F}_4$ vers $\mathbb{F}_4$. Autrement dit,

les lignes de la table d'addition (qui est symétrique, car l'addition est commutative) du corps sont donc des permutations de $\{0, 1, a, b\}$. Tout cela contraint cette table d'addition à être comme suit :

"+"	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

FIGURE 4.1 – Table d'addition de $\mathbb{F}_4$

La portion en bleu est forcée par les règles de calcul, et ne restent à déterminer que les valeurs en rouge. En effet, on a toujours $x \neq x+1$, d'où $a+1 = b$ et $a+b = 1$, puisque toutes les autres possibilités sont exclues.

Un raisonnement du même genre montre qu'il n'y a qu'une seule possibilité pour la table de multiplication. Encore une fois, pour y fixé, la fonction $x \mapsto x \cdot y$ est une bijection, et les seules valeurs à déterminer dans la table sont celles en rouge. Mais, on est forcé de choisir $ab = 1$, puisque le seul

"."	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

FIGURE 4.2 – Table de multiplication de $\mathbb{F}_4$

autre choix serait $ab = b$, ce qui est impossible, car autrement la loi de cancellation entraînerait $a = 1$. Tout le reste est alors uniquement déterminé. ∎

4.1 Cardinal des corps finis

Rappelons qu'on désigne par $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$. De fait, la proposition suivante montre que c'est le "seul" corps ayant p éléments à isomorphisme près.

Proposition 4.1. *La caractéristique d'un corps fini $\mathbb{K}$ est un nombre premier p et $\mathbb{K}$ contient un sous-corps isomorphe à $\mathcal{F}_p$, son sous-corps premier.*

Preuve. Rappelons que cette caractéristique est l'entier p tel que $p\mathbb{Z}$ soit le noyau de l'homomorphisme

$$\mathbb{Z} \longrightarrow \mathbb{K}, \qquad n \mapsto n \cdot 1_{\mathbb{K}}.$$

Comme $\mathbb{K}$ est fini, cet homomorphisme n'est pas injectif, donc $p \neq 0$, Par le théorème 1.20, $\mathbb{Z}/p\mathbb{Z}$ s'injecte dans $\mathbb{K}$. Il s'ensuit que $\mathbb{Z}/p\mathbb{Z}$ est intègre, et donc que p est premier (voir proposition 1.27). En particulier, $\mathbb{F}_p$ s'injecte dans $\mathbb{K}$. ∎

Proposition 4.2. *Soit $\mathbb{K}$ un corps, et $\mathbb{F}$ un sous-corps commutatif. Alors $\mathbb{K}$ est un espace vectoriel sur $\mathbb{F}$, de manière naturelle*

Preuve. On considère les éléments α de $\mathbb{F}$ comme des scalaires, et les éléments v de $\mathbb{K}$ comme des vecteurs. L'addition dans $\mathbb{K}$ comme corps est aussi l'addition dans $\mathbb{K}$ comme espace vectoriel, et le produit par des scalaires est la restriction de la multiplication dans $\mathbb{K}$ (ce qui a un sens, puisque que $\mathbb{F}$ est un sous-corps). La commutativité de $\mathbb{F}$ assure qu'on a sans problème les propriétés usuelles de la multiplication par des scalaires. On peut alors identifier $\mathbb{F}$ au sous-espace vectoriel (de dimension 1) :

$$\mathbb{F} = \{\alpha \cdot 1 \mid \alpha \in \mathbb{F}\},$$

où le vecteur 1 est l'élément neutre multiplicatif de $\mathbb{K}$, et donc aussi de $\mathbb{F}$. Si $\mathbb{K}$ est de dimension finie (disons n) sur $\mathbb{F}$, alors on peut choisir une base $\{v_1, v_2, \ldots, v_n\}$ de $\mathbb{K}$ de façon à ce que $v_1 = 1$. ■

Corollaire 4.3. *Soit $\mathbb{K}$ un corps fini de caractéristique p. Alors, il existe $n \in \mathbb{N}$ tel que $|\mathbb{K}| = p^n$.*

Preuve. Cela découle simplement du fait que la dimension $\dim_{\mathbb{F}_p}(\mathbb{K})$ est forcément finie, puisque $\mathbb{K}$ l'est. Pour $n := \dim_{\mathbb{F}_p}(\mathbb{K})$, il est clair que le cardinal de $\mathbb{K}$ est p^n, puisque ceci compte le nombre de combinaisons linéaires possibles

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n, \qquad \alpha_i \in \mathbb{F},$$

des éléments d'une base $\{v_1, v_2, \ldots, v_n\}$ de $\mathbb{K}$ (les coefficients variant librement comme scalaires parmi les p éléments de $\mathbb{F}_p$). Autrement dit, chaque α_i peut prendre p valeurs distinctes, et l'indépendance linéaire des v_i assure que tous ces choix donnent des vecteurs distincts deux à deux. ■

Pour se faire une idée de la suite de notre démarche, on considère le cas spécial suivant.

Exemple. Supposons que, pour $q = p^2$ avec p premier, on a un corps commutatif $\mathbb{F}_q$ à q-éléments. C'est un espace vectoriel de dimension 2 sur le corps $\mathbb{F}_p$, et il admet comme base l'ensemble $\{1, t\}$, pour un certain $t \in \mathbb{F}_q$, qui n'est pas un multiple entier[1] de 1, c.-à-d. $t \neq n \cdot 1$ pour tout $n \in \mathbb{N}$. Autrement dit, $t \in (\mathbb{F}_q \setminus \mathbb{F}_p)$. Alors, tous les éléments de $\mathbb{F}_q$ s'écrivent comme une combinaison linéaire de la forme $(n \cdot 1 + k \cdot t)$, avec des coefficients n et k dans $\mathbb{F}_p$, et cette écriture est unique. On écrit cette combinaison linéaire plus simplement comme $(n + k\,t)$. Ainsi, pour n_1, n_2, k_1, k_2 dans $\mathbb{F}_p$, on a

- $(n_1 + k_1\,t) = (n_2 + k_2\,t)$ ssi $(n_1 = n_2)$ et $(k_1 = k_2)$; et
- $(n_1 + k_1\,t) + (n_2 + k_2\,t) = (n_1 + n_2) + (k_1 + k_2)\,t$.

Pour calculer le produit de deux éléments de $\mathbb{F}_q$, il suffit de connaître l'unique combinaison linéaire qui correspond à t^2 :

$$t^2 = a\,t + b, \qquad \text{avec} \qquad a, b \in \mathbb{F}_p.$$

En effet, on a alors la "règle de multiplication" :

$$\begin{aligned}(n_1\,t + k_1) \cdot (n_2\,t + k_2) &= n_1\,n_2\,t^2 + (n_1\,k_2 + n_2\,k_1)\,t + (k_1\,k_2) \\ &= (a\,n_1\,n_2 + k_1\,k_2)\,t + (b\,n_1\,n_2 + n_1\,k_2 + n_2\,k_1). \qquad (4.1.1)\end{aligned}$$

Il est utile d'observer que, dans l'anneau de polynômes $\mathbb{F}_p[x]$ (qui est euclidien et intègre), on a que

(1) le polynôme $f(x) = x^2 - a\,x - b$ est irréductible dans $\mathbb{F}_p[x]$;

1. Rappelons que, pour $k \in \mathbb{N}$, on désigne par $k \cdot a = a + a + \ldots + a$ la somme de k copies de a.

(2) $\mathbb{F}_p[x]/\langle f(x)\rangle$ est donc un corps, de caractéristique p ;

(3) l'existence d'un corps à q éléments revient à montrer qu'il existe un polynôme irréductible de degré 2 dans $\mathbb{F}_p[x]$;

(4) les classes d'équivalences modulo $\langle f(x)\rangle$, dans $\mathbb{F}_p[x]$, contiennent un unique polynôme de degré 1 : donc de la forme $n + k\,x$, avec n et k dans $\mathbb{F}_p$;

(5) la fonction qui associe a chaque classe dans $\mathbb{F}_p[x]/\langle f(x)\rangle$ ce reste, donne un isomorphisme entre le corps $\mathbb{F}_p[x]/\langle f(x)\rangle$ et $\mathbb{F}_q$.

(6) il existe (au plus) un seul corps à $q = p^2$ éléments (à isomorphisme près). ∎

Questions 1. Pour chacun des items ci-dessus, justifier l'affirmation en question (l'item (5) demande plus de réflexion). Pour $p = 5$, et donc $q = 25$, expliciter ce que les items affirment. Ainsi, pour l'item (3), montrer que le polynôme $x^2 + x + 1$ est irréductible dans $\mathbb{F}_5[x]$ (suggestion : voir qu'il n'a pas de racine, et expliquer pourquoi cela suffit).

Défi. Montrer qu'il y a toujours au moins un polynôme irréductible de degré 2 dans $\mathbb{F}_p[x]$, de la forme $x^2 - a\,x - b$, en comparant le nombre de polynômes de cette forme et le nombre de polynômes réductibles de degré 2, à savoir les polynômes de la forme $(x-\alpha)(x-\beta)$ pour $\alpha, \beta \in \mathbb{F}_p$. ∎

Nous allons généraliser tout ceci dans la suite.

4.2 Théorème de Wedderburn [2]

Nous allons maintenant montrer que tout corps fini est commutatif. À la section suivante, nous donnerons une classification de tous ces corps. Donnons d'abord quelques notions en préparation.

Le **centre** d'un corps $\mathbb{K}$ est l'ensemble des éléments qui commutent avec tous les autres, c.-à-d.

$$Z(\mathbb{K}) := \{z \in \mathbb{K} \mid \forall x \in \mathbb{K},\ x\,z = z\,x\}.$$

On a les propriétés suivantes. On a une **action par conjugaison** du groupe [3] $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ sur $\mathbb{K}$, définie comme $x \mapsto yxy^{-1}$, pour $x \in \mathbb{K}$ et $y \in \mathbb{K}^*$. Pour cette action, le **centralisateur** $C(x)$ d'un élément $x \in \mathbb{K}$ est l'ensemble

$$C(x) := \{y \in \mathbb{K} \mid x\,y = y\,x\}.$$

Pour $x \in \mathbb{K}^*$ (on exclut donc ici simplement $x = 0$), une notion toute proche de celle-ci est la notion de **stabilisateur** $\mathrm{Stab}(x)$ de x dans le groupe $\mathbb{K}^*$, défini comme l'ensemble

$$\mathrm{Stab}(x) := \{y \in \mathbb{K}^* \mid y^{-1}\,x\,y = x\}.$$

(1) Un corps $\mathbb{K}$ est commutatif si et seulement si $Z(\mathbb{K}) = \mathbb{K}$.

(2) $Z(\mathbb{K})$ est un sous-corps (clairement commutatif) de $\mathbb{K}$.

(3) Pour tout $x \in \mathbb{K}$, le centralisateur $C(x)$ est un sous-corps de $\mathbb{K}$.

(4) Pour tout $x \in \mathbb{K}^*$, le centralisateur $\mathrm{Stab}(x)$ est égal à $C(x) \setminus \{0\}$ (dénoté $C(x)^*$), et c'est un sous-groupe de $\mathbb{K}^*$.

2. Joseph Wedderburn (1882-1948).
3. Voir l'annexe sur les groupes pour les notions considérées dans ce qui suit.

(5) $\mathbb{K}$ est un $Z(\mathbb{K})$-espace vectoriel [4], qui est évidemment de dimension finie si $\mathbb{K}$ est fini, et qu'on note n dans la suite.

(6) Si q est le cardinal de $Z(\mathbb{K})$, et n est la dimension de $\mathbb{K}$ (comme espace vectoriel sur $Z(\mathbb{K})$), alors le cardinal de $\mathbb{K}$ est q^n. Comme $\mathbb{K}$ est un corps, il est clair que le cardinal du groupe $\mathbb{K}^*$, des éléments inversibles de $\mathbb{K}$, est $q^n - 1$ (tous les éléments de $\mathbb{K}$ sauf 0).

(7) $Z(\mathbb{K}) \subseteq C(x) \subseteq \mathbb{K}$, d'où $C(x)$ est un sous-espace vectoriel (sur $Z(\mathbb{K})$) de $\mathbb{K}$, de dimension q^m pour $m \leq n$.

(8) $x \in Z(\mathbb{K})$ si et seulement si $C(x)^* = \mathbb{K}^*$ (ce qui équivaut à dire que $C(x) = \mathbb{K}$). Donc, si $x \notin Z(\mathbb{K})$, alors $C(x)$ est strictement inclus dans $\mathbb{K}$, et sa dimension m est alors strictement inférieure à n.

Questions 2. Montrez les assertions ci-dessus. ∎

Notre but est donc de démontrer que $Z(\mathbb{K}) = \mathbb{K}$, pour tout corps fini. On ne peut donc pas donner d'exemple de corps fini pour lequel $Z(\mathbb{K}) \neq \mathbb{K}$. On considère plutôt ici la notion de centre comme outils pour organiser la présentation de la preuve du théorème.

Théorème 4.4 (de Wedderburn)**.** *Tout corps fini est commutatif.*

Preuve. Soit $\mathbb{K}$ un corps fini, qu'on suppose par l'absurde non commutatif ; autrement dit, $Z(\mathbb{K}) \neq \mathbb{K}$ et $n > 1$. Avec les notations de la discussion qui précède l'énoncé du théorème, on observe que $x \in Z(\mathbb{K})$ si et seulement si $C(x)^* = \mathbb{K}^*$ (ce qui équivaut à dire que $C(x) = \mathbb{K}$). L'hypothèse est donc qu'il existe $x \notin Z(\mathbb{K})$, pour lequel $C(x)$ est strictement inclus dans $\mathbb{K}$, et donc sa dimension m est strictement inférieure à n.

Dans l'action de $\mathbb{K}^*$ sur lui-même par conjugaison, on a deux sortes d'orbites (on note l'orbite de x par $O(x)$) :

- $O(x)$ est un singleton, si et seulement si $x \in Z(\mathbb{K})$;
- les autres qui sont de cardinal $(q^n - 1)/(q^m - 1)$, pour $m < n$. On observe que le théorème de Lagrange assure que $q^m - 1$ divise $q^n - 1$. Le quotient est d'ailleurs le cardinal d'une orbite.

Il s'ensuit que l'équation aux classes (A.6) correspond à dire qu'il existe des entiers $n_1, \ldots, n_s$ tels que

$$q^n - 1 = (q-1) + \sum_{i=1}^{s} \frac{q^n - 1}{q^{n_i} - 1}. \qquad (*)$$

On montre alors (en exercice) que chacun des n_i divise n. Rappelons que la décomposition de $x^m - 1$ comme produit de polynômes cyclotomique (voir section 3.4) donne les expressions

$$q^n - 1 = \prod_{d \mid n} \varphi_d(q) \qquad \text{et} \qquad q^{n_i} - 1 = \prod_{d \mid n_i} \varphi_d(q).$$

Comme n_i divise n, on trouve

$$\frac{q^n - 1}{q^{n_i} - 1} = \prod_{d \mid n,\ d \nmid n_i} \varphi_d(q).$$

En particulier, comme $n_i < n$ et donc n ne divise pas n_i, on conclut que $\varphi_n(q)$ divise $(q^n - 1)/(q^{n_i} - 1)$, et il divise $q^n - 1$ bien sûr. L'équation $(*)$ entraîne alors que $\varphi_n(q)$ divise $q - 1$, ce qui est impossible (voir exercice 4.4). D'où le théorème. ∎

4. La multiplication de $x \in \mathbb{K}$ par un scalaire $z \in \mathbb{Z}(\mathbb{K})$ est simplement le produit dans $\mathbb{K}$.

4.3 Classification des corps finis

Le théorème 4.4 assure que tout corps fini est commutatif. En admettant quelques résultats de la théorie des extensions de corps [5], nous allons montrer (voir théorème 4.10) que : pour tout premier p et tout entier $n \geq 1$, il existe un et un seul corps de cardinal $q = p^n$. On le notera $\mathbb{F}_q$. Ce sont les seuls corps finis.

Attention, on ne démontrera pas le théorème suivant.

Théorème 4.5. *Soit $\mathbb{K}$ est un corps commutatif, et $f(x) \in \mathbb{K}[x]$. À isomorphisme près, il existe un et un seul sur-corps $\mathbb{L}$ de $\mathbb{K}$, tel que*

- *on a des éléments $\alpha_1, \ldots, \alpha_j$ dans $\mathbb{L}$, avec*

$$f(x) = \lambda \prod_{i=1}^{j} (x - \alpha_i), \qquad \text{et} \qquad \lambda \in \mathbb{K}$$

- *$\mathbb{L}$ est engendré par $\mathbb{K}$ et les éléments $\alpha_1, \ldots, \alpha_j$.*

On dit de $\mathbb{L}$ que c'est le **corps de décomposition** de $f(x)$.

Proposition 4.6. *Soit $\mathcal{A}$ un anneau commutatif de caractéristique p, avec p premier. Alors, pour $n \in \mathbb{N}$ et $q = p^n$, la fonction $a \mapsto a^q$ est un endomorphisme de $\mathcal{A}$.*

Preuve. D'après la proposition 1.33, on a l'endomorphisme F de $\mathcal{A}$, défini en posant $F(a) = a^p$. On observe que $a \mapsto a^q$ est simplement le composé F^n. ∎

Corollaire 4.7. *Si $\mathbb{K}$ est un corps fini (commutatif) à $q = p^n$ éléments, alors l'homomorphisme de Frobenius $F : \mathbb{K} \longrightarrow \mathbb{K}$ est un automorphisme [6] de $\mathbb{K}$. De plus, on a $F^n = \mathrm{Id}$.*

Preuve. L'endomorphisme F est injectif, car $\mathrm{Ker}(F) = \{a \mid a^p = 0\} = \{0\}$ puisque $\mathbb{K}$ est intègre. Or, une fonction injective d'un ensemble fini vers lui-même est forcément bijective. Comme $\mathbb{K}$ est un corps, le groupe $\mathbb{K}^*$ a $q - 1 = p^n - 1$ éléments. Par le théorème de Lagrange [7] on a donc $a^{q-1} = 1$, pour tout $a \in \mathbb{K}^*$. Il s'ensuit, en incluant le cas $a = 0$, que $a^q = a$ pour tout $a \in \mathbb{K}$. Autrement dit $F^n = \mathrm{Id}$. ∎

Corollaire 4.8. *Soit $\mathbb{K}$ est un corps fini à $q = p^n$ éléments. Alors, dans $\mathbb{K}[x]$ on a l'égalité des polynômes*

$$x^q - x = \prod_{a \in \mathbb{K}} (x - a).$$

Par exemple, dans le cas $\mathbb{K} = \mathbb{F}_p$, avec le calcul des coefficients modulo p on a

$$x^p - x \equiv x\,(x-1)\cdots(x-(p-1)) \mod p.$$

5. Cette théorie est au coeur de la théorie de Galois.
6. On observe que pour $\mathbb{K} = \mathbb{F}_p$, ceci est le petit théorème de Fermat.
7. En théorie des groupes, cela correspond à dire que l'ordre d'un élément d'un groupe fini divise toujours le nombre d'éléments du groupe. Voir Théorème de Lagrange.

Pour $\mathbb{F}_4$ (de caractéristique 2, et donc $1 = -1$) de l'exemple plus haut, avec les tables d'addition et de multiplication données, on calcule que

$$\begin{aligned} x(x-1)(x-a)(x-b) &= x(x-1)(x^2-(a+b)x+ab) \\ &= x(x-1)(x^2-x+1) \\ &= x(x^3-1) \\ &= x^4-1. \end{aligned}$$

Preuve. [du corollaire 4.8] Rappelons que, si $\mathbb{K}$ est un corps commutatif, et si $\alpha_1, \ldots, \alpha_n$ sont des racines distinctes de $f(x) \in \mathbb{K}[x]$, alors $(x-\alpha_1)\cdots(x-\alpha_n)$ divise $f(x)$. Le corollaire 4.7 équivaut à dire que tout $a \in \mathbb{K}$ est racine du polynôme $x^q - x$. Il s'ensuit que $\prod_{a\in\mathbb{K}}(x-a)$ divise $x^q - x$. Or, ces deux polynômes ont même degré et même coefficient dominant (celui de x^q). Ils sont donc égaux. ■

Proposition 4.9. *Soit $\mathbb{K}$ un corps commutatif, et G un endomorphisme de $\mathbb{K}$. Alors*

$$\mathbb{L} = \{a \in \mathbb{K} \mid G(a) = a\}$$

est un sous-corps de $\mathbb{K}$.

Preuve. À faire en exercice ci-dessous. ■

Questions 3. Dans ce qui suit (pour raison de clarté des formules), on écrit $\mathbb{Z}_p$ pour $\mathbb{Z}/p\mathbb{Z}$.

- Rappeler pourquoi, dans $\mathbb{Z}_p$, on $a^p = a$ pour tout $a \in \mathbb{Z}_p$.
- Soit p un nombre premier congru à 3 modulo 4. Rappeler pourquoi $\mathbb{Z}_p[i] = \{a + b\,i \,|\, a, b \in \mathbb{Z}_p\}$, avec $i^2 = -1$, est un corps de cardinal $q = p^2$, qui contient $\mathbb{Z}_p$ comme sous-corps.
- Avec $p = 7$, montrer que dans $\mathbb{Z}_p[i]$ on a

  $$(a+b\,i)^7 = a - b\,i$$

  en conclure que dans $\mathbb{Z}_7[i]$

  $$x^7 - x = \prod_{a\in\mathbb{Z}_7}(x-a), \qquad \text{et} \qquad x^{49} - x = \prod_{\alpha\in\mathbb{Z}_7[i]}(x-\alpha).$$

- Pouvez-vous généraliser pour tout nombre premier p congru à 3 modulo 4 ?
- Faut-il que p soit congru à 3 modulo 4 pour que ce qui précède fonctionne ? Expliquer pourquoi.
- Dans $\mathbb{Z}_7[i]$ montrer qu'il y a un élément de la forme $\rho = 1 + b\,i$, tel que

  $$\{\rho, \rho^2, \rho^3, \ldots, \rho^{48}\} = \{(c+d\,i) \,|\, c + d\,i \neq 0\}.$$

  Autrement dit, on a $\rho^j \neq \rho^k$ pour tout j, k distincts entre 1 et 48. Trouver un tel élément.
- Pouvez-vous généraliser pour tout nombre premier p congru à 3 modulo 4 ?
- Montrer la Proposition 4.9.

Théorème 4.10. *Pour tout nombre premier p, et tout entier $n \geq 1$, il existe un corps à $q = p^n$ éléments, qui est unique à isomorphisme près.*

Preuve.

Existence : On considère le polynôme $x^q - x \in \mathbb{F}_p[x]$. D'après le théorème 4.5, il existe un sur-corps $\mathbb{L}$ de $\mathbb{F}_p$, tel qu'on a des éléments $\alpha_1, \dots, \alpha_q$ dans $\mathbb{L}$, avec

$$x^q - x = \prod_{i=1}^{q} (x - \alpha_i),$$

et $\mathbb{L}$ est engendré par $\mathbb{F}_p$ et les éléments $\alpha_1, \dots, \alpha_q$. Définissons $\mathbb{E} = \{\alpha_1, \dots, \alpha_q\}$. Montrons que $\mathbb{E}$ est de cardinalité q, c'est-à-dire que les α_i sont distincts, en exploitant la proposition 2.12 pour voir que $x^q - x$ n'a pas de facteurs multiples. On constate en effet que

$$D(x^q - x) = q\, x^{q-1} - 1 \equiv -1 \mod p.$$

D'après la proposition 4.9 on obtient que $\mathbb{E} = \{\alpha \in \mathbb{L} \mid \alpha^q = \alpha\} = \{\alpha_1, \dots, \alpha_q\}$ est un sous-corps de $\mathbb{L}$, qui a q-éléments. On a donc montré l'existence.

Unicité : Soit $\mathbb{L}$ un corps à q éléments. Il contient $\mathbb{F}_p$ (les multiples de 1). D'après le corollaire 4.8, $x^q - x = \prod_{\alpha \in \mathbb{L}} (x - \alpha)$. Clairement $\mathbb{L}$ est engendré par $\mathbb{F}_p$ et les α. IL s'ensuit que $\mathbb{L}$ est unique à isomorphisme près de par le théorème 4.5. ∎

Nous allons maintenant montrer comment construire explicitement le corps $\mathbb{F}_q$ (toujours avec $q = p^n$), comme quotient de l'anneau $\mathbb{F}_p[x]$ par un polynôme irréductible de degré n, supposant qu'un tel polynôme existe (le choix de ce polynôme n'importe pas). Par exemple, le corps $\mathbb{F}_4$ du début de cette section est isomorphe à $\mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$. À cette fin, on débute par une caractérisation des sous-groupes finis de $\mathbb{K}^*$ pour un corps $\mathbb{K}$. Un exemple typique est celui des racines de l'unité (voir 3.4) dans $\mathbb{C}^*$.

Proposition 4.11. *Soit $\mathbb{K}$ un corps commutatif, et U un sous-groupe fini de $\mathbb{K}^*$. Alors U est cyclique.*

Preuve. Pour U un sous-groupe fini de $\mathbb{K}^*$, posons $U(p) := \{u \in U \mid \exists r \geq 0,\ u^{(p^r)} = 1\}$ pour p premier. C'est un sous-groupe de U. Montrons qu'il est cyclique. À cette fin, considérons $a \in U(p)$ d'ordre maximal, disons $q = p^s$. Le polynôme $x^q - 1 \in \mathbb{K}[x]$ admet les q racines $1, a, a^2 \dots a^{q-1}$, qui sont toutes dans $U(p)$. D'autre part, par définition de $U(p)$, tout élément b de $U(p)$ est d'ordre p^r avec $r \leq s$, car a est d'ordre maximal. Donc, b est racine de $x^q - 1$. Comme un polynôme de degré q a au plus q racines, $b = a^j$ pour un certain j, d'où $U(p) = \{1, a, a^2 \dots a^{q-1}\}$. On a donc que $U(p)$ est cyclique, et clairement isomorphe à $\mathbb{Z}/q\mathbb{Z}$.

Le théorème de décomposition des groupes commutatifs (abélien) fins comme produit de sous-groupes cycliques primaires[8] assure que

$$U \simeq \prod_p U(p),$$

où le produit est fini (car U l'est par hypothèse). Il découle alors que U est cyclique, puisque chaque $U(p) \simeq \mathbb{Z}/p^{s_p}\mathbb{Z}$ pour un certain entier s_p selon la première partie de cette preuve, et le théorème 2.18 montre que

$$\prod_p \mathbb{Z}/p^{s_p}\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z}, \qquad \text{avec} \qquad m = \prod_p p^{s_p}.$$

∎

8. Voir notes de théorie des groupes, thm 6.12.

Corollaire 4.12. *Si $\mathbb{K}$ est un corps fini, alors $\mathbb{K}^*$ est cyclique. Un générateur de $\mathbb{K}^*$ et alors appelé* **racine primitive** *de $\mathbb{K}^*$.*

Nos résultats des chapitres précédents assure le résultat suivant.

Proposition 4.13. *Soit $\mathbb{K}$ un corps commutatif. Pour tout polynôme $f(x)$, l'anneau $\mathcal{A} = \mathbb{K}[x]/\langle f(x)\rangle$ est un espace vectoriel de dimension $n = \deg(f)$, qui admet comme base l'ensemble $\{1, x, \ldots, x^{n-1}\}$. L'anneau $\mathcal{A}$ est un corps si et seulement si $f(x)$ est irréductible.*

Preuve. Essayer d'écrire une preuve est un bon exercice de synthèse. ∎

On est maintenant en mesure d'atteindre notre objectif de description explicite de $\mathbb{F}_q$.

Théorème 4.14. *Tout corps fini $\mathbb{K}$ de cardinal $q = p^n$ est isomorphe à $\mathbb{F}_p[x]/\langle f(x)\rangle$, pour $f(x)$ n'importe quel polynôme irréductible de degré n. Il existe toujours un tel polynôme irréductible.*

Preuve. D'après le corollaire 4.12, il existe un racine primitive α de $\mathbb{K}$. Soit $\varphi : \mathbb{F}_p[x] \longrightarrow \mathbb{K}$, la fonction qui envoie $g(x)$ sur $g(a)$. C'est un homomorphisme d'anneau (vérifier en exercice). Il est surjectif, car α est racine primitive, et donc tout $b \in \mathbb{K}^*$ s'exprime sous la forme $b = \alpha^k = \varphi(x^k)$, pour un certain k. Bien entendu 0 est aussi dans l'image, puisque c'est $\varphi(0)$. Son noyau $\mathrm{Ker}(\varphi) = \langle f\rangle$, pour un certain f, car $\mathbb{K}[x]$ est principal. D'où $\mathbb{K} \simeq \mathbb{F}_p[x]/\langle f\rangle$. La proposition 4.13 assure que $\dim_{\mathbb{F}_p}(\mathbb{K}) = \deg(f) = n$.

D'autre part, si $\mathbb{K} \simeq \mathbb{F}_p[x]/\langle g\rangle$ pour g irréductible de degré n, la proposition 4.13 donnant $\dim_{\mathbb{F}_p}(\mathbb{K}) = \deg(f) = n$, on a $|\mathbb{K}| = q$, et l'unicité découle du théorème 4.10. ∎

4.4 Un peu de théorie de Galois

Un des problèmes fondamentaux de la théorie de Galois est de comprendre la structure du groupe des automorphismes d'un corps, laissant fixe un sous-corps. Ce sont les **groupes de Galois**.

Soit $q = p^n$. On a vu que $\mathbb{F}_p$ est un sous-corps de $\mathbb{F}_q$. On a aussi vu que l'automorphisme de Frobenius, $F(a) := a^p$, est tel que $F^n = \mathrm{Id}$ sur $\mathbb{F}_q$. Enfin, la dimension de $\mathbb{F}_q$ sur $\mathbb{F}_p$ est n. D'autre part, il est clair que tout automorphisme φ de $\mathbb{F}_q$ **fixe** $\mathbb{F}_p$, c.-à-d. $\varphi(x) = x$ pour tout $x \in \mathbb{F}_p$. Nous allons déterminer quels sont tous les automorphismes de $\mathbb{F}_q$. D'abord un résultat auxiliaire.

Proposition 4.15. *Soit $f(x) \in \mathbb{F}_p[x]$ un polynôme irréductible de degré n. On suppose que α est une racine de $f(x)$ dans un sur-corps $\mathbb{K}$ de $\mathbb{F}_p$. Alors, dans $\mathbb{K}[x]$, on a*

$$f(x) = \prod_{0\le i\le n-1} (x - \alpha^{(p^i)}),$$

et les $\alpha^{(p^i)}$ sont distincts pour $0 \le i \le n-1$.

Preuve. Écrivons $f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_0$, avec les a_i dans $\mathbb{F}_p$ (par hypothèse). Si β est une racine de f, c'est donc qu'on a

$$\beta^n + a_1\beta^{n-1} + \ldots + a_{n-1}\beta + a_0 = 0. \qquad (*)$$

Comme $F(a) = a$ pour tout a dans $\mathbb{F}_p$, il en découle que $F(\beta)$ est aussi une racine de f, puisque l'image par F de $(*)$ est

$$F(\beta)^n + a_1 F(\beta)^{n-1} + \ldots + a_{n-1} F(\beta) + a_0 = 0.$$

Donc, $\alpha, F(\alpha), \ldots, F^{n-1}(\alpha)$ sont des racines de $f(x)$. Pour conclure, il suffit de vérifier qu'elles sont distinctes. Si l'on a $F^i(\alpha) = F^j(\alpha)$, avec $0 \leq i \leq j \leq n-1$, c'est que $F^{j-i}(\alpha) = \alpha$. C'est donc dire que $\alpha^{(p^{j-i})} = \alpha$, avec $j - i < n$. Ainsi, α est racine du polynôme $x^{(p^{j-i})} - x$, et donc appartient au corps $\mathbb{F}_{p^{j-i}}$, d'après la preuve du théorème 4.10. On aurait alors, $\mathbb{F}_q = \mathbb{F}_p[\alpha] \subseteq \mathbb{F}_{p^{j-i}}$, ce qui n'est pas possible, car $q > p^{j-i}$. ■

Théorème 4.16. *Le groupe des automorphismes de $\mathbb{F}_q$ est constitué des n fonctions*

$$\{\mathrm{Id}, F, F^2, \ldots, F^{n-1}\}$$

avec la composition. Il est donc cyclique.

Preuve. Comme F est un automorphisme, toutes ses puissances le sont. Si l'on a $F^i = F^j$, avec $0 \leq i \leq j \leq n-1$, c'est que $F^{j-i} = \mathrm{Id}$. C'est donc dire que

$$a^{(p^{j-i})} = a, \qquad \text{pour tout } a \in \mathbb{F}_q,$$

avec $j - i < n$. Autrement dit, les q éléments de $\mathbb{F}_q$ sont des racines d'un polynôme de degré $p^{j-1} < q$, à savoir $x^{(p^{j-i})} - x$, ce qui est impossible. D'où le fait que les F^i, pour $0 \leq i \leq n-1$, sont tous distincts.

Maintenant, soit G un automorphisme de $\mathbb{F}_q$; et α une racine primitive de $\mathbb{F}_q$: α engendre le groupe $\mathbb{F}_q^*$. Il existe un polynôme irréductible $f(x) \in \mathbb{F}_p[x]$ de degré n, ayant α comme racine (voir la preuve du théorème 4.14). On a $G(a) = a$ pour tout a dans $\mathbb{F}_p$. Donc $G(\alpha)$ est une racine de $f(x)$. On en déduit de la proposition 4.15 l'existence de i, $0 \leq i \leq n-1$ tel que $G(\alpha) = F^i(\alpha)$. Or, pour $\beta \in \mathbb{F}_q^*$ quelconque, on a $\beta = \alpha^j$, et donc $G(\beta) = G(\alpha)^j = (F^i(\alpha))^j = F^i(\alpha^j) = F^i(\beta)$. Comme de plus, $G(0) = 0 = F^i(0)$, on conclut que $G = F^i$. ■

Théorème 4.17. *Soient $\mathbb{K}$ et $\mathbb{L}$ deux corps finis, tels que $\mathbb{K}$ soit un sous corps de $\mathbb{L}$. Alors il existe un nombre premier p, et des entiers $d, e \geq 1$, tels que $\mathbb{K} = \mathbb{F}_{p^d}$, $\mathbb{L} = \mathbb{F}_{p^e}$ et $d \mid e$. Inversement, si $d \mid e$, alors $\mathbb{F}_{p^d}$ est un sous-corps de $\mathbb{F}_{p^e}$, et*

$$\mathbb{F}_{p^d} = \{a \in \mathbb{F}_{p^e} \mid F^d(a) = a\}.$$

Preuve. En cours ■

Nous avons vu, à la proposition 4.15, que si $f(x) \in \mathbb{F}_p[x]$ est un polynôme irréductible de degré n. Alors, dans $\mathbb{F}_{p^n}$ il existe une racine α de $f(x)$ dans $\mathbb{F}_{p^n}$ telle que les racines de $f(x)$ soient

$$\alpha, F(\alpha), \ldots, F^{n-1}(\alpha)$$

et qu'elles sont distinctes.

Définition 32. Pour $q = p^n$, une **base normale** de $\mathbb{F}_q$ est de base (comme espace vectoriel sur $\mathbb{F}_p$) de $\mathbb{F}_q$ de la forme $a, F(a), \ldots, F^{n-1}(a)$.

Par exemple, il y a 2 polynômes irréductible de degré 3 sur $\mathbb{F}_2$: à savoir

$$x^3 + x + 1, \qquad \text{et} \qquad x^3 + x^2 + 1.$$

Soit a une racine du premier, et b une racine du second. Alors $\mathbb{F}_{2^3}$ est engendré par a et par b. Cependant,

$$\{a, F(a), F^2(a)\} = \{a, a^2, a^4\}$$

n'est pas une base normale, car $a^3 + a + 1$ implique $a^4 + a^2 + a = 0$; et donc $\{a, F(a), F^2(a)\}$ est linéairement dépendant. Par contre, on vérifie comme suit que $\{b, F(b), F^2(b)\} = \{b, b^2, b^4\}$ est bien une base de $\mathbb{F}_{2^3}$. En effet, on sait déjà que $\{1, b, b^2\}$ est une base de $\mathbb{F}_{2^3}$, Mais $b^3 + b^2 + 1 = 0$ implique que $b^3 = b^2 + 1$. On calcule alors que $b^4 = b^3 + b = b^2 + b + 1$, d'où $1 = b + b^2 + b^4$, ce qui montre que $\{b, b^2, b^4\}$ engendre le même espace que $\{1, b, b^2\}$, à savoir $\mathbb{F}_{2^3}$.

Nous avons l'objectif de montrer que $\mathbb{F}_q$ admet une base normale. À cette fin, montrons d'abord quelques résultats auxiliaires.

Lemme 4.18 (d'Artin)**.** *Soit $\mathbb{K}$ un corps commutatif, et $\psi_1, \ldots, \psi_m$ des automorphismes distincts de $\mathbb{K}$. Soient $a_1, \ldots, a_m$ dans $\mathbb{K}$, non tous nuls. Alors, il existe $a \in \mathbb{K}$ tel que*

$$a_1\psi_1(a) + \cdots + a_m\psi_m(a) \neq 0.$$

Preuve. Par récurrence sur m. Le cas $m = 1$ est clair. Supposons donc l'énoncé vrai pour $m - 1$. Si $a_1 = 0$, on est ramené au cas $m - 1$. On peut donc supposer $a_1 \neq 0$. Supposons que l'énoncé soit faux. Alors, pour tout $a \in \mathbb{K}$, on a

$$a_1\psi_1(a) + \cdots + a_m\psi_m(a) = 0. \qquad (*)$$

Comme $\psi_1 \neq \psi_m$, il existe $b \in \mathbb{K}^*$ tel que $\psi_1(b) \neq \psi_m(b)$. Alors, remplaçant a par ba dans $(*)$, on trouve

$$\begin{aligned} 0 &= a_1\psi_1(ba) + \cdots + a_m\psi_m(ba) \\ &= a_1\psi_1(b)\psi_1(a) + \cdots + a_m\psi_m(b)\psi_m(a) \end{aligned}$$

Multipliant par $\psi_m(b)^{-1}$ (qui est non nul car b non nul et ψ_m automorphisme), et posant $b_i = a_i\psi_i(b)\psi_m(b)^{-1}$, il 'ensuit qu'on a

$$b_1\psi_1(a) + \cdots + b_{m-1}\psi_{m-1}(a) + a_m\psi_m(a) = 0$$

Soustrayant ceci de $(*)$, on trouve

$$(a_1 - b_1)\psi_1(a) + \cdots + (a_{m-1} - b_{m-1})\psi_{m-1}(a) = 0, \qquad \text{avec} \qquad a_1 - b_1 \neq 0,$$

ce qui contredit l'hypothèse de récurrence. ∎

Nous utiliserons un résultat de l'algèbre linéaire, que nous ne démontrerons pas. Soit V un espace vectoriel de dimension finie, et T une transformation linéaire de V vers V ($T \in \mathrm{End}(V)$). Si le polynôme caractéristique de T est égal au polynôme minimal de T, alors il existe un vecteur v tel que V admet comme base l'ensemble

$$\{v, T(v), T^2(v), \ldots, T^{n-1}(v)\},$$

où $n = \dim(V)$.

Théorème 4.19. *Pour tout $q = p^n$, $\mathbb{F}_q$ admet une base normale.*

Preuve. Considérons l'automorphisme de Frobenius F de $\mathbb{F}_q$. Il est $\mathbb{F}_p$-linéaire, car $F(a) = a$ pour tout $a \in \mathbb{F}_p$. On considère le $\mathbb{F}_p$-espace vectoriel $\mathbb{F}_q$, et son automorphisme (d'espace vectoriel) F.

On a $F^n = \mathrm{Id}$. Donc le polynôme minimal de F divise $x^n - 1$. Les automorphismes $\mathrm{Id}, F, \ldots, F^{n-1}$ sont distincts. D'après le lemme d'Artin, ils sont linéairement indépendants. Donc le polynôme minimal est de degré au moins n. Par suite, c'est $x^n - 1$.

Or le polynôme caractéristique est de degré n. Comme il a pour diviseur le polynôme minimal, les deux polynômes coïncident.

D'après le résultat d'algèbre linéaire ci-dessus, il existe $a \in \mathbb{F}_q$ tel que $a, F(a), \ldots, F^{n-1}(a)$ est une base de $\mathbb{F}_q$. ■

4.5 Exercices du chapitre 4

Exercice 4.1. Pour $\mathbb{K}$ un corps, et $\psi : \mathbb{K} \longrightarrow \mathbb{K}$ un de ses automorphismes, montrer que

$$\mathrm{fix}(\psi) := \{x \in \mathbb{K} \mid \psi(x) = x\}$$

est un sous-corps de $\mathbb{K}$.

Exercice 4.2. Soit $\mathbb{K}$ un corps et $y \in \mathbb{K}^*$ fixé. On considère la fonction $\psi : \mathbb{K} \longrightarrow \mathbb{K}$ telle que $x \mapsto y\,x\,y^{-1}$.

1) Montrer que ψ est un automorphisme de $\mathbb{K}$, et déterminer l'automorphisme inverse.
2) Montrer que $\mathrm{fix}(\psi)$ est égal au centralisateur $C(y)$ de y.
2) Déduire que $C(y)$ est un sous-corps de $\mathbb{K}$.

Exercice 4.3. Pour tout corps $\mathbb{K}$, montrer que

$$Z(\mathbb{K}) = \bigcap_{x \in \mathbb{K}} C(x).$$

Exercice 4.4. Soit $q > 1$ et $n > 1$. Montrer que $\varphi_n(q)$ divise $q-1$ est impossible, car $|\varphi_n(q)-1| > |q-1|$. Exploiter le fait que

$$\varphi_n(q) = \prod_{\omega} (q - \omega),$$

où ω est une racine primitive n^{e} de l'unité, avec le fait que $|q - \omega| > |q - 1|$.

Exercice 4.5. Soit $f : \mathcal{A} \longrightarrow \mathcal{B}$ un homomorphisme d'anneau

1) Si $a \in \mathcal{A}$ est inversible, montrer que $f(a)$ est inversible. En particulier $f(a) \neq 0$.
2) Montrer que $\mathrm{Ker}(f) \cap \mathcal{A}^* = \varnothing$.

Exercice 4.6. Pour q^{12} avec p premier, énumérer les sous-corps de $\mathbb{F}_q$ à isomorphisme près.

Exercice 4.7.

1) Imiter la démonstration d'Euclide de l'infinitude des nombres premiers pour montrer que si $\mathbb{K}$ est un corps, alors il existe une infinité de polynômes irréductibles dans $\mathbb{K}[x]$.
2) Déduire que tout corps algébriquement clos est infini.

Exercice 4.8. Soit a racine carrée de 2. Montrer que $\mathbb{Q}[a]$ est le corps de décomposition de $x^2 - 2$ sur $\mathbb{Q}$.

Exercice 4.9. Soit b la racine cubique réelle de 2. Montrer que $\mathbb{Q}[b]$ n'est pas le corps de décomposition de $x^3 - 2$ sur $\mathbb{Q}$.

Exercice 4.10. Soit $z = exp(2i\pi/n)$. Montrer que $\mathbb{Q}[z]$ est le corps de décomposition de $x^n - 1$ sur $\mathbb{Q}$.

Exercice 4.11. Montrer que l'équation $\sqrt{3} = x + y\sqrt{2}$ n'a pas de solution dans $\mathbb{Q}$. En déduire que $\sqrt{3}$ n'est pas dans $\mathbb{Q}(\sqrt{2})$. En déduire que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, et que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. Montrer que $\{1,\ 2,\ 3,\ 6\}$ forment une base de $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ sur $\mathbb{Q}$.

Exercice 4.12.

1) Soit $\mathbb{K}$ un corps. Soit f un polynôme irréductible dans $\mathbb{K}[x]$, et g un polynôme non nul de degré inférieur à celui de f. En utilisant l'équation de Bézout pour les polynômes f et g, exprimer l'inverse de $g \mod f$ dans le corps $\mathbb{K}[x]/\langle f \rangle$ par un polynôme de degré inférieur à $\deg(f)$.

2) Appliquer l'exercice précédent pour exprimer l'inverse de la racine cubique de 2 comme combinaison $\mathbb{Q}$-linéaire de 1, $\sqrt[3]{2}$ et $\sqrt[3]{4}$.

Exercice 4.13. Soit $\mathbb{K}$ un corps et $\mathbb{L}/\mathbb{K}$ une extension de corps. Soient f et $g \in \mathbb{K}[x]$.

1) Montrer que $f \mid g$ dans $\mathbb{K}[x]$ si et seulement $f \mid g$ dans $\mathbb{L}[x]$.

2) Montrer que f et g ont le même pgcd dans $\mathbb{K}[x]$ et $\mathbb{L}[x]$.

Exercice 4.14.

1) Montrer que $x^2 + 1$ est irréductible dans $\mathbb{F}_3[x]$.

2) Montrer que $\mathbb{F}_3[x]/\langle x^2 + 1\rangle$ est isomorphe au corps $\mathbb{F}_9$, et que $a \equiv x \mod \langle x^2 + 1\rangle$ satisfait $a^2 + 1 = 0$.

3) Montrer que le a en question est tel que $a^3 = -a$, et en déduire que $\{a, a^3\}$ n'es pas un base normale de $\mathbb{F}_9$.

Exercice 4.15. Dans le corps $\mathbb{F}_{32}$, combien y a-t-il de racines primitives ?

Chapitre 5

Algèbres de Lie

$\mathbb{K}$ est un corps commutatif.

$\mathbb{K}$ algèbre (associative). Exemples : polynômes, matrices sur $\mathbb{K}$.

$\mathbb{K}$-algèbre de Lie : crochet de Lie, $[x,x]=0$, $[[x,y],z]+[[y,z],x]+[[z,x],y]=0$ (Jacobi).

Conséquences : anti-symétrie ;

Structure de Lie sur une algèbre associative.

Algèbre de Lie des matrices, de $\mathrm{End}(V)$ (V espace vectoriel), des matrices de trace nulle.

Sous-algèbre de Lie, idéaux, homomorphismes, dérivations.

Algèbre de Lie abéliennes = espace vectoriels.

Algèbre enveloppante d'une algèbre de Lie. Propriété universelle.

Théorème de Poincaré-Birkhoff-Witt.

Monoïde libre A^* engendré par l'alphabet A. Propriété universelle : pour toute fonction $f : A \to M$, où M est un monoïde, il existe un unique homomorphisme de monoïde du monoïde libre A^* vers M qui prolonge f.

K-algèbre des polynômes non commutatifs, base. Propriété universelle.

Algèbre de Lie libre, polynômes de Lie.

Etant donné un alphabet totalement ordonné A, on définit l'*ordre lexicographique* sur A^* de la manière suivante : $u < v$ si, soit u est un préfixe propre de v (c'est-à-dire $v = ux$, x mot non vide), soit $u = wau', v = wbv'$ pour certains mots w, u', v' et certaines lettres a, b satisfaisant $a < b$.

Mots de Lyndon : un *mot de Lyndon* est un mot w dans A^* tel que pour toute factorisation $w = uv$, avec u, v non vides, on a $w < vu$.

Mots primitifs et circulaires Un mot est dit *primitif* s'il n'est pas puissance d'un autre mot. De manière équivalente, si w est de longueur n, w est primitif si et seulement si $\{i \in \mathbb{Z} \mid C(w) = w\} = n\mathbb{Z}$, où C est défini dans l'exercice 5.5.

Dénombrement des mots de Lyndon. Théorème de factorisation de Lyndon.

Dénombrement des polynômes irréductibles sur un corps fini.

Base de Lyndon l'algèbre de Lie libre.

Exercice 5.1. Montrer que dans une algèbre de Lie, on a

$$[x,[y,z]] = [[x,y],z] - [[x,z],y].$$

Utiliser cette identité pour montrer que si une algèbre de Lie est engendrée par un sous-ensemble A, alors tout élément est combinaisons linéaire des éléments $[\dots[[a_1,a_2,],a_3],\dots,a_n]$, $a_i \in A$.

Exercice 5.2. Une *dérivation* d'une algèbre de Lie L est une application linéaire $D : L \to L$ telle que $L([x,y]) = [L(x),y)] + [x,L(y)]$ (formule de Leibniz, identique à celle des dérivations usuelles). La fonction $ad(x)$ dans une algèbre de Lie est définie par $ad(a)(x) = [a,x]$. Montrer que $ad(a)$ est une dérivation de L. Utiliser l'identité $[[x,y],z] = [[x,y],z] + [y,[x,z]]$, prouvée au préalable.

Montrer que la fonction $L \to \mathrm{End}(L)$ (la K-algèbre des endomorphismes $\mathbb{K}$-linéaires de L dans L, avec sa structure de Lie canonique), $a \mapsto ad(a)$, est un homomorphisme d'algèbre de Lie. Utiliser l'identité $[x,[y,z]] - [y,[x,z]] = [[x,y],z]$.

Exercice 5.3. On appelle *algèbre non associative* un espace vectoriel A muni d'une opération bilinéaire notée $(x,y) \mapsto xy$. Une dérivation est un endomorphisme D tel que $D(xy) = D(x)y + xD(y)$. Montrer que l'ensemble des dérivations de A est une sous-algèbre de Lie de $\mathrm{End}(A)$.

Exercice 5.4. Décrire l'homomorphisme de A^* dans N (additif) qui correspond par la propriété universelle à la fonction $f(a) = 1$, $\forall a \in A$. Faire de même avec la fonction $f(a) = \delta_{a,c}$, où c est une lettre fixée de A.

Exercice 5.5. Pour un mot $w = a_1 \cdots a_n$ de longueur n sur A, on note $C(w) = a_2 \cdots a_n a_1$. On fait agir le groupe cyclique $\mathbb{Z}$ sur l'ensemble A^n des mots de longueur n sur l'alphabet A par $i \cdot w = C^i(w)$, $i \in \mathbb{Z}$. Montrer que ceci est bien défini. On appelle période de w l'unique $p \in \mathbb{N}$ tel que le stabilisateur de w soit $p\mathbb{Z}$. Montrer que la période de w divise sa longueur. Montrer que tout mot w est de manière unique la puissance u^k d,un mot de longueur p = période de w, et que $p\times$ longueur de $u = n$.

Exercice 5.6. Dans l'algèbre des polynômes non commutatifs sur $\{a,b\}$, calculer $1 + (a+b-1)(2 + a+b+ab)(a+b-1)$.

Exercice 5.7. On considère l'application linéaire de $K < A >$ dans lui-même qui envoie tout mot $a_1 \cdots a_n$ sur la somme $\sum_{1 \le i \le n} a_1 \cdots a_{i-1} a_{i+1} \cdots a_n$. Montrer que c'est une dérivation de la K-algèbre des polynômes non commutatifs.

Exercice 5.8. Dans $\mathbb{K} < A >$, calculer $[a,[a,\dots,[a,b]\dots]]$ en utilisant les coefficients binomiaux.

Chapitre 6

Solutionnaire

1.1 Par division euclidienne de P par $X - a$, il existe $Q \in A[X]$ et $r \in A$ tels que

$$P(X) = (X - a)Q(X) + r.$$

En évaluant en $X = a$, on obtient

$$P(a) = r.$$

Donc

$$P(a) = 0 \iff r = 0 \iff X - a \text{ divise } P.$$

1.4

1. Si a est racine simple, on peut écrire

   $$P(X) = (X - a)Q(X)$$

   avec

   $$Q(a) \neq 0.$$

   Alors

   $$P'(X) = Q(X) + (X - a)Q'(X),$$

   donc

   $$P'(a) = Q(a) \neq 0.$$

   Réciproquement, si $P(a) = 0$, on écrit

   $$P(X) = (X - a)^m Q(X)$$

   avec $Q(a) \neq 0$. Alors

   $$P'(a) = 0$$

   si $m \geq 2$, et

   $$P'(a) = Q(a) \neq 0$$

   si $m = 1$. Donc a est simple si et seulement si $P'(a) \neq 0$.

2. Si
$$P(X) = (X-a)^m Q(X)$$
avec $Q(a) \neq 0$, alors chaque dérivée d'ordre $< m$ contient encore un facteur $(X-a)$, donc s'annule en a. En caractéristique nulle, la dérivée m-ième donne un terme principal
$$m!Q(a),$$
qui est non nul. Donc
$$P^{(m)}(a) \neq 0.$$

3. On a
$$P'(X) = 12X^{11}.$$
Une racine α de P vérifie
$$\alpha^{12} = 239,$$
donc $\alpha \neq 0$. Ainsi
$$P'(\alpha) = 12\alpha^{11} \neq 0.$$
Les racines sont donc simples.

4. En caractéristique 5,
$$P'(X) = 12X^{11} = 2X^{11}.$$
Si α est racine de P, alors $\alpha^{12} = 239$. Comme
$$239 \equiv 4 \pmod 5,$$
on a $\alpha \neq 0$. Donc
$$P'(\alpha) = 2\alpha^{11} \neq 0.$$
Les racines sont encore simples.

1.8

1. Si $0 \neq 1$, alors l'anneau contient au moins deux éléments distincts, donc $|A| \geq 2$. Réciproquement, si $0 = 1$, alors pour tout $a \in A$,
$$a = 1a = 0a = 0.$$
Donc $A = \{0\}$ et $|A| = 1$. Par contraposée, si $|A| \geq 2$, alors $0 \neq 1$.

2. Si xy est inversible, il existe $u \in A$ tel que
$$(xy)u = 1 \qquad \text{et} \qquad u(xy) = 1.$$
Alors
$$x(yu) = 1,$$
donc x est inversible à droite. De même,
$$(ux)y = 1,$$
donc y est inversible à gauche.

3. Soit a inversible. Supposons qu'il existe $b \neq 0$ tel que $ab = 0$. En multipliant à gauche par a^{-1}, on obtient
$$b = a^{-1}(ab) = a^{-1}0 = 0,$$
contradiction. De même, si $ba = 0$, en multipliant à droite par a^{-1}, on obtient $b = 0$, contradiction. Donc un élément inversible n'est pas diviseur de zéro.
Par contraposée, un diviseur de zéro ne peut pas être inversible.

1.9 Soient $m, n \in \mathbb{N}$ tels que $a^m = 0$ et $b^n = 0$.

1. Si A est commutatif, alors
$$(ab)^m = a^m b^m = 0.$$
Donc ab est nilpotent.
2. Si A est commutatif, on applique le binôme :
$$(a+b)^{m+n-1} = \sum_{k=0}^{m+n-1} \binom{m+n-1}{k} a^{m+n-1-k} b^k.$$
Dans chaque terme, soit $k \geq n$, alors $b^k = 0$, soit $k < n$, alors
$$m + n - 1 - k \geq m,$$
donc $a^{m+n-1-k} = 0$. Ainsi tous les termes sont nuls, d'où
$$(a+b)^{m+n-1} = 0.$$
Donc $a + b$ est nilpotent.
3. Si $a^m = 0$, alors
$$(1-a)(1 + a + a^2 + \cdots + a^{m-1}) = 1 - a^m = 1.$$
Comme l'anneau est commutatif, on a aussi l'égalité dans l'autre sens. Donc $1-a$ est inversible et son inverse est
$$1 + a + a^2 + \cdots + a^{m-1}.$$
4. Supposons $(ab)^n = 0$. Alors
$$(ba)^{n+1} = b(ab)^n a = 0.$$
Donc ba est nilpotent.

1.11

1. L'évaluation en 0 donne
$$A[X]/(X) \simeq A.$$
2. En quotientant par (X), on met $X = 0$, donc
$$A[X, Y]/(X) \simeq A[Y].$$
3. On met toutes les variables à 0, donc
$$A[X_1, \ldots, X_n]/(X_1, \ldots, X_n) \simeq A.$$

4. Le quotient
$$\mathbb{R}[X]/(X^2+1)$$
est isomorphe à $\mathbb{C}$.
5. On obtient
$$\mathbb{Z}[X]/(X^2-d) \simeq \mathbb{Z}[\sqrt{d}]$$
au sens où l'image de X joue le rôle de $\sqrt{d}$.
6. Comme X^2-2 est irréductible sur $\mathbb{Q}$,
$$\mathbb{Q}[X]/(X^2-2) \simeq \mathbb{Q}(\sqrt{2}).$$
7. On a déjà vu que
$$A[X,Y]/(XY-1) \simeq A[X,X^{-1}].$$

2.1

1. Les seuls diviseurs communs de 2 et X dans $\mathbb{Z}[X]$ sont les inversibles ± 1, donc ils sont premiers entre eux au sens de la divisibilité. En revanche, si
$$1 = 2P(X) + XQ(X),$$
en évaluant en $X = 0$ on obtiendrait
$$1 = 2P(0),$$
impossible dans $\mathbb{Z}$. Donc
$$1 \notin (2,X).$$
2. Si $(2,X)$ était principal, disons
$$(2,X) = (f),$$
alors f diviserait 2 et X. Donc f serait inversible puisque 2 et X sont premiers entre eux. Alors
$$(f) = \mathbb{Z}[X],$$
ce qui impliquerait $1 \in (2,X)$, contradiction. Donc $(2,X)$ n'est pas principal.
3. Si
$$(X,Y) = (f)$$
dans $A[X,Y]$, alors f divise X et Y. Dans un anneau polynomial, cela force f à être inversible, donc $(f) = A[X,Y]$, contradiction car $1 \notin (X,Y)$. Ainsi (X,Y) n'est pas principal.
4. On a
$$k[X,Y]/(X) \simeq k[Y]$$
par spécialisation $X \mapsto 0$. Comme $k[Y]$ est intègre, l'idéal (X) est premier.
5. On a
$$\mathbb{Z}[X,Y]/(2,X) \simeq (\mathbb{Z}/2\mathbb{Z})[Y],$$
qui est intègre mais pas un corps. Donc $(2,X)$ est premier, non maximal.
De même
$$\mathbb{Z}[X,Y]/(X,Y) \simeq \mathbb{Z},$$

qui est intègre mais pas un corps. Donc (X, Y) est premier, non maximal.
Enfin

$$\mathbb{Z}[X, Y]/(2, X, Y) \simeq \mathbb{Z}/2\mathbb{Z},$$

qui est un corps. Donc $(2, X, Y)$ est maximal, donc premier.

6. Considérons l'évaluation en a :

$$\varphi : A[X] \to A, \qquad P(X) \mapsto P(a).$$

C'est un morphisme d'anneaux surjectif, et son noyau est exactement l'idéal $(X - a)$. Le premier théorème d'isomorphisme donne donc

$$A[X]/(X - a) \simeq A.$$

2.3 Dans le quotient, on prend l'image i de x ; alors $i^2 = -1$.

3.3

i) ⇒ ii) Si un ensemble non vide d'idéaux n'admettait pas d'élément maximal, on pourrait construire par récurrence une chaîne strictement croissante infinie, contradiction.

ii) ⇒ iii) Soit I un idéal. Considérons l'ensemble des sous-idéaux de type fini de I. Il admet un élément maximal J. Si $J \neq I$, il existe $x \in I \setminus J$ et alors

$$J + (x)$$

est de type fini et contient strictement J, contradiction. Donc $I = J$ est de type fini.

iii) ⇒ i) (vu en cours) Soit

$$I_1 \subset I_2 \subset \cdots$$

une suite croissante. Posons

$$I = \bigcup_{n \geq 1} I_n.$$

C'est un idéal. Par hypothèse, il est de type fini, engendré par des éléments appartenant tous à un certain I_N. Alors

$$I = I_N,$$

donc la suite est stationnaire.

3.5

1. Écrivons

$$P(X) = a_n X^n + \cdots + a_0$$

avec $a_n \neq 0$ et $n \geq 1$. Alors

$$P'(X) = n a_n X^{n-1} + \cdots.$$

Comme A est de caractéristique nulle, l'élément $n \cdot 1_A$ est non nul, donc $n a_n \neq 0$. Ainsi

$$\deg(P') = n - 1 = \deg(P) - 1.$$

2. Dans $\mathbb{F}_p[X]$,

$$P'(X) = (X^p)' = p X^{p-1} = 0.$$

Donc un polynôme non constant peut avoir dérivée nulle en caractéristique positive. On en déduit que le résultat de **1)** est faux en général si la caractéristique n'est pas nulle.

3.12

1. Si X^4+1 était réductible dans $\mathbb{Q}[X]$, il se factoriserait en deux quadratiques. Écrivons
$$X^4+1=(X^2+aX+b)(X^2-aX+d).$$
En identifiant, on obtient
$$b+d-a^2=0, \qquad a(d-b)=0, \qquad bd=1.$$
On vérifie que cela n'a pas de solution rationnelle. Donc X^4+1 est irréductible dans $\mathbb{Q}[X]$. Dans $\mathbb{R}[X]$,
$$X^4+1=(X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1).$$
2. Par le critère des racines rationnelles, les seules racines rationnelles possibles sont ± 1. Or
$$P(1)=-3, \qquad P(-1)=-5.$$
Donc il n'a pas de racine rationnelle. Comme il est de degré 3, il est irréductible dans $\mathbb{Q}[X]$.
3. On a
$$X^2+Y^2+2X+1=(X+1)^2+Y^2.$$
Dans $\mathbb{R}[X,Y]$, cela ne se factorise pas car il faudrait une racine carrée réelle de -1. Dans $\mathbb{C}[X,Y]$,
$$(X+1)^2+Y^2=(X+1+iY)(X+1-iY),$$
donc c'est réductible.
4. Dans $\mathbb{R}[X,Y]$,
$$X^2+Y^2$$
ne peut pas se factoriser linéairement car il faudrait des coefficients complexes. Donc il est irréductible.
Pour
$$X^2+Y,$$
si ce polynôme se factorisait, ce serait en produit de deux polynômes de degré 1 en X :
$$(X+a)(X+b)=X^2+(a+b)X+ab.$$
Il faudrait alors $a+b=0$ et $ab=Y$, donc $a^2=-Y$, impossible dans $\mathbb{R}[Y]$. Donc X^2+Y est irréductible.
5. Dans $\mathbb{C}[X,Y]$,
$$X^2+Y^2=(X+iY)(X-iY),$$
donc il est réductible.
En revanche, X^2+Y reste irréductible : s'il se factorisait, on aurait encore
$$(X+a)(X+b)=X^2+(a+b)X+ab$$
avec $a,b\in\mathbb{C}[Y]$, ce qui imposerait $a+b=0$ et $ab=Y$, donc $a^2=-Y$, impossible dans $\mathbb{C}[Y]$.

6. Dans $\mathbb{C}[X,Y]$,
$$X^n - Y^n = \prod_{k=0}^{n-1}(X - \zeta_n^k Y),$$
où $\zeta_n = e^{2i\pi/n}$.
De même,
$$X^n + Y^n = \prod_{k=0}^{n-1}(X - \eta_k Y),$$
où les η_k sont les racines n-ièmes de -1.
Dans $\mathbb{R}[X,Y]$, on regroupe les facteurs complexes conjugués deux à deux pour obtenir des facteurs quadratiques irréductibles.

Bibliographie

[1] I. Assem et P.-Y. Leduc, *Cours d'algèbre : groupes, anneaux, modules, corps*, Montréal, Presses Internationales Polytechnique, 2009.

[2] A. Casamayou, N. Cohen, G. Connan, T. Dumont, L. Fousse, F. Maltey, M. Meulien, M. Mezzarobba, C. Pernet, N. M. Thiéry, et P. Zimmermann, *Calcul mathématique avec Sage*. Disponible sur le web : http ://sagebook.gforge.inria.fr.
C'est la référence pour apprendre à travailler avec Sage. En particulier, voir le chapitre 7, sur les anneaux polynômes, idéaux, quotients ; ainsi que le chapitre 9 sur les système d'équations polynomiales.

[3] F. Bergeron, *Introduction à la théorie des groupes*, 2015. Voir site web du cours.

[4] D. Dummit et R. Foote, *Abstract algebra*, John Wiley and Sons, 2004.
Un livre qui couvre un large spectre de l'algèbre, et donc adéquat pour plusieurs cours.

[5] F.M. Goodman, *Algebra : Abstract and Concrete*, Disponible sur le web.
En anglais, mais très bien présenté avec un point de vue original soulignant le rôle des symétries en mathématiques.

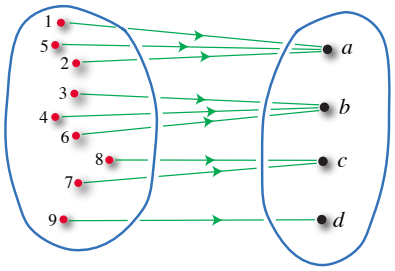
[6] T. Judson, *Abstract Algebra : Theory and Applications*, Disponible sur le web : abstract.ups.edu.
Recommandé par le American Institute of Mathematics. Contient des exemples d'utilisation de Sage.

[7] G. Birkoff et S. Maclane, *Algebra*, American Mathematical Society ; 3 edition, 1999.
C'est un des grands classiques, très ben écrit mais avec une approche qui s'adresse aux étudiants plus avancés.

[8] B. Sturmfels, *Solving Systems of Polynomial Equations*, accessible librement sur le web : math.berkeley.edu/ bernd/cbms.pdf.
Un peu plus avancé, mais contient des exemples explicites d'applications à des domaines comme les sciences économiques et les statistiques.

[9] B.L. van der Waerden, *Algebra : Volume I et 2*, Springer, 2003.
La version originale en allemand a été publiée en 1930. C'est le premier livre qui présente l'algèbre abstraite dans sa version moderne, et il a été d'une grande influence. Il vaut la peine d'y jeter un coup d'oeil. Voir le commentaire de Saunders Mac Lane dans les, *Notices of the American Mathematical Society*, 1997 : www.ams.org/notices/199703/maclane.pdf.

Rappels sur les ensembles et fonctions



La théorie des ensembles a été introduite par Georg Cantor (1845-1918). On peut en donner une axiomatique rigoureuse qui n'est pas discutée ici. Un **ensemble** est une collection d'objets. La théorie suppose que les ensembles contiennent des **éléments**, et on écrit $a \in A$ pour dire que « a est un élément de A » ou que « a appartient à A ». Si a n'est pas un élément de A, on écrit $a \notin A$ et on lit « a n'appartient pas à A » ou « a n'est pas dans A ». L'appartenance (ou pas) à un ensemble doit être claire. Autrement dit, cette appartenance ne doit pas être question de point de vue, on d'interprétation. Comme pour tout concept mathématique, il est important de bien comprendre quand deux ensembles sont égaux. La règle est toute simple (mais on l'oublie parfois) :

« Deux ensembles sont égaux si et seulement si ils ont les mêmes éléments. »

Autrement dit, pour « connaître » un ensemble il faut savoir dire quels en sont les éléments.

Deux façons typiques de décrire un ensemble consistent à : soit, donner la liste de tous ses éléments (quand il n'en contient pas trop), soit via la description d'une propriété qui caractérise ses éléments. L'écriture $E = \{x_1, x_2, ..., x_m\}$ signifie donc que E est composé des éléments $x_1, x_2, \ldots, x_m$; il peut y avoir des répétitions d'éléments : par exemple, $\{a, b, a\}$ représente le même ensemble que $\{a, b\}$. On a donc les présentations équivalentes

$$\{a, b, c\} = \{c, a, b\} = \{a, b, a, b, c, a, b, a\},$$

d'un même ensemble qui contient les trois éléments : a, b et c. L'ordre dans lequel on écrit les éléments n'importe pas : par exemple, $\{b, a\}$ représente le même ensemble que $\{a, b\}$. Fréquemment, on se donne une propriété P pour définir un ensemble. On écrit $A = \{x \in E \,|\, x \text{ possède } P\}$ pour dire que A est l'ensemble des éléments de E qui possèdent la propriété P. Pour montrer qu'un élément x de E est en fait dans A, il suffira donc de montrer que x a la propriété P.

Typiquement, on commence par considérer des ensembles de base comme

$$\begin{aligned}
\mathcal{A} &:= \{a, b, c, d, \ \ldots\ , z\},\\
\mathbb{N} &:= \{0, 1, 2, 3, \ \ldots\ \},\\
\mathbb{Z} &:= \{\ldots\ , -3, -2, -1, 0, 1, 2, 3, \ \ldots\ \},\\
\mathbb{Q} &:= \{\text{Frac}ab \mid a \in \mathbb{Z}, \quad b \in \mathbb{N}, \text{ et } b \neq 0\ \},\\
\mathbb{C} &:= \{x + i\,y \mid x, y \in \mathbb{R}\},
\end{aligned}$$

où $\mathbb{R}$ désigne l'ensemble ds **nombres réels**, ou encore des ensembles d'objets divers comme

$$\{\bullet, \bullet, \bullet\}, \qquad \text{ou} \qquad \{\clubsuit,\ \diamondsuit,\ \heartsuit,\ \spadesuit\}.$$

L'ensemble qui ne contient aucun élément est, par définition, l'ensemble **vide**, et on le représente par le symbole $\varnothing$. Un **singleton** est un ensemble à un élément. Si $a \neq b$, alors on dit de l'ensemble $\{a, b\}$ que c'est une **paire**. Rappelons que $\{a, b\} = \{b, a\}$, et que $\{a, a\} = \{a\}$ n'est pas une paire.

Remarque. Il a été historiquement bien établi que l'imprécision de la définition d'un ensemble peut engendrer des paradoxes (voir par exemple le paradoxe de Bertrand Russell (1872-1970) dans tout bon livre de logique). Pour éviter cela, nous ne travaillerons qu'avec un petit nombre d'ensembles bien étudiés et stables. Tous les ensembles considérés s'obtiennent à partir de l'ensemble vide et d'axiomes de construction d'ensembles.

Un ensemble E est **fini** si on peut écrire $E = \{x_1, \ldots, x_n\}$, avec $n \in \mathbb{N}$ fixé. Si les éléments x_i sont tous distincts, alors on dit que l'entier n est le **cardinal** de E et on le note : $n = |E|$. Par convention $|\varnothing| = 0$. Un ensemble E est **infini** s'il n'est pas fini. Par exemple, $\{1, 3, 6, 7, 8, 9, 10, 34\}$ est fini, mais $\mathbb{N}$ ne l'est pas. On dit que A est un **sous-ensemble** de E, si tous les éléments de A appartiennent à E. On dit aussi que A est **contenu** dans E et on écrit $A \subseteq E$. C'est la relation **d'inclusion**. Les ensembles $\varnothing$ et E sont des sous-ensembles particuliers de E. Tout autre sous-ensemble de E est un **sous-ensemble propre**. Si A n'est pas un sous-ensemble de E, on écrit $A \not\subseteq E$. Par exemple, on a $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. Ce qui signifie que $\mathbb{N} \subseteq \mathbb{Z}$, $\mathbb{Z} \subseteq \mathbb{Q}$, etc., mais aussi que $\mathbb{N} \subseteq \mathbb{Q}$. On dit que l'inclusion est **transitive**. Il est clair que tout sous-ensemble d'un ensemble fini est fini.

On note $\mathcal{P}(E)$ l'ensemble des sous-ensembles de l'ensemble E :

$$\mathcal{P}(E) = \{A \,|\, A \subseteq E\}.$$

Par exemple, pour $E = \{1, 2, 3\}$, on a $\mathcal{P}(E) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, E\}$. Si $|E| = n$, alors $|\mathcal{P}(E)| = 2^n$. Pour montrer qu'un ensemble A est inclus dans un ensemble E, on doit montrer qu'un élément quelconque de A est forcément aussi un élément de E. Autrement dit que : $x \in A \Rightarrow x \in E$. Montrer que $A = E$ équivaut à montrer que $A \subseteq E$ et $E \subseteq A$. La **différence** de deux ensembles A et B, notée $A \setminus B$, est l'ensemble défini par

$$A \setminus B = \{x \in A \,|\, x \notin B\}.$$

Si le contexte fait en sorte que l'ensemble E est clair, et si $A \subseteq E$, alors on écrit parfois $A^c := E \setminus A$. On dit que A^c est le **complément** de A (dans E). Dans le cas d'un ensemble de nombres positifs E, qui contient 0, on écrit souvent E^+ pour l'ensemble $E \setminus \{0\}$.

Deux **couples** (a, b) et (a', b') sont égaux, si et seulement si $a = a'$ et $b = b'$. On admet le cas $a = b$, pour obtenir le couple (a, a). Soulignons que l'ordre gauche droite est important, c.-à-d. $(a, b) \neq (b, a)$ sauf si $a = b$. Pour deux ensembles A et B, le **produit cartésien** de A et B est l'ensemble

$$A \times B = \{(a, b) \,|\, a \in A, b \in B\}.$$

On observe que $\varnothing \times E = E \times \varnothing = \varnothing$. En effet, il n'existe pas de couple (a, b) tel que $a \in E$ et $b \in \varnothing$. En général $A \times B \neq B \times A$. Le cardinal de $A \times B$ est le produit du cardinal de A et du cardinal de B. Par exemple, le plan cartésien est $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$. Pour $n \in \mathbb{N}$, et E est un ensemble, le produit cartésien n fois de E est l'ensemble défini par récurrence

$$E^n = E \times E^{n-1},$$

avec $E^0 := \{E\}$ (c'est un singleton, un ensemble à un seul élément), dont les éléments sont appelés **n-uplets**. On écrit d'habitude

$$x = (x_1, x_2, \ldots, x_n), \qquad \text{où} \qquad x_i \in E,$$

pour un élément de E^n, et alors l'unique élément de E^0 s'écrit $x = (\,)$. Il est facile de voir qu'il y a une bijection (naturelle) entre $E^n \times E^k$ et E^{n+k} ; mais, à strictement parler, ces deux ensembles ne sont pas « égaux ». En effet, les éléments du premier ensemble sont de la forme

$$((x_1, \ldots, k_k), (y_1, \ldots, y_n)),$$

tandis que ceux du deuxième sont de la forme (très similaire, mais différente)

$$(x_1, \ldots, k_k, y_1, \ldots, y_n).$$

Il est souvent « correct » de les identifier, mais il faut parfois faire attention. On peut donner un sens mathématique précis à au terme « naturel », mais intuitivement cela signifie que la notion s'impose. Pour tout ensemble E et tout singleton $\{\star\}$, on a aussi une bijection naturelle

$$\eta : E \longrightarrow E \times \{\star\}, \qquad \text{avec} \qquad \eta(x) := (x, \star).$$

L'union, de deux ensembles A et B, est l'ensemble formé de tous les éléments qui appartiennent à A **ou** à B (ou aux deux). On le note $A \cup B$, et donc

$$A \cup B := \{x \,|\, x \in A \text{ ou } x \in B\}.$$

L'intersection de deux ensembles A et B l'ensemble des éléments communs à A **et** B. On le note $A \cap B$ et donc

$$A \cap B = \{x \,|\, x \in A \text{ et } x \in B\}.$$

Pour tout A et B, on a l'inclusion $A \subseteq A \cup B$. De plus, $A \cap B$ est un sous-ensemble de A et de B. D'autre part, $A \cap B = A$ si et seulement si $A \subseteq B$. Si $A \cap B = \varnothing$, on dit que A et B sont **disjoints**. Si A et B sont disjoints, on écrit souvent $A + B$ pour l'union de A et de B. On dit que c'est **l'union disjointe**[1]. Les principales propriétés de ces opérations sur les suivantes sont les suivantes. Pour A, B, C des ensembles, alors

1. $A \cap A = A$ et $A \cup A = A$ (idempotence) ;
2. $A \cup B = B \cup A$ et $A \cap B = B \cap A$ (commutativité) ;
3. $A \cup \varnothing = A$ et $A \cap \varnothing = \varnothing$; et si $A \subseteq B$ alors $A \cup B = B$ et $A \cap B = A$ (existence d'éléments neutres).

Bien que ce soit l'une des notions les plus importantes des mathématiques, la définition rigoureuse moderne de la notion de fonction n'apparaît qu'au XIX$^{\text{e}}$(en 1837). Elle est due à Johann Dirichlet (1805-1859). Dans le langage de la théorie des ensembles, elle prend la forme suivante. Soit A et B deux ensembles. Une **fonction** f, de A vers B (on écrit $f : A \longrightarrow B$), est une règle qui associe à chaque élément de a un unique élément de B. Plus techniquement, f est un sous-ensemble de $A \times B$, et on écrit $f(a) = b$ si et seulement si le couple (a, b) appartient à ce sous-ensemble. Pour que f soit une fonction, il suffit que

1. On préfère ici la notation $A + B$ pour l'union disjointe de A et de B, plutôt que les notations $A \uplus B$ ou $A \uplus B$.

1. pour tout $a \in A$, il existe un b tel que $f(a) = b$, et
2. si $f(a) = b$ et $f(a) = c$, alors $b = c$.

Une fonction f de A vers B, est une **Fonction !bijection**, si on a une fonction **inverse** $f^{-1} : B \longrightarrow A$, pour la composition, c.-à-d. :

$$f^{-1} \circ f = \mathrm{Id}_A, \text{ et } f \circ f^{-1} = \mathrm{Id}_B. \tag{A.1}$$

Une fonction $f : A \longrightarrow B$ est injective si et seulement si, pour tout a et tout b dans A

$$a \neq b \qquad \Longrightarrow \qquad fa) \neq f(b), \tag{A.2}$$

ce qui équivaut (c'est la contraposée) à dire aussi que

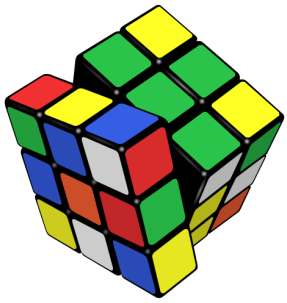
$$f(a) = f(b) \quad \text{entraine forcément} \quad b = b. \tag{A.3}$$

Une fonction $f : A \Rightarrow B$ est dite **surjective** si et seulement si pour chaque élément y de B, il existe au moins un élément x de A tel que $f(x) = y$. On montre qu'une fonction qui est à la fois surjective et injective est une fonction bijective, et inversement. Par définition [2], deux ensembles ont le même cardinal si et seulement si il existe une bijection entre les deux ensembles.

Pour A et B donnés, on désigne par B^A ou $\mathrm{Fonct}(A, B)$ **l'ensemble des fonctions** de A dans B.

2. La définition est nécessaire pour des ensembles infinis.

Rappels sur les groupes



Pour en savoir plus sur l'histoire du développement de la théorie des groupes, voir

- http ://mathshistory.st-andrews.ac.uk/HistTopics/Development_group_theory.html#41

Groupes quotients

Rappelons qu'un sous-groupe H d'un groupe G est dit normal si $xH = Hx$ pour tout $x \in G$. Soit N un sous-groupe normal d'un groupe G, alors on a une opération

$$G/N \times G/N \longrightarrow G/N \qquad \text{définie par} \qquad (x\,N)\cdot(y\,N) := (xy)\,N, \tag{A.4}$$

qui muni G/N d'une structure de groupe. Les éléments de G/N sont les classe latérales à gauches :

$$x\,N := \{x\,n \mid n \in N\}.$$

On obtient ainsi le groupe quotient de G par N. Son élément neutre est la classe à gauche $N = 1_G\,N$, et l'inverse de $x\,N$ est $(x\,N)^{-1} = x^{-1}N$. La fonction $\pi : G \to G/N$ définie en posant $\pi(x) = xN$ est un épimorphisme de groupes, et son noyau est $\ker(\pi) = N$.

Traduite dans le contexte des groupes abéliens, avec la notation additive, cette construction prend la forme suivante, sachant que tout sous-groupe d'un groupe abélien G est normal. Si H un sous-groupe d'un groupe abélien G, alors on a l'opération

$$G/H \times G/H \longrightarrow G/H \qquad \text{définie par} \qquad (x+H)+(y+H) := (x+y)+H, \tag{A.5}$$

qui muni G/H d'une structure de groupe abélien. Les éléments de G/H sont les classe latérales à gauches :

$$x + H := \{x + h \mid h \in H\}.$$

L'élément neutre est la classe à gauche $H = 0_G + H$, et l'inverse de $x + H$ est $-(x+H) = (-x+H)$.

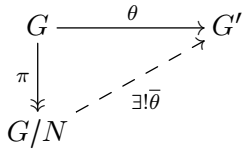
Le théorème d'isomorphisme pour les groupes affirme que : si G un groupe, et N un sous-groupe normal de G, alors pour tout morphisme de groupes $\theta : G \to G'$ tel que $N \subseteq \ker(\theta)$, il existe un unique morphisme $\overline{\theta} : G/N \to G'$ tel que $\theta = \overline{\theta} \circ \pi$. De plus

(1) si $N = \ker(\theta)$ alors $\overline{\theta}$ est un monomorphisme ;

(2) on a toujours $G/\ker(\theta) \simeq \mathrm{Im}(\theta)$;

(3) si θ est un épimorphisme, alors $\overline{\theta}$ l'est aussi.

En terme de diagramme commutatif, on a donc



La fonction $K \mapsto \pi(K)$ est une bijection de l'ensemble des sous-groupes de G contenant N vers l'ensemble des sous-groupes de G/N.

Pour deux groupes G_1 et G_2, le produit $G_1 \times G_2$ s'obtient en munissant l'ensembke

$$G_1 \times g_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}.$$

de l'opération

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 g_1', g_2 g_2').$$

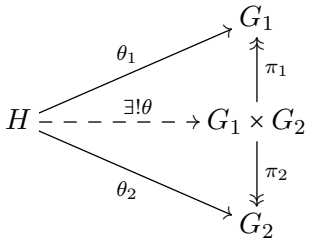
L'élément neutre est (e_1, e_2), avec e_i le neutre de G_i, et l'inverse

$$(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1}).$$

Ce produit est "caractérisé" par la propriété universelle suivante. Pour tout groupe H, et des morphismes $\theta_1 : H \to G_1$ et $\theta_2 : H \to G_2$, il existe un unique morphisme $\theta : H \to G_1 \times G_2$, tel que

$$\pi_1 \circ \theta = \theta_1, \qquad \text{et} \qquad \pi_2 \circ \theta = \theta_2.$$

On écrit alors $\theta = (\theta_1, \theta_2)$, puisque $f(h) = (\theta_1(h), \theta_2(h))$. Formulé en terme de diagramme commutatif, ceci prend la forme



Action de groupe

Une **action** (à gauche) d'un groupe G (multiplicatif) sur un ensemble X (on dit aussi que G **agit (à gauche)**) sur X), est une fonction

$$G \times X \longrightarrow X, \qquad (g, x) \mapsto g \cdot x,$$

telle que

- $1_G \cdot x = x$, pour tout $x \in X$,
- $g \cdot (h \cdot x) = (g\,h) \cdot x$, pour tout $g, h \in G$ et $x \in X$.

Pour un telle action, on appelle **stabilisateur** de $x \in X$ le sous-groupe

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

L'**orbite** $O(x)$ de $x \in X$, est l'ensemble

$$O(x) := \{g \cdot x \mid g \in G\}.$$

Si G est un groupe fini, alors on a

$$|O(x)| = |G|/|\mathrm{Stab}(x)|.$$

Rappelons que, pour un groupe fini, l'ordre d'un sous-groupe divise toujours l'ordre du groupe (Théorème de Lagrange). L'ensemble X est réunion disjointe des orbites. Si X et G sont finis, alors on a l'**équation aux classes**

$$|X| = \sum_{\omega \in \mathcal{O}} |G|/|\mathrm{Stab}(x_\omega)|, \tag{A.6}$$

où la somme a lieu sur l'ensemble $\mathcal{O}$ des orbites, et où x_ω est un représentant de l'orbite $\omega \in \mathcal{O}$.