DESS
Cryptologie, sécurité
et codage de l'information

CORPS FINIS ET COURBES ELLIPTIQUES

Module 2B

(15 Février 2024)

Emmanuel Peyre

Résumé. — Ce texte constitue une version préliminaire des notes d'un cours de mise à niveau en mathématiques délivré à Grenoble dans le cadre du DESS Cryptologie, sécurité et codage de l'information. Il se décompose en deux parties : la première est formée de rappels sur les corps finis, la seconde d'une brève introduction aux courbes elliptiques sur les corps finis.

Attention. — **Les bribes de codes données dans ce texte ont pour unique but d'illustrer le propos. Elles ne sauraient être utilisées telles quelles. D'autre part, plusieurs algorithmes donnés dans ce texte sont inspirés de [IEEE]. Pour plus de détails, le lecteur intéressé peut se reporter à cette référence.**

Emmanuel Peyre
Institut Fourier, UFR de Mathématiques, UMR 5582, Université de Grenoble I et CNRS, BP 74, 38402 Saint-Martin d'Hères CEDEX, France.
E-mail : `Emmanuel.Peyre@ujf-grenoble.fr`
Url : `http://www-fourier.ujf-grenoble.fr/~peyre/`

CONVENTION

Certaines parties de ce texte sont fournies comme compléments d'information et sont destinées à une seconde lecture. Ces parties sont en caractères plus fins et les titres y sont en caractères italiques.

Table des matières

Convention 2

Partie I. Corps finis 7

1. Les entiers 8
1.1. Divisibilité 8
1.2. pgcd et ppcm 8
1.3. Factorisation des entiers 11
1.4. Congruences 11
1.5. Relations d'équivalence et ensembles quotients 12
1.6. Entiers modulo n 13
Exercices 15

2. Les groupes 16
2.1. Structure de groupe 16
2.2. Sous-groupes 17
2.2.1. Définition 17
2.2.2. Exemples 18
2.2.3. Classes à gauches, à droites 18
2.3. Sous-groupes distingués, groupes quotient 19
2.4. Description des groupes abéliens finis 21
Exercices 25

3. Les anneaux et les corps 26
3.1. Structure d'anneau 26
3.2. Sous-anneaux, sous-corps 29
3.3. Idéaux et anneaux quotients 29
3.4. Divisibilité dans les anneaux 31
3.5. Anneau de polynômes, division euclidienne 32
3.6. Séries formelles 36
3.7. Anneau de polynômes à plusieurs variables 37
3.8. Anneau euclidien, anneau principal 38
3.9. Décomposition en facteurs irréductibles 40
3.10. Théorème des restes chinois 42
3.11. Retour sur les entiers 44

3.11.1. Éléments inversibles dans $\mathbf{Z}/n\mathbf{Z}$ 44
3.11.2. Application à la cryptographie : RSA 45
3.11.3. Le corps $\mathbf{F}_p$ 45
3.11.4. Caractéristique d'un corps, sous-corps premier 45
Exercices 46

4. Modules et espaces vectoriels 47
4.1. Notion de module 47
4.2. Sous-modules 48
4.3. Rappels sur les espaces vectoriels 48
4.4. Matrices de changement de bases 50
4.5. Transformée de Fourier discrète 50
4.6. Transformée de Fourier rapide 52

5. Extensions de corps 54
5.1. Polynômes et racines 54
5.2. Polynômes d'interpolation 55
5.3. Degré d'une extension 56
5.4. Corps de rupture 57
5.5. Premiers critères d'irréductibilité 58
5.6. Élément algébrique, extensions algébriques 58
5.7. Clôture algébrique 60
5.8. Corps de décomposition 61
Exercices 61

6. Structure des corps finis 62
6.1. Sous-groupe fini de $\mathbf{K}^\times$ 62
6.2. Les polynômes cyclotomiques 63
6.3. Frobenius 64
6.4. Structure des corps finis 65
6.5. Polynômes sur $\mathbf{F}_q$ 66
6.6. Carrés dans $\mathbf{F}_q^\times$ 68
6.7. Le cas des extensions de degré un nombre premier 70
6.8. Application à la cryptographie : El Gamal 73
Exercices 73

7. Algorithmes de factorisation 76
7.1. Éléments sans facteurs carrés 76
7.2. Stratégie de la factorisation 77
7.3. Factorisation sans facteur carré 78
7.4. Factorisation suivant les degrés 79
7.5. Factorisation finale de Cantor-Zassenhaus 80
7.6. Factorisation de Berlekamp 83

8. Bases 85
8.1. Base normale 85

8.2. Base normale gaussienne 86
8.3. Quelques algorithmes associés 87
Exercices 88

Partie II. Courbes elliptiques 89

9. L'espace projectif 90
9.1. Définitions 90
9.2. Cartes affines 91
9.3. Sous-ensembles algébriques 92
9.4. Topologie de Zariski 94
9.5. Equations homogènes et inhomogènes 94
9.6. Morphismes 96
Exercices 97

10. Courbes 98
10.1. Courbe plane 98
10.2. La lissité dans le cadre analytique 98
10.3. Courbe non-singulière 99
10.4. Équivalence birationnelle entre courbes 99
10.5. Notion de genre 99
10.6. Multiplicités d'intersection 101
Exercices 103

11. Courbes sur les corps finis 104
11.1. Le théorème de Chevalley-Warning 104
11.2. Fonction zêta d'une courbe 105
Exercices 106

12. Courbes elliptiques 107
12.1. Définition 107
12.2. Forme de Weierstrass 107
12.3. Loi de groupe sur une courbe elliptique 110
12.4. Expression explicite de la loi de groupe 111
Exercices 113

Appendices 115

Appendice A 116
A.1. Algorithmes de base 116
A.1.1. Calcul d'une puissance 116
A.1.3. Calcul du pgcd 117
A.1.4. Coefficients de Bezout 118
A.1.5. Détermination de l'ordre 118
A.2. Les polynômes 120
A.2.7. Définition de la classe 120

A.2.12. Division euclidienne des polynômes 125
A.3. Les quotients d'un anneau euclidien 128
A.3.17. Définition de la classe 128
A.3.21. Calcul de l'inverse 131
A.3.25. Exemples d'utilisation 132
A.3.26. Symbole de Legendre 132
Exercices 134
A.4. Polynômes sur $\mathbf{F}_2$ 135
A.4.1. Référence à une valeur booléenne 135
A.4.16. Polynômes sur $\mathbf{F}_2$ 143

Appendice B 149
B.1. Annales d'examen 149

Bibliographie 153

Glossaire 154

Index 155

PARTIE I

CORPS FINIS

CHAPITRE 1

LES ENTIERS

1.1. Divisibilité

Commençons par fixer quelques notations pour l'ensemble de ce texte.

Notations 1.1.1. — On notera $\mathbf{Z}$ l'ensemble des entiers relatifs, $\mathbf{N}$ l'ensemble des entiers positifs ou nuls, $\mathbf{Q}$ l'ensemble des nombres rationnels, $\mathbf{R}$ l'ensemble des nombres réels, et $\mathbf{C}$ l'ensemble des nombres complexes. Si X est un ensemble, on notera $\sharp X$ son cardinal. Si a est un nombre réel, on note $|a| = \sup(a, -a)$ sa valeur absolue.

Définition 1.1.2. — Si a et b sont deux entiers relatifs, on dit que a *divise* b et on note $a \mid b$ s'il existe un entier relatif c tel que $b = ac$. On dit également que b est un *multiple* de a ou que a est un *diviseur* de b. On note $a\mathbf{Z}$ l'ensemble des multiples de a.

Un nombre entier positif p est dit *premier* s'il est strictement supérieur à 1 et si ses seuls diviseurs positifs sont 1 et p. On notera $\mathscr{P}$ l'ensemble des nombres premiers.

Rappelons quelques propriétés de base de la divisibilité :

Proposition 1.1.3. — *Si a, b, c sont des entiers relatifs, on a*

(i) $a \mid a$,
(ii) *si* $a \mid b$ *et* $b \mid c$, *alors* $a \mid c$,
(iii) *si* $a \mid b$ *et* $a \mid c$, *alors* $a \mid b + c$.

Définition 1.1.4. — Si b est un entier relatif non nul et a un entier relatif, il existe une unique paire (q, r) d'entiers relatifs tels que $a = bq + r$ avec $0 \leqslant r < |b|$. L'entier q est appelé le quotient de a par b, et r le reste de la division, on le notera ici $a\%b$.

1.2. pgcd et ppcm

Définition 1.2.1. — Soit I un ensemble et $(a_i)_{i\in I}$ une famille d'entiers.

(i) On dit que $d \in \mathbf{N}$ est un pgcd de la famille $(a_i)_{i\in I}$ si

$$(\forall i \in I, d \mid a_i) \quad \text{et} \quad \forall r \in \mathbf{Z},\ (\forall i \in I, r \mid a_i) \Rightarrow r \mid d.$$

(ii) On dit que $m \in \mathbf{N}$ est un ppcm de la famille $(a_i)_{i\in I}$ si

$$(\forall i \in I, a_i \mid d) \quad \text{et} \quad \forall r \in \mathbf{Z},\ (\forall i \in I, a_i \mid m) \Rightarrow m \mid r.$$

Par abus de langage, on note $d = \mathrm{pgcd}_{i\in I}(a_i)$ et $m = \mathrm{ppcm}_{i\in I}(a_i)$. Si 1 est un pgcd de la famille $(a_i)_{i\in I}$, alors on dit que les entiers a_i sont premiers entre eux dans leur ensemble.

Remarque 1.2.2. — Si $I = \emptyset$, alors le pgcd vaut 0 et le ppcm vaut 1. Si $I = \{1\}$ et $a_1 \geqslant 0$, alors le pgcd et le ppcm coïncident avec a_1.

Nous montrerons dans le paragraphe 3.8 l'existence du pgcd et du ppcm pour une famille arbitraire dans tout anneau euclidien. Dans le cas où la famille est finie, l'existence du pgcd résulte directement de la proposition suivante :

Proposition 1.2.3. — *Soient $a_1, \ldots, a_m$ des entiers relatifs non tous nuls. Soit d le plus petit des entiers strictement positifs de la forme*

$$b_1 a_1 + \cdots + b_m a_m$$

avec $(b_1, \ldots, b_m) \in \mathbf{Z}^m$. Alors d est l'unique pgcd *positif de $(a_1, \ldots, a_m)$.*

Démonstration. — Notons I l'ensemble des entiers relatifs de la forme $b_1 a_1 + \cdots + b_m a_m$ avec $(b_1, \ldots, b_m) \in \mathbf{Z}^m$. L'ensemble I vérifie les deux propriétés suivantes :

$$\forall x, y \in I, \qquad x + y \in I,$$

et

$$\forall x \in I, \forall n \in \mathbf{Z}, \qquad nx \in I.$$

En outre $a_1, \ldots, a_m \in I$. Soit x un élément arbitraire de I, on effectue alors la division euclidienne de x par l'entier d défini dans l'énoncé de la proposition $x = dq + r$. Compte tenu des propriétés de I, $r = dq - x$ appartient à I. D'autre part $0 \leqslant r < d$. Par minimalité de d, $r = 0$ et $d \mid x$. Donc $d \mid a_i$ pour $i = 1, \ldots, n$. Si r divise chacun des a_i, alors r divise tous les élément de I, donc il divise d. L'entier d est donc bien un pgcd de la famille $(a_1, \ldots, a_m)$. Si d' est un autre pgcd positif, alors $d \mid d'$ et $d' \mid d$, d'où $d \leqslant d' \leqslant d$ et $d = d'$. □

Remarque 1.2.4. — Le lecteur assidu pourra comparer avec profit cette démonstration avec celle de la proposition 3.8.5.

Corollaire 1.2.5. — *Il existe $b_1, \ldots, b_m \in \mathbf{Z}$ tels que*

$$b_1 a_1 + \cdots + b_m a_m = \mathrm{pgcd}(a_1, \ldots, a_m).$$

Corollaire 1.2.6 (Théorème de Bezout). — *Si a et b sont deux entiers relatifs, alors a et b sont premiers entre eux si et seulement s'il existe des entiers relatifs u et v tels que*

$$au + bv = 1.$$

Démonstration. — Si a et b sont premiers entre eux, alors u et v existent par le corollaire précédent. Réciproquement, si $au + bv = 1$, alors

$$\mathrm{pgcd}(a, b) \mid au + bv = 1.$$

Donc $\mathrm{pgcd}(a, b) = 1$. □

Corollaire 1.2.7 (Lemme de Gauss). — *Soient a, b et c trois entiers. Si a est premier avec b et $a \mid bc$ alors $a \mid c$.*

Démonstration. — Par le théorème de Bezout, il existe des entiers u et v tels que

$$1 = au + bv.$$

Comme $a \mid auc$ et $a \mid bvc$ par hypothèse, $a \mid auc + bvc = c$. □

Corollaire 1.2.8 (Lemme d'Euclide). — *Soit p un nombre premier et soient a et b deux nombres entiers. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.*

Démonstration. — Supposons que p divise ab et ne divise pas a. Comme p est premier, ces seuls diviseurs positifs sont 1 et p. Le pgcd de a et p divise p et a. Il vaut donc 1. On peut alors appliquer le lemme de Gauss et $p \mid b$. □

Corollaire 1.2.9. — *On se donne r entiers $a_1, \ldots, a_r$. Soit b un entier. Si b est premier à a_i pour $i \in \{1, \ldots, r\}$, alors b est premier au produit $a_1 \ldots a_r$.*

Démonstration. — Montrons ce corollaire par récurrence. Le résultat est vrai si $r = 1$. Si $r = 2$, en appliquant le théorème de Bezout, on obtient des entiers u_1, v_1, u_2 et v_2 tels que

$$a_1u_1 + bv_1 = 1 \quad \text{et} \quad a_2u_2 + bv_2 = 1.$$

En faisant le produit,

$$1 = (a_1u_1 + bv_1)(a_2u_2 + bv_2) = a_1a_2(u_1u_2) + b(a_1u_1v_2 + v_1a_2u_2 + bv_1v_2).$$

Par conséquent, a_1a_2 est premier à b. Si le résultat est vrai pour $r - 1 \geqslant 2$, alors b est premier au produit $a_1 \ldots a_{r-1}$ et, en appliquant le cas $r = 2$, au produit $a_1 \ldots a_r$. □

Donnons maintenant des algorithmes pour calculer pgcd et ppcm. Par récurrence, en utilisant les formules

$$\mathrm{pgcd}(a_1, \ldots, a_r) = \mathrm{pgcd}(\mathrm{pgcd}(a_1, \ldots, a_{r-1}), a_r)$$

et

$$\mathrm{ppcm}(a_1, \ldots, a_r) = \mathrm{ppcm}(\mathrm{ppcm}(a_1, \ldots, a_{r-1}), a_r).$$

On voit qu'il suffit de donner un algorithme pour le pgcd et le ppcm de deux entiers pour avoir un algorithme pour toute famille finie. Pour calculer $\mathrm{pgcd}(a, b)$, on note que si b est nul alors le pgcd est a sinon on fait la division euclidienne de a par b et d est un pgcd de a et b si et seulement si c'est un pgcd de b et r. L'entier r étant strictement majoré par la valeur absolue de b, l'algorithme se termine.

Algorithme 1.2.10.

Entrée:

- Entiers a et b.

Sortie:

- $\mathrm{pgcd}(a, b)$.

Algorithme:

1. Si $a < 0$, $a \leftarrow -a$.
   Si $b < 0$, $b \leftarrow -b$.
2. Tant que b n'est pas nul,
   3.1. $t \leftarrow b$.
   3.2. $b \leftarrow a\%b$.
   3.3. $a \leftarrow t$.
3. Renvoyer a.

Pour le ppcm on utilise la formule (cf. corollaire 3.9.8)

$$\mathrm{ppcm}(a,b)\,\mathrm{pgcd}(a,b) = ab. \tag{1.2.1}$$

1.3. Factorisation des entiers

Proposition 1.3.1. — *Soit n un entier strictement positif, alors il existe un unique entier r, une unique famille de nombre premiers $p_1, \dots, p_r$ avec $p_1 < \cdots < p_r$ et une unique famille d'entiers strictement positifs $m_1, \dots, m_r$ tels que*

$$n = p_1^{m_1} \dots p_r^{m_r}.$$

Cette écriture de n est appelée la décomposition de n en facteurs irréductibles.

Démonstration. — **Existence.** Nous allons montrer l'existence de cette décomposition par récurrence sur n. Si $n = 1$ alors l'unique décomposition avec $r = 0$ convient. Si n est premier, alors la décomposition avec $r = 1$, $p_1 = n$ et $m_1 = 1$ convient. Supposons le résultat vrai pour tout entier $< n$. Si $n \neq 1$ et si n n'est pas premier, alors n admet un diviseur positif s distinct de 1 et de n. On peut écrire $n = st$ avec t un entier distinct de n. Par hypothèse de récurrence s et t se décomposent en produit de nombre premiers. Il en est de même de $n = st$.

Unicité. Soient r et r' deux entiers, soient $p_1, \dots, p_r$ et $p'_1, \dots p'_{r'}$ deux familles de nombres premiers avec $p_1 \leqslant \dots \leqslant p_r$ et $p'_1 \leqslant \dots \leqslant p'_{r'}$. Quitte à échanger r et r' ainsi que les familles de nombres premiers, on peut supposer que $r \geqslant r'$. Montrons par récurrence sur r que si

$$p_1 \dots p_r = {p'}_1 \dots {p'}_{r'}, \tag{1.3.1}$$

alors $r = r'$ et $p_i = p'_i$ pour $i \in \{1, \dots, r\}$. Si $r = 0$ alors $r' = 0$ et les familles coïncident. Si $r > 0$, alors $p_1 \mid {p'}_1 \dots {p'}_{r'}$. Par le lemme d'Euclide, p_1 divise l'un des p'_i et, comme p'_i est premier, on a $p_1 = p'_i$. En appliquant l'hypothèse de récurrence à l'égalité

$$p_2 \dots p_r = p'_1 \dots p'_{i-1} p'_{i+1} \dots p'_{r'}$$

on obtient que $r = r'$ et l'égalité des deux familles. □

Remarque 1.3.2. — Notons que cette démonstration ne donne pas de méthode de décomposition. En fait on ne connaît pas à l'heure actuelle de méthode efficace pour factoriser un entier.

1.4. Congruences

Définition 1.4.1. — Si a, b et m sont trois entiers relatifs, on dit que *a est congru à b modulo m* et on note

$$a \equiv b \pmod{m}$$

si et seulement si m divise $b - a$.

Proposition 1.4.2. — *si a, b, c, d, m et n sont des entiers relatifs,*

(i) $a \equiv a \pmod{m}$,

(ii) *si* $a \equiv b \pmod{m}$, *alors* $b \equiv a \pmod{m}$,

(iii) *si* $a \equiv b \pmod{m}$ *et* $b \equiv c \pmod{m}$, *alors* $a \equiv c \pmod{m}$,
(iv) *si* m *est non nul et si* r *est le reste de la division euclidienne de* a *par* m, *alors on a* $a \equiv r \pmod{m}$,
(v) *si* $a \equiv b \pmod{m}$ *et si* $n \mid m$, *alors* $a \equiv b \pmod{n}$,
(vi) *si* $a \equiv b \pmod{m}$ *et si* $c \equiv d \pmod{m}$, *alors* $a + c \equiv b + d \pmod{m}$,
(vii) *si* $a \equiv b \pmod{m}$ *et si* $c \equiv d \pmod{m}$, *alors* $ac \equiv bd \pmod{m}$,
(viii) *si* $a \equiv b \pmod{m}$ *et si* n *est un entier positif,* $a^n \equiv b^n \pmod{m}$.

Démonstration. — Montrons (vii) à titre d'exemple : Si $a \equiv b \pmod{m}$ et $c \equiv d \pmod{m}$, alors il existe des entiers relatifs q_1 et q_2 tels que

$$a - b = mq_1 \quad \text{et} \quad c - d = mq_2,$$

par conséquent,

$$ac - bd = (a - b)c + b(c - d) = m(cq_1 + bq_2). \quad \square$$

Exemple 1.4.3. — Si a est entier positif ou nul et $a_r a_{r-1} \dots a_0$ son écriture en base 10 (i.e. $a = \sum_{i=0}^{r} a_i 10^i$ avec $0 \leqslant a_i \leqslant 9$ pour $i \in \{0, \dots, r\}$), alors

(i) $a \equiv a_0 \pmod{10}$,
(ii) $a \equiv \sum_{i=0}^{r} a_i \pmod{9}$,
(iii) $a \equiv \sum_{i=0}^{r} (-1)^i a_i \pmod{11}$.

1.5. Relations d'équivalence et ensembles quotients

La congruence est une relation d'équivalence. Rappelons ce dont il s'agit.

Définition 1.5.1. — Une relation binaire $\mathscr{R}$ sur une ensemble E est une *relation d'équivalence* si et seulement si elle vérifie les trois conditions suivantes :

Réflexive. $\forall a \in E,\ a \mathscr{R} a$,
Symétrique. Si a et b appartiennent à E et si $a \mathscr{R} b$, alors $b \mathscr{R} a$,
Transitive. Si a, b et c sont des éléments de E, si $a \mathscr{R} b$ et $b \mathscr{R} c$, alors $a \mathscr{R} c$.

Pour tout x de E on appelle *classe d'équivalence* de x modulo $\mathscr{R}$, notée $\overline{x}$, la partie

$$\{y \in E \mid x \mathscr{R} y\}$$

de E. On dit également que x est un *représentant* de la classe d'équivalence $\overline{x}$.

L'ensemble des classes d'équivalences modulo $\mathscr{R}$ est appelé ensemble-quotient de E par $\mathscr{R}$. On le note $E/\mathscr{R}$.

Proposition 1.5.2. — *L'ensemble quotient* $E/\mathscr{R}$ *forme une partition de* E, *autrement dit aucune classe d'équivalence n'est vide et deux classes d'équivalences sont soit disjointes, soit identiques.*

Définition 1.5.3. — L'application

$$\begin{array}{rccc} \pi : & E & \to & E/\mathscr{R} \\ & x & \mapsto & \overline{x} \end{array}$$

est surjective, on l'appelle la *projection canonique*.

Exemple 1.5.4. — L'égalité est une relation d'équivalence. L'ensemble quotient, formé des singletons $\{x\}$ pour x dans E est en bijection avec E.

Proposition 1.5.5. — *Si $f : E \to F$ est une application d'un ensemble E vers un ensemble F, alors la relation $\mathscr{R}$ définie par $x\mathscr{R}y$ si et seulement si $f(x) = f(y)$ est une relation d'équivalence sur E. Notons $f(E)$ l'image de l'application f et $j : f(E) \to F$ l'injection canonique définie par $j(x) = x$ pour tout x de $f(E)$. Il existe alors une unique application $\overline{f} : E/\mathscr{R} \to f(E)$ telle que f coïncide avec la composée des applications*

$$E \xrightarrow{\pi} E/\mathscr{R} \xrightarrow{\overline{f}} f(E) \xrightarrow{j} E.$$

En outre $\overline{f}$ est bijective.

1.6. Entiers modulo n

Définition 1.6.1. — Pour tout entier n la relation de congruence $x \equiv y \pmod{n}$ est une relation d'équivalence sur $\mathbf{Z}$. On note $\mathbf{Z}/n\mathbf{Z}$ l'ensemble quotient associé.

Exemple 1.6.2. — Si $n = 0$ alors la relation de congruence $x \equiv y \pmod{n}$ coïncide avec l'égalité. Le quotient $\mathbf{Z}/0\mathbf{Z}$ est donc en bijection avec $\mathbf{Z}$. On identifie $\mathbf{Z}$ avec $\mathbf{Z}/0\mathbf{Z}$.

Remarque 1.6.3. — (i) Si $n < 0$ la relation de congruence $x \equiv y \pmod{n}$ coïncide avec la relation $x \equiv y \pmod{-n}$.

Supposons $n > 0$. Soit $a \in \mathbf{Z}$, notons r le reste de la division euclidienne de a par n. on a $\overline{a} = \overline{r}$ dans $\mathbf{Z}/n\mathbf{Z}$. Tout élément de $\mathbf{Z}/n\mathbf{Z}$ possède donc un réprésentant dans l'ensemble $\{0, 1, \ldots, n-1\}$. De plus, si r et r' appartiennent à $\{0, 1, \ldots, n-1\}$ et vérifient $\overline{r} = \overline{r}'$, alors il existe $k \in \mathbf{Z}$ tel que $r' - r = kn$. Mais on a les inégalités $-n - 1 \leqslant r - r' \leqslant n - 1$. Donc $k = 0$ et $r = r'$. Toute classe d'équivalence dans $\mathbf{Z}/n\mathbf{Z}$ admet donc un unique représentant dans l'ensemble $\{0, 1, \ldots, n-1\}$. En particulier, $\mathbf{Z}/n\mathbf{Z}$ est de cardinal n. Notons également que le représentant de $\overline{a}$ dans cet ensemble est le reste de la division euclidienne de a par n. Dans la pratique toute manipulation dans $\mathbf{Z}/n\mathbf{Z}$ se fait donc en manipulant des entiers dans $\{0, \ldots, n-1\}$.

(ii) On peut voir tous les calculs faits par un processeur à 32 bits comme effectués dans $\mathbf{Z}/2^{32}\mathbf{Z}$.

Définition 1.6.4. — L'assertion (vi) de la proposition 1.4.2 permet de définir une addition sur $\mathbf{Z}/n\mathbf{Z}$ par la formule

$$\overline{x} + \overline{y} = \overline{x + y}.$$

En effet la classe d'équivalence $\overline{x + y}$ ne dépend pas des représentants choisis x et y dans $\overline{x}$ et $\overline{y}$.

De même, on peut définir une multiplication dans $\mathbf{Z}/n\mathbf{Z}$ par

$$\overline{x}.\overline{y} = \overline{xy}$$

et si $m > 0$ la puissance m-ième d'un élément de $\mathbf{Z}/n\mathbf{Z}$

$$\overline{x}^m = \overline{x^m}.$$

D'un point de vue pratique, ces calculs peuvent être implémentés de la façon suivante : pour l'addition

Algorithme 1.6.5.
Entrée:
- Entier n de congruence,
- Entiers a et b (entre 0 et $n-1$).

Sortie:
- Représentant de $a+b$ (entre 0 et $n-1$).

Algorithme:
1. Calculer $c = a + b$ avec une précision suffisante.
2. Calculer le reste r de la division de c par n.
3. Renvoyer c.

Noter que dans ce cas l'étape 2 peut se faire avec un test et une simple soustraction. Un algorithme analogue peut être écrit pour la multiplication. Pour l'exponentiation, il convient de minimiser le nombre de multiplications effectuées. L'idée pour cela est de considérer l'écriture en base 2 de la puissance cherchée :

$$n = \sum_{i=0}^{r} n_i 2^i$$

avec $n_i = 0$ ou 1. On a alors la relation

$$\overline{a}^n = \prod_{\substack{0 \leqslant i \leqslant r \\ n_i = 1}} \overline{a}^{2^i}.$$

Algorithme 1.6.6.
Entrée:
- Entier m de congruence,
- Puissance n,
- Elément a de $\mathbf{Z}/m\mathbf{Z}$.

Sortie:
- Valeur de a^n dans $\mathbf{Z}/m\mathbf{Z}$.

Algorithme:
1. $x \leftarrow a$.
2. $y \leftarrow 1$.
3. Tant que n n'est pas nul,
   3.1. Si n est impair, $y \leftarrow y * x$ (calculé modulo m).
   3.2. $x \leftarrow x * x$ (calculé modulo m).
   3.3. $n \leftarrow n/2$.
4. renvoyer y.

Exemple 1.6.7. — Ecrivons, à titre d'exemple, les tables d'addition et de multiplication pour $\mathbf{Z}/2\mathbf{Z}$:

$+$	0	1
0	0	1
1	1	0

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

L'addition correspond donc au « ou exclusif » de la logique et la multiplication à l'opérateur « et ».

EXERCICES

1.1. Calculer de tête le dernier chiffre de l'écriture en base 10 des nombres suivants : 2309786^{34657}, $8786652^{3544619}$ et $654565198^{3548217}$.

1.2. Calculer de tête le reste de la division par 9 des nombres suivants : $8^{68498353}$, 54648381^{54648} et 354872846^{21353}.

1.3. Soit b un entier strictement positif, énoncer et démontrer l'analogue de l'exemple 1.4.3 pour l'écriture en base b d'un entier positif a (i.e. $a = \sum_{i=0}^{r} a_i b^i$ avec $0 \leqslant a_i < b$ pour $i \in \{1, \ldots, r\}$).

CHAPITRE 2

LES GROUPES

Pour des compléments sur les structures algébriques de base, le lecteur peut se reporter à [**RDO**].

2.1. Structure de groupe

Définition 2.1.1. — Un *groupe* est un ensemble G muni d'une loi interne

$$\begin{array}{ccc} G \times G & \to & G \\ (x, y) & \mapsto & xy \end{array}$$

qui est associative :

Gr1. $\forall x, y, z \in G, \quad x(yz) = (xy)z,$

admet un élément neutre e :

Gr2. $\forall x \in G, \quad xe = ex = x,$

et tout élément x du groupe G admet un *inverse* (ou *symétrique*) y :

Gr3. $\forall x \in G, \quad \exists y \in G, \quad xy = yx = e,$

cet élément y est alors unique, on le note x^{-1}.

En outre le groupe est dit commutatif ou abélien s'il vérifie également la condition suivante :

Comm. $\forall x, y \in G, \quad xy = yx.$

Remarque 2.1.2. — Nous prendrons souvent une notation additive pour la loi d'un groupe abélien, la loi s'écrira alors $(x, y) \mapsto x + y$ et le symétrique (ou *opposé*) d'un élément x sera noté $-x$.

Exemple 2.1.3. — L'ensemble $\mathbf{Z}$ muni de l'addition est un groupe commutatif. Il en est de même pour $\mathbf{Q}$, $\mathbf{R}$ munis de l'addition. L'addition munit également $\mathbf{Z}/n\mathbf{Z}$ d'une structure de groupe abélien. Par contre, $\mathbf{N}$ muni de l'addition n'est pas un groupe puisque les éléments strictement positifs n'ont pas de symétriques dans $\mathbf{N}$.

Exemple 2.1.4. — Soient I un ensemble et $(G_i)_{i\in I}$ une famille de groupe. L'ensemble produit $\prod_{i\in I} G_i$ muni de la loi interne définie par

$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}$$

est un groupe qu'on appelle groupe-produit. L'élement neutre est donné par la famille $(e_i)_{i\in I}$ où e_i est l'élément neutre de G_i et l'inverse d'un élément $(x_i)_{i\in I}$ est la famille des inverses $(x_i^{-1})_{i\in I}$. Ce groupe est abélien si tous les groupes G_i sont abéliens.

Dans le cas particulier du produit $G_1 \times \cdots \times G_r$ d'une famille finie de groupes, le produit s'écrit

$$(g_1, \ldots, g_r)(h_1, \ldots, h_r) = (g_1 h_1, \ldots, g_r h_r).$$

Exemple 2.1.5. — Si X est un ensemble et G un groupe, l'ensemble G^X des applications de X vers G est un groupe pour la loi définie par

$$\forall f, g \in G^X, \quad \forall x \in X, \quad (fg)(x) = f(x)g(x).$$

C'est un cas particulier de l'exemple précédent si on prend $I = X$ et $G_i = G$ pour tout i de l'ensemble I.

Exemple 2.1.6. — Si X est un ensemble, l'ensemble des bijections de X dans X, aussi appelées *permutations de* X forment un groupe pour la loi de composition que l'on note $\mathfrak{S}_X$. On note $\mathfrak{S}_n$ pour le groupe des permutations de $\{ 1, \ldots, n \}$. Si $n \geqslant 3$, alors ce groupe n'est pas abélien.

Définition 2.1.7. — Soient G et H deux groupes. Une application $\phi : G \to H$ est un *morphisme de groupes* si elle vérifie la condition :

Mor. $\forall x, y \in G, \quad \phi(xy) = \phi(x)\phi(y)$.

Remarque 2.1.8. — Comme $\phi(ee) = \phi(e)\phi(e) = \phi(e)$, on obtient que ϕ envoie l'élément neutre de G sur celui de H. De même la relation $\phi(x)\phi(x^{-1}) = \phi(e) = e$ montre que $\phi(x^{-1}) = \phi(x)^{-1}$.

Exemple 2.1.9. — Si G est un groupe et g un élément de G, on définit, pour tout n de $\mathbf{Z}$, g^n de la façon suivante :

$$g^0 = e, \quad \forall n \in \mathbf{N}, \quad g^{n+1} = g^n g \quad \text{et} \quad g^{-n} = (g^n)^{-1}.$$

On vérifie que l'application ainsi définie

$$\begin{array}{ccc} \mathbf{Z} & \to & G \\ n & \mapsto & g^n \end{array}$$

est un morphisme de groupes. Si G est un groupe abélien et la loi de G notée additivement, on notera ng pour g^n.

Remarque 2.1.10. — L'algorithme d'exponentiation 1.6.5 peut être également utilisé pour calculer g^n.

Définition 2.1.11. — Un isomorphisme de groupes est un morphisme de groupes qui est bijectif. Son inverse est alors un morphisme de groupes.

2.2. Sous-groupes

2.2.1. Définition

Définition 2.2.1. — Si G est un groupe, un *sous-groupe* est une partie H de G vérifiant les trois conditions suivantes :

SG1. $e \in H$,
SG2. $\forall x, y \in H, \quad xy \in H$,

SG3. $\forall x \in H, \quad x^{-1} \in H$.

H est alors un groupe pour la loi induite

$$\begin{array}{ccc} H \times H & \to & H \\ (h_1, h_2) & \mapsto & h_1 h_2. \end{array}$$

2.2.2. Exemples

Exemple 2.2.2. — Si G est un groupe, G et $\{e\}$ sont des sous-groupes de G.

Exemple 2.2.3. — Si $(H_i)_{i\in I}$ est une famille de sous-groupes d'un groupe G, alors l'intersection $\bigcap_{i\in I} H_i$ est un sous-groupe de G. En particulier, si X est une partie de G, l'intersection des sous-groupes de G contenant X est un sous-groupe de G. C'est le plus petit sous-groupe de G contenant X, on l'appelle le *sous-groupe de G engendré par X*. On notera $\langle X \rangle$ le sous-groupe engendré par X. On peut remarquer que le sous-groupe engendré par $\emptyset$ est le sous-groupe réduit à l'élément neutre $\{ e \}$.

Définition 2.2.4. — Un groupe G est dit *monogène* s'il existe un élément g de G tel que $\{ g \}$ engendre G. On dit alors que g est un *générateur* de G. Un groupe monogène fini est dit *cyclique*.

Exemple 2.2.5. — Si $\phi : G \to H$ est un morphisme de groupe, alors pour tout sous-groupe H' de H, son image inverse dans G, $\phi^{-1}(H')$ est un sous-groupe de G et pour tout sous-groupe G' de G, son image $\phi(G')$ est un sous-groupe de H. En particulier, l'ensemble

$$\mathrm{Ker}(\phi) = \{ x \in H \mid \phi(x) = e \}$$

est un sous-groupe de G, qu'on appelle le *noyau* de ϕ. L'image de ϕ, notée $\mathrm{Im}\,\phi$, est un sous-groupe de H.

Exemple 2.2.6. — Soit I un sous-groupe de $\mathbf{Z}$. Si I est distinct du sous-groupe $\{ 0 \}$, alors I contient un élément non nul et, contenant aussi son opposé, un élément strictement positif. Soit n le plus petit élément strictement positif de I. Soit i un élément quelconque de I. La division euclidienne de i par n s'écrit $i = nq + r$ avec $0 \leqslant r < n$. Mais $r = i - nq$ appartient également à I. En conséquence, par minimalité de n, $r = 0$. Donc $i \in n\mathbf{Z}$. Réciproquement tout élément de $n\mathbf{Z}$ est dans I. En notant que $\{ 0 \} = 0\mathbf{Z}$, on obtient donc que tout sous-groupe de $\mathbf{Z}$ est de la forme $n\mathbf{Z}$ pour un élément n de $\mathbf{N}$.

Exemple 2.2.7. — Si G est un groupe, l'ensemble $\mathrm{Aut}(G)$ des isomorphismes de groupes de G dans G forment un sous-groupe de $\mathfrak{S}_G$ appelé groupe des *automorphismes* de G.

2.2.3. Classes à gauches, à droites

Définition 2.2.8. — Soient G un groupe et H un sous-groupe de G. Si $g \in G$, l'ensemble

$$gH = \{ gh, h \in H \} \quad (\text{resp. } Hg = \{ hg, h \in H \})$$

est appelé *classe à gauche* (resp. *à droite*) de g pour H. On note G/H (resp. $H\backslash G$) l'ensembles des classes à gauche (resp. à droite) de G pour H.

Remarque 2.2.9. — Soient $\mathscr{R}_g$ et $\mathscr{R}_d$ les relations définies par

$$x\mathscr{R}_g y \Leftrightarrow x^{-1}y \in H \quad \text{et} \quad x\mathscr{R}_d y \Leftrightarrow xy^{-1} \in H.$$

Alors on a les équivalences

$$x\mathscr{R}_g y \Leftrightarrow xH = yH \quad \text{et} \quad x\mathscr{R}_d y \Leftrightarrow Hx = Hy.$$

Les relations $\mathscr{R}_g$ et $\mathscr{R}_d$ sont donc des relations d'équivalence et les ensembles-quotients sont donnés par $G/H = G/\mathscr{R}_g$ et $H\backslash G = G/\mathscr{R}_d$.

Exemple 2.2.10. — Soit n un entier et prenons $G = \mathbf{Z}$, $H = n\mathbf{Z}$, les relations $\mathscr{R}_g$ et $\mathscr{R}_d$ coïncident avec la relation de congruence modulo n et l'ensemble quotient est $\mathbf{Z}/n\mathbf{Z}$.

Notons que si a et b sont des éléments de G, alors on a une bijection

$$\begin{array}{rcl} aH & \to & bH \\ g & \mapsto & ba^{-1}g. \end{array}$$

De même on a une bijection

$$\begin{array}{rcl} aH & \to & Ha^{-1} \\ g & \mapsto & g^{-1}. \end{array}$$

En particulier, toutes ces classes ont le même cardinal, à savoir le cardinal du sous-groupe H. En outre cela définit une bijection

$$\begin{array}{rcl} G/H & \to & H\backslash G \\ aH & \mapsto & Ha^{-1}. \end{array}$$

Définition 2.2.11. — Si G/H ou $H\backslash G$ est fini, alors ces deux ensembles sont finis et de même cardinal, qu'on appelle indice de H dans G. On le note $(G : H)$.

Nous avons en outre montré la propriété suivante :

Proposition 2.2.12. — *Si G est un groupe fini et H un sous-groupe de G, alors*

$$\sharp G = \sharp H \times (G : H).$$

En particulier, le cardinal d'un sous-groupe divise le cardinal de G.

Remarque 2.2.13. — Si H est un sous-groupe de G et K un sous-groupe de H, alors les classes aK pour $a \in H$ sont à la fois des classes à gauche de H et des classes à gauche de G. On a donc des inclusions

$$H/K \subset G/K \quad \text{et} \quad K\backslash H \subset K\backslash G.$$

2.3. Sous-groupes distingués, groupes quotient

Soit $\phi : G \to H$ un morphisme de groupes, alors pour tout x de $\mathrm{Ker}\,\phi$ et tout g de G, on a

$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e.$$

Par conséquent, gxg^{-1} appartient également au noyau de ϕ. Ceci amène à la définition suivante :

Définition 2.3.1. — Soient G un groupe et H un sous-groupe de G. On dit que H est distingué dans G et on note $H \lhd G$ si et seulement si

$$\forall h \in H, \quad \forall g \in G, \quad ghg^{-1} \in H$$

Nous venons de voir que si ϕ est un morphisme, son noyau est distingué. Montrons qu'inversement tout sous-groupe distingué est le noyau d'un morphisme

Définition 2.3.2. — Si H est un sous-groupe distingué de G alors il existe sur G/H une unique loi de groupe de sorte que la projection canonique

$$\begin{array}{rcl} \pi : G & \to & G/H \\ g & \mapsto & gH \end{array}$$

soit un morphisme de groupes. On dit alors que G/H est le groupe-quotient de G par H.

Exemple 2.3.3. — Si G est un groupe abélien, tout sous-groupe est distingué. En particulier le sous-groupe $n\mathbf{Z}$ est distingué dans $\mathbf{Z}$. On retrouve ainsi l'addition dans $\mathbf{Z}/n\mathbf{Z}$.

Exemple 2.3.4. — Si $\phi : G \to H$ est un morphisme de groupes et H' un sous-groupe distingué de H, alors $\phi^{-1}(H')$ est un sous groupe distingué de G. En effet pour tout g de G et tout h de $\phi^{-1}(H')$, on a $\phi(h) \in H'$ et

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} \in H'.$$

Proposition 2.3.5. — *Si $\phi : G \to H$ est un morphisme de groupes, il existe un unique isomorphisme de groupes $\overline{\phi} : G/H \to \operatorname{Im}\phi$ tel que ϕ coïncide avec la composée*

$$G \xrightarrow{\pi} G/H \xrightarrow{\overline{\phi}} \operatorname{Im}\phi \xrightarrow{j} H$$

où π désigne la projection canonique et j l'injection canonique.

Exemple 2.3.6. — Si G est un groupe et g un élément de G, on a, par l'exemple 2.1.9 un morphisme surjectif

$$\begin{array}{rcl} \mathbf{Z} & \to & \langle g \rangle \\ n & \mapsto & g^n. \end{array}$$

Le noyau de ce groupe est un sous-groupe de $\mathbf{Z}$, de la forme $m\mathbf{Z}$ avec $m \in \mathbf{N}$. On obtient ainsi un isomorphisme $\mathbf{Z}/m\mathbf{Z} \xrightarrow{\sim} \langle g \rangle$. Si $\langle g \rangle$ est infini, alors $m = 0$, sinon m est nombre entier positif égal au cardinal de $\langle g \rangle$.

Définition 2.3.7. — Soient G un groupe et g un élement de G. On appelle ordre de g et on note $\operatorname{ord}(g)$ le cardinal de $\langle g \rangle$.

Proposition 2.3.8. — *Soit G un groupe.*

(i) *Si G est fini, alors l'ordre de tout élément de G divise le cardinal de G.*
(ii) *Si g est d'ordre fini, $\operatorname{ord}(g)\mathbf{Z}$ est le noyau de l'application $n \mapsto g^n$. Par conséquent $\operatorname{ord}(g)$ est le plus petit entier strictement positif tel que $g^{\operatorname{ord}(g)} = e$ et $g^n = e$ si et seulement si $\operatorname{ord}(g) \mid n$.*
(iii) *Si g est d'ordre mn, alors g^m est d'ordre n.*

(iv) *Si m et n sont deux entiers strictement positifs premier entre eux, si g et h sont deux éléments de G qui commutent (i.e. $gh = hg$), et si g est d'ordre m et h d'ordre n, alors* $\mathrm{ord}(gh) = mn$.

Démonstration. — La première assertion est une conséquence de la proposition 2.2.12, la seconde résulte de la définition.

Montrons l'assertion (iii). Notons r l'ordre de g^m. Comme $g^{mn} = 1$, $r \mid n$. D'un autre coté $(g^m)^r = 1$ donc $mn = \mathrm{ord}(g) \mid mr$. Par conséquent $n = r$.

Si g, h sont deux éléments de G qui commutent et si g est d'ordre m et h d'ordre n, alors

$$(gh)^{mn} = g^{mn}h^{mn} = e.$$

Par conséquent $\mathrm{ord}(gh) \mid mn$. Si m et n sont premiers entre eux, le théorème de Bezout 1.2.6 assure qu'il existe des entiers u et v tels que $1 = um + vn$. Si $(gh)^k = e$ alors

$$g^k = g^{k(um+vn)} = g^{kvn} = g^{kvn}h^{kvn} = e.$$

Donc $\mathrm{ord}(g) \mid \mathrm{ord}(gh)$. Par conséquent, $\mathrm{ppcm}(m, n) \mid \mathrm{ord}(gh)$. Comme m et n sont premiers entre eux, par la relation (1.2.1), $\mathrm{ppcm}(m, n) = mn$. □

Proposition 2.3.9. — *Si K est un sous-groupe distingué de G, alors les sous-groupes de G/K sont les quotients H/K où H décrit l'ensemble des sous-groupes de G contenant K. En outre H/K est distingué dans G/K si et seulement si H est distingué dans G, et, dans ce cas, on a un isomorphisme canonique*

$$(G/K)/(H/K) \xrightarrow{\sim} G/H.$$

Démonstration. — La projection $\pi : G \to G/K$ est un morphisme de groupes Donc si $\overline{H}$ est un sous-groupe de G/K, par l'exemple 2.2.5, $\pi^{-1}(\overline{H})$ est un sous-groupe H de G qui contient K. Par construction, H est la réunion des classes $\overline{g}$ pour $\overline{g} \in \overline{H}$, et donc H/K coïncide avec $\overline{H}$. Inversement si H est un sous-groupe de G contenant K, alors $\pi(H)$, qui coïncide avec H/K est un sous-groupe de G/K.

Si H/K est distingué dans G/K, alors par l'exemple 2.3.4, $H = \pi^{-1}(H/K)$ est distingué. Si H est distingué dans G alors H/K est distingué par définition de la loi dans le groupe-quotient. Enfin, on a un morphisme naturel

$$\begin{array}{ccc} G/K & \to & G/H \\ aK & \mapsto & aH \end{array}$$

dont le noyau est H/K. □

Exemple 2.3.10. — Les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ sont les groupes $m\mathbf{Z}/n\mathbf{Z}$ pour $m \mid n$.

2.4. Description des groupes abéliens finis

La plupart des groupes utilisés en cryptographie sont des groupes abéliens finis. Dans cette section nous allons montrer que tous ces groupes, à isomorphisme près, s'écrivent comme un produit de groupes cycliques finis. Dans ce paragraphe nous prendrons des notations additives pour un groupe abélien G.

Théorème 2.4.1. — *Soit G un groupe abélien fini. Il existe une unique famille de nombres premiers $p_1, \ldots, p_r$ avec $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_r$, une unique famille d'entiers strictement positifs $n_1, \ldots, n_r$ vérifiant $n_i \leqslant n_{i+1}$ si $p_i = p_{i+1}$ pour $1 \leqslant i \leqslant r-1$ telle qu'il existe un isomorphisme de groupes*

$$G \xrightarrow{\sim} \mathbf{Z}/p_1^{n_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p_r^{n_r}\mathbf{Z}.$$

Remarque 2.4.2. — Notons qu'on a la relation

$$\sharp G = \prod_{i=1}^{r} p_i^{n_i}$$

La première étape de la démonstration consiste à décomposer G suivant ses composantes p-primaires.

Notation 2.4.3. — Soit G un groupe abélien. Si $(H_i)_{i\in I}$ est un famille de sous-groupes de de G, on note $\sum_{i\in I} H_i$ le sous-groupe engendré par la réunion $\bigcup_{i\in I} H_i$.

Pour tout nombre premier p, on notera G_{p^∞} l'ensemble des éléments de G dont l'ordre est une puissance de p. La partie G_{p^∞} est appelée la *composante p-primaire de G*.

Remarques 2.4.4. — **(i)** Par convention $n^0 = 1$ pour tout entier non nul n. Par conséquent, l'élément neutre 0 de G appartient a tous les sous-ensembles G_{p^∞}.

(ii) Si g est un élément de G, $\mathrm{ord}(g) \mid \sharp G$. Il en résulte que G_{p^∞} est réduit à $\{0\}$ si p ne divise pas le cardinal de G.

Proposition 2.4.5. — *Pour tout nombre premier p, G_{p^∞} est un sous-groupe de G et l'application*

$$\begin{array}{rcl} \prod\limits_{\{p\in\mathscr{P}\,|\,p|\sharp G\}} G_{p^\infty} & \to & G \\ (g_p)_p & \mapsto & \sum_p g_p \end{array}$$

est un isomorphisme de groupes.

Démonstration. — Si n est un entier strictement positif, on note G_n le sous-ensemble de G formé des éléments de G dont l'ordre divise n. Ce sous-ensemble G_n est le noyau du morphisme de multiplication par $n : g \mapsto ng$, c'est donc un sous-groupe de G. Soit p un nombre premier et q la plus grande puissance de p divisant l'ordre de G. L'ordre de tout élément de G divisant le cardinal de celui-ci, on a l'égalité

$$G_{p^\infty} = G_q$$

et G_{p^∞} est un sous-groupe de G.

Soit m et n deux nombres premiers entre eux. Montrons que l'application naturelle

$$\begin{array}{rcl} G_m \times G_n & \to & G_{mn} \\ (g,h) & \mapsto & g+h \end{array}$$

est un isomorphisme de groupes.

Cette application est bien définie ; en effet si $x \in G_m$ et $y \in G_n$, on a $mx = 0$ et $ny = 0$ d'où $mn(x+y) = 0$. C'est un morphisme de groupes et son noyau est formé des couples de

la forme $(x, -x)$ avec $x \in G_m \cap G_n$. Son image est le sous-groupe de G_{mn} engendré par $G_m \cup G_n$, c'est-à-dire $G_m + G_n$. Il faut donc montrer les deux relations suivantes :

$$G_m \cap G_n = \{O\} \quad \text{et} \quad G_m + G_n = G_{mn}.$$

Soient x un élément de $G_m \cap G_n$. On a $\mathrm{ord}(x) \mid m$ et $\mathrm{ord}(y) \mid n$. Par conséquent l'ordre de x divise $\mathrm{pgcd}(m, n) = 1$. Donc $x = 0$ et l'intersection des deux sous-groupes est réduite à $\{0\}$.

Par le théorème de Bezout (corollaire 1.2.6), il existe des entiers relatifs u et v tels que $1 = um + vn$. Soit x un élément de G_{mn}. On a $x = umx + vnx$. Mais $n(umx) = u(nmx) = 0$ et $m(vnx) = v(mnx) = 0$. Donc $G_{mn} = G_m + G_n$.

Montrons par récurrence sur r que si $m_1, m_2, \ldots, m_r$ sont des entiers premiers entre eux deux à deux, alors l'application

$$\begin{array}{rcl} G_{m_1} \times \cdots \times G_{m_r} & \to & G_{m_1 \ldots m_r} \\ (g_1, \ldots, g_r) & \mapsto & \sum_{i=1}^{r} g_i \end{array}$$

est un isomorphisme de groupes. C'est vrai si $r = 1$ ou si $r = 2$ par le paragraphe précédent. Supposons le résultat vérifié pour $r - 1$. Par le corollaire 1.2.9, comme $m_1, m_2, \ldots, m_r$ sont premiers entre eux deux à deux, l'entier m_1 est premier au produit $m_2 \ldots m_r$. Par le cas $r = 2$, l'application naturelle

$$\begin{array}{rcl} G_{m_1} \times G_{m_2 \ldots m_r} & \to & G_{m_1 \ldots m_r} \\ (g, h) & \mapsto & g + h \end{array}$$

est un isomorphisme et par hypothèse de récurrence, $G_{m_2 \ldots m_r}$ est isomorphe au produit $G_{m_2} \times \cdots \times G_{m_r}$.

Soit n le cardinal de G. On a $G = G_n$. Soit $n = \prod_{i=1}^{r} p_i^{m_i}$ la décomposition de n en facteurs irréductibles. Alors l'application

$$\begin{array}{rcl} G_{p_1^{m_1}} \times \cdots \times G_{p_r^{m_r}} & \to & G_n \\ (g_1, \ldots, g_r) & \mapsto & \sum_{i=1}^{r} g_i \end{array}$$

est un isomorphime. Mais, par le début de la démonstration, on a $G_{p_i^\infty} = G_{p_i^{m_i}}$. □

Proposition 2.4.6. — *Soit p un nombre premier. Soit G un groupe abélien fini tel que $G = G_{p^\infty}$. Alors il existe une unique famille d'entiers strictement positifs $n_1, \ldots, n_r$ vérifiant $n_1 \geqslant \ldots \geqslant n_r$ telle qu'il existe un isomorphisme*

$$\mathbf{Z}/p^{n_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{n_r}\mathbf{Z} \xrightarrow{\sim} G.$$

Démonstration. — **Existence.** Nous allons montrer le résultat par récurrence sur le cardinal de G. Si ce cardinal vaut 1, le resultat est vrai avec $r = 0$. Soit g_1 un élément d'ordre maximal p^{n_1} dans G. Notons $C_1 = \langle g_1 \rangle$, $G' = G/C_1$ et π la projection canonique de G vers G'. Le cardinal de G' est strictement inférieur à celui de G et pour tout x de G', si y est un représentant de x, $\mathrm{ord}(y)x = \pi(\mathrm{ord}(y)y) = 0$. Par conséquent, on peut appliquer l'hypothèse de récurrence à G' et il existe un isomorphisme

$$C_2 \times \cdots \times C_r \xrightarrow{\sim} G. \tag{2.4.1}$$

où C_i est un groupe cyclique de cardinal p^{n_i}, avec $n_1 \geqslant n_2 \geqslant \ldots \geqslant n_r$.

Montrons que si x est un élément d'ordre p^k dans G', alors x posséde un représentant y dans G d'ordre p^k. Soit z un représentant quelconque de x. Comme $\pi(p^k z) = 0$, on a $p^k z \in C_1$ et il existe un entier n tel que $p^k z = n g_1$. Par définition de g_1, l'ordre de z divise p^{n_1}. Donc $p^{n_1-k} n g_1 = 0$ et $p^{n_1} \mid p^{n_1-k} n$. Il en résulte que $p^k \mid n$. Soit $d = n/p^k$. La différence $z - d g_1$ est un représentant de x et son ordre divise p^k. Or on a vu que $p^k = ord(x)$ divise l'ordre de tout représentant de x. Par conséquent $y = z - d g_1$ est d'ordre p^k.

Notons g'_i l'image d'un générateur de C_i dans G' et g_i un représentant de g'_i dans G tel que $\mathrm{ord}(g_i) = \mathrm{ord}(g'_i)$. Montrons que l'application

$$\begin{array}{rcl} \mathbf{Z}/p^{n_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{n_r}\mathbf{Z} & \xrightarrow{\sim} & G \\ (k_1, \ldots, k_r) & \mapsto & \sum_{i=1}^{r} k_i g_i \end{array} \tag{2.4.2}$$

est un isomorphisme de groupes. Soit g un élément de G, $\overline{g}$ sa classe dans G'. Par l'isomorphisme (2.4.1), il existe des entiers $m_2, \ldots, m_r$ tels que

$$\overline{g} = m_2 g'_2 + \cdots + m_r g'_r.$$

La différence $g - m_2 g_2 - \cdots - m_r g_r$ appartient au noyau de la projection canonique. Il existe donc m_1 tel que g soit égal à $m_1 g_1 + m_2 g_2 + \cdots + m_r g_r$. L'application (2.4.2) est donc surjective. Soient $m_1, \ldots, m_r$ des entiers tels que $0 \leqslant m_i < p^{n_i}$ pour $i \in \{1, \ldots, r\}$. Supposons qu'on ait la relation

$$m_1 g_1 + m_2 g_2 + \cdots + m_r g_r = 0.$$

En appliquant la projection canonique, on obtient la relation $m_2 g'_2 + \cdots + m_r g'_r = 0$ et l'application (2.4.1) étant un isomorphisme, les entiers m_i sont nuls. Par conséquent $m_1 g_1$ est nul et g_1 étant d'ordre p^{n_1}, $m_1 = 0$.

Unicité. Soient $n_1, \ldots, n_r$ et $n'_1, \ldots, n'_{r'}$ deux familles d'entiers strictement positifs vérifiant $n_1 \geqslant \ldots \geqslant n_r$ et $n'_1 \geqslant \ldots \geqslant n'_{r'}$. Nous allons montrer par récurrence sur $d = \sum_{i=1}^{r} n_i$ que s'il existe un isomorphisme

$$\mathbf{Z}/p^{n_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{n_r} \xrightarrow{\sim} \mathbf{Z}/p^{n'_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{n'_{r'}},$$

alors les deux familles coïncident. Si $d = 0$ le groupe-produit est réduit à $\{0\}$ et les familles sont égales. Supposons que $d \geqslant 1$, et que le résultat soit vrai pour les entiers strictement inférieurs à d. Notons H le groupe produit et $pH = \{px, x \in H\}$. Alors pH est un sous-groupe de H et le quotient H/pH est isomorphe à $(\mathbf{Z}/p\mathbf{Z})^r \xrightarrow{\sim} (\mathbf{Z}/p\mathbf{Z})^{r'}$. En comparant les cardinaux on obtient $r = r'$. Soit r_0 (resp. r'_0) le plus grand des entiers tel que $n_i \geqslant 2$ (resp. $n'_i \geqslant 2$). On a des isomorphismes

$$pH \xrightarrow{\sim} \mathbf{Z}/p^{n_1-1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{n_{r_0}-1} \xrightarrow{\sim} \mathbf{Z}/p^{n'_1-1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{n'_{r'_0}-1}\mathbf{Z}.$$

Par hypothèse de récurrence $r_0 = r'_0$ et les familles $n_1, \ldots, n_{r_0}$ et $n'_1, \ldots, n'_{r'_0}$ coïncident. □

EXERCICES

2.1. Soient G un groupe, K et H des sous-groupes de G tels que $K \subset H$. Montrer la formule

$$(G : K) = (G : H)(H : K).$$

2.2. Soit G un groupe de cardinal 4. Montrer que G est isomorphe à $\mathbf{Z}/4\mathbf{Z}$ ou à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

CHAPITRE 3

LES ANNEAUX ET LES CORPS

Par la suite nous nous intéresserons surtout à l'anneau $\mathbf{Z}$, aux anneaux de polynômes et à leurs quotients.

3.1. Structure d'anneau

Commençons par rappeler les définitions de base :

Définition 3.1.1. — Un *anneau* A est un groupe abélien $(A, +)$ muni d'une loi interne

$$\begin{array}{rcl} \times : A \times A & \to & A \\ (x, y) & \mapsto & xy, \end{array}$$

appelée *produit* ou *multiplication*, qui est associative :

An1. $\forall x, y, z \in A, \quad x(yz) = (xy)z,$

et distributive à droite et à gauche par rapport à l'addition :

An2. $\forall x, y, z \in A, \quad x(y + z) = xy + xz,$
An3. $\forall x, y, z \in A, \quad (x + y)z = xz + yz.$

On prendra également la convention que tout anneau est *unifère*, c'est-à-dire que la multiplication est munie d'un élément neutre 1 :

An4. $\forall x \in A, \quad 1x = x1 = x.$

L'anneau est dit *commutatif* si la loi $\times$ est commutative :

Comm. $\forall x, y \in A, \quad xy = yx.$

Sauf mention du contraire, tous les anneaux considérés dans ce texte sont commutatifs.

Si A est un anneau commutatif, un *diviseur strict de* 0 dans A est un élément non nul x de A tel qu'il existe $y \in A - \{0\}$ tel que $xy = 0$. Un anneau *intègre* est un anneau commutatif non réduit à $\{0\}$ sans diviseur strict de 0.

Si A est un anneau, un élément x de A est dit *inversible* si et seulement s'il existe un élément y de A tel que

$$xy = yx = 1.$$

Cet élément est alors unique on le note y^{-1}. On note $A^\times$ l'ensemble des élément inversibles de A. Cet ensemble forme un groupe pour la multiplication.

Un *corps* est un anneau commutatif non réduit à $\{0\}$ dans lequel tout élément non nul est inversible.

Corps. $\forall x \in A - \{0\}, \quad \exists y \in A, \quad xy = 1.$

Exemple 3.1.2. — L'ensemble $A = \{0\}$, muni des lois $+$ et $\times$ définies par $0 + 0 = 0$ et $0 \times 0 = 0$ est un anneau d'unité $1 = 0$. C'est le seul anneau dans lequel $1 = 0$. On l'appelle l'*anneau nul*.

Exemple 3.1.3. — L'addition et la multiplication des entiers munit $\mathbf{Z}$ d'une structure d'anneau. De même l'ensemble des nombres réels $\mathbf{R}$ et celui des nombres complexes $\mathbf{C}$ sont munis d'une structure de corps.

Exemple 3.1.4. — Soit I un ensemble et $(A_i)_{i\in I}$ une famille d'anneaux. Le produit $\prod_{i\in I} A_i$ muni de la loi de groupe produit et de la multiplication

$$(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}$$

est un anneau qu'on appelle anneau-produit. Un élément $(x_i)_{i\in I}$ est inversible dans le produit si et seulement $x_i \in A_i^\times$ pour tout i de I. En particulier, on obtient un isomorphisme de groupes

$$\Big(\prod_{i\in I} A_i\Big)^\times \xrightarrow{\sim} \prod_{i\in I} A_i^\times.$$

Exemple 3.1.5. — Si X est un ensemble et A un anneau, alors l'ensemble A^X des applications de X vers A, muni de sa loi de groupe et de la multiplication définie par

$$\forall f, g \in A^X, \quad \forall x \in X, \quad (fg)(x) = f(x)g(x)$$

est un anneau, dont le groupe des inversibles est $(A^\times)^X$.

Exemple 3.1.6. — Si A est un anneau, pas nécessairement commutatif, on note

$$\mathscr{M}_{m,n}(A) = \{\, (m_{i,j})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}} \in A^{mn} \,\}$$

l'ensemble des matrices à m lignes et n colonnes. La matrice $(m_{i,j})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}$ est également notée

$$\begin{pmatrix} m_{1,1} & m_{1,2} & \dots & m_{1,n} \\ m_{2,1} & m_{2,2} & \dots & m_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{m,1} & m_{m,2} & \dots & m_{m,n} \end{pmatrix}$$

On dispose d'une addition

$$\begin{array}{rcl} \mathscr{M}_{m,n}(A) \times \mathscr{M}_{m,n}(A) & \to & \mathscr{M}_{m,n}(A) \\ \Big((m_{i,j})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}, (n_{i,j})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}\Big) & \mapsto & (m_{i,j} + n_{i,j})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}} \end{array}$$

et du produit de matrices

$$\begin{array}{rcl} \mathscr{M}_{m,n}(A) \times \mathscr{M}_{n,p}(A) & \to & \mathscr{M}_{m,p}(A) \\ \Big((m_{i,j})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}, (n_{i,j})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant p}}\Big) & \mapsto & \Big(\sum_{j=1}^n m_{i,j} n_{j,l}\Big)_{\substack{1\leqslant i\leqslant m\\ 1\leqslant l\leqslant p}}. \end{array}$$

Si n est un entier stictement positif, on note $\mathscr{M}_n(A) = \mathscr{M}_{n,n}(A)$. Alors $\mathscr{M}_n(A)$ munie de l'addition et de la multiplication de matrices est un anneau. Cet anneau n'est pas commutatif pour $n \geqslant 2$.

Définition 3.1.7. — Soit A et B deux anneaux. Une application $\phi : A \to B$ est un *morphisme d'anneaux* si c'est un morphisme de groupes et si elle vérifie les conditions :

Mor1. $\forall x, y \in A, \quad \phi(xy) = \phi(x)\phi(y)$.
Mor2. $\phi(1) = 1$.

Un *isomorphisme d'anneaux* est un morphisme d'anneaux qui est bijectif. Son inverse est alors un morphisme d'anneaux.

Si A et B sont des corps on dira *morphisme* (resp. *isomorphisme*) *de corps* pour morphisme (resp. isomorphisme) d'anneaux. Enfin si $A = B$, on parlera d'*automorphisme* pour un isomorphisme $A \to A$.

Exemple 3.1.8. — Si A est un anneau commutatif, il existe un unique morphisme d'anneau $\phi : \mathbf{Z} \to A$ donné par $\phi(n) = n.1$. Son noyau, $\mathrm{Ker}\,\phi$ est un sous-groupe de $\mathbf{Z}$. Le générateur strictement positif de ce sous-groupe est appelé la *caractéristique* de A et est noté $\mathrm{car}(A)$.

Proposition 3.1.9. — *Si A est un anneau intègre, alors il existe un corps $\mathbf{K}$ appelé* corps des fractions *de A et noté $\mathrm{Fr}(A)$ tel que*

(i) $A \subset \mathbf{K}$,
(ii) *Pour tout corps $\mathbf{L}$ et tout morphisme d'anneaux injectif $\phi : A \to \mathbf{L}$ il existe un unique morphisme de corps ψ de $\mathbf{K}$ vers $\mathbf{L}$ tel que $\psi_{|A} = \phi$.*

Démonstration. — **Construction.** On définit sur $A \times (A - \{0\})$ la relation $\mathscr{R}$ par

$$(a, b)\ \mathscr{R}\ (c, d) \Leftrightarrow ad = bc.$$

On vérifie en utilisant l'intégrité de A que $\mathscr{R}$ est une relation d'équivalence. On note $\mathbf{K}$ l'ensemble quotient $A \times (A - \{0\})/\mathscr{R}$ et $\frac{a}{b}$ l'image de (a, b) dans ce quotient. L'application de A dans $\mathbf{K}$ qui envoie a sur $(a, 1)$ est injective et on identifie A avec son image. On munit alors $\mathbf{K}$ des lois

$$\begin{array}{rcl} + : \mathbf{K} \times \mathbf{K} & \to & \mathbf{K} \\ \left(\frac{a}{b}, \frac{c}{d}\right) & \mapsto & \frac{ad+bc}{bd} \end{array} \quad \text{et} \quad \begin{array}{rcl} \times : \mathbf{K} \times \mathbf{K} & \to & \mathbf{K} \\ \left(\frac{a}{b}, \frac{c}{d}\right) & \mapsto & \frac{ac}{bd}. \end{array}$$

On vérifie que ces lois sont bien définies et munissent $\mathbf{K}$ d'une structure de corps, l'élément neutre pour l'addition étant $0/1$, l'opposé de a/b étant $-a/b$, l'élément neutre pour la multiplication $1/1$ et l'inverse d'un élément non nul a/b étant b/a.

Propriété universelle. Soit $\mathbf{L}$ un corps et $\phi : A \to \mathbf{L}$ un morphisme injectif, alors l'application

$$\begin{array}{rcl} A \times A - \{0\} & \to & \mathbf{L} \\ (a, b) & \mapsto & \frac{\phi(a)}{\phi(b)} \end{array}$$

passe au quotient et définit un morphisme de corps $\mathbf{K} \to \mathbf{L}$ qui convient. D'un autre coté si ψ est un tel morphisme de corps, alors $\psi(a/b) = \phi(a)/\phi(b)$, ce qui montre l'unicité de ψ. □

Exemple 3.1.10. — Le corps $\mathbf{Q}$ est le corps des fractions de $\mathbf{Z}$. Par conséquent tout corps de caractéristique 0 contient un sous-corps isomorphe à $\mathbf{Q}$.

3.2. Sous-anneaux, sous-corps

Nous passons aux constructions standards sur les anneaux.

Définition 3.2.1. — Soit A un anneau. Un *sous-anneau* est un sous-groupe B de A tel que :

Sous-Anneau1. $\forall x, y \in B, \quad xy \in B$.

Sous-Anneau2. $1 \in B$.

La restriction de l'addition et de la multiplication munissent alors B d'une structure d'anneau de sorte que l'inclusion de B dans A soit un morphisme d'anneaux.

Exemple 3.2.2. — L'anneau des entiers $\mathbf{Z}$ est un sous-anneau de l'anneau des nombres rationnels $\mathbf{Q}$.

L'intersection $\bigcap_{i\in I} A_i$ d'une famille de sous-anneaux de A est un sous-anneau de A. En particulier, si X est une partie de A, l'intersection des sous-anneaux de A contenant X est un sous-anneau de A. C'est le plus petit sous-anneau de A contenant X. On l'appelle le *sous-anneau de A engendré par X*.

Si B est sous-anneau de A et X une partie de A, alors on note $B[X]$ le sous-anneau de A engendré par $B \cup X$.

Si $\phi : A \to B$ est un morphisme d'anneaux, alors son image $\mathrm{Im}\,\phi$ est sous-anneau de B.

Définition 3.2.3. — Si $\mathbf{L}$ est un corps, un *sous-corps* de $\mathbf{L}$ est un sous-anneau qui est un corps. Autrement dit, c'est un sous anneau $\mathbf{K}$ tel que

Sous-Corps. $\forall x \in \mathbf{K} - \{0\}, x^{-1} \in \mathbf{K}$.

Exemples 3.2.4. — On peut définir de même le *sous-corps engendré par une partie X* d'un corps $\mathbf{L}$; Si $\mathbf{K}$ est un sous-corps de $\mathbf{L}$ on note $\mathbf{K}(X)$ le sous-corps engendré par $\mathbf{K} \cup X$. On notera $\mathbf{K}(x_1, \ldots, x_n)$ le sous-corps engendré par $\mathbf{K} \cup \{ x_1, \ldots, x_n \}$.

3.3. Idéaux et anneaux quotients

Si $\phi : A \to B$ est un morphisme d'anneaux alors pour tout x de Ker ϕ et tout a de A, on a

$$\phi(ax) = \phi(a)\phi(x) = \phi(a)0 = 0.$$

Donc ax appartient à Ker ϕ. Ceci conduit à la définition suivante :

Définition 3.3.1. — Si A est un anneau commutatif, une partie I de A est un *idéal* de A si c'est un sous-groupe de $(A, +)$, qui est stable par multiplication par les éléments de A :

Idéal. $\forall a \in A, \quad \forall x \in I, \quad ax \in I$.

Par ce qui précède, le noyau de tout morphisme d'anneaux est un idéal. Nous allons maintenant montrer que tout idéal est le noyau d'un morphisme.

Définition 3.3.2. — Comme le groupe $(A, +)$ est abélien, tout sous-groupe est distingué. Si I est un sous-groupe de $(A, +)$, alors le groupe-quotient A/I peut être muni d'une structure d'anneau de sorte que la projection canonique $\pi : A \to A/I$ soit un morphisme d'anneaux si et seulement si I est un idéal de A. Cette structure d'anneau est alors unique, on dit que A/I est *l'anneau-quotient* de A par I.

Exemple 3.3.3. — L'intersection d'une famille d'idéaux de A est un idéal de A. En particulier, si X est un partie de A l'intersection des idéaux contenant X est un idéal de A appelé *l'idéal engendré* par X. On le note (X). On notera également $(x_1, x_2, \ldots, x_n)$ l'idéal engendré par $\{x_1, x_2, \ldots, x_n\}$. On peut décrire cet idéal comme

$$(x_1, \ldots, x_n) = \{\, a_1x_1 + \cdots + a_nx_n, (a_1, \ldots, a_n) \in A^n \,\}.$$

Exemple 3.3.4. — Si $I_1, I_2, \ldots, I_n$ sont des idéaux d'un anneau commutatif A alors l'ensemble

$$\sum_{i=1}^{n} I_i = \{\, a_1 + \cdots + a_n, (a_1, \ldots, a_n) \in I_1 \times \ldots I_n \,\}$$

est un idéal de A, appelé somme des idéaux $I_1, \ldots, I_n$. C'est en fait l'idéal engendré par la réunion de ces idéaux.

Exemple 3.3.5. — Si I est un idéal de $\mathbf{Z}$, alors I est un sous-groupe de $\mathbf{Z}$. Il existe donc un entier n de $\mathbf{N}$ tel que $I = n\mathbf{Z}$. On retrouve ainsi la définition de la multiplication dans $\mathbf{Z}/n\mathbf{Z}$. et l'ensemble $\mathbf{Z}/n\mathbf{Z}$ des entiers modulo n muni de l'addition et de la multiplication de la définition 1.6.4 est un anneau.

Exemple 3.3.6. — Si $\phi : A \to B$ est un morphisme d'anneaux commutatifs et si J est un idéal de B alors $\phi^{-1}(J)$ est un idéal de A.

Exemple 3.3.7. — Si $\mathbf{K}$ est un corps et I un idéal de $\mathbf{K}$ distinct de (0), soit $x \in I - \{0\}$. On a $1 = x^{-1}x \in I$ et donc $I = \mathbf{K}$. Les seuls idéaux de $\mathbf{K}$ sont 0 et $\mathbf{K}$.

Inversement, si A est un anneau commutatif non nul dont les seuls idéaux sont (0) et A, pour tout $x \in A - \{0\}$, on a $(x) = A$ donc il existe un élément y de A tel que $xy = 1$. donc A est un corps.

Proposition 3.3.8. — *Si I est un idéal d'un anneau commutatif A, alors les idéaux de A/I sont les groupes-quotients J/I où J décrit les idéaux de A contenant J. Si J est un tel idéal, on a un isomorphisme canonique d'anneaux*

$$(A/I)/(J/I) \xrightarrow{\sim} A/J.$$

Démonstration. — La démonstration est semblable à celle de la proposition 2.3.9. □

Proposition 3.3.9. — *Pour tout morphisme d'anneaux commutatifs $\phi : A \to B$, il existe un unique isomorphisme d'anneaux $\overline{\phi} : A/\operatorname{Ker}\phi \to \operatorname{Im}\phi$ de sorte que ϕ coïncide avec la composée*

$$A \xrightarrow{\pi} A/\operatorname{Ker}\phi \xrightarrow{\overline{\phi}} \operatorname{Im}\phi \xrightarrow{j} B$$

où π désigne la projection canonique et j l'injection naturelle.

Définition 3.3.10. — Soit A un anneau commutatif, un idéal I de A est dit *premier* si et seulement si A/I est intègre, *maximal* si et seulement si A/I est un corps.

Remarques 3.3.11. — (i) Tout idéal maximal est premier.

(ii) Par l'exemple 3.3.7 et la proposition 3.3.8, un idéal $\mathfrak{m}$ de A est maximal si et seulement si $\mathfrak{m} \neq A$ et pour tout idéal J de A,

$$\mathfrak{m} \subset J \subset A \Rightarrow (J = \mathfrak{m} \text{ ou } J = A)$$

Autrement dit, les idéaux maximaux de A sont maximaux pour l'inclusion parmi les idéaux de A distincts de A.

(iii) Le lemme de Zorn permet de montrer que tout idéal de A distinct de A est contenu dans un idéal maximal.

3.4. Divisibilité dans les anneaux

Définition 3.4.1. — Soit A un anneau commutatif. Si $a, b \in A$, on dit que a *divise* b ou que b est un *multiple* de a et on note $a \mid b$ si et seulement si

$$\exists c \in A, \quad b = ac$$

ce qui équivaut à $(b) \subset (a)$.

Notation 3.4.2. — Dans la suite de ce paragraphe, on note A un anneau commutatif intègre.

Définition 3.4.3. — Deux éléments a et b de A sont dits *associés* si et seulement s'ils vérifient une des conditions équivalentes suivantes :

(i) $\exists u \in A^\times, \quad b = au$,
(ii) $a \mid b$ et $b \mid a$,
(iii) $(a) = (b)$.

On notera dans ce paragraphe $a \sim b$.

Démonstration. — L'équivalence entre (ii) et (iii) résulte des définitions.

(i)⇒(ii) : si $b = au$ avec $u \in A^\times$, alors $a = bu^{-1}$.

(ii)⇒(i) : si $a \mid b$ et $b \mid a$, alors il existe deux éléments c et d de A tels que $b = ca$ et $a = db$. Donc $a = dca$ et $(1 - dc)a = 0$. Mais si $a = 0$, alors $b = 0$; sinon, comme A est intègre, $1 - dc = 0$ et $c \in A^\times$. □

Remarque 3.4.4. — On peut vérifier que $a \sim b$ est une relation d'équivalence et que la divisibilité définit une relation d'ordre dans $A/\sim$, pour laquelle 1 est un minimum et 0 un maximum.

Définition 3.4.5. — Un élément a de A est dit *irréductible* si et seulement s'il vérifie les deux conditions suivantes :

Irr1. $a \notin A^\times$,
Irr2. Si $a = bc$, avec $b, c \in A$, alors $b \in A^\times$ ou $c \in A^\times$.

Exemple 3.4.6. — Les éléments irréductibles de $\mathbf{Z}$ sont les éléments de la forme p ou $-p$ avec p un nombre premier.

Proposition 3.4.7. — *Soit $p \in A - \{0\}$. Si (p) est premier, alors p est irréductible.*

Remarque 3.4.8. — La réciproque est fausse en général.

Démonstration. — Si $p = bc$ alors $bc \in (p)$. Comme (p) est premier, $b \in (p)$ ou $c \in (p)$. Quitte à échanger b et c, on peut supposer $b \in (p)$ alors $b = dp$ avec $d \in A$. Donc $p = dcp$ et $(1 - dc)p = 0$. Comme A est intègre et $p \neq 0$, $1 - dc = 0$ donc $c \in A^\times$. □

Définition 3.4.9. — Soit $(a_i)_{i \in I}$ une famille d'éléments de A.

(i) On dit que $d \in A$ est un pgcd de la famille $(a_i)_{i\in I}$ si

$$(\forall i \in I, d \mid a_i) \quad \text{et} \quad \forall r \in A, (\forall i \in I, r \mid a_i) \Rightarrow r \mid d.$$

(ii) On dit que $m \in A$ est un ppcm de la famille $(a_i)_{i\in I}$ si

$$(\forall i \in I, a_i \mid m) \quad \text{et} \quad \forall r \in A, (\forall i \in I, a_i \mid r) \Rightarrow m \mid r.$$

Par abus de langage et paresse, on note :

$$d = \mathrm{pgcd}_{i\in I}(a_i) \qquad m = \mathrm{ppcm}_{i\in I}(a_i).$$

Les $(a_i)_{i\in I}$ sont dits *premiers entre eux* si $\mathrm{pgcd}_{i\in I}(a_i) = 1$.

Remarque 3.4.10. — Il faut noter qu'il n'existe pas toujours de pgcd et de ppcm. Et s'ils existent, ils ne sont en fait pas uniques. Seules leur classes d'équivalence dans $A/\sim$ le sont.

3.5. Anneau de polynômes, division euclidienne

Sur un corps fini, il convient de distinguer les polynômes et les fonctions polynômes. Nous revenons donc sur la définition des polynômes.

Définition 3.5.1. — Si A est un anneau commutatif, *l'anneau des polynômes* à une variable T sur A est l'anneau $A[T]$ formé des suites $(a_i)_{i\in\mathbf{N}}$ d'éléments de A telles que $a_i = 0$ sauf pour un nombre fini d'entiers i. Cet ensemble est muni de la somme

$$(a_i)_{i\in\mathbf{N}} + (b_i)_{i\in\mathbf{N}} = (a_i + b_i)_{i\in\mathbf{N}}$$

et du produit

$$(a_i)_{i\in\mathbf{N}} \times (b_i)_{i\in\mathbf{N}} = \Big(\sum_{j+k=i} a_j b_k\Big)_{i\in\mathbf{N}}.$$

On a une application injective $A \to A[T]$ qui envoie a sur $(a, 0, 0, \ldots)$ et on identifie A avec son image. On note T l'élément donné par la suite $(c_i)_{i\in\mathbf{N}}$ avec

$$c_i = \begin{cases} 1 & \text{si } i = 1, \\ 0 & \text{sinon.} \end{cases}$$

Tout élément de $A[T]$ s'écrit de manière unique $\sum_{i\in\mathbf{N}} a_i T^i$.

Si $P = \sum_{i\in\mathbf{N}} a_i T^i$ est un polynôme, le *polynôme dérivé* de P est le polynôme

$$P' = \sum_{i\geqslant 1} i a_i T^{i-1}.$$

Remarque 3.5.2. — Si A est l'anneau $\mathbf{Z}/2\mathbf{Z} = \{0, 1\}$, alors un polynôme correspond à une suite de 0 et de 1. Ainsi le polynôme $T^4 + T^2 + T + 1$ correspond à 10111. Par l'exemple 1.6.7, la somme de deux polynômes dans cette représentation est le « ou exclusif » effectué bit à bit.

Quand à la multiplication, elle est donnée par l'algorithme suivant

Algorithme 3.5.3.

Entrée:

- $P = \sum_{i=0}^{d} a_i T^i$ avec $a_i = 0$ ou 1,
- $Q = \sum_{i=0}^{e} b_i T^i$ représenté par la suite $b_e \dots b_0$.

Sortie:

- Le produit PQ.

Algorithme:

1. *Aux* $\leftarrow 0$, $S \leftarrow Q$.
2. Pour i variant de 0 à d,
   2.1. Si $a_i = 1$, alors
      2.1.1. *Aux* $\leftarrow$ *Aux* $+ S$ calculé à l'aide du « ou exclusif ».
   2.2. $S \leftarrow S \ll 1$.
3. Renvoyer *Aux*.

Ici, nous désignons par $\ll$ l'opérateur de décalage vers la droite, qui correspond dans le cadre des polynômes sur $\mathbf{Z}/2\mathbf{Z}$ à la multiplication par T.

Définition 3.5.4. — Le *degré* d'un polynôme non nul $P = \sum_{i \in \mathbf{N}} a_i T^i$ est défini par

$$\deg(P) = \sup\{\, i \in \mathbf{N} \mid a_i \neq 0 \,\}$$

on prendra la convention $\deg(0) = -\infty$. Un polynôme non nul $P = \sum_{i \in \mathbf{N}} a_i T^i$ est dit *unitaire* si son *coefficient dominant* $a_{\deg(P)}$ vaut 1.

Proposition 3.5.5. — *Pour tous polynômes P et Q de $A[T]$, on a*

(i) $\deg(P+Q) \leqslant \sup(\deg(P), \deg(Q))$ *avec égalité si* $\deg(P) \neq \deg(Q)$.
(ii) $\deg(PQ) \leqslant \deg(P) + \deg(Q)$ *avec égalité si A est intègre ou si le coefficient dominant de P ou de Q est inversible.*

Remarque 3.5.6. — On prend la convention $\sup(-\infty, m) = -\infty$ et $-\infty + m = -\infty$ pour $m \in \mathbf{N} \cup \{-\infty\}$.

Corollaire 3.5.7. — *Si A est intègre, alors $A[T]$ est intègre.*

Notation 3.5.8. — Si $\mathbf{K}$ est un corps, on note $\mathbf{K}(T)$ et on appelle *corps des fractions rationnelles en une variable* le corps des fractions de $\mathbf{K}[T]$.

Proposition 3.5.9 (Propriété universelle). — *Soient A et B des anneaux commutatifs. Si $\phi : A \to B$ est un morphisme d'anneaux et b un élément de B, il existe un unique morphisme d'anneaux $\psi : A[T] \to B$ tel que la restriction de ψ à A coïncide avec ϕ et $\psi(T) = b$. On note $P(b) = \psi(P)$.*

Démonstration. — **Unicité.** Supposons que ψ soit un morphisme vérifiant les conditions de l'énoncé. Comme ψ est un morphisme d'anneaux, on a pour tout polynôme $P = \sum_{i=0}^{d} a_i T^i$ les relations

$$\psi\Big(\sum_{i=0}^{d} a_i T^i\Big) = \sum_{i=0}^{d} \psi(a_i T^i) = \sum_{i=0}^{d} \psi(a_i)\psi(T)^i = \sum_{i=0}^{d} \phi(a_i) b^i. \tag{3.5.1}$$

Existence. On vérifie que l'application ψ définie par la relation 3.5.1 définit bien un morphisme d'anneaux. □

Remarque 3.5.10. — Si $A = B$ et si $\phi = \mathrm{Id}_A$, on a par définition pour tout polynôme $P = \sum_{i=0}^{d} a_i T^i$ de $A[T]$,

$$P(b) = \psi(\sum_{i=0}^{d} a_i T^i) = \sum_{i=0}^{d} a_i b^i.$$

On retrouve la fonction polynômiale associée à P.

Proposition 3.5.11. — *Si A est un anneau intègre, alors*

$$A[T]^\times = A^\times.$$

Démonstration. — On a une inclusion $A^\times \subset A[T]^\times$. Inversement si $P \in A[T]^\times$, il existe Q tel que $PQ = 1$. Comme A est intègre, $\deg(P) + \deg(Q) = 0$ et donc les degrés de P et de Q sont nuls. Le polynôme P appartient donc à l'image de $A^\times$. □

Corollaire 3.5.12. — *Si $\mathbf{K}$ est un corps et P un élément de $\mathbf{K}[T] - \{0\}$, alors il existe un unique polynôme unitaire Q tel que $P \sim Q$.*

Proposition 3.5.13 (Division euclidienne). — *Soit A un anneau commutatif non nul. On se donne un polynôme $P = \sum_{i=0}^{d} a_i T^i$ à coefficients dans A tel que a_d soit un élément inversible de P. Alors pour tout polynôme F de $A[T]$ il existe une unique paire $(Q, R) \in A[T]$ telle que*

$$F = PQ + R \quad \textit{avec}\, \deg(R) < \deg(P).$$

Démonstration. — **Existence.** Nous allons procéder par récurrence sur le degré de F. Si $\deg(F) < d$ alors $(0, F)$ convient. Sinon on écrit $F = \sum_{i=0}^{n} b_i T^i$ avec $b_n \neq 0$ et $n \geqslant d$. Alors $F - b_n a_d^{-1} T^{n-d} P$ est un polynôme de degré strictement inférieur à n. Par hypothèse de récurrence, il existe Q_0 et R_0 tels que

$$F - b_n a_d^{-1} T^{n-d} P = PQ_0 + R_0$$

avec $\deg(R_0) < d$. La paire $(b_n a_d^{-1} T^{n-d} + Q_0, R_0)$ convient.

Unicité. Si

$$PQ_0 + R_0 = PQ_1 + R_1$$

avec $\deg(R_0) < \deg(P)$ et $\deg(R_1) < \deg(P)$ alors $P(Q_0 - Q_1) = (R_1 - R_0)$. Comme le coefficient dominant de P est inversible, on a $\deg(P(Q_0 - Q_1)) = \deg(P) + \deg(Q_0 - Q_1)$. Mais ce degré est strictement inférieur à celui de P si et seulement si $\deg(Q_0 - Q_1) = -\infty$, c'est-à-dire $Q_0 = Q_1$ ce qui entraîne que $R_0 = R_1$. □

Remarque 3.5.14. — Notons que cette démonstration donne un algorithme pour calculer le quotient et le reste d'une division euclidienne. Illustrons sur un exemple la façon d'effectuer

une telle division dans $\mathbf{Z}[T]$

$$\begin{array}{rr|l}
3T^4 + 7T^3 - 7T^2 + 16T - 5 & T^2 + 3T - 2 & \\
\cline{2-2}
-3T^4 - 9T^3 + 6T^2 & 3T^2 - 2T + 5 & \\
\cline{1-1}
-2T^3 - T^2 + 16T - 5 & & \\
2T^3 + 6T^2 - 4T & & \\
\cline{1-1}
5T^2 + 12T - 5 & & \\
-5T^2 - 15T + 10 & & \\
\cline{1-1}
-3T + 5 & &
\end{array}$$

ce qui nous donne l'égalité

$$3T^4 + 7T^3 - 7T^2 + 16T - 5 = (T^2 + 3T - 2)(3T^2 - 2T + 5) - 3T + 5.$$

L'algorithme est donc le suivant :

Algorithme 3.5.15.
Entrée:
- $P = \sum_{i=0}^{d} a_i T^i$ avec $a_d \in A^\times$.
- $F \in A[T]$.

Sortie:
- (Q, R) tels que :
  a. $F = PQ + R$,
  b. $R = 0$ ou $\deg(R) < \deg(P)$.

Algorithme:
1. $Q \leftarrow 0$, $c \leftarrow a_d^{-1}$.
2. Si $F = 0$ ou $\deg(F) < \deg(P)$, alors
   2.1 Renvoyer (Q, F). Fin de l'algorithme.
3. $S \leftarrow b_n c T^{n-d}$.
4. $Q \leftarrow Q + S$, $F \leftarrow F - SP$.
5. Retourner à l'étape 2.

Corollaire 3.5.16. — *Si A est un anneau commutatif et $P = \sum_{i=0}^{d} a_i T^i$ un polynôme de $A[T]$ tel que $a_d \in A^\times$, alors pour tout α de $A[T]/(P)$, il existe un unique représentant R de α dans $A[T]$ tel que* $\deg(R) < \deg(P)$.

Démonstration. — Si $F \in A[T]$, l'unique représentant de sa classe $\overline{F} \in A[T]/(P)$ vérifiant $\deg(F) < \deg(P)$ est le reste de la division euclidienne de F par P. □

Remarque 3.5.17. — Dans la pratique, la manipulation d'éléments de $A[T]/(P)$ se fait donc en utilisant des polynômes de $A[T]$ de degré strictement inférieur à $\deg(P)$.

3.6. Séries formelles

Définition 3.6.1. — Si A est un anneau commutatif, *l'anneau des séries formelles* en une variable T sur A est l'anneau $A[[T]]$ formés des suites $(a_i)_{i\in\mathbf{N}}$ de $A^{\mathbf{N}}$ muni de la somme

$$(a_i)_{i\in\mathbf{N}} + (b_i)_{i\in\mathbf{N}} = (a_i + b_i)_{i\in\mathbf{N}}$$

et du produit

$$(a_i)_{i\in\mathbf{N}} \times (b_i)_{i\in\mathbf{N}} = \Big(\sum_{j+k=i} a_j b_k\Big)_{i\in\mathbf{N}}.$$

On *note* $\sum_{i\in\mathbf{N}} a_i T^i$ la suite $(a_i)_{i\in\mathbf{N}}$.

Remarque 3.6.2. — L'anneau des polynômes est un sous-anneau de $A[[T]]$.

Proposition 3.6.3. — *Un élément $S = \sum_{i\in\mathbf{N}} a_i T^i$ est inversible dans $A[[T]]$ si et seulement si a_0 est inversible dans A.*

Démonstration. — $\Rightarrow$: Si S est inversible, soit $\sum_{i\in\mathbf{N}} b_i T^i$ son inverse, on a $a_0 b_0 = 1$ et donc a_0 est inversible.

$\Leftarrow$: Si a_0 est inversible, on définit par récurrence

$$b_0 = a_0^{-1} \quad \text{et si } n \geqslant 1, \quad b_n = -a_0^{-1} \sum_{i=0}^{n-1} b_i a_{n-i}$$

La série $\sum_{i\in\mathbf{N}} b_i T^i$ est alors un inverse de la série S. □

Exemple 3.6.4. — La série $\sum_{i\in\mathbf{N}} T^i$ est l'inverse de la série $1 - T$.

Définition 3.6.5. — Si $F = \sum_{i\in\mathbf{N}} a_i T^i$ est une série formelle non nulle, alors *l'ordre* de F est défini comme

$$v_0(F) = \inf\{i \in \mathbf{N} \mid a_i \neq 0\}.$$

On pose également $v_0(0) = +\infty$.

Remarque 3.6.6. — Toute série formelle non nulle s'écrit donc

$$F = T^{v_0(F)} \sum_{i\in\mathbf{N}} b_i T^i$$

avec $b_0 \neq 0$.

Proposition 3.6.7. — *Si F, G sont des séries formelles sur A,*

(i) $v_0(F + G) \geqslant \inf(v_0(F), v_0(G))$ *avec égalité si* $v_0(F) \neq v_0(G)$,
(ii) $v_0(FG) \geqslant v_0(F) + v_0(G)$ *avec égalité si A est intègre.*

Définition 3.6.8. — Si $(F_i)_{i\in\mathbf{N}}$ est une suite de séries formelles telles que pour tout entier n l'ensemble $\{i \in \mathbf{N} \mid v_0(F_i) \leqslant n\}$ soit fini, alors on écrit $F_i = \sum_{j\in\mathbf{N}} a_{i,j} T^n$. Pour tout entier j, l'hypothèse assure que l'ensemble $\{i \in \mathbf{N} \mid a_{i,j} \neq 0\}$ est fini et on peut définir

$$\sum_{j\in\mathbf{N}} F_j = \sum_{j\in\mathbf{N}} \Big(\sum_{i\in\mathbf{N}} a_{i,j}\Big) T^j.$$

En particulier si $P = \sum_{i\in\mathbf{N}} a_i T^i$ est une série formelle et Q une série formelle telle que $v_0(Q) \geqslant 1$ alors la suite $(a_i Q^i)_{i\in\mathbf{N}}$ vérifie la condition ci-dessus puisque $v_0(a_i Q^i) \geqslant i$. On définit la *composée des séries P et Q* par

$$P(Q) = P \circ Q = \sum_{i\in\mathbf{N}} a_i Q^i.$$

Remarque 3.6.9. — Notons que la notation donnée ici est compatible avec la notation $\sum_{i\in\mathbf{N}} a_i T^i$ définie précédemment.

3.7. Anneau de polynômes à plusieurs variables

Définition 3.7.1. — *L'anneau des polynômes à n variables* peut être défini par récurrence comme

$$A[T_1, \ldots, T_n] = A[T_1, \ldots, T_{n-1}][T_n].$$

Si $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ appartient à $\mathbf{N}^n$, on note $T^{\boldsymbol{\alpha}}$ pour le produit $\prod_{i=1}^n T_i^{\alpha_i}$. Tout polynôme de $A[T_1, \ldots, T_n]$ s'écrit alors de manière unique

$$P = \sum_{\boldsymbol{\alpha}\in\mathbf{N}^n} a_{\boldsymbol{\alpha}} T^{\boldsymbol{\alpha}}$$

avec $(a_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha}\in\mathbf{N}^n}$ une famille de $A^{\mathbf{N}^n}$ telle que $a_{\boldsymbol{\alpha}} = 0$ sauf pour un nombre fini d'éléments $\boldsymbol{\alpha}$ de $\mathbf{N}^n$.

Pour tout élément $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ de $\mathbf{N}^n$, on note $|\boldsymbol{\alpha}| = \sum_{i=1}^n \alpha_i$. On définit alors le *degré total* d'un polynôme $P = \sum_{\boldsymbol{\alpha}\in\mathbf{N}^n} a_{\boldsymbol{\alpha}} T^{\boldsymbol{\alpha}}$ comme

$$\deg(P) = \begin{cases} \sup\{\, |\boldsymbol{\alpha}|, a_{\boldsymbol{\alpha}} \neq 0 \,\} \text{ si } P \neq 0, \\ -\infty \text{ sinon.} \end{cases}$$

Proposition 3.7.2. — *Pour tous polynômes P et Q de $A[T_1, \ldots, T_n]$, on a*

(i) $\deg(P+Q) \leqslant \sup(\deg(P), \deg(Q))$ *avec égalité si* $\deg(P) \neq \deg(Q)$.
(ii) $\deg(PQ) \leqslant (\deg P) + \deg(Q)$ *avec égalité si A est intègre.*

Définition 3.7.3. — Un polynôme $P = \sum_{\boldsymbol{\alpha}\in\mathbf{N}^n} a_{\boldsymbol{\alpha}} T^{\boldsymbol{\alpha}}$ est dit homogène de degré d si et seulement si

$$\forall \boldsymbol{\alpha} \in \mathbf{N}^n, \quad |\boldsymbol{\alpha}| \neq d \Rightarrow a_{\boldsymbol{\alpha}} = 0.$$

Proposition 3.7.4 (Propriété universelle). — *Si A et B sont deux anneaux commutatifs et $\phi : A \to B$ un morphisme d'anneaux et b_1,…,b_n des éléments de B, il existe un unique morphisme d'anneaux $\psi : A[T_1, \ldots, T_n] \to B$ tel que la restriction de ψ à A coïncide avec ϕ et $\psi(T_i) = b_i$. On note $P(b_1, \ldots, b_n)$ pour $\psi(P)$.*

Définition 3.7.5. — Soit $P = \sum_{\boldsymbol{\alpha}\in\mathbf{N}^n} a_{\boldsymbol{\alpha}} T^{\boldsymbol{\alpha}}$ un élément de $A[T_1, \ldots, T_n]$. La *dérivée partielle de P par rapport à la variable T_i*, notée $\frac{\partial P}{\partial T_i}$ est définie par

$$\frac{\partial P}{\partial T_i} = \sum_{\substack{\boldsymbol{\alpha}\in\mathbf{N}^n \\ \alpha_i \geqslant 1}} \alpha_i a_{\boldsymbol{\alpha}} T_i^{\alpha_i - 1} \prod_{j\neq i} T_j^{\alpha_j}$$

Proposition 3.7.6. — *Pour tous polynômes $P, Q \in A[T_1, \ldots, T_n]$, on a*

$$\frac{\partial P+Q}{\partial T_i} = \frac{\partial P}{\partial T_i} + \frac{\partial Q}{\partial T_i} \quad \textit{et} \quad \frac{\partial PQ}{\partial T_i} = \frac{\partial P}{\partial T_i}Q + P\frac{\partial Q}{\partial T_i}.$$

Proposition 3.7.7. — *Soit $P \in A[T_1, \ldots, T_n]$. Soient $(x_1, \ldots, x_n)$ et $(l_1, \ldots, l_n)$ des éléments de A^n. Notons $Q \in A[T]$ le polynôme défini par*

$$Q(T) = P(x_1 + l_1T, \ldots, x_n + l_nT).$$

Alors la valeur de la dérivée de Q en 0 est donnée par la formule

$$Q'(0) = \sum_{i=0}^{n} \frac{\partial P}{\partial T_i}(x_1, \ldots, x_n)l_i.$$

3.8. Anneau euclidien, anneau principal

La notion de division sur les polynômes et les entiers conduit à la notion d'anneau euclidien.

Définition 3.8.1. — Un anneau intègre A est dit *euclidien* s'il existe une application ϕ de $A - \{0\}$ dans $\mathbf{N}$ appelée *stathme* telle que

$$\forall b \in A - 0,\ \forall a \in A,\ \exists (q, r) \in A^2, \quad a = bq + r \text{ avec } r = 0 \text{ ou } \phi(r) < \phi(b).$$

Exemple 3.8.2. — L'anneau des entiers est euclidien pour la valeur absolue.

Exemple 3.8.3. — Si $\mathbf{K}$ est un corps, l'anneau des polynômes $\mathbf{K}[T]$ est un anneau euclidien pour le degré.

Définition 3.8.4. — Un idéal I est dit *principal* s'il est engendré par un de ses éléments : $I = (x)$. Un anneau intègre est dit *principal* si tout ses idéaux sont principaux.

Proposition 3.8.5. — *Tout anneau euclidien est principal.*

Démonstration. — Soit A un anneau euclidien et I un idéal de A. Si $I \neq (0)$, il existe un élément non nul dans I. On choisit un élément x de $I - \{0\}$ tel que $\phi(x)$ soit minimal. Alors $I = (x)$. En effet pour tout $y \in I$, on écrit $y = xq + r$ avec $r = 0$ ou $\phi(r) < \phi(x)$. Comme $r = y - xq$, $r \in I$ et par minimalité de $\phi(x)$, $r = 0$. Donc $y \in (x)$. □

Proposition 3.8.6. — *Soit A un anneau principal. Les trois assertions suivantes sont équivalentes :*

(i) $\mathfrak{a}$ *est un idéal maximal non nul de A.*
(ii) $\mathfrak{a}$ *est un idéal premier non nul de A.*
(iii) *Il existe un élément p de A irréductible tel que $\mathfrak{a} = (p)$.*

Démonstration. — (i)⇒(ii) Puisqu'un idéal maximal est premier.

(ii)⇒(iii) Comme A est principal, il existe p tel que $\mathfrak{a} = (p)$ mais comme (p) est premier et p non nul, p est irréductible.

(iii)⇒(i) Soit p irréductible et $\mathfrak{a} = (p)$. Par hypothèse $p \notin A^\times$, donc $\mathfrak{a} \neq A$. Soit $\mathfrak{b}$ tel que $\mathfrak{a} \subset \mathfrak{b}$. Comme A est principal, $\mathfrak{b} = (q)$. Donc $q \mid p$. si $\mathfrak{a} \neq \mathfrak{b}$, alors q et p ne sont pas associés. Donc $q \in A^\times$ et $\mathfrak{b} = A$. □

Corollaire 3.8.7 (Lemme d'Euclide). — *Soit A un anneau principal, p un élément irréductible dans A et a, b deux éléments de A. Alors*

$$p \mid ab \Rightarrow (p \mid a \text{ ou } p \mid b).$$

Proposition 3.8.8. — *Si A est principal, toute famille $(a_i)_{i\in I}$ d'éléments de A admet un* pgcd *et un* ppcm.

Démonstration. — Le pgcd est donné comme un générateur de l'idéal $\sum_{i\in I}(a_i)$ et le ppcm comme générateur de l'idéal $\bigcap_{i\in I}(a_i)$. □

Proposition 3.8.9 (Bezout). — *Si A est un anneau principal et si $a_1, \ldots, a_n \in A$, alors il existe $b_1, \ldots, b_n \in A$ tels que*

$$a_1b_1 + \cdots + a_nb_n = \mathrm{pgcd}(a_1, \ldots, a_n).$$

Démonstration. — En effet, dans ce cas $\mathrm{pgcd}(a_1, \ldots, a_n)$ est un générateur de $(a_1, \ldots, a_n)$ dont les éléments sont de la forme $a_1b_1 + \cdots + a_nb_n$ avec $(b_1, \ldots, b_n) \in A^n$. □

Corollaire 3.8.10. — *Si A est principal, alors a_1,…,a_n sont premiers dans leur ensemble si et seulement s'il existe b_1,…,b_n dans A tels que*

$$a_1b_1 + \ldots a_nb_n = 1.$$

Démonstration. — Par la proposition précédente, il suffit de montrer que si

$$a_1b_1 + \ldots a_nb_n = 1,$$

alors a_1,…,a_n sont premiers entre eux. Mais dans ce cas

$$\mathrm{pgcd}(a_1, \ldots, a_n) \mid 1$$

et est donc associé à 1. □

Remarque 3.8.11. — Si A est un anneau euclidien, il est possible de calculer les coefficients b_1,…,b_n de la proposition 3.8.9. Tout d'abord on peut se ramener au cas $n = 2$. En effet, on a $\mathrm{pgcd}(a_1, \ldots, a_n) = \mathrm{pgcd}(\mathrm{pgcd}(a_1, \ldots, a_{n-1}), a_n)$ et si

$$b_1a_1 + \ldots b_{n-1}a_{n-1} = \mathrm{pgcd}(a_1, \ldots, a_{n-1})$$

et

$$u\,\mathrm{pgcd}(a_1, \ldots, a_{n-1}) + va_n = \mathrm{pgcd}(a_1, \ldots, a_n),$$

alors

$$ub_1a_1 + \cdots + ub_{n-1}a_{n-1} + va_n = \mathrm{pgcd}(a_1, \ldots, a_n).$$

Dans le cas $n = 2$, on utilise l'algorithme de calcul de $\mathrm{pgcd}(a, b)$: on pose $a_0 = a$, $b_0 = b$ et on effectue la division euclidienne $a_{n-1} = a_nq_n + a_{n+1}$ jusqu'au moment où $a_{n+1} = 0$ auquel cas $a_n = \mathrm{pgcd}(a, b)$. L'idée est donc de trouver des coefficients $(u_n, v_n) \in A$ tels que $a_n = u_na + v_nb$. Ils sont donnés de manière récursive par les relations

$$\begin{array}{rclcrcl} u_0 & = & 1 & \text{et} & v_0 & = & 0 \\ u_1 & = & 0 & \text{et} & v_1 & = & 1 \\ u_{n+1} & = & u_{n-1} - q_nu_n & \text{et} & v_{n+1} & = & v_{n-1} - q_nv_n \end{array}$$

ce qui donne l'algorithme suivant :

Algorithme 3.8.12.
Entrée:
- a, $b \in A$, A anneau euclidien.

Sortie:
- (d, u, v) tel que
  a. $d = \mathrm{pgcd}(a, b)$,
  b. $ua + vb = d$.

Algorithme:
1. $u_0 \leftarrow 1$, $u_1 \leftarrow 0$, $v_0 \leftarrow 0$, $v_1 \leftarrow 1$.
2. Si $b = 0$, alors
   2.1 Renvoyer (a, u_0, v_0). Fin de l'algorithme.
3. Effectuer la division euclidienne $a = bq + r$.
4. $a \leftarrow b$, $b \leftarrow r$.
5. $t \leftarrow u_1$, $u_1 \leftarrow u_0 - qu_1$, $u_0 \leftarrow t$.
6. $t \leftarrow v_1$, $v_1 \leftarrow v_0 - qv_1$, $v_0 \leftarrow t$.
7. Retourner à l'étape 2.

Corollaire 3.8.13. — *Soient A un anneau principal et a, b deux éléments de A. Alors $\overline{b}$ est inversible dans $A/(a)$ si et seulement si b est premier avec a.*

Démonstration. — $\Rightarrow$: Si $\overline{b}$ est inversible, il existe $v \in A$ tel que $\overline{b}\overline{v} = 1$, c'est-à-dire que a divise $bv - 1$. Il existe donc $u \in A$ tel que $1 = bv + au$. Par conséquent b est premier à a.

$\Leftarrow$: Si $\mathrm{pgcd}(a, b) = 1$, par le théorème de Bezout, il existe deux éléments u et v de A tels que $au + bv = 1$. D'où la relation $\overline{b}\overline{v} = 1$. □

Remarque 3.8.14. — Si A est euclidien, l'algorithme permettant de calculer les coefficients de Bezout permet donc également de calculer les inverses dans $A/(a)$.

Proposition 3.8.15 (Lemme de Gauss). — *Si A est principal, alors il vérifie le lemme de Gauss : Si a est premier avec b et $a \mid bc$, alors $a \mid c$.*

Démonstration. — La démonstration est exactement la même que dans le cas des entiers (cf. proposition 1.2.7). Par le théorème de Bezout, il existe u et v tels que $au + bv = 1$. Comme $a \mid auc$ et $a \mid bvc$ par hypothèse, $a \mid auc + bvc = c$. □

3.9. Décomposition en facteurs irréductibles

Définition 3.9.1. — Un anneau intègre est dit factoriel si et seulement s'il vérifie les conditions suivantes :

Existence. Pour tout élément non nul a de A il existe un entier positif ou nul n, un élément inversible u de A et des éléments irréductibles $p_1, \ldots, p_n$ de A tels que

$$a = up_1 \ldots p_n.$$

Unicité. Soient $m, n \in \mathbf{N}$, $p_1, \ldots, p_m, q_1, \ldots, q_n$ des éléments irréductibles et u, v des éléments inversibles tels que

$$up_1 \ldots p_m = vq_1 \ldots q_n.$$

alors $m = n$ et il existe une permutation $\sigma \in \mathfrak{S}_n$ telle que $q_i \sim p_{\sigma(i)}$ pour $i = 1, \ldots, n$.

Cette condition peut s'exprimer d'une deuxième façon en utilisant la notion de système de représentants des irréductibles.

Définition 3.9.2. — Un partie $\mathscr{I}$ de A est appelée un *système de représentants des irréductibles de* A si et seulement si tout élément de $\mathscr{I}$ est irréductible et tout élément irréductible de A est associé à un unique élément de $\mathscr{I}$.

Dans la suite nous utiliserons uniquement les deux exemples fondamentaux suivants :

Exemple 3.9.3. — Si $A = \mathbf{Z}$, l'ensemble $\mathscr{P}$ des nombres premiers positifs est un système de représentants des irréductibles de $\mathbf{Z}$. Si $A = \mathbf{K}[T]$, l'ensemble $\mathscr{I}$ des polynômes irréductibles unitaires convient.

On peut alors donner une nouvelle définition des anneaux factoriels qui est équivalente à la précédente :

Définition 3.9.4. — Soit A un anneau intègre et $\mathscr{I}$ un système de représentants des irréductibles de A. L'anneau A est factoriel si et seulement si pour tout élément non nul a de A ; il existe un unique élément inversible u de A et une unique application

$$\begin{array}{ccc} \mathscr{I} & \to & \mathbf{N} \\ p & \mapsto & v_p(a) \end{array}$$

telle que $v_p(a) = 0$ sauf pour un nombre fini de p et

$$a = u \prod_{p \in \mathscr{I}} p^{v_p(a)}.$$

Pour tout p de $\mathscr{I}$, $v_p(a)$ est appelée la *valuation p-adique* de a.

Théorème 3.9.5. — *Tout anneau principal est factoriel.*

Exemple 3.9.6. — En particulier, l'anneau des entiers $\mathbf{Z}$ est un anneau factoriel de même que l'anneau $\mathbf{K}[T]$ si $\mathbf{K}$ est un corps.

Démonstration. — **Existence.** On raisonne par l'absurde : soit a_0 un élément de $A - 0$, non inversible, qui ne s'écrit pas comme produit d'éléments irréductibles. En particulier a_0 n'est pas irréductible et on peut écrire $a_0 = a_1 a_1'$ avec a_1 et a_1' non inversibles. Si ces deux éléments sont produits d'irréductibles, alors il en est de même de a_0. Quitte à échanger a_1 et a_1', on peut supposer que a_1 n'est pas produit d'irréductibles. En itérant, on obtient une suite infinie $a_0, \ldots, a_n, \ldots$ d'éléments tels que

$$(a_0) \subsetneq (a_1) \subsetneq \cdots \subsetneq (a_n) \subsetneq \ldots$$

La réunion $I = \bigcup_{n=0}^{+\infty}(a_i)$ est un idéal de A, En effet $0 \in I$ et si b_1 et b_2 appartiennent à I, il existe n_1 et n_2 tels que $b_1 \in (a_{n_1})$ et $b_2 \in (a_{n_2})$. Soit $n = \sup(n_1, n_2)$, alors $b_1 - b_2 \in (a_n)$

donc I est un sous-groupe de A et si b appartient à I et a à A il existe n tel que $b \in (a_n)$ et $ab \in (a_n)$. Comme A est principal, il existe $a \in A$ tel que $I = (a)$. Comme $a \in I$, il existe n tel que $a \in (a_n)$ donc

$$(a_n) \subsetneq (a_{n+1}) \subset I = (a) \subset (a_n)$$

ce qui est absurde.

Unicité. Si on a une égalité de la forme

$$up_1 \dots p_m = vq_1 \dots q_n$$

avec u et v inversibles et $p_1, \dots, p_m, q_1 \dots q_n$ irréductibles. Quitte à échanger les deux membres de l'égalité, on peut supposer $m \geqslant n$. On procède alors par récurrence sur m. Si $m = 0$, alors $n = 0$ et le résultat annoncé est vrai. Supposons le résultat montré pour $m - 1$ avec $m \geqslant 1$. On a

$$p_1 \mid vq_1 \dots q_n.$$

Mais, par le lemme d'Euclide, p_1 divise v ou l'un des q_i. Comme v est inversible, si $p_1 \mid v$, alors p_1 est inversible ce qui contredit le fait que p_1 soit irréductible. Donc p_1 divise l'un des q_i. Quitte à échanger les q_i, on peut supposer que $p_1 \mid q_1$. Donc $q_1 = wp_1$. Comme q_1 est irréductible et p_1 non-inversible, w est inversible. On obtient une égalité

$$up_2 \dots p_m = (vw)q_2 \dots q_n$$

et on applique l'hypothèse de récurrence. □

Proposition 3.9.7. — *Si A est un anneau factoriel et $\mathscr{I}$ un système de représentants des irréductibles de A, alors*

(i) $\forall a, b \in A, \quad a \mid b \Leftrightarrow (\forall p \in \mathscr{I}, v_p(a) \leqslant v_p(b))$

(ii) *Pour tout n-uplet $(a_1, \dots, a_n)$ d'éléments de A,*

$$\operatorname{pgcd}(a_1, \dots, a_n) = \prod_{p \in \mathscr{I}} p^{\inf_{1 \leqslant i \leqslant n} v_p(a_i)}$$

(iii) *Pour tout n-uplet $(a_1, \dots, a_n)$ d'éléments de A,*

$$\operatorname{ppcm}(a_1, \dots, a_n) = \prod_{p \in \mathscr{I}} p^{\sup_{1 \leqslant i \leqslant n} v_p(a_i)}$$

Corollaire 3.9.8. — *Si A est un anneau factoriel et $a, b \in A$, alors*

$$\operatorname{pgcd}(a, b) \operatorname{ppcm}(a, b) = ab$$

3.10. Théorème des restes chinois

Commençons par énoncer deux résultats préliminaires :

Lemme 3.10.1. — *Soit A un anneau principal et soient $a_1, \dots, a_n, b$ des éléments de A. Si b est premier avec chacun des a_i pour $1 \leqslant i \leqslant n$, alors b est premier avec $a_1 \dots a_n$.*

Démonstration. — On procède par récurrence. L'énoncé est vrai si $n = 1$. Montrons le pour $n = 2$. Par le théorème de Bezout, comme b est premier avec a_1 et a_2, il existe des éléments x_1, y_1, x_2 et y_2 de A tels que

$$1 = x_1 b + y_1 a_1 \quad \text{et} \quad 1 = x_2 b + y_2 a_2.$$

Par conséquent,

$$1 = (x_1 b + y_1 a_1)(x_2 b + y_2 a_2) = (x_1 x_2 b + y_1 a_1 x_2 + x_1 y_2 a_2) b + (y_1 y_2) a_1 a_2$$

ce qui implique le résultat dans ce cas. Si le résultat est vrai pour $n - 1$, par hypothèse de récurrence, b est premier avec $\prod_{i=1}^{n-1} a_i$ et a_n. Donc, en utilisant le cas $n = 2$, on obtient que b est premier avec le produit $\prod_{i=1}^{n} a_i$. □

Lemme 3.10.2. — *Si A est un anneau principal et a_1,...,a_n des éléments premiers entre eux deux à deux, alors*

$$\mathrm{ppcm}(a_1, \ldots, a_n) = \prod_{i=1}^{n} a_i$$

Démonstration. — On montre la proposition par récurrence. Elle est vraie pour $n = 1$. Si $n = 2$, comme

$$a_1 \mid \frac{\mathrm{ppcm}(a_1, a_2)}{a_2} \times a_2,$$

en appliquant le lemme de Gauss, a_1 divise $\mathrm{ppcm}(a_1, a_2)/a_2$ et donc $a_1 a_2 \mid \mathrm{ppcm}(a_1, a_2)$. Le résultat pour $n = 2$ découle alors du fait que $\mathrm{ppcm}(a_1, a_2) \mid a_1 a_2$ par définition. Enfin pour la récurrence on utilise l'assertion qui précède et l'égalité

$$\mathrm{ppcm}(a_1, \ldots, a_n) = \mathrm{ppcm}(\mathrm{ppcm}(a_1, \ldots, a_{n-1}), a_n). \quad \square$$

Théorème 3.10.3. — *Si A est un anneau principal et a_1,...,a_n des éléments premiers entre eux deux à deux, alors*

$$A/(a_1 \ldots a_n) \xrightarrow{\sim} A/(a_1) \times \cdots \times A/(a_n).$$

Démonstration. — Pour $i \in \{1, \ldots, n\}$, notons $\pi_i : A \to A/(a_i)$ la projection canonique et considérons l'application

$$\begin{array}{rl} A & \to A/(a_1) \times \ldots A/(a_n) \\ a & \mapsto (\pi_1(a_1), \ldots, \pi_n(a_n)) \end{array}$$

produit des projection canoniques. Son noyau est $\bigcap_{i=1}^{n} \mathrm{Ker}\, \pi_i$, c'est-à-dire $\bigcap_{i=1}^{n} (a_i)$ qui, par la proposition précédente coïncide avec $(\prod_{i=1}^{n} a_i)$. On obtient donc un morphisme injectif

$$A/(a_1 \ldots a_n) \to A/(a_1) \times \cdots \times A/(a_n).$$

Il reste donc à montrer que cette application est surjective. Cela revient donc à montrer que, sous les hypothèses du théorème, pour toute famille $(x_1, \ldots, x_n)$ de A^n, il existe x dans A tel que $a_i \mid x - x_i$ pour tout i entre 1 et n. Là encore, nous allons procéder par récurrence. Pour $n = 1$, le résultat est vrai. Pour $n = 2$, en utilisant Bezout, on peut écrire $1 = a_1 b_1 + a_2 b_2$, avec b_1 et b_2 des éléments de A. On pose $x = a_2 b_2 x_1 + a_1 b_1 x_2$. On obtient

$$x - x_1 = a_1 b_1 (x_2 - x_1) \quad \text{et} \quad x - x_2 = a_2 b_2 (x_1 - x_2).$$

Donc x convient.

Si le résultat est vrai pour $n-1$, il existe y telque $a_i \mid y - x_i$ pour $1 \leqslant i \leqslant n-1$ et, en utilisant le cas $n = 2$, il existe un élément x de A tel que $\prod_{i=1}^{n-1} a_i \mid x - y$ et $a_n \mid x_n - y$. Par conséquent $a_i \mid x - y_i$ pour $i = 1, \ldots, n$. □

3.11. Retour sur les entiers

3.11.1. Éléments inversibles dans $\mathbf{Z}/n\mathbf{Z}$

Proposition 3.11.1. — *Soit m un entier strictement positif, et a un entier relatif. Les conditions suivantes sont équivalentes :*

(i) *$\overline{a}$ est un générateur du groupe $(\mathbf{Z}/m\mathbf{Z}, +)$,*
(ii) *$\overline{a}$ est inversible dans l'anneau $\mathbf{Z}/m\mathbf{Z}$,*
(iii) *a est premier à m.*

On note $\varphi(m)$ le cardinal de $(\mathbf{Z}/m\mathbf{Z})^\times$. La fonction φ est appelée fonction indicatrice d'Euler. *On a la relation*

$$\varphi(m) = m \prod_{\{p \in \mathscr{P} \,|\, p|m\}} \left(1 - \frac{1}{p}\right)$$

Démonstration. — $(i) \Rightarrow (ii)$: $1 \in \mathbf{Z}/m\mathbf{Z}$ appartient au sous-groupe engendré par $\overline{a}$. Donc, il existe un entier b tel que $1 = b\overline{a}$ et donc $\overline{b}$ est un inverse de $\overline{a}$.

$(ii) \Rightarrow (iii)$: Découle du résultat général pour les anneaux principaux.

$(iii) \Rightarrow (i)$: Soit x un entier $x \in (a, m) = \mathbf{Z}$. Donc il existe des entiers u et v tels que $x = au + mv$ et donc $\overline{x} = u\overline{a}$. Donc $\mathbf{Z}/n\mathbf{Z}$ est engendré par a.

Par le théorème des restes chinois, si $m = p_1^{n_1} \ldots p_r^{n_r}$ est la décomposition de m en facteur irréductibles, on a un isomorphisme d'anneaux

$$\mathbf{Z}/m\mathbf{Z} \xrightarrow{\sim} \prod_{i=1}^{r} \mathbf{Z}/p_i^{n_i}\mathbf{Z}.$$

En considérant les éléments inversibles, on obtient un isomorphisme de groupes

$$(\mathbf{Z}/m\mathbf{Z})^\times \xrightarrow{\sim} \prod_{i=1}^{r} (\mathbf{Z}/p_i^{n_i}\mathbf{Z})^\times.$$

Par conséquent

$$\varphi(m) = \prod_{i=1}^{r} \varphi(p_i^{n_i}).$$

Mais si p est premier, a est premier à p si et seulement s'il n'est pas divisible par p. Donc

$$\varphi(p^n) = p^{n-1}(p-1). \quad \square$$

Corollaire 3.11.2. — *Pour tout entier n strictement positif et tout élément a de $(\mathbf{Z}/n\mathbf{Z})^\times$, on a*

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

Démonstration. — Cela résulte de la proposition 2.3.8 (i). □

3.11.2. Application à la cryptographie : RSA. — Ce système cryptographique à clef publique, qui est la première implémentation du système général de Diffie et Hellman [**DH**] a été développé par R. Rivest, A. Shamir et L. Adleman [**RSA**]. Il repose sur le manque d'algorithme efficace pour donner la décomposition en facteurs premiers d'un entier. La procédure est la suivante :

Choix des clefs.

Alice choisit deux nombre premiers de grande taille p et q et un nombre e tel que

$$\mathrm{pgcd}(e, \varphi(pq)) = 1,$$

où $\varphi(pq) = (p-1)(q-1)$. Elle calcule alors $N = pq$ et $d = e^{-1}$ dans $\mathbf{Z}/\varphi(N)\mathbf{Z}$. La clef publique est alors la paire (N, e) et la clef secrète la valeur de d.

Cryptage.

Pour crypter un message m appartenant à $(\mathbf{Z}/N\mathbf{Z})^\times$, Bob reçoit la clef (N, e) d'Alice, il calcule $c = m^e$ dans $(\mathbf{Z}/N\mathbf{Z})^\times$. Le texte crypté est c.

Décryptage.

Alice reçoit c et en déduit le message m par la formule $m = c^d$. En effet on a la congruence $ed \equiv 1 \pmod{\varphi(N)}$ et $m^{\varphi(N)} = 1$. Donc $c^d = m^{ed} = m$ dans $\mathbf{Z}/N\mathbf{Z}$.

Hypothèse.

Il est difficile de retrouver $(p-1)(q-1)$ à partir de pq. C'est-à-dire qu'il est difficile de trouver les facteurs irréductibles de N.

3.11.3. Le corps $\mathbf{F}_p$

Proposition 3.11.3. — *Si m est un nombre entier positif ou nul, l'idéal (m) de $\mathbf{Z}$ est un idéal premier si et seulement si m est nul ou un nombre premier et un idéal maximal si et seulement si m est un nombre premier.*

Démonstration. — Il s'agit d'une reformulation pour les entiers de 3.8.6. □

Définition 3.11.4. — Si p est un nombre premier, on note $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$.

Proposition 3.11.5 (Petit théorème de Fermat). — *Pour tout nombre premier p, on a*

$$\forall x \in \mathbf{F}_p, \quad x^p = x.$$

Démonstration. — Si $x \neq 0$ alors cela résulte du corollaire 3.11.2. Si $x = 0$, c'est immédiat. □

3.11.4. Caractéristique d'un corps, sous-corps premier

Proposition 3.11.6. — *La caractéristique d'un corps $\mathbf{K}$ est 0 ou un nombre premier. Si la caractéristique du corps est nulle, celui-ci contient un sous-corps isomorphe à $\mathbf{Q}$. Sinon, il contient un sous-corps isomorphe à $\mathbf{F}_p$ où p est sa caractéristique. Le corps ainsi obtenu est le plus petit corps contenu dans $\mathbf{K}$, on l'appelle* sous-corps premier *de $\mathbf{K}$.*

Démonstration. — Notons p la caractéristique du corps $\mathbf{K}$. Si $p = 0$ la proposition découle de l'exemple 3.1.10. Si $p > 0$, alors, par définition de la caractéristique, on a un morphisme injectif d'anneaux

$$\mathbf{Z}/p\mathbf{Z} \hookrightarrow \mathbf{K},$$

donc $\mathbf{Z}/p\mathbf{Z}$ est intègre et p premier. □

EXERCICES

3.1. Effectuer la division euclidienne de $2T^4 - 3T^3 + 6T^2 - 15T$ par $T^2 - T + 4$ et de T^5 par $T^2 + T - 3$.

3.2. On considère l'équation

$$(*) \qquad X^2 - X = 0$$

1. Résoudre l'équation $(*)$ dans $\mathbf{Z}/10\mathbf{Z}$, $\mathbf{Z}/8\mathbf{Z}$ et $\mathbf{Z}/40\mathbf{Z}$.
2. Soient p et q deux nombres premiers distincts. Combien l'équation $(*)$ a-t-elle de solutions dans $\mathbf{Z}/pq\mathbf{Z}$?
3. Soient p, q et r trois nombres premiers deux à deux distincts. Combien l'équation $(*)$ a-t-elle de solutions dans $\mathbf{Z}/pqr\mathbf{Z}$?

CHAPITRE 4

MODULES ET ESPACES VECTORIELS

4.1. Notion de module

Définition 4.1.1. — Soit A un anneau commutatif. Un A-*module* est la donnée d'un groupe abélien M muni d'une loi externe

$$\begin{array}{rcl} A \times M & \to & M \\ (a, m) & \mapsto & am \end{array}$$

satisfaisant aux propriétés suivantes :

Mo1. $\forall a \in A, \quad \forall x, y \in M, \quad a(x + y) = ax + ay$,
Mo2. $\forall a, b \in A, \forall x \in M, \quad (a + b)x = ax + bx$,
Mo3. $\forall a, b \in A, \forall x \in M, \quad a(bx) = (ab)x$.
Mo4. $\forall x \in M, \quad 1x = x$.

Si $\mathbf{K}$ est un corps *un espace vectoriel* sur $\mathbf{K}$ est un $\mathbf{K}$-module.

Exemple 4.1.2. — Si $A = \mathbf{Z}$ la notion de $\mathbf{Z}$-module coïncide avec celle de groupe abélien. En effet si M est un groupe abélien alors il existe une unique structure de $\mathbf{Z}$-module sur M ; elle est donnée par la loi externe

$$\begin{array}{rcl} \mathbf{Z} \times M & \to & M \\ (a, m) & \mapsto & am \end{array}$$

définie dans l'exemple 2.1.9.

Exemple 4.1.3. — Si A est un anneau commutatif et $n \in \mathbf{N}$, A^n est un A-module pour la loi externe définie par

$$\begin{array}{rcl} A \times A^n & \to & A^n \\ (\lambda, (a_1, \ldots, a_n)) & \mapsto & (\lambda a_1, \ldots, \lambda a_n). \end{array}$$

Exemple 4.1.4. — Si X est un ensemble et M un A-module alors l'ensemble M^X des applications de X vers M qui est un groupe abélien par la loi définie dans l'exemple 2.1.5 est muni d'une structure de A-module par la lois externe

$$\begin{array}{rcl} A \times M^X & \to & M^X \\ (\lambda, f) & \mapsto & (x \mapsto \lambda f(x)). \end{array}$$

Exemple 4.1.5. — Si A est un anneau commutatif, alors $A[T]$ muni de l'addition de polynômes et de la loi externe

$$\begin{array}{rcl} A \times A[T] & \to & A[T] \\ (\lambda, \sum_{i=0}^{d} a_i T^i) & \mapsto & \sum_{i=0}^{d} \lambda a_i T^i \end{array}$$

est un A-module.

Définition 4.1.6. — Soient M et N deux A-modules. Une application $\phi : M \to N$ est un *morphisme de A-modules* si c'est un morphisme de groupe et si elle vérifie la condition suivante :

Mor. $\forall \lambda \in A, \quad \forall m \in M, \quad \phi(\lambda m) = \lambda \phi(m)$.

On dit également *application linéaire* pour morphisme de A-modules. Un *isomorphisme de A-modules* est un morphisme de A-modules qui est bijectif. Son inverse est alors un morphisme de A-modules.

4.2. Sous-modules

Définition 4.2.1. — Soit A un anneau commutatif et M un A-module, un sous-module de M est un sous-groupe N de M tel que

Sous-module. $\forall \lambda \in A, \quad \forall x \in N, \quad \lambda x \in N$.

La restriction de la loi externe à N munit alors N d'une structure de A-modules de sorte que l'inclusion $M \hookrightarrow N$ soit un morphisme de A-modules. Si $\mathbf{K}$ est un corps, un sous-module d'un $\mathbf{K}$-espace vectoriel est appelé *sous-espace vectoriel*.

Exemple 4.2.2. — Si A est un anneau commutatif, un sous-module du A-module A est un idéal de A.

Exemple 4.2.3. — Si M et N sont deux A-modules, l'ensemble $\mathscr{L}(M, N)$ des applications linéaires de M vers N est un sous A-module de N^M. En particulier, si $\mathbf{K}$ est un corps et E un $\mathbf{K}$-espace vectoriel, le *dual de E*, noté $E^\vee$ est l'espace vectoriel $\mathscr{L}(E, \mathbf{K})$.

4.3. Rappels sur les espaces vectoriels

Définition 4.3.1. — Soit $\mathbf{K}$ un corps une famille $(a_i)_{i \in I}$ d'éléments de $\mathbf{K}$ est dite *presque nulle* si seulement si l'ensemble

$$\{\, i \in I \mid a_i \neq 0 \,\}$$

est fini. Soient E un espace vectoriel sur $\mathbf{K}$ et $\boldsymbol{e} = (e_i)_{i \in I}$ une famille d'éléments de E. La famille $\boldsymbol{e}$ est

- une famille *génératrice* si et seulement si pour tout x de E, il existe une famille presque nulle $(a_i)_{i \in I}$ d'éléments de $\mathbf{K}$ tels que

$$x = \sum_{i \in I} a_i e_i,$$

- une famille *libre* si et seulement si pour toute famille presque nulle $(a_i)_{i \in I}$ d'éléments de $\mathbf{K}$, on a

$$\sum_{i \in I} a_i e_i = 0 \Rightarrow \forall i \in I,\ a_i = 0,$$

On dit alors que les éléments de $\{a_i, i \in I\}$ sont linéairement indépendants.

- une *base* de E si elle est à la fois libre et génératrice. Tout élément x de E s'écrit alors de manière unique sous la forme

$$x = \sum_{i \in I} a_i e_i$$

pour une famille presque nulle $(a_i)_{i \in I}$. Dans ce cas, si $x = \sum_{i \in I} a_i e_i$, on dit que $(a_1, \ldots, a_n)$ sont les coordonnées de x dans la base $\boldsymbol{e}$.

Proposition 4.3.2. — *Si E est un espace vectoriel et $\boldsymbol{e} = (e_i)_{i \in I}$ une famille d'éléments de E, les conditions suivantes sont équivalentes :*

(i) *la famille $\boldsymbol{e}$ est une base de E,*
(ii) *la famille $\boldsymbol{e}$ est une famille génératrice et toute sous-famille de $\boldsymbol{e}$ distincte de $\boldsymbol{e}$ n'est pas génératrice,*
(iii) *la famille $\boldsymbol{e}$ est une famille libre et toute famille contenant $\boldsymbol{e}$ distincte de $\boldsymbol{e}$ n'est pas libre.*

Définition 4.3.3. — Un espace vectoriel est dit *de dimension finie* si et seulement s'il admet une famille génératrice finie.

Théorème 4.3.4. — *Si E est un espace vectoriel de dimension finie, toute les bases de E ont le même cardinal appelé* dimension *de E et noté* $\dim E$. *En outre,*

- *une famille génératrice a au moins* $\dim E$ *composantes et est une base si elle en a exactement* $\dim E$*,*
- *une famille libre a au plus* $\dim E$ *composantes et est un base si elle en a exactement* $\dim E$*.*

Exemple 4.3.5. — Si $\mathbf{K}$ est un corps l'ensemble $\mathbf{K}[T]_d$ des polynômes de degré inférieur ou égal à d est un sous-espace vectoriel de $\mathbf{K}[T]$ de dimension $d+1$, une base de cet espace vectoriel étant donné par les monômes $1, T, \ldots, T^d$.

Exemple 4.3.6. — Si $\mathbf{K}$ est un corps et P un polynôme non nul de $\mathbf{K}[T]$ alors par le corollaire 3.5.16, le quotient $\mathbf{K}[T]/(P)$ est un espace vectoriel de dimension $\deg(P)$, une base de cet espace vectoriel étant $(\overline{1}, \ldots, \overline{T}^{\deg P - 1})$.

Exemple 4.3.7. — Si E est un $\mathbf{K}$-espace vectoriel de dimension finie et $(e_1, \ldots, e_n)$ une base de E, alors $E^\vee$ est un espace vectoriel de dimension finie, une base étant donnée par $(e_1^\vee, \ldots, e_n^\vee)$ où $e_i^\vee$ est définie par

$$\forall (a_1, \ldots, a_n) \in \mathbf{K}^n, \quad e_i^\vee \Big(\sum_{i=1}^n a_i e_i \Big) = a_i.$$

$(e_1^\vee, \ldots, e_n^\vee)$ est appelée la base duale de $(e_1, \ldots, e_n)$.

4.4. Matrices de changement de bases

Définition 4.4.1. — Soit E un $\mathbf{K}$-espace vectoriel de dimension finie. Si $\boldsymbol{e} = (e_1, \ldots, e_n)$ et $\boldsymbol{e}' = (e'_1, \ldots, e'_n)$ sont deux bases de E, la matrice $(e_i^\vee(e'_j))_{1 \leqslant i,j \leqslant n}$ qui a pour j-ième colonne les coordonnées de e'_j dans la base $\boldsymbol{e}$ est appelée *matrice de changement de bases*. On la notera $P_{\boldsymbol{e}}^{\boldsymbol{e}'}$.

Proposition 4.4.2. — *(i) Soit $\boldsymbol{x}$ un élément de E. On pose*

$$\boldsymbol{x} = \sum_{i=1}^{n} x_i e_i \quad \textit{et} \quad \boldsymbol{x} = \sum_{i=1}^{n} x'_i e'_i$$

Alors

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = P_{\boldsymbol{e}}^{\boldsymbol{e}'} \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix}$$

(ii) On a les relations

$$P_{\boldsymbol{e}}^{\boldsymbol{e}'} P_{\boldsymbol{e}'}^{\boldsymbol{e}''} = P_{\boldsymbol{e}}^{\boldsymbol{e}''} \quad \textit{et} \quad P_{\boldsymbol{e}'}^{\boldsymbol{e}} = (P_{\boldsymbol{e}}^{\boldsymbol{e}'})^{-1}.$$

4.5. Transformée de Fourier discrète

Définition 4.5.1. — Si G est un groupe, on appelle *caractère* de G tout morphisme de groupes de G dans $\mathbf{C}^\times$. On note $X^*(G)$ le groupe des caractères de G.

Exemple 4.5.2. — Si $G = \mathbf{Z}/n\mathbf{Z}$ un morphisme χ de G dans $\mathbf{C}^\times$ est déterminé par l'image de $\overline{1}$ qui vérifie $\chi(\overline{1})^n = \chi(\overline{0}) = 1$. Il appartient donc au groupe des racines n-ième de l'unité dans $\mathbf{C}$ défini par $\mu_n(\mathbf{C}) = \{x \in \mathbf{C} \mid x^n = 1\}$. Inversement si ζ est une racine n-ième de l'unité, l'application

$$\begin{array}{rcl} \mathbf{Z}/n\mathbf{Z} & \to & \mathbf{C}^\times \\ \overline{x} & \mapsto & \zeta^x \end{array}$$

est un caractère de $\mathbf{Z}/n\mathbf{Z}$ on a ainsi obtenu une bijection du groupe $\mu_n(\mathbf{C})$ des racines n-ièmes de $\mathbf{C}$ sur $X^*(\mathbf{Z}/n\mathbf{Z})$. Notons en outre que l'exponentielle complexe fournit un isomorphisme de groupes

$$\begin{array}{rcl} \mathbf{Z}/n\mathbf{Z} & \to & \mu_n(\mathbf{C}) \\ \overline{x} & \mapsto & e^{\frac{2i\pi x}{n}}. \end{array}$$

Notation 4.5.3. — Si X est un ensemble fini, on considère la forme

$$\begin{array}{rcl} \mathbf{C}^X \times \mathbf{C}^X & \to & \mathbf{C} \\ (f, g) & \mapsto & \langle f, g \rangle = \frac{1}{\sharp X} \sum_{x \in X} \overline{f(x)} g(x). \end{array}$$

Proposition 4.5.4. — *Si G est un groupe fini et χ, χ' deux caractères de G, alors*

$$\langle \chi, \chi' \rangle = \begin{cases} 1 & \textit{si } \chi = \chi', \\ 0 & \textit{sinon.} \end{cases}$$

Démonstration. — Comme G est un groupe fini, pour tout x de G et tout caractère χ, on a

$$\chi(x)^{\sharp G} = \chi(x^{\sharp G}) = \chi(e) = 1.$$

Donc χ est à valeur dans les racines de l'unité et $\overline{\chi(x)} = \chi(x)^{-1}$. Par conséquent l'application $g \mapsto \overline{\chi(g)}\chi'(g)$ est un caractère de G qui n'est trivial, c'est à dire constant de valeur 1, que si $\chi = \chi'$. Il reste à montrer que si χ est un caractère de g, alors

$$\frac{1}{\sharp G}\sum_{g\in G}\chi(g) = \begin{cases} 1 & \text{si } \chi = 1, \\ 0 & \text{sinon.} \end{cases}$$

L'égalité dans le premier est immédiate. Montrons la seconde. Si χ n'est pas trivial, soit $g_0 \in G$ tel que $\chi(g_0) \neq 1$. On a

$$\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(g_0 g) = \chi(g_0)\sum_{g\in G}\chi(g).$$

Par conséquent,

$$(1-\chi(g_0))\sum_{g\in G}\chi(g) = 0.$$

Mais $1-\chi(g_0) \neq 0$ et le résultat en découle. □

Corollaire 4.5.5. — *Si G est un groupe fini, la famille $(\chi)_{\chi\in X^*(G)}$ est une famille libre du $\mathbf{C}$-espace vectoriel X^G. Si G est un groupe abélien fini, alors c'est une base de $\mathbf{C}^G$.*

Démonstration. — Soit n le cardinal de $X^*(G)$ et $\chi_1, \ldots, \chi_n$ les éléments de cet ensemble. Si on a une relation

$$\sum_{j=1}^{n} a_j\chi_j = 0,$$

alors pour tout i, $a_i = \langle \chi_i, \sum_{j=1}^n a_j\chi_j\rangle = 0$. D'autre part $\mathbf{C}^G$ est un $\mathbf{C}$-espace vectoriel de dimension $\sharp G$ avec une base donnée par les applications

$$\begin{array}{rcl} \delta_{g_0} : G & \to & \mathbf{C} \\ g & \mapsto & \begin{cases} 1 & \text{si } g = g_0, \\ 0 & \text{sinon.} \end{cases} \end{array}$$

où g_0 parcourt G. Si G est un groupe abélien fini, par le théorème 2.4.1, il est isomorphe à un produit de groupes abéliens $\mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}$. Mais pour tout $(\overline{k}_1, \ldots, \overline{k}_r)$ de $\mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}$ l'application

$$\begin{array}{rcl} \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z} & \to & \mathbf{C}^\times \\ (\overline{m}_1, \ldots, \overline{m}_r) & \mapsto & \prod_{i=1}^r e^{\frac{2i\pi k_i m_i}{n_i}} \end{array}$$

induit un caractère de G, ce qui montre que $n \geqslant \sharp G$. La famille libre $(\chi)_{\chi\in X^*(G)}$ a donc au moins $\sharp G$ éléments. C'est donc une base de $\mathbf{C}^G$. □

Définition 4.5.6. — Soit n un entier strictement positif. Notons $\zeta = e^{\frac{2i\pi}{n}}$. Pour toute application $f : \mathbf{Z}/n\mathbf{Z} \to \mathbf{C}$ on appelle *transformée de Fourier discrète de* f l'application de $\mathbf{Z}/n\mathbf{Z}$ dans $\mathbf{C}$ définie par

$$\widehat{f}(x) = \sum_{y \in \mathbf{Z}/n\mathbf{Z}} f(y)\zeta^{-yx}.$$

Proposition 4.5.7 (Formule d'inversion de Fourier). — *Pour toute application f de $\mathbf{Z}/n\mathbf{Z}$ dans $\mathbf{C}$, on a*

$$\forall x \in \mathbf{Z}/n\mathbf{Z}, \quad f(x) = \frac{1}{n} \sum_{y \in \mathbf{Z}/n\mathbf{Z}} \widehat{f}(y)\zeta^{xy}.$$

Démonstration. — En effet si on note χ_k le caractère de $\mathbf{Z}/n\mathbf{Z}$ tel que $\chi_k(1) = \zeta^k$, on a

$$\frac{1}{n} \sum_{y \in \mathbf{Z}/n\mathbf{Z}} \widehat{f}(y)\zeta^{xy} = \frac{1}{n} \sum_{y,z \in \mathbf{Z}/n\mathbf{Z}} f(z)\zeta^{-zy+xy} = \sum_{z \in \mathbf{Z}/n\mathbf{Z}} f(z)\langle \chi_z, \chi_x \rangle$$

Mais

$$\langle \chi_z, \chi_y \rangle = \begin{cases} 1 & \text{si } z = x \\ 0 & \text{sinon.} \end{cases} \qquad \square$$

Remarque 4.5.8. — La notion de transformée de Fourier peut être vue comme un changement de base pour les bases considérées dans le corollaire 4.5.5. De manière équivalente, on peut voir le calcul de la transformée de Fourier comme un calcul matriciel

$$\begin{pmatrix} \widehat{f}(0) \\ \widehat{f}(1) \\ \vdots \\ \widehat{f}(n-1) \end{pmatrix} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \zeta^{-1} & \dots & \zeta^{-(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{-(n-1)} & \dots & \zeta^{-(n-1)^2} \end{pmatrix} \begin{pmatrix} f(0) \\ f(1) \\ \vdots \\ f(n-1) \end{pmatrix} \tag{4.5.1}$$

4.6. Transformée de Fourier rapide

La transformée de Fourier rapide consiste en un algorithme de calcul efficace de la transformée de Fourier discrète dans le cas où n est une puissance de 2. A priori le calcul de l'expression (4.5.1) nécessite n^2 multiplication complexes. Voyons comment simplifier ce calcul dans le cas $n = 4$. Dans ce cas on a $i = \zeta$. Le calcul à effectuer est

$$\begin{pmatrix} \widehat{f}(0) \\ \widehat{f}(1) \\ \widehat{f}(2) \\ \widehat{f}(3) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix} \begin{pmatrix} f(0) \\ f(1) \\ f(2) \\ f(3) \end{pmatrix}$$

ce qui peut se réécrire comme

$$\begin{pmatrix} \widehat{f}(0) \\ \widehat{f}(2) \\ \widehat{f}(1) \\ \widehat{f}(3) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -i \\ 0 & 0 & 1 & i \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} f(0) \\ f(1) \\ f(2) \\ f(3) \end{pmatrix}$$

Ce qui ramène de 16 multiplications a priori à une triviale.

Dans le cas général où $n = 2^r$, On considère le morphisme de groupes

$$\psi : \mathbf{Z}/2^r\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z}.$$

La transformée de Fourier s'écrit

$$\begin{aligned} \widehat{f}(x) &= \sum_{y \in \mathbf{Z}/2^r\mathbf{Z}} f(y)\zeta^{-yx} \\ &= \sum_{\{y \in \mathbf{Z}/2^r\mathbf{Z} | \psi(y)=0\}} f(y)\zeta^{-yx} + \sum_{\{y \in \mathbf{Z}/2^r\mathbf{Z} | \psi(y)=1\}} f(y)\zeta^{-yx} \\ &= \sum_{\{y \in \mathbf{Z}/2^r\mathbf{Z} | \psi(y)=0\}} f(y)\zeta^{-yx} + \zeta^{-x} \sum_{\{y \in \mathbf{Z}/2^r\mathbf{Z} | \psi(y)=0\}} f(y+1)\zeta^{-yx} \end{aligned}$$

Mais on a un isomorphisme de groupe

$$\begin{array}{ccc} \mathbf{Z}/2^{r-1}\mathbf{Z} & \to & \operatorname{Ker}\psi \\ \overline{x} & \mapsto & \overline{2x} \end{array}$$

On notant $\widehat{f_0}$ (resp. $\widehat{f_1}$) la transformée de Fourier discrète de l'application

$$f_0 : \begin{array}{ccc} \mathbf{Z}/2^{r-1}\mathbf{Z} & \to & \mathbf{C} \\ x & \mapsto & f(2x) \end{array} \quad \left(\text{resp. } f_1 : \begin{array}{ccc} \mathbf{Z}/2^{r-1}\mathbf{Z} & \to & \mathbf{C} \\ x & \mapsto & f(2x+1) \end{array} \right)$$

On obtient, en notant $\rho : \mathbf{Z}/2^r\mathbf{Z} \to \mathbf{Z}/2^{r-1}\mathbf{Z}$ la projection canonique

$$\widehat{f}(x) = \widehat{f_0}(\rho(x)) + \zeta^{-x}\widehat{f_1}(\rho(x)).$$

En outre

$$\widehat{f}(x + 2^{r-1}) = \widehat{f_0}(\rho(x)) - \zeta^{-x}\widehat{f_1}(\rho(x)).$$

En itérant ce procédé on décompose notre matrice initiale en un produit de r matrices et le nombre de multiplications complexes à faire est de l'ordre de $r2^{r-2}$ à la place de 2^{2r}, c'est à dire $n \log n$ à la place de n^2.

CHAPITRE 5

EXTENSIONS DE CORPS

5.1. Polynômes et racines

Rappelons quelques faits de base sur les racines d'un polynôme.

Définition 5.1.1. — Soit A un anneau commutatif, $P \in A[T]$, $a \in A$. On dit que a est une *racine* de P s'il vérifie une des conditions équivalentes suivantes :

(i) $P(a) = 0$,
(ii) $(T - a) \mid P$.

Si $P \in A[T]$, $a \in A$ et $k \geqslant 1$, on dit que a est *racine d'ordre* k de P s'il vérifie une des conditions équivalentes suivantes :

(i) $\exists Q \in A[T], P = (T - a)^k Q$ et $Q(a) \neq 0$,
(ii) $(T - a)^k \mid P$ et $(T - a)^{k+1}$ ne divise pas P.

Démonstration. — En effectuant la division euclidienne de P par $(T - a)$, on obtient qu'il existe $Q \in Q[T]$ et $c \in A$ tels que

$$P = (T - a)Q + c.$$

En considérant les valeurs en a, on obtient $c = P(a)$. Donc $P(a)$ est le reste de la division de P par $T - a$ et la première équivalence en résulte.

Pour la seconde : (i)⇒(ii) : on fait la division de Q par $T - a$.

$$Q = (T - a)S + Q(a).$$

D'où

$$P = (T - a)^{k+1} S + (T - a)^k Q(a)$$

et $(T - a)^k Q(a) \neq 0$ est le reste de la division de P par $(T - a)^{k+1}$.

(ii)⇒(i)

$$\exists Q \in A[T], \quad P = (T - a)^k Q$$

On écrit $Q = (T - a)S + Q(a)$. Si $Q(a) = 0$, alors $(T - a)^{k+1} \mid P$, ce qui contredit l'hypothèse. □

Proposition 5.1.2. — *Si A est un anneau intègre, $P \in A[T] - \{0\}$, $a_1, \ldots, a_r \in A$ avec $a_i \neq a_j$ si $i \neq j$, $k_1, \ldots, k_r$ avec $k_i \geqslant 1$, alors on a équivalence entre :*

(i) *chacun des a_i est racine d'ordre $\geqslant k_i$ de P.*
(ii) $\prod_{i=1}^{r} (T - a_i)^{k_i} \mid P$.

Démonstration. — (ii)⇒(i) Cela résulte de la défintion.

(ii)⇒(i) Si $A = \mathbf{K}$ un corps, $\mathbf{K}[T]$ est principal, les $(T - a_i)$ sont irréductibles, 2 à 2 distincts. Donc les $(T - a_i)^{k_i}$ sont premiers 2 à 2. En utilisant la proposition 3.10.2, on obtient $\prod_{i=1}^{r}(T - a_i)^{k_i} \mid P$. Dans le cas général, on considère le corps des fractions $\mathbf{K}$ de A, $A[T]$ est alors un sous-anneau de $\mathbf{K}[T]$. Soit

$$P = \prod_{i=1}^{r}(T - a_i)^{k_i}Q + R$$

la division euclidienne de P par $\prod_{i=1}^{r}(T-a_i)^{k_i}$ dans $A[T]$. Le polynôme R est aussi le reste de cette division dans $\mathbf{K}[X]$. Donc, par le cas des corps, $R = 0$. □

Corollaire 5.1.3. — *Avec les notations de la proposition précédente,* $\sum_{i=1}^{r} k_i \leqslant \deg(P)$ *: le nombre des racines, comptées avec multiplicité est majoré par le degré.*

Proposition 5.1.4. — *Soit A un anneau, P un polynôme non nul de $A[T] - \{0\}$ et $a \in A$, alors a est racine d'ordre au moins 2 de P si et seulement si $P(a) = P'(a) = 0$.*

Démonstration. — ⇒ : Si $(T - a)^2 \mid P$, alors P s'écrit $P = (T - a)^2Q$ avec $Q \in A[T]$ et

$$P' = 2(T - a)Q + (T - a)^2Q'.$$

Donc $P(a) = P'(a) = 0$.

⇐ Si $P(a) = 0$ et $P'(a) = 0$, alors $(T - a) \mid P$, donc P s'écrit $P = (T - a)Q$ avec $Q \in A[T]$, $P' = Q+(T-a)Q'$. Donc $Q(a) = P'(a) = 0$. Par conséquent $(T-a)^2 \mid P$. □

Définition 5.1.5. — Si A est un anneau intègre et P un polynôme non nul sur A, P est dit *scindé* si et seulement s'il existe $c \in A$ et $\alpha_1, \ldots \alpha_d \in A$ tels que

$$P = c(T - \alpha_1) \ldots (T - \alpha_d).$$

A permutation près, $(\alpha_1, \ldots \alpha_d)$ ne dépend que de P ; on dit que $\alpha_1, \ldots \alpha_d$ sont les *racines de P, comptées avec multiplicités.*

Remarque 5.1.6. — Avec les notations qui précèdent, on a également

$$\{\, x \in A \mid P(x) = 0 \,\} = \{\, \alpha_1, \ldots, \alpha_d \,\}.$$

5.2. Polynômes d'interpolation

Proposition 5.2.1 (Formule d'interpolation de Lagrange). — *Soit $\mathbf{K}$ un corps. Pour toute famille d'éléments deux à deux distincts $(\alpha_1, \ldots, \alpha_n)$ de $\mathbf{K}^n$ et toute famille $(\beta_1, \ldots, \beta_n)$ de $\mathbf{K}^n$, l'ensemble des polynômes P de $\mathbf{K}[T]$ tels que*

$$\forall i \in \{1, \ldots, n\}, \quad P(\alpha_i) = \beta_i \tag{5.2.1}$$

est formé des polynômes de la forme

$$\sum_{i=1}^{n} \beta_i \frac{\prod_{j\neq i}(T - \alpha_j)}{\prod_{j\neq i}(\alpha_i - \alpha_j)} + (T - \alpha_1) \ldots (T - \alpha_n)Q$$

avec Q un élément de $\mathbf{K}[T]$.

Démonstration. — Effectivement le polynôme

$$\sum_{i=1}^{n} \beta_i \frac{\prod_{j\neq i}(T-\alpha_j)}{\prod_{j\neq i}(\alpha_i-\alpha_j)}$$

vérifie la condition (5.2.1). Mais si P et Q verifient tout deux cette condition, alors $P-Q$ admet $\alpha_1,\dots,\alpha_n$ comme racines et donc est divisible par $(T-\alpha_1)\dots(T-\alpha_n)$. □

Remarque 5.2.2. — On peut également dire que si $\mathbf{K}[T]_{n-1}$ est le $\mathbf{K}$-espace vectoriel des polynômes de $\mathbf{K}[T]$ de degré strictement inférieur à n alors les applications linéaires

$$\text{év}_{\alpha_i} : P \mapsto P(\alpha_i)$$

forment une base de l'espace vectoriel $\mathbf{K}[T]_{n-1}^{\vee}$ qui est duale de la base formée des polynômes $\prod_{j\neq i}(T-\alpha_j)/\prod_{j\neq i}(\alpha_i-\alpha_j)$.

5.3. Degré d'une extension

Nous allons maintenant définir le degré d'une extension de corps.

Définition 5.3.1. — Un *extension* de corps, notée $\mathbf{L}/\mathbf{K}$ est une inclusion de corps $\mathbf{K}\subset\mathbf{L}$.
La loi externe

$$\begin{array}{ccc} \mathbf{K}\times\mathbf{L} & \to & \mathbf{L} \\ (k,l) & \mapsto & kl \end{array}$$

munit alors $\mathbf{L}$ d'une structure de $\mathbf{K}$-espace vectoriel. Le *degré de l'extension* $[\mathbf{L}:\mathbf{K}]$ est alors défini comme la dimension (finie ou infinie) de cet espace vectoriel. L'extension est dite *finie* si cette dimension est finie.

Proposition 5.3.2 (Multiplicativité des degrés). — *Si $\mathbf{M}/\mathbf{L}/\mathbf{K}$ sont deux extensions de corps, alors $\mathbf{M}/\mathbf{K}$ est finie si et seulement si $\mathbf{M}/\mathbf{L}$ et $\mathbf{L}/\mathbf{K}$ le sont. Dans ce cas on a la formule*

$$[\mathbf{M}:\mathbf{K}] = [\mathbf{M}:\mathbf{L}][\mathbf{L}:\mathbf{K}].$$

Remarque 5.3.3. — En particulier si $[\mathbf{L}:\mathbf{K}]$ est nombre premier, $\mathbf{L}=\mathbf{K}(\alpha)$ pour tout $\alpha\in\mathbf{L}-\mathbf{K}$.

Démonstration. — $\Rightarrow$: Si $\mathbf{M}/\mathbf{K}$ est une extension finie, alors $\mathbf{L}$ est un sous-espace vectoriel du $\mathbf{K}$-espace vectoriel $\mathbf{M}$. Donc $\mathbf{L}/\mathbf{K}$ est finie. Soit $(m_1,\dots,m_n)$ une base de $\mathbf{M}$ sur $\mathbf{K}$. Alors $(m_1,\dots,m_n)$ est une famille génératrice du $\mathbf{L}$-espace vectoriel $\mathbf{M}$. L'extension $\mathbf{M}/\mathbf{L}$ est donc également finie.

$\Leftarrow$: Soit $(l_1,\dots,l_t)$ une base de $\mathbf{L}$ sur $\mathbf{K}$ et $(m_1,\dots,m_r)$ une base de $\mathbf{M}$ sur $\mathbf{L}$. Montrons que $(l_i m_j)_{\substack{1\leqslant i\leqslant t\\ 1\leqslant j\leqslant r}}$ est une base de $\mathbf{M}$ sur $\mathbf{K}$, ce qui fournira la réciproque et la multiplicativité du degré.

La famille est génératrice : Soit $m\in\mathbf{M}$. La famille $m_1,\dots,m_r$ étant une famille génératrice du $\mathbf{L}$-espace vectoriel $\mathbf{M}$, il existe $(\lambda_1,\dots,\lambda_r)\in\mathbf{L}^r$ tels que $m=\sum_{i=1}^r \lambda_i m_i$.

La famille $l_1, \ldots, l_t$ étant une famille génératrice du $\mathbf{K}$-espace vectoriel $\mathbf{M}$, pour tout i de $\{1, \ldots, r\}$, il existe $(\kappa_{i,1}, \ldots, \kappa_{i,r}) \in \mathbf{K}^t$ tels que $\sum_{j=1}^t \kappa_{i,j} l_j = \lambda_i$. Par conséquent

$$m = \sum_{i=1}^{r} \sum_{j=1}^{t} \kappa_{i,j} l_j m_i.$$

La famille est libre : Soit $(\kappa_{i,j})_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant t}} \in \mathbf{K}^{rt}$ Supposons que

$$\sum_{i=1}^{r} \sum_{j=1}^{t} \kappa_{i,j} l_j m_i = 0.$$

La famille $(m_1, \ldots, m_r)$ étant libre dans le $\mathbf{L}$-espace vectoriel $\mathbf{M}$, on a $\sum_{j=1}^t \kappa_{i,j} l_j = 0$ pour tout i de $\{ 1, \ldots, r \}$. La famille $(l_1, \ldots, l_t)$ étant libre, on en déduit que $\kappa_{i,j} = 0$ pour $1 \leqslant i \leqslant r$ et $1 \leqslant j \leqslant t$. □

5.4. Corps de rupture

Définition 5.4.1. — Soient $\mathbf{K}$ un corps et $P \in \mathbf{K}[T]$ un polynôme irréductible. On dit que $\mathbf{L}/\mathbf{K}$ est un *corps de rupture* de P sur $\mathbf{K}$ s'il existe $\alpha \in \mathbf{L}$ tel que $\mathbf{L} = \mathbf{K}(\alpha)$ et $P(\alpha) = 0$.

Proposition 5.4.2. — *Pour tout polynôme irréductible $P \in \mathbf{K}[T]$, l'anneau $\mathbf{K}[T]/(P)$ est un corps de rupture pour P sur $\mathbf{K}$ et si $\mathbf{L}$ est un corps de rupture de P sur $\mathbf{K}$ et α une racine de P dans $\mathbf{L}$, alors il existe un unique isomorphisme de $\mathbf{K}[T]/(P)$ dans $\mathbf{L}$ qui envoie la classe de T sur α et dont la restriction à $\mathbf{K}$ soit l'identité.*

Démonstration. — Comme le polynôme P est irréductible et $\mathbf{K}[T]$ principal, (P) est maximal et $\mathbf{K}[T]/(P)$ est un corps, engendré par la classe $\overline{T}$ de T. En outre $P(\overline{T}) = \overline{P(T)} = 0$. Donc $\mathbf{K}[T]/(P)$ est un corps de rupture pour P sur $\mathbf{K}$.

Inversement, soit $\mathbf{L}$ un corps de rupture sur $\mathbf{K}$ et soit $\alpha \in \mathbf{L}$ tel que $P(\alpha) = 0$. Le morphisme d'évaluation en α, $\text{év}_\alpha : \mathbf{K}[T] \to \mathbf{L}$ défini par $\text{év}_{\alpha|\mathbf{K}} = \text{Id}_{\mathbf{K}}$ et $\text{év}_\alpha(T) = \alpha$ induit par passage au quotient un morphisme d'anneaux de $\mathbf{K}[T]/(P)$ dans $\mathbf{L}$. Comme $\mathbf{K}[T]/(P)$ est un corps, il est injectif et $[\mathbf{K}(\alpha) : \mathbf{K}] = \deg(P)$. Mais il existe une racine de P dans $\mathbf{L}$ qui engendre $\mathbf{L}$. Donc $[\mathbf{L} : \mathbf{K}] = \deg(P)$ et $\mathbf{L} = \mathbf{K}(\alpha)$. Le morphisme d'évaluation est donc surjectif. □

Remarque 5.4.3. — La division euclidienne montre que tout polynôme $U \in \mathbf{K}[T]$ s'écrit de manière unique

$$U = PQ + R$$

avec $\deg(R) < \deg(P)$. Par conséquent $1, \overline{T}, \ldots, \overline{T}^{\deg(P)-1}$ forment une base de $\mathbf{K}[T]/(P)$ et $[\mathbf{K}[T]/(P) : \mathbf{K}] = \deg(P)$.

Corollaire 5.4.4. — *Si $\mathbf{L}$ est un corps de rupture de P sur $\mathbf{K}$, alors* $[\mathbf{L} : \mathbf{K}] = \deg(P)$.

5.5. Premiers critères d'irréductibilité

Remarque 5.5.1. — Tout polynôme de degré un est irréductible.

Si $2 \leqslant \deg(P) \leqslant 3$, alors P est irréductible dans $\mathbf{K}[T]$ si et seulement s'il n'admet pas de racine dans $\mathbf{K}$. En effet, comme $\mathbf{K}[T]^\times = \mathbf{K}^\times$, P est irréductible si et seulement s'il ne s'écrit pas sous la forme $P = QR$ avec $\deg(Q) \geqslant 1$ et $\deg(R) \geqslant 1$.

Le critère plus général suivant peut être utilisé pour les polynômes de petit degré :

Proposition 5.5.2. — *Soit $P \in \mathbf{K}[T]$ de degré n. Le polynôme P est irréductible sur $\mathbf{K}$ si et seulement si P n'a pas de racines dans les extensions $\mathbf{L}$ de $\mathbf{K}$ telles que $[\mathbf{L} : \mathbf{K}] \leqslant n/2$.*

Démonstration. — $\Rightarrow$: Si P est irréductible et si P a une racine α dans $\mathbf{L}$ extension de $\mathbf{K}$. Alors on a un morphisme d'anneaux

$$\begin{array}{ccc} \mathbf{K}[T]/(P) & \to & \mathbf{L} \\ T & \mapsto & \alpha. \end{array}$$

Comme P est irréductible, $\mathbf{K}[T]/(P)$ est un corps, ce morphisme est donc injectif. Donc $[\mathbf{L} : \mathbf{K}] = \dim_{\mathbf{K}}(\mathbf{L}) \geqslant \dim_{\mathbf{K}} \mathbf{K}[T]/(P) = n$.

$\Leftarrow$: Si P n'est pas irréductible, $P = QR$ avec $Q, R \in \mathbf{K}[T] - \mathbf{K}^\times$ et $\deg(Q) + \deg(R) = \deg(P)$. Donc $\deg(Q) \leqslant n/2$ ou $\deg(R) \leqslant n/2$. Quitte à échanger Q et R, on peut supposer $\deg(Q) \leqslant n/2$ et quitte à remplacer Q par un de ses facteurs irréductibles, on peut supposer Q irréductible. Mais alors $\mathbf{L} = \mathbf{K}[T]/(Q)$ est un corps de degré $[\mathbf{L} : \mathbf{K}] \leqslant \deg(Q) \leqslant n/2$ et la classe de T dans ce quotient est une racine de P. □

5.6. Élément algébrique, extensions algébriques

Définition 5.6.1. — Soit $\mathbf{L}/\mathbf{K}$ une extension de corps, $\alpha \in \mathbf{L}$ est dit *algébrique* sur $\mathbf{K}$ si et seulement s'il vérifie une des cinq conditions équivalentes suivantes :

(i) $\exists P \in \mathbf{K}[T] - \{0\}$ tel que $P(\alpha) = 0$,

(ii) Le morphisme d'anneaux $\begin{array}{ccc} \text{év}_\alpha : \mathbf{K}[T] & \to & \mathbf{L} \\ P & \mapsto & P(\alpha) \end{array}$ a un noyau non nul,

(iii) $\mathbf{K}[\alpha]$ est un corps,

(iv) $\dim_{\mathbf{K}} \mathbf{K}(\alpha)$ est fini,

(v) $\dim_{\mathbf{K}} \mathbf{K}[\alpha]$ est fini.

Si α est algébrique, on note $\text{Irr}^\alpha_{\mathbf{K}}(T) \in \mathbf{K}[T]$ le générateur unitaire de $\text{Ker}(\text{év}_\alpha)$. On l'appelle *polynôme minimal* de α. Le polynôme $\text{Irr}^\alpha_{\mathbf{K}}(T)$ est un polynôme irréductible de degré $[\mathbf{K}(\alpha) : \mathbf{K}]$ et on a un isomorphisme de corps

$$\mathbf{K}[T]/(\text{Irr}^\alpha_{\mathbf{K}}(T)) \xrightarrow{\sim} \mathbf{K}[\alpha] = \mathbf{K}(\alpha).$$

Démonstration. — (i)$\Rightarrow$(ii) Cela résulte de la définition du noyau.

(ii)$\Rightarrow$(iii) $\text{Im}(\text{év}_\alpha) = \mathbf{K}[\alpha]$. Donc év_α induit un isomorphisme

$$\mathbf{K}[T]/\operatorname{Ker}(\text{év}_\alpha) \xrightarrow{\sim} \mathbf{K}[\alpha] \subset \mathbf{L}.$$

Comme $\mathbf{L}$ est un corps, $\mathbf{K}[\alpha]$ est intègre et $\text{Ker}(\text{év}_\alpha)$ est un idéal premier non nul de $\mathbf{K}[T]$. Comme $\mathbf{K}[T]$ est principal, $\text{Ker}(\text{év}_\alpha)$ est maximal. Donc $\mathbf{K}[\alpha]$ est un corps.

(iii)⇒(iv) $\mathbf{K}(\alpha) = \mathbf{K}[\alpha]$. Si $\alpha = 0$, $\mathbf{K}(\alpha) = \mathbf{K}$ et le résultat est vrai. Sinon $\alpha^{-1} \in \mathbf{K}[\alpha]$, donc

$$\exists d \in \mathbf{N}, \quad \exists (a_i)_{0 \leqslant i \leqslant d} \in \mathbf{K}^{d+1}, \quad \alpha^{-1} = \sum_{i=0}^{d} a_i \alpha^i$$

On pose $P = \sum_{i=0}^{d} a_i T^{i+1} - 1$. Pour tout S de $\mathbf{K}[T]$, $S = PQ + R$ avec $\deg(R) < \deg(P) = d + 1$. Donc $S(\alpha) = R(\alpha)$ appartient au $\mathbf{K}$-espace vectoriel engendré par $1, \ldots, \alpha^d$. Cette famille est donc une famille génératrice de $\mathbf{K}(\alpha) = \mathbf{K}[\alpha]$.

(iv)⇒(v) En effet, $\mathbf{K}[\alpha] \subset \mathbf{K}(\alpha)$.

(v)⇒(i) $\mathbf{K}[\alpha]$ étant de dimension finie, la famille $(\alpha^i)_{i \in \mathbf{N}}$ est liée. Il existe donc un polynôme P de $\mathbf{K}[T]$ tel que $P(\alpha) = 0$.

Il reste à montrer les dernières assertions. Comme $\mathbf{K}[T]$ est principal et $\mathrm{Ker}(\mathrm{év}_\alpha)$ est un idéal non nul, il existe un unique polynôme unitaire tel que $\mathrm{Ker}(\mathrm{év}_\alpha) = (\mathrm{Irr}_{\mathbf{K}}^{\alpha})$. On a vu que

$$\mathbf{K}[T]/(\mathrm{Irr}_{\mathbf{K}}^{\alpha}) \xrightarrow{\sim} \mathbf{K}[\alpha] = \mathbf{K}(\alpha)$$

et donc $\mathrm{Irr}_{\mathbf{K}}^{\alpha}$ est irréductible. En outre

$$\dim_{\mathbf{K}} \mathbf{K}(\alpha) = \deg(\mathrm{Irr}_{\mathbf{K}}^{\alpha})$$

puisque $\mathbf{K}(\alpha)$ est un corps de rupture de $\mathrm{Irr}_{\mathbf{K}}^{\alpha}$. □

Remarque 5.6.2. — Notons que si $\mathbf{M}/\mathbf{L}/\mathbf{K}$ sont deux extensions de corps et α un élément de $\mathbf{M}$ algébrique sur $\mathbf{K}$, alors, par l'assertion (i), α est algébrique sur $\mathbf{L}$.

Proposition 5.6.3. — *Si* $\mathbf{L}/\mathbf{K}$ *est une extension de corps,*

$$\{\, \alpha \in \mathbf{L} \mid \alpha \textit{ est algébrique sur } \mathbf{K} \,\}$$

est un sous-corps dit clôture algébrique relative de $\mathbf{K}$ dans $\mathbf{L}$.

Démonstration. — Si $\alpha, \beta \in \mathbf{L}$ sont algébriques sur $\mathbf{K}$, alors β est algébrique sur $\mathbf{K}(\alpha)$. Donc $\mathbf{K}(\alpha, \beta)/\mathbf{K}(\alpha)$ est fini de même que $\mathbf{K}(\alpha)/\mathbf{K}$. Par la proposition 5.3.2 $\mathbf{K}(\alpha, \beta)/\mathbf{K}$ est également finie. Mais $\alpha - \beta \in \mathbf{K}(\alpha, \beta)$ et $\alpha\beta \in \mathbf{K}(\alpha, \beta)$ Donc $\mathbf{K}(\alpha - \beta)/\mathbf{K}$ et $\mathbf{K}(\alpha\beta)/\mathbf{K}$ sont finies et $\alpha - \beta$ et $\alpha\beta$ sont algébriques sur $\mathbf{K}$. De même, si $\alpha \neq 0$, $\alpha^{-1} \in \mathbf{K}(\alpha)$. □

Définition 5.6.4. — Une extension de corps $\mathbf{L}/\mathbf{K}$ est dite algébrique, si tout élément de $\mathbf{L}$ est algébrique sur $\mathbf{K}$.

Exemple 5.6.5. — Toute extension finie est algébrique, mais la réciproque est fausse.

Proposition 5.6.6. — *Soient* $\mathbf{M}/\mathbf{L}/\mathbf{K}$ *deux extensions de corps, Si* $\mathbf{L}/\mathbf{K}$ *est algébrique et* $\alpha \in \mathbf{M}$ *algébrique sur* $\mathbf{L}$*, alors* α *est algébrique sur* $\mathbf{K}$.

Démonstration. — Comme α est algébrique sur $\mathbf{L}$ il existe un polynôme non nul P égal à $\sum_{i=0}^{d} a_i T^i$ tel que $P(\alpha) = 0$. Donc α est algébrique sur $\mathbf{K}(a_0, \ldots, a_d)$. Par récurrence, on obtient que $[\mathbf{K}(a_0, \ldots, a_d) : \mathbf{K}]$ est fini et par la multiplicativité des degrés il en est de même pour $[\mathbf{K}(a_0, \ldots, a_d, \alpha) : \mathbf{K}]$. Par conséquent, α est algébrique sur $\mathbf{K}$. □

5.7. Clôture algébrique

Définition 5.7.1. — Un corps $\mathbf{K}$ est *algébriquement clos* s'il vérifie une des trois conditions équivalentes suivantes :

(i) Tout polynôme P non constant admet une racine dans $\mathbf{K}$,
(ii) Tout polynôme $P \in \mathbf{K}[T]$ est scindé,
(iii) Les seuls polynômes irréductibles de $\mathbf{K}[T]$ sont les polynômes de degré 1.

Proposition 5.7.2. — *Pour tout corps $\mathbf{K}$, il existe une extension $\overline{\mathbf{K}}$ de $\mathbf{K}$ qui est algébrique sur $\mathbf{K}$ et algébriquement close. On dit que cette extension est une* clôture algébrique *de $\mathbf{K}$.*

Lemme 5.7.3. — *Si $\mathbf{K}$ est un corps, il existe une extension $\mathbf{L}$ de $\mathbf{K}$ tel que tout polynôme non constant $P \in \mathbf{K}[T]$ ait une racine dans $\mathbf{L}$.*

Démonstration. — Si $P_1, \ldots, P_m$ est une famille finie de polynômes non constants de $\mathbf{K}[T]$, alors on peut construire une suite d'extension

$$\mathbf{K} = \mathbf{K}_0 \subset \mathbf{K}_1 \subset \ldots \subset \mathbf{K}_m$$

de $\mathbf{K}$ telle que P_i ait une racine dans $\mathbf{K}_i$ pour $i = 1, \ldots, m$. En effet si P_i a une racine dans $\mathbf{K}_{i-1}$, on pose $\mathbf{K}_i = \mathbf{K}_{i-1}$, sinon on choisit un facteur irréductible Q_i de P_i et on pose $\mathbf{K}_i = \mathbf{K}_{i-1}[T]/(Q_i)$ un corps de rupture pour Q_i.

Soit $\mathscr{I}$ l'ensemble des polynômes irréductibles unitaires de $\mathbf{K}$. On considère l'anneau de polynômes avec une infinité de variables

$$A = \mathbf{K}[T_P, P \in \mathscr{I}] = \bigcup_{\substack{J \subset \mathscr{I} \\ J \text{ fini}}} \mathbf{K}[T_P, P \in J].$$

On considére l'idéal I de A engendré par les polynômes $P(T_P)$ pour $P \in \mathscr{I}$. L'idéal I est distinct de A. En effet, dans le cas contraire, on aurait $1 \in I$. Il existerait donc des éléments $g_1, \ldots, g_m$ de A, et $P_1, \ldots, P_m$ de $\mathscr{I}$ tels que $1 = \sum_{i=1}^m g_i P_i(T_{P_i})$. Quitte à augmenter m, on peut supposer que $g_i \in \mathbf{K}[T_{P_i}, 1 \leqslant i \leqslant m]$ puisque chacun des g_i n'a qu'un nombre fini de coefficients non nuls. Donc

$$\sum_{i=1}^m g_i(T_{P_1}, \ldots, T_{P_m}) P_i(T_{P_i}) = 1.$$

Par la remarque précédente, il existe une extension $\mathbf{K}'$ de $\mathbf{K}$ telle que tous les P_i aient une racine α_i dans $\mathbf{K}'$. Mais on obtient

$$1 = \sum_{i=1}^m g_i(\alpha_1, \ldots, \alpha_m) P_i(\alpha_i) = 0.$$

Donc $I \neq A$. Donc, par le lemme de Zorn, ou l'axiome du choix, il existe un idéal maximal $\mathfrak{m}$ de A tel que $I \subset \mathfrak{m} \subset A$. Le corps $\mathbf{L} = A/\mathfrak{m}$ convient : comme $\mathfrak{m}$ est maximal, c'est bien un corps, comme $I \subset \mathfrak{m}$, pour tout P de $\mathscr{I}$, la classe de T_P est une racine de P dans $\mathbf{L}$. □

Démonstration de la proposition. — On construit par récurrence une suite de corps

$$\mathbf{K} = \mathbf{K}_0 \subset \mathbf{K}_1 \subset \ldots \subset \mathbf{K}_n \subset \ldots$$

de sorte que tout polynôme de $\mathbf{K}_n[T]$ ait une racine dans $\mathbf{K}_{n+1}$. Soit $\mathbf{L} = \bigcup_{n\in\mathbf{N}} \mathbf{K}_n$. Alors $\mathbf{L}$ est algébriquement clos. En effet, soit $P \in \mathbf{L}[T]$, il existe n tel que P provienne de $\mathbf{K}_n[T]$, donc P a une racine dans $\mathbf{K}_{n+1}$ et, a fortiori dans $\mathbf{L}$. Soit $\overline{\mathbf{K}}$ la clôture algébrique relative de $\mathbf{K}$ dans $\mathbf{L}$, alors $\overline{\mathbf{K}}$ est une clôture algébrique de $\mathbf{K}$: par construction, il est algébrique sur $\mathbf{K}$ et si $P \in \overline{\mathbf{K}}[T]$, P a une racine α dans $\mathbf{L}$; α est algébrique sur $\overline{\mathbf{K}}$ et par la proposition 5.6.6 sur $\mathbf{K}$. Donc $\alpha \in \overline{\mathbf{K}}$. □

Proposition 5.7.4. — *Si* $\mathbf{M}$ *est une extension finie de* $\mathbf{K}$ *et* $\overline{\mathbf{K}}$ *une clôture algébrique de* $\mathbf{K}$*, il existe un morphisme* $\phi : \mathbf{M} \to \overline{\mathbf{K}}$ *dont la restriction à* $\mathbf{K}$ *est l'identité.*

Démonstration. — Si $\mathbf{M} = \mathbf{K}(\alpha)$ est une extension monogène, soit Q le polynôme minimal de α sur $\mathbf{K}$. $\mathbf{M}$ est un corps de rupture de Q, ce qui donne par la proposition 5.4.2 un isomorphisme $\mathbf{K}[T]/(Q) \xrightarrow{\sim} \mathbf{M}$. Mais si β est une racine de Q dans $\overline{\mathbf{K}}$, on a également un isomorphisme $\mathbf{K}[T]/(Q) \xrightarrow{\sim} \mathbf{K}(\beta)$ ce qui fournit le morphisme de corps cherché.

Dans le cas général, soit $(\alpha_1, \ldots, \alpha_n)$ une base du $\mathbf{K}$ espace vectoriel $\mathbf{M}$. On a alors l'égalité $\mathbf{M} = \mathbf{K}(\alpha_1, \ldots, \alpha_m)$ et on procède par récurrence. □

5.8. Corps de décomposition

Définition 5.8.1. — Si P est un polynôme sur un corps $\mathbf{K}$, un *corps de décomposition* de P sur $\mathbf{K}$ est une extension $\mathbf{L}$ de $\mathbf{K}$ tel que P soit scindé sur $\mathbf{K}$ et $\mathbf{L}$ soit engendré par les racines de P en tant qu'extension de corps de $\mathbf{K}$.

Proposition 5.8.2. — *Si* $P \in \mathbf{K}[T]$*, alors il existe un corps de décomposition de* P *sur* $\mathbf{K}$ *et si* $\mathbf{L}$ *et* $\mathbf{L}'$ *sont deux tels corps, alors il existe un isomorphisme* ϕ *de* $\mathbf{L}$ *sur* $\mathbf{L}'$ *tel que* $\phi_{|\mathbf{K}} = \mathrm{Id}_{\mathbf{K}}$.

Démonstration. — Pour l'existence, il suffit de prendre une clôture algébrique $\overline{\mathbf{K}}$ de $\mathbf{K}$ et le sous-corps $\mathbf{L}$ engendré par les racines de P dans $\overline{\mathbf{K}}$.

Montrons la deuxième assertion. En appliquant la proposition 5.7.4, pour tout corps de décomposition $\mathbf{L}'$ de P sur $\mathbf{K}$, il existe un morphisme $\phi : \mathbf{L}' \to \overline{\mathbf{K}}$ dont la restriction à $\mathbf{K}$ est l'identité. Soient c, $\beta_1, \ldots, \beta_d$ des éléments de $\mathbf{L}'$ tels que $\mathbf{L}' = \mathbf{K}(\beta_1, \ldots, \beta_d)$ et

$$P = c(T - \beta_1) \ldots (T - \beta_d)$$

dans $\mathbf{L}'[T]$. En appliquant Φ on obtient

$$P = \phi(c)(T - \phi(\beta_1)) \ldots (T - \phi(\beta_d))$$

dans $\overline{\mathbf{K}}[T]$. Donc $\phi(\beta_1), \ldots, \phi(\beta_d)$ sont les racines de P dans $\overline{\mathbf{K}}$. D'où $\phi(\mathbf{L}') \subset \mathbf{L}$. Inversement, $\mathbf{L}$ étant engendré par les racines de P, $\mathbf{L} \subset \phi(\mathbf{L}')$. Par conséquent $\phi : \mathbf{L}' \to \mathbf{L}$ est morphisme de corps surjectif, donc un isomorphisme. □

EXERCICES

5.1. Donner les polynômes minimaux de $\sqrt{2} + \sqrt{3}$ et de $\sqrt[3]{2} + \sqrt{3}$ sur $\mathbf{Q}$.

CHAPITRE 6

STRUCTURE DES CORPS FINIS

Pour des compléments, le lecteur pourra également consulter le cours d'arithmétique de Serre [**Se**].

6.1. Sous-groupe fini de $\mathbf{K}^\times$

Proposition 6.1.1. — *Si* $\mathbf{K}$ *est un corps et* G *un sous-groupe fini de* $\mathbf{K}^\times$*, alors* G *est un groupe cyclique.*

Démonstration. — Par la proposition 3.11.1, pour tout entier $d \geqslant 1$, $\varphi(d) = \sharp(\mathbf{Z}/d\mathbf{Z})^\times$, l'indicateur d'Euler de d, est aussi le nombre de générateurs d'un groupe cyclique d'ordre d, puisque celui-ci est isomorphe à $\mathbf{Z}/d\mathbf{Z}$.

Lemme 6.1.2. — *On a la relation* $n = \sum_{d|n} \varphi(d)$.

Démonstration. — En effet si $d \mid n$, soit $m = n/d$, alors on a un isomorphisme de groupes

$$\begin{array}{ccc} \mathbf{Z}/d\mathbf{Z} & \xrightarrow{\sim} & \{\, x \in \mathbf{Z}/n\mathbf{Z} \mid dx = 0 \,\} \\ 1 & \mapsto & \overline{m}. \end{array}$$

En effet, si $x \in \mathbf{Z}$ est tel que $dx \equiv 0 \pmod{n}$ alors $md \mid dx$ et $m \mid x$. On a donc l'égalité $\sharp\{\, x \in \mathbf{Z}/n\mathbf{Z} \mid \operatorname{ord} x = d \,\} = \varphi(d)$. On en déduit les relations

$$n = \sharp(\mathbf{Z}/n\mathbf{Z}) = \sum_{d|n} \sharp\{\, x \in \mathbf{Z}/n\mathbf{Z} \mid \operatorname{ord}(x) = d\} = \sum_{d|n} \varphi(d). \quad \square$$

Lemme 6.1.3. — *Soit* H *un groupe d'ordre fini* n*. Si pour tout diviseur* d *de* n*,*

$$\sharp\{\, x \in H \mid x^d = 1 \,\} \leqslant d$$

alors H *est cyclique.*

Démonstration. — Supposons x est d'ordre d dans H, alors les éléments $1, x, \ldots, x^{d-1}$ sont deux à deux distincts. Par hypothèse, tout élément d'ordre divisant d dans H appartient au sous-groupe de H engendré par x. En conséquence, on a

$$\sharp\{\, y \in H \mid \operatorname{ord}(y) = d\} = \sharp\{y \in \langle x \rangle \mid \operatorname{ord}(y) = d\} = \varphi(d).$$

On a donc montré que pour tout diviseur d de n, $\sharp\{\, y \in H \mid \operatorname{ord}(y) = d\}$ vaut 0 ou $\varphi(d)$. donc

$$\sharp\{\, x \in H \mid \operatorname{ord}(x) = n\} \geqslant n - \sum_{\substack{d|n \\ d \neq n}} \varphi(d) = \varphi(n) > 0$$

Donc H est engendré par un de ses éléments. □

Fin de la demonstration de la proposition 6.1.1. — On applique le lemme précédent à G en utilisant le fait que $T^d - 1$ a au plus d racines. □

Remarque 6.1.4. — Notons que cette preuve n'est pas constructive : elle ne fournit pas de générateur explicite.

6.2. Les polynômes cyclotomiques

Pour ce paragraphe, notre référence sera le cours d'algèbre de Perrin [**Per**].

Définition 6.2.1. — Si $\mathbf{K}$ est un corps, on note $\mu_n(\mathbf{K})$ l'ensemble des *racines n-ièmes de l'unité* dans $\mathbf{K}$ défini par

$$\mu_n(\mathbf{K}) = \{\, \lambda \in \mathbf{K} \mid \lambda^n = 1 \,\}.$$

Exemple 6.2.2. — Si $\mathbf{K} = \mathbf{Q}$, alors

$$\mu_n(\mathbf{Q}) = \begin{cases} \{1, -1\} & \text{si } 2 \mid n, \\ \{1\} & \text{sinon.} \end{cases}$$

Si $\mathbf{K}$ est un corps de caractéristique p, alors $T^p - 1 = (T-1)^p$. Par conséquent $\mu_p(\mathbf{K})$ est réduit à $\{1\}$.

Si $\mathbf{K} = \mathbf{C}$ les racines de l'unité sont les $e^{\frac{2ik\pi}{n}}$ pour $0 \leqslant k \leqslant n-1$, il y en a donc exactement n.

Par la proposition 6.1.1, $\mu_n(\mathbf{K})$ est un groupe cyclique. Notons d son cardinal. Soit ζ un de ses générateurs. On a $\mathrm{ord}(\zeta) = d$ et $\zeta^n = 1$, par conséquent $d \mid n$.

Définition 6.2.3. — On appelle racine *primitive* n-ième de l'unité une racine n-ième de l'unité d'ordre exactement n. On notera $\mu_n^*(\mathbf{K})$ leur ensemble.

Remarque 6.2.4. — Il existe une racine primitive n-ième de l'unité si et seulement si $\mu_n(\mathbf{K})$ est isomorphe à $\mathbf{Z}/n\mathbf{Z}$, si et seulement si le polynôme $T^n - 1$ est scindé et toutes ses racines sont simples. Par la proposition 3.11.1, il existe alors exactement $\varphi(n)$ racine primitive n-ième de l'unité, où φ désigne l'indicatrice d'Euler.

Exemple 6.2.5. — Si $\mathbf{K} = \mathbf{C}$, $\zeta = e^{\frac{2i\pi}{n}}$ est une racine primitive de l'unité.

Définition 6.2.6. — Le n-ième *polynôme cyclotomique*, est le polynôme

$$\phi_n(T) = \prod_{\zeta \in \mu_n^*(\mathbf{C})} (T - \zeta) \in \mathbf{C}[T].$$

Proposition 6.2.7. — *Les polynômes cyclotomiques vérifient les conditions suivantes :*

(i) *$\phi_n(T)$ est un polynôme unitaire de degré $\varphi(n)$,*
(ii) *$T^n - 1 = \prod_{d \mid n} \phi_d(T)$,*
(iii) *le polynôme $\phi_n(T)$ est à coefficients entiers.*

Démonstration. — L'assertion (i) résulte de la définition et de du fait que $\mu_n^*(\mathbf{C})$ est de cardinal $\varphi(n)$.

(ii). Dans $\mathbf{C}[T]$, on a la relation

$$T^n - 1 = \prod_{\zeta \in \mu_n(\mathbf{C})} (T - \zeta).$$

Mais pour tout élément ζ de $\mu_n(\mathbf{C})$ on a $\mathrm{ord}(\zeta) \mid n$ et $\zeta \in \mu^*_{\mathrm{ord}(\zeta)}(\mathbf{C})$. On en déduit que $\mu_n(\mathbf{C})$ est la réunion disjointe des $\mu_d^*(\mathbf{C})$ pour $d \mid n$.

(iii). On procède par récurrence : pour $n = 1$, on a $\phi_1(T) = T - 1$ et le résultat est vrai dans ce cas. Supposons le résultat vérifié pour $d < n$. Le polynôme

$$P = \prod_{\substack{d|n \\ d \neq n}} \phi_d(T)$$

est un polynôme unitaire de $\mathbf{Z}[T]$. On peut donc effectuer la division euclidienne de $T^n - 1$ par P, on obtient une paire de polynômes (Q, R) de $\mathbf{Z}[T]^2$ avec $\deg(R) < \deg(P)$ et $T^n - 1 = PQ + R$. Mais Q est aussi le quotient de la division euclidienne de $T^n - 1$ par P dans $\mathbf{C}[T]$. Par le point (ii), $T^n - 1 = P\phi_n(T)$ dans $\mathbf{C}[T]$. Par unicité dans la division euclidienne $\phi_n(T) = Q$ appartient à $\mathbf{Z}[T]$. □

Remarque 6.2.8. — On peut montrer que $\phi_n(T)$ est un polynôme irréductible de $\mathbf{Z}[T]$ (cf. **[Per]**).

Définition 6.2.9. — Si A est un anneau commutatif, l'image de $\phi_n(T)$ par le morphisme d'anneaux naturel $\mathbf{Z}[T] \to A[T]$ est également appelé n-ième polynôme cyclotomique.

Exemple 6.2.10. — Les premiers polynômes cyclotomiques sont donnés par :

$$\begin{aligned}
\phi_1(T) &= T - 1, \\
\phi_2(T) &= T + 1, \\
\phi_3(T) &= T^2 + T + 1, \\
\phi_4(T) &= T^2 + 1, \\
\phi_5(T) &= T^4 + T^3 + T^2 + T + 1, \\
\phi_6(T) &= T^2 - T + 1 \\
\phi_8(T) &= T^4 + 1
\end{aligned}$$

et si p est un nombre premier

$$\phi_p(T) = T^{p-1} + \cdots + T + 1.$$

6.3. Frobenius

Proposition 6.3.1. — *Soient p un nombre premier et A un anneau commutatif de caractéristique p. L'application Fr_p définie par*

$$\forall x \in A, \quad \mathrm{Fr}_p(x) = x^p$$

est un morphisme d'anneaux appelé morphisme de Frobenius.

Démonstration. — Il s'agit bien d'un morphisme d'anneaux. En effet, soient x et y deux éléments de A. Comme A est commutatif, on peut appliquer la formule du binôme :

$$(x+y)^p = \sum_{i=0}^{p} C_p^i x^i y^{p-i}$$

Mais si $0 < i < p$, p divise $p!$ mais ne divise ni $i!$, ni $(p-i)!$; donc p divise le facteur binômial $C_p^i = p!/(i!(p-i)!)$. Par conséquent, $(x+y)^p = x^p + y^p$.

D'autre part, si $x, y \in A$, $(xy)^p = x^p y^p$ et $1^p = 1$. □

Notation 6.3.2. — Plus généralement si q est une puissance d'un nombre premier p et A un anneau commutatif de caractéristique p, on note Fr_q l'application $x \mapsto x^q$.

6.4. Structure des corps finis

Commençons par énoncer le théorème de structure des corps finis

Théorème 6.4.1. — *Soit* $\mathbf{K}$ *un corps fini, alors la caractéristique de* $\mathbf{K}$ *est un nombre premier* p*. Le cardinal de* $\mathbf{K}$ *est* $q = p^d$ *où* $d = [\mathbf{K} : \mathbf{F}_p]$*. Inversement, si* p *est un nombre premier et* d *un entier strictement positif, il existe à isomorphisme près un unique corps fini à* $q = p^d$ *éléments, qui est un corps de décomposition du polynôme* $T^q - T$ *sur* $\mathbf{F}_p$*. Ce corps est noté* $\mathbf{F}_q$*.*

Avec les notations précédentes,

- *Il existe un isomorphisme du groupe additif* $(\mathbf{F}_q, +)$ *sur* $((\mathbf{Z}/p\mathbf{Z})^d, +)$*.*
- *Le groupe multiplicatif* $\mathbf{F}_q^\times$ *est un groupe cyclique d'ordre* $q-1$*; autrement dit il existe un isomorphisme de groupes de* $\mathbf{F}_q^\times$ *sur* $\mathbf{Z}/(q-1)\mathbf{Z}$*.*

Démonstration. — Soit p la caractéristique de $\mathbf{K}$. Comme $\mathbf{K}$ est fini, $p \neq 0$. Par la proposition 3.11.6, p est un nombre premier et $\mathbf{K}$ une extension de $\mathbf{F}_p$. Vérifions qu'un corps $\mathbf{K}$ à q élément est un corps de décomposition pour $T^q - T$. Comme $\mathbf{K}$ a q éléments, $\mathbf{K}^\times$ est un groupe d'ordre $q-1$. Par conséquent,

$$\forall x \in \mathbf{K}^\times, \quad x^{q-1} = 1.$$

Autrement dit tous les éléments de $\mathbf{K}$ sont racines de $T^q - T$. Comme ce polynôme a au plus q racines, on obtient

$$T^q - T = \prod_{x \in \mathbf{K}} (T - x). \tag{6.4.1}$$

En particulier, $\mathbf{K}$ est un corps de décomposition pour $T^q - T$.

Inversement si $\mathbf{K}$ est un corps de décomposition pour $T^q - T$ sur $\mathbf{F}_p$. Comme Fr_q est un automorphisme de $\mathbf{K}$ l'ensemble des racines de $T^q - T$ est un sous-corps de $\mathbf{K}$. Comme $\mathbf{K}$ est engendré par ces racines, $\mathbf{K}$ est l'ensembles des racines de $P = T^q - T$. Comme $P' = -1$, par la proposition 5.1.4, toutes les racines de P sont d'ordre 1, il a donc toutes ses racines distinctes dans $\mathbf{K}$. Par la formule (6.4.1), $\mathbf{K}$ a exactement q éléments.

L'assertion concernant le groupe additif résulte de la structure de $\mathbf{F}_q$ comme espace vectoriel.

Celle sur la structure multiplicative découle de la proposition 6.1.1. □

6.5. Polynômes sur $\mathbf{F}_q$

Proposition 6.5.1. — *Soit p un nombre premier et $q = p^d$ avec $d \geqslant 1$. Pour tout entier $n \geqslant 1$, il existe un polynôme P unitaire irréductible de degré n sur $\mathbf{F}_q$ et le corps $\mathbf{F}_{q^n}$ est à la fois un corps de rupture et un corps de décomposition de P. En particulier $\mathbf{F}_{q^n}$ est isomorphe à $\mathbf{F}_q[T]/(P)$.*

En outre, si α est une racine de P dans $\mathbf{F}_{q^n}$, alors

$$P = \prod_{i=0}^{n-1} (T - \alpha^{q^i}).$$

Démonstration. — Soit θ un générateur du groupe cyclique $\mathbf{F}_{q^n}^\times$. Alors $\mathbf{F}_{q^n} = \mathbf{F}_q[\theta]$. Soit P le polynôme minimal de θ sur $\mathbf{F}_q$. Alors P est un polynôme irréductible et $\mathbf{F}_{q^n}$ est un corps de rupture pour P. Autrement dit, on a un isomorphisme $\mathbf{F}_q[T]/(P) \to \mathbf{F}_{q^n}$ qui envoie la classe de T sur θ. En particulier,

$$\deg P = \dim_{\mathbf{F}_q}(\mathbf{F}_q[T]/(P)) = \dim_{\mathbf{F}_q} \mathbf{F}_{q^n} = n.$$

On écrit $P = \sum_{i=0}^n a_i T^i$ avec $a_i \in \mathbf{F}_q$. Si α est une racine de P, alors, Fr_q étant un morphisme de corps sur $\mathbf{F}_q$,

$$\mathrm{Fr}_q(P(\alpha)) = \sum_{i=0}^n \mathrm{Fr}_q(a_i)\,\mathrm{Fr}_q(\alpha)^i = P(\mathrm{Fr}_q(\alpha))$$

où la dernière égalité vient du fait que $\mathrm{Fr}_q(x) = x$ pour tout x de $\mathbf{F}_q$. Par conséquent $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ sont des racines de P. Montrons par l'absurde que ces racines sont deux à deux distinctes. En effet, dans le cas contraire, il existe i et j distincts avec $0 \leqslant i, j \leqslant n-1$ tels que $\alpha^{q^i} = \alpha^{q^j}$ et donc $\alpha^{q^i - q^j} = 1$. Quitte à échanger i et j, on peut supposer $i > j$. Par conséquent

$$\mathrm{ord}(\alpha) \mid q^i - q^j = q^j(q^{i-j} - 1).$$

Mais, comme $\alpha \in \mathbf{F}_{q^n}$, $\mathrm{ord}(\alpha) \mid q^n - 1$ et donc l'ordre de α est premier à q donc, par le lemme de Gauss, $\mathrm{ord}(\alpha) \mid q^{i-j} - 1$ et $\alpha^{q^{i-j}} = \alpha$ et α appartient au corps $\mathbf{F}_{q^{i-j}}$ ce qui est en contradiction avec le fait que $[\mathbf{F}_q(\alpha) : \mathbf{F}_q] = \deg(P) = n$. Par conséquent,

$$P = (T - \alpha)\ldots(T - \alpha^{q^{n-1}}). \quad \square$$

Remarques 6.5.2. — **(i)** Deux polynômes irréductibles de même degré n sur $\mathbf{F}_q$ fournissent donc deux corps isomorphes. Il n'est toutefois pas toujours facile d'expliciter cet isomorphisme.

(ii) Si on s'est donné un tel polynôme P unitaire, et θ racine de P dans $\mathbf{F}_{q^n}$, tout élément de $\mathbf{F}_{q^n}$ s'écrit de manière unique

$$\lambda_0 + \lambda_1\theta + \cdots + \lambda_{n-1}\theta^{n-1}$$

avec λ_0, λ_1,...λ_{n-1} des éléments de $\mathbf{F}_p$. La somme de deux tels éléments est immédiate. Si $P = a_0 + a_1T + \cdots + a_{n-1}T^{n-1} + T^n$, on a la formule

$$\theta^n = -a_0 - a_1\theta + \cdots - a_{n-1}\theta^{n-1}$$

ce qui permet de calculer le produit. Cette méthode n'est toutefois pas la plus efficace pour le calcul de puissances. La base $1, \theta, \ldots, \theta^{n-1}$ est dite *polynômiale*

(iii) Une autre difficulté est de trouver de bons polynômes irréductibles P, c'est-à-dire avec un nombre minimal de coefficients non nuls.

Proposition 6.5.3. — *Notons $\mathscr{I}$ l'ensemble des polynômes irréductibles unitaires de $\mathbf{F}_q[T]$. Alors on a les relations*

$$T^{q^n} - T = \prod_{x \in \mathbf{F}_{q^n}} (T - x) = \prod_{\{\, P \in \mathscr{I} \mid \deg P \mid n \,\}} P.$$

Démonstration. — La relation

$$T^{q^n} - T = \prod_{x \in \mathbf{F}_{q^n}} (T - x)$$

a été démontrée pour le théorème de structure des corps finis. On considère alors l'application

$$\begin{array}{rcl} \rho : \mathbf{F}_{q^n} & \to & \mathscr{I} \\ \alpha & \mapsto & \mathrm{Irr}^{\alpha}_{\mathbf{F}_q}. \end{array}$$

Si $x \in \mathbf{F}_{q^n}$, alors $\deg \mathrm{Irr}^{\alpha}_{\mathbf{F}_q} = [\mathbf{F}_q(\alpha) : \mathbf{F}_q] \mid [\mathbf{F}_{q^n} : \mathbf{F}_q] = n$ donc tout polynôme P de l'image est de degré un diviseur de n. Inversement tout tel polynôme est scindé sur $\mathbf{F}_{q^n}$ et l'image inverse d'un polynôme P est formé des racines de P. On obtient

$$T^{q^d} - T = \prod_{\{\, P \in \mathscr{I} \mid \deg P \mid d \,\}} \prod_{\{x \in \mathbf{F}_{q^d} \mid P(x) = 0\}} (X - x).$$

Et on en déduit la formule souhaitée. □

Exemple 6.5.4. — Le polynôme $T^4 + 1$ est irréductible dans $\mathbf{Q}[T]$ mais réductible dans $\mathbf{F}_p[T]$ pout tout nombre premier p. En effet, il n'a pas de solution dans $\mathbf{Q}$, donc s'il n'est pas irréductible dans $\mathbf{Q}$ il se met sous la forme

$$T^4 + 1 = (T^2 + aT + b)(T^2 + cT + d).$$

On a alors les relations $a = -c$, $-a^2 + b + d = 0$, $a(b - d) = 0$ et $bd = 1$. Les nombres b et d sont de même signes donc a est non nul et $b = d$. Par conséquent $b = d = 1$, mais 2 n'est pas un carré dans $\mathbf{Q}$.

Si $p = 2$, on a $T^4 + 1 = (T + 1)^4$ dans $\mathbf{F}_2[T]$. Si p est un nombre premier impair, $\mathbf{F}^{\times}_{p^2}$ est un groupe cyclique d'ordre $p^2 - 1 = (p - 1)(p + 1)$. Or $p - 1$ et $p + 1$ sont des nombres pairs et l'un des deux est divisible par 4. Par conséquent, $8 \mid p^2 - 1$. Donc $\mathbf{F}^{\times}_{p^2}$ contient un

élément d'ordre 8. Cet élément est racine de ϕ_8 si bien que ϕ_8 admet une racine dans $\mathbf{F}_{p^2}^\times$. Par le critère 5.5.2, T^4+1 n'est pas irréductible dans $\mathbf{F}_p$.

Passons maintenant à un algorithme permettant de tester si un polynôme de $\mathbf{F}_q[T]$ est irréductible. Cet algorithme repose sur la proposition suivante :

Proposition 6.5.5. — *Un polynôme P de $\mathbf{F}_q[T]$ de degré n est irréductible si et seulement s'il vérifie les deux conditions suivantes :*

(i) $P \mid T^{q^n} - T$

(ii) *P est premier à $T^{q^{\frac{n}{l}}} - T$ pour tout nombre premier l divisant n.*

Démonstration. — $\Rightarrow$: Si P est irréductible de degré n, alors, par la proposition 6.5.1, P divise $T^{q^n} - T$ et ne divise aucun des $T^{q^{\frac{n}{l}}} - T$ pour $l \mid n$.

$\Leftarrow$: Si $P \mid T^{q^n} - T$, alors, par la proposition 6.5.1, P s'écrit $\prod_{i=1}^n P_i$ avec P_i irréductible, $\deg P_i \mid n$. Si P n'est pas irréductible, alors il existe un nombre premier l tel que $\deg P_1$ divise n/l. Donc P n'est pas premier à $T^{q^{\frac{n}{l}}} - T$. □

Algorithme 6.5.6.

Entrée:

- Polynôme P de $\mathbf{F}_q[T]$,

Sortie:

- Vrai si P est irréductible, Faux sinon.

Algorithme:

1. Calculer le reste B de la division de T^{q^n} par P. On utilisera pour cela le calcul de puissances dans $\mathbf{F}_q[T]/(P)$.
2. Si $B \neq T$, alors
   2.1. Renvoyer Faux, fin de l'algorithme.
3. Pour l diviseur premier de n :
   3.1. Calculer le reste B de la division de $T^{q^{n/l}}$ par P. (Puissance dans $\mathbf{F}_q[T]/(P)$).
   3.2. Calculer $\mathrm{pgcd}(B-T, P)$.
   3.3. S'il est différent de 1, alors
      3.3.1. Renvoyer Faux, fin de l'algorithme.
4. Retourner Vrai.

Nous implémentons cet algorithme sur $\mathbf{F}_2$ en appendice dans le paragraphe A.4.

6.6. Carrés dans $\mathbf{F}_q^\times$

Dans ce paragraphe nous allons étudier les carrés dans les corps finis. En effet, si x n'est pas un carré dans $\mathbf{F}_q$, on peut obtenir $\mathbf{F}_{q^2}$ en adjoignant à $\mathbf{F}_q$ une racine carrée de x.

Proposition 6.6.1. — *Soit p un nombre premier et $q = p^d$ avec $d \geqslant 1$. Alors*

- *Si $p = 2$, $\mathbf{F}_q^\times = \mathbf{F}_q^{\times 2}$.*

- *Si $p \neq 2$,*

$$x \in \mathbf{F}_q^{\times 2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$$

et $\mathbf{F}_q^2$ est de cardinal $(q+1)/2$.

Démonstration. — Si $p = 2$, cela résulte de la surjectivité du Frobenius.

Si $p \neq 2$, on a une suite exacte

$$\begin{array}{ccccccc} 1 & \to & \{-1,1\} & \to & \mathbf{F}_q^\times & \to & \mathbf{F}_q^{\times 2} \to 1 \\ & & & & x & \mapsto & x^2 \end{array}$$

ce qui nous donne $\sharp(\mathbf{F}_q^{\times 2}) = (q-1)/2$ et donc, l'ordre d'un élément divisant l'ordre du groupe,

$$\forall x \in \mathbf{F}_q^{\times 2}, \quad x^{\frac{q-1}{2}} = 1.$$

Comme $T^{\frac{q-1}{2}} - 1$ a au plus $(q-1)/2$ racines dans $\mathbf{F}_q^\times$, on a

$$\mathbf{F}_q^{\times 2} = \{\, x \in \mathbf{F}_q^\times \mid x^{\frac{q-1}{2}} = 1 \,\}. \quad \square$$

Définition 6.6.2. — Soit p un nombre premier, $p \neq 2$, $n \in \mathbf{Z}$, Le symbole de Legendre est définit par

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{si } p \mid n, \\ 1 & \text{si } n \in \mathbf{F}_p^{\times 2}, \\ -1 & \text{sinon.} \end{cases}$$

Corollaire 6.6.3. — *On a la relation*

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \quad (p).$$

Remarque 6.6.4. — En particulier, si p est un nombre premier impair, -1 est un carré dans $\mathbf{F}_p$ si et seulement si p est congru à 1 modulo 4. En particulier $\mathbf{F}_9$ est isomorphe à $\mathbf{F}_3[T]/(T^2+1)$.

Démonstration. — Le corollaire résulte de la proposition si n est premier à p et des définitions sinon. $\square$

Proposition 6.6.5. — *Si p est un nombre premier impair,*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Démonstration. — Soit α une racine primitive huitième de l'unité dans une clôture algébrique de $\mathbf{F}_p$. On pose $y = \alpha + \alpha^{-1}$. Comme $\alpha^4 + 1 = 0$, on a $\alpha^2 + \alpha^{-2} = 0$. Donc

$$y^2 = \alpha^2 + 2 + \alpha^{-2} = 2.$$

On a donc obtenu une racine carré de 2 dans une extension de $\mathbf{F}_p$ et 2 est un carré dans $\mathbf{F}_p$ si et seulement si $y \in \mathbf{F}_p$, c'est-à-dire $\mathrm{Fr}_p(y) = y$. Or on a les relation $y^p = (\alpha + \alpha^{-1})^p = \alpha^p + \alpha^{-p}$ et donc

$$y^p = \begin{cases} y & \text{si } p \equiv \pm 1 \quad (8), \\ -y & \text{sinon.} \end{cases}$$

ce qui donne le résultat annoncé. □

6.7. *Le cas des extensions de degré un nombre premier*

Dans ce paragraphe on veut décrire les extensions $\mathbf{F}_{q^l}/\mathbf{F}_q$ pour un nombre premier l. Commençons par le cas où $l \neq p$.

***Remarque* 6.7.1**. — Si $l = 2$, on peut choisir un élément x de $\mathbf{F}_{q^2} - \mathbf{F}_q$. Le polynôme minimal de x sur $\mathbf{F}_q$ est de degré 2. x est donc racine d'un polynôme $aT^2 + bT + c = 0$ avec $a \neq 0$. Comme $p \neq 2$, Les formules usuelles nous donnent donc que

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

autrement dit il existe $y \in \mathbf{F}_{q^2}$ tel que $\mathbf{F}_{q^2} = \mathbf{F}_q(y)$ et $y^2 \in \mathbf{F}_q$. Cette assertion découle également directement du paragraphe précédent : $\mathbf{F}_q \neq \mathbf{F}_q^2$. Nous allons maintenant généraliser ce résultat à d'autres nombres premiers l.

***Proposition* 6.7.2**. — *Soit* $\mathbf{K}$ *un corps et* a *un élément de* $\mathbf{K}$. *Soit* l *un nombre premier distinct de la caractéristique de* $\mathbf{K}$, *alors le polynôme* $T^l - a$ *est soit irréductible, soit admet une racine sur* $\mathbf{K}$.

Démonstration. — Soit ζ une racine primitive l-ième de l'unité dans une clôture algébrique de $\mathbf{K}$ et b une racine l-ième de a dans ce corps. On a alors l'égalité $T^l - a = \prod_{k=0}^{l-1}(T - \zeta^k b)$. Si $T^l - a$ n'est pas irréductible sur $\mathbf{K}$, alors il existe une partie I stricte de $\{0, \ldots, l-1\}$ telle que $\prod_{k\in I}(T - \zeta^k b)$ appartienne à $\mathbf{K}[T]$. Or son terme constant est de la forme $\zeta^r b^s$ avec $s = \sharp I$. Comme $0 < s < l$, il est premier à l et en utilisant le théorème de Bezout, il existe un entier t tel que $\zeta^t b$ appartienne à $\mathbf{K}$, c'est-à-dire a a une racine l-ième dans $\mathbf{K}$. □

Réciproquement on va montrer le résultat suivant :

***Théorème* 6.7.3 (Extensions de Kummer)**. — *Si* p *et* l *deux nombres premiers distincts et* q *une puissance de* p. *Supposons que* $\mathbf{F}_q$ *contienne une racine primitive* l*-ième de l'unité. Alors il existe* $\alpha \in \mathbf{F}_{q^l}$ *telle que*

$$\mathbf{F}_{q^l} = \mathbf{F}_q(\alpha) \quad \textit{et} \quad \alpha^l \in \mathbf{F}_q.$$

***Remarque* 6.7.4**. — Notons que l'adjonction de racine l-ième de l'unité correspond à une extension de degré inférieur à $l - 1$ et donc premier à l.

***Lemme* 6.7.5**. — *Si* $d \geqslant 1$, *Le frobenius* Fr_q *est un automorphisme de* $\mathbf{F}_{q^d}$ *d'ordre* d *dans le groupe des automorphisme de* $\mathbf{F}_{q^d}$.

Démonstration. — Le morphisme $\mathrm{Fr}_q : \mathbf{F}_{q^d} \to \mathbf{F}_{q^d}$ est un morphisme de corps. Il est donc injectif. Comme $\mathbf{F}_{q^d}$ est fini, ce morphisme est également surjectif. Calculons l'ordre de cet automorphisme. L'ordre de Fr_q est le plus petit entier strictement positif k tel que

$$\forall x \in \mathbf{F}_{q^d}, \quad x^{q^k} = x \tag{6.7.1}$$

Comme le polynôme $T^{q^k} - T$ a au plus q^k racines dans $\mathbf{F}_{q^d}$, on obtient que cet ordre est minoré par d. D'un autre coté, tout élément de $\mathbf{F}_{q^d}$ vérifie (6.7.1) pour $k = d$. On obtient que d est bien l'ordre du Frobenius. □

***Théorème* 6.7.6 (Dedekind).** — *Soient $\rho_1,\ldots,\rho_n$ n automorphisme distincts d'un corps $\mathbf{K}$. Alors $\rho_1,\ldots,\rho_n$ sont linéairement indépendants en tant qu'éléments de $\mathbf{K}^{\mathbf{K}}$.*

Démonstration. — Supposons qu'il existe une relation linéaire non triviale entre automorphismes distincts de $\mathbf{K}$. On peut choisir une telle relation de longueur minimale. Elle s'écrit

$$a_1\rho_1 + \cdots + a_n\rho_n = 0 \tag{6.7.2}$$

avec $a_i \in \mathbf{K}$. Comme cette relation est de longueur minimale, tous ses coefficients sont non nuls. Les automorphismes étant deux à deux distincts, il existe $x \in \mathbf{K}$ tel que $\rho_1(x) \neq \rho_2(x)$. En appliquant (6.7.2) on obtient

$$\forall y \in \mathbf{K}, \quad a_1\rho_1(xy) + \cdots + a_n\rho_n(xy) = 0.$$

Autrement dit

$$a_1\rho_1(x)\rho_1 + \cdots + a_n\rho_n(x)\rho_n = 0.$$

En combinant cette equation avec (6.7.2), cela donne

$$a_2(\rho_2(x) - \rho_1(x))\rho_2 + \cdots + a_n(\rho_n(x) - \rho_1(x))\rho_n = 0.$$

Comme $\rho_2(x) - \rho_1(x) \neq 0$ on a obtenu une relation non triviale plus courte, ce qui contredit la minimalité de la relation. □

***Théorème* 6.7.7 (Hilbert 90 multiplicatif).** — *Soit $\mathbf{K}$ un corps et σ un automorphisme d'orde n de $\mathbf{K}$. On considère l'application*

$$\begin{array}{rccc} N_\sigma : & \mathbf{K} & \to & \mathbf{K} \\ & x & \mapsto & \prod_{i=0}^{n-1} \sigma^i(x). \end{array}$$

On a l'équivalence

$$N_\sigma(x) = 1 \quad \Leftrightarrow \quad (\exists y \in \mathbf{K}^\times, x = y/\sigma(y)).$$

***Remarque* 6.7.8.** — Notons que si $x \in \mathbf{K}^\times$, alors $\sigma(N_\sigma(x)) = N_\sigma(x)$ et donc on a $N_\sigma(x) \in \mathbf{K}^\sigma = \{\, x \in \mathbf{K} \mid \sigma(x) = x \,\}$.

Démonstration. — Si $x = y/\sigma(y)$, alors $N_\sigma(x) = N_\sigma(y)/N_\sigma(y) = 1$. La difficulté est dans la démonstration de la réciproque. Si $N_\sigma(x) = 1$, on considère

$$\mathrm{Id}_{\mathbf{K}} + x\sigma + \cdots + (x\sigma(x)\ldots\sigma^{n-2}(x))\sigma^{n-1}.$$

Par le lemme 6.7.6, cette application est non nulle. Il existe donc z tel que

$$y = z + x\sigma(z) + \cdots + (x\sigma(x)\ldots\sigma^{n-2}(x))\sigma^{n-1}(z) \neq 0.$$

Mais on a la relation

$$\begin{aligned} x\sigma(y) &= x\sigma(z) + \cdots + x(\sigma(x)\ldots\sigma^{n-1}(x))\sigma^n(z) \\ &= y - z + N_\sigma(x)z = y. \end{aligned}$$ □

Démonstration du théorème 6.7.3. — Soit ζ une racine primitive l-ième de l'unité dans $\mathbf{F}_q$. On a $N_{\mathrm{Fr}_q}(\zeta^{-1}) = \zeta^{-l} = 1$. Par le théorème d'Hilbert 90, il existe $y \in \mathbf{F}_{q^l}$ tel que $\mathrm{Fr}_q(y) = y\zeta$. En particulier $y \notin \mathbf{F}_q$ et donc $\mathbf{F}_{q^l} = \mathbf{F}_q(y)$. Par contre $\mathrm{Fr}_q(y^l) = y^l$ et donc $y^l \in \mathbf{F}_q$. □

Parlons maintenant du cas où le degré de l'extension est égal à la caractéristique.

***Proposition* 6.7.9**. — *Soit* $\mathbf{K}$ *un corps de caractéristique* $p > 0$ *et* $a \in \mathbf{K}$. *Alors le polynôme* $T^p - T - a$ *est soit scindé soit irréductible.*

Démonstration. — Soit b une racine de $T^p - T - a$ dans une clôture algébrique de $\mathbf{K}$. Alors pour tout x de $\mathbf{F}_p$, on a

$$(b+i)^p - (b+i) - a = b^p + i^p - b - i - a = b^p - b - a = 0.$$

Donc

$$T^p - T - a = \prod_{x \in \mathbf{F}_p} (T - b - x).$$

Si b appartient à $\mathbf{K}$, alors toutes les racines de $T^p - T - a$ aussi et ce polynôme est scindé. Si $T^p - T - a$ n'est pas irréductible, soit P un facteur irréductible unitaire de ce polynôme. Alors

$$P = \prod_{x \in I} (T - b - x)$$

avec $I \subset \mathbf{F}_p$ et $1 \leqslant \sharp(I) \leqslant p-1$. Le coeff de T^{d-1} dans P est égal à

$$-\sum_{x \in I} (b + x) = -\sharp(I)\, b - \sum_{x \in I} x$$

donc $b \in \mathbf{K}$ et le polynôme est scindé par ce qui précède. □

***Théorème* 6.7.10 (Extensions d'Artin-Schreier)**. — *Si* p *est un nombre premier et* q *une puissance de* p, *alors il existe* $\alpha \in \mathbf{F}_{q^p}$ *tel que* $\mathbf{F}_{q^p} = \mathbf{F}_q(\alpha)$ *et* $\alpha^p - \alpha \in \mathbf{F}_q$.

La démonstration repose sur le lemme suivant.

***Lemme* 6.7.11 (Théorème d'Hilbert 90 additif)**. — *Soit* σ *un automorphisme d'ordre* n *d'un corps* $\mathbf{K}$. *On considère l'application*

$$\begin{array}{rccc} \mathrm{Tr}_\sigma : & \mathbf{K} & \to & \mathbf{K} \\ & x & \mapsto & \sum_{i=0}^{n-1} \sigma^i(x). \end{array}$$

On a l'équivalence

$$\mathrm{Tr}_\sigma(x) = 0 \quad \Leftrightarrow \quad (\exists y \in K^\times, x = y - \sigma(y)).$$

***Remarque* 6.7.12**. — Là encore, $\mathrm{Tr}_\sigma(x) \in \mathbf{K}^\sigma$ pour tout x de $\mathbf{K}$.

Démonstration. — Si $x = y - \sigma(y)$, alors $\mathrm{Tr}_\sigma(x) = \mathrm{Tr}_\sigma(y) - \mathrm{Tr}_\sigma(y) = 0$. Inversement, soit $x \in \mathbf{K}$ tel que $\mathrm{Tr}_\sigma(x) = 0$. Par le lemme 6.7.6 l'application

$$\mathrm{Id} + \sigma + \cdots + \sigma^{n-1}$$

est non nulle. Il existe donc θ tel que $\mathrm{Tr}_\sigma(\theta) \neq 0$. On pose

$$y = \frac{1}{\mathrm{Tr}_\sigma(\theta)} \Big(x\sigma(\theta) + (x + \sigma(x))\sigma^2(\theta) + \cdots + \Big(\sum_{i=0}^{n-2} \sigma^i(x) \Big) \sigma^{n-1}(\theta) \Big)$$

et on vérifie l'égalité $y - \sigma(y) = x$. □

Démonstration du théorème. — On $\mathrm{Tr}_{\mathrm{Fr}_q}(-1) = -p = 0$. Donc par le théorème d'Hilbert 90 additif, il existe $\alpha \in \mathbf{F}_{q^p}$ tel que $-1 = \alpha - \mathrm{Fr}_q(\alpha)$. Autrement dit $\mathrm{Fr}_q(\alpha) = \alpha + 1$. En particulier, $\alpha \notin \mathbf{F}_q$ et $\mathbf{F}_{q^p} = \mathbf{F}_q(\alpha)$. D'autre part,

$$\mathrm{Fr}_q(\alpha^p - \alpha) = \mathrm{Fr}(\alpha)^p - \mathrm{Fr}(\alpha) = (\alpha+1)^p - \alpha - 1 = \alpha^p - \alpha.$$

Donc $\alpha^p - \alpha \in \mathbf{F}_q$. □

***Exemple* 6.7.13**. — Le corps $\mathbf{F}_4$ est isomorphe à $\mathbf{F}_2[T]/(T^2+T+1)$.

6.8. Application à la cryptographie : El Gamal

Définition 6.8.1. — On considère un élément $x \in \mathbf{F}_q^\times$ d'ordre un nombre l dans $\mathbf{F}_q^\times$. Si $y = x^a$, a est appelé le *logarithme discret* de y relativement à x.

Remarque 6.8.2. — Il n'existe pas à l'heure actuelle d'algorithme publiquement connu pour calculer de manière efficace le logarithme discret.

Ceci conduit à la procédure suivante en cryptographie, appelée du nom de son inventeur El Gamal [**EG**]. Il s'agit à nouveau d'une implémentation du concept de cryptographie à clef publique de Diffie et Hellman :

Choix des clefs.

Alice choisit un élément x dans $\mathbf{F}_q^\times$ et un exposant a. Elle calcule alors $w = x^a$ dans $\mathbf{F}_q$. La clef publique est alors la paire (x, w) et la clef secrète l'entier a.

Cryptage.

Pour crypter un message m appartenant à $\mathbf{F}_q^\times$, Bob reçoit la clef (x, w) d'Alice, il choisit un exposant b et calcule $w' = x^b$ ainsi que $c = w^b m$. Le texte crypté est alors la paire (c, w').

Décryptage.

Alice reçoit (c, w') et en déduit le mesage m par la formule $w'^{-a}c = x^{-ab}x^{ab}c$.

Hypothèse.

Il est difficile de retrouver x^{ab} à partir de x, x^a, x^b.

Pour illustrer la différence entre le calcul du logarithme sur les nombres réels et le problème du log discret, nous avons représenté côte à côte sur la figure 1, inspirée d'une illustration parue dans un journal de vulgarisation [**Me**], la fonction exponentielle et la fonction $x \mapsto 77^x \% 503$.

EXERCICES

6.1. Qu'est-ce que suggère la figure 1 au sujet de la période de 77 dans $\mathbf{F}_{503}^\times$?

6.2. Ecrire la table d'addition et de multiplication dans $\mathbf{F}_4$.

6.3. Donner une construction de $\mathbf{F}_{25}$, $\mathbf{F}_{49}$, $\mathbf{F}_{121}$ et $\mathbf{F}_{169}$.

6.4. Montrer que $T^4 + T + 1$ est irréductible sur $\mathbf{F}_2$. En déduire une description de $\mathbf{F}_{16}$.

6.5. Donner une description du corps $\mathbf{F}_{125}$.

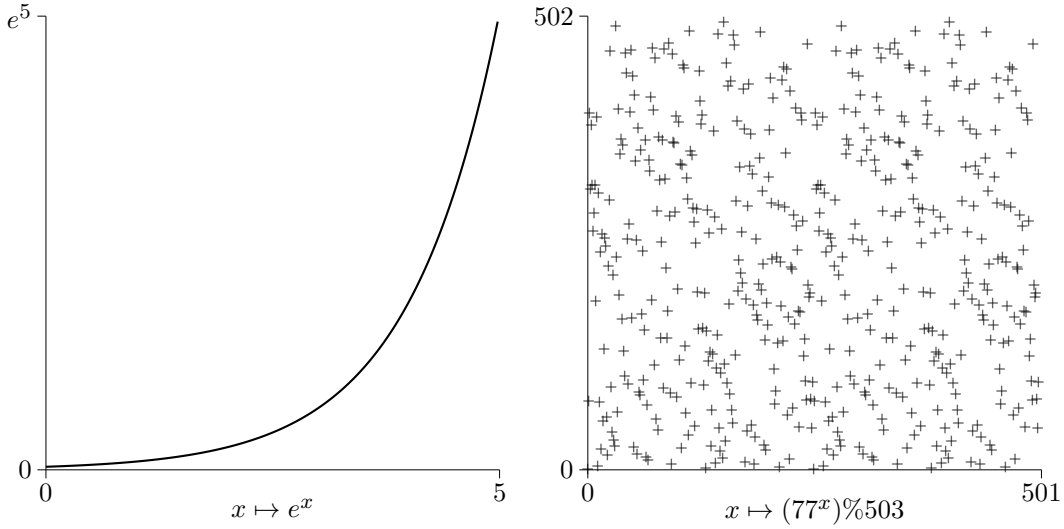
6.6. Soit p un nombre premier, Montrer que $1 + T + T^2$ est irréductible dans $\mathbf{F}_p[T]$ si et seulement si $p \equiv 2 \pmod 3$.

6.7. Soit p un nombre premier.

1. Montrer que si $x \in \mathbf{F}_p^\times$, alors $T^p - T + x$ est irréductible dans $\mathbf{F}_p[T]$.
2. Retrouver directement le théorème 6.7.10 dans le cas où $q = p$.
3. Donner une construction de $\mathbf{F}_{p^p}$ pour tout nombre premier p.

6.8. Soit p un nombre premier, $d \geqslant 1$ et $q = p^d$.

FIGURE 1. Log réel et discret



1. Si $p = 3$, montrer que tout élément de $\mathbf{F}_q$ s'écrit de manière unique comme un cube.
   Dans la suite de l'exercice, on suppose $p \neq 3$.
2. Montrer que $\mathbf{F}_q$ contient une racine cubique de l'unité si et seulement si $3 \mid (q-1)$.
3. On note $\mathbf{F}_q^3$ l'ensemble des cubes dans $\mathbf{F}_q$.

(**a**) Si $3 \mid q-1$, montrer que $\sharp(\mathbf{F}_q^3) = (q+2)/3$ et que x est un cube dans $\mathbf{F}_q^\times$ si et seulement si $x^{\frac{q-1}{3}} = 1$.

(**b**) Si 3 ne divise pas $q-1$, montrer que pour tout élément x de $\mathbf{F}_q$, il existe un unique y de $\mathbf{F}_q$ tel que $x = y^3$.

(**4.**) Donner une construction de $\mathbf{F}_{343}$, $\mathbf{F}_{2\,197}$.

6.9. Soit p un nombre premier $d \geqslant 1$ et $q = p^d$. On note l un nombre premier tel que $l \mid q-1$ et θ un générateur de $\mathbf{F}_q^\times$.

1. Montrer que $T^l - \theta$ est irréductible dans $\mathbf{F}_q[T]$.
2. Soit ρ une racine de $T^l - \theta$ dans $\mathbf{F}_{q^l}$. Le groupe $\mathbf{F}_{q^l}^\times$ est-il engendré par ρ ?
3. Montrer que le polynôme
$$P = \prod_{i=0}^{d-1} (T^l - \mathrm{Fr}_{p^i}(\theta))$$
appartient à $\mathbf{F}_p[T]$. Quel est son degré ?
4. Que peut-on dire de P et du polynôme minimal de ρ ?
5. Donner une construction de $\mathbf{F}_{64}$ en tant qu'extension de $\mathbf{F}_2$.

6.10. Soit p un nombre premier et q une puissance de p. On note $a_n(q)$ le nombre de polynômes irréductibles de degré n dans $\mathbf{F}_q[T]$ et $b_n(q)$ le nombre de polynômes irréductibles unitaires de degré n dans $\mathbf{F}_q[T]$.

1. Montrer la relation
$$q^n = \sum_{d \mid n} d b_d(q).$$

(On pourra considérer les polynômes minimaux sur $\mathbf{F}_q$ des éléments de $\mathbf{F}_{q^n}$.)

2. On définit la fonction de Möbius $\mu : \mathbf{N}^* \to \{-1, 0, 1\}$ par :

$$\forall a, b \in \mathbf{N}^*, \quad \mathrm{pgcd}(a, b) = 1 \Rightarrow \mu(a, b) = \mu(a)\mu(b)$$

et si l est un nombre premier

$$\mu(l^k) = \begin{cases} 1 & \text{si } k = 0, \\ -1 & \text{si } k = 1, \\ 0 & \text{sinon.} \end{cases}$$

On pose, si $n \geqslant 1$,

$$\phi(n) = \sum_{d|n} \mu(d).$$

(**a**) Montrer que si $a, b \geqslant 1$ et $\mathrm{pgcd}(a, b) = 1$, alors $\phi(ab) = \phi(a)\phi(b)$.

(**b**) Montrer que

$$\phi(n) = \begin{cases} 1 \text{ si } n = 1, \\ 0 \text{ sinon.} \end{cases}$$

(**c**) Soient $f, g : \mathbf{N}^* \to \mathbf{Z}$. Montrer que si on a

$$\forall n \in \mathbf{N}^*, \quad f(n) = \sum_{d|n} g(d),$$

alors

$$\forall n \in \mathbf{N}^*, \quad g(n) = \sum_{d|n} \mu(d) f(n/d).$$

3. Montrer que $nb_n(q) = \sum_{d|n} \mu(d) q^{n/d}$.

4. Montrer que

$$a_n(q) \geqslant \frac{q^n(q-2)}{n}.$$

(On pourra d'abord calculer $\sum_{m<n} q^m$ puis minorer $nb_n(q)$). En déduire que si $q \neq 2$, alors $a_n(q) \geqslant q^{n+1}/3n$.

CHAPITRE 7

ALGORITHMES DE FACTORISATION

Pour tout ce chapitre, le lecteur pourra se reporter au livre d'Henri Cohen [**Co**], dont nous nous inspirons largement. Soit $\mathbf{K}$ un corps. On s'intéresse dans ce chapitre à la question de la décomposition d'un polynôme P en facteurs irréductibles.

7.1. Éléments sans facteurs carrés

Définition 7.1.1. — Soit A un anneau, un élément a de A est dit sans facteur carré si

$$\forall b \in A, \quad b^2 \mid a \Rightarrow b \in A^\times.$$

Remarque 7.1.2. — Si A est un anneau factoriel et $\mathscr{P}$ un système de représentants des irréductibles de A un élément non nul a est sans facteur carré si et seulement si $v_p(a) \leqslant 1$ pour tout p de $\mathscr{P}$.

Définition 7.1.3. — Un corps $\mathbf{K}$ est dit *parfait* s'il est de caractéristique 0 ou s'il est de caractéristique non nulle p et vérifie la condition

$$\forall x \in \mathbf{K}, \quad \exists y \in \mathbf{K}, \quad x = y^p.$$

Exemple 7.1.4. — Si $\mathbf{K}$ est un corps fini, le morphisme de Frobenius est surjectif et $\mathbf{K}$ est parfait.

Proposition 7.1.5. — *Si $\mathbf{K}$ est un corps parfait, un polynôme P de $\mathbf{K}[T]$ est sans facteur carré si et seulement si P est premier avec le polynôme dérivé P'.*

Exemple 7.1.6. — Soit $\mathbf{K} = \mathbf{F}_p(X)$ et $P = T^p - X \in \mathbf{K}[T]$. Le polynôme P est irréductible et donc sans facteur carré, mais $P' = 0$ et donc P et P' ne sont pas premiers entre eux.

Démonstration. — Si $Q^2 \mid P$ avec $Q \in \mathbf{K}[T]$ non inversible, alors P se met sous la forme $P = Q^2R$ et $P' = 2QQ'R + Q^2R'$. Par conséquent $Q \mid P'$ et comme Q n'est pas inversible, P n'est pas premier à P'.

Réciproquement supposons que P n'est pas premier à P'. Soit Q un polynôme irréductible facteur de P et P'. On peut donc écrire $P = QR$. On a $P' = Q'R + QR'$. Par conséquent $Q \mid Q'R$. Par le lemme d'Euclide, $Q \mid Q'$ ou $Q \mid R$. Dans le deuxième cas, $Q^2 \mid P$ et P n'est pas sans facteur carré. Dans le premier, on $\deg(Q') \leqslant \deg(Q) - 1$ avec égalité si la

caractéristique de $\mathbf{K}$ est nulle. Comme $Q \mid Q'$, on en déduit que $\mathbf{K}$ est de caractéristique finie p et $Q' = 0$. Ecrivons $Q = \sum_{i=0}^{d} a_i T^i$ On a donc

$$Q' = \sum_{i=1}^{d} a_i i T^{i-1}.$$

Ce polynôme est nul si et seulement si $a_i = 0$ dès que $p \nmid i$. Autrement dit Q peut s'écrire

$$Q = \sum_{i=0}^{\lfloor \frac{d}{p} \rfloor} a_{pi} T^{pi}$$

Mais, comme K est parfait, pour tout i il existe b_i tel que $a_{ip} = b_i^p$. Et comme le Frobenius définit un morphisme d'anneau $\mathbf{K}[T] \to \mathbf{K}[T]$, on obtient

$$Q = \Big(\sum_{i=0}^{\lfloor \frac{d}{p} \rfloor} b_i T^i \Big)^p$$

ce qui contredit l'irréductibilité de Q. □

7.2. Stratégie de la factorisation

On se place dans la suite sur un corps fini $\mathbf{F}_q$ de caractéristique p. La structure générale de l'algorithme de factorisation est la suivante :

Algorithme 7.2.1.

Entrée:

- P un polynôme unitaire de $\mathbf{F}_q[T]$.

Sortie:

- Des paires (P_i, a_i) avec $1 \leqslant i \leqslant r$ de sorte que :
  a. P_i est irréductible,
  b. a_i est un entier strictement positif,
  c. $P = \prod_{i=1}^{r} P_i^{a_i}$.

Algorithme:

1. Trouver les polynômes unitaires A_i de $\mathbf{F}_q[T]$ tels que
   a. $P = A_1 A_2^2 \dots A_k^k$,
   b. les A_i sont sans facteurs carrés et premiers deux à deux,
   Cette décomposition s'appelle décomposition sans facteur carré.
2. Pour chaque A_i, trouver les polynômes $A_{i,d}$ tels que
   a. $A_i = \prod_d A_{i,d}$,
   b. Les composantes irréductibles de $A_{i,d}$ sont toutes de degré d.
3. Décomposer chaque $A_{i,d}$ en facteurs irréductibles.
4. Retourner les paires obtenues.

7.3. Factorisation sans facteur carré

L'algorithme se base sur le lemme suivant :

Lemme 7.3.1. — *Soit P un polynôme unitaire de $\mathbf{F}_q[T]$ et $P = \prod_{i=1}^{r} P_i^{a_i}$ sa décomposition en facteurs irréductibles, alors*

$$\operatorname{pgcd}(P, P') = \prod_{p \nmid a_i} P_i^{a_i - 1} \prod_{p \mid a_i} P_i^{a_i}. \tag{7.3.1}$$

Démonstration. — Le polynôme P' s'écrit

$$P' = \sum_{\{i \mid p \nmid a_i\}} a_i P_i' P_i^{a_i - 1} \prod_{j \neq i} P_j^{a_j}.$$

Le terme de droite de (7.3.1) divise donc bien $\operatorname{pgcd}(P, P')$. Inversement soit Q un facteur irréductible de $\operatorname{pgcd}(P, P')$, alors $Q \mid P$ et donc $Q = P_i$ pour un i compris entre 1 et r. Notons $n = v_Q(\operatorname{pgcd}(P, P'))$ la valuation de $\operatorname{pgcd}(P, P')$ en Q. On a $a_i - 1 \leqslant n \leqslant a_i$. si $p \mid a_i$, alors par ce qui précède $n = a_i$. Sinon $P_i^{a_i} \mid P'$ si et seulement si $P_i^{a_i} \mid a_i P_i' P_i^{a_i - 1}$ si et seulement si $P_i \mid P_i'$ ce qui est impossible par la proposition 7.1.5. □

Voici l'algorithme correspondant

Algorithme 7.3.2.

Entrée:

- P un polynôme unitaire de $\mathbf{F}_q[T]$.

Sortie:

- Des paires (A_i, i) avec $1 \leqslant i \leqslant r$ de sorte que :
  a. $P = A_1 A_2^2 \dots A_k^k$,
  b. les A_i sont sans facteurs carrés, premiers deux à deux,

Algorithme:

1. $e \leftarrow 1$.
2. Tant que P n'est pas de degré 0,
   2.1. $F \leftarrow \operatorname{pgcd}(P, P')$ et $V \leftarrow P/F$, $k \leftarrow 0$.
   2.2. Si V est constant, alors
      2.2.1. On a $F = \sum_i a_{ip} T^{ip}$. Calculer Q tel que $F = Q^p$.
      2.2.2. $P \leftarrow Q$, $e \leftarrow ep$.
      2.2.3. Retourner à l'étape 2.
   2.3. $k \leftarrow k + 1$.
   2.4. Si $p \mid k$, alors
      2.4.1. $F \leftarrow F/V$, $k \leftarrow k + 1$.
   2.5. $W \leftarrow \operatorname{pgcd}(F, V)$, $A_{ek} \leftarrow V/W$.
   2.6. Si A_{ek} n'est pas constant, alors,
      2.6.1. Ajouter (A_{ek}, ek) à la liste des résultats.
   2.7. $V \leftarrow W$, $F \leftarrow F/V$.
   2.8. Retourner à l'étape 2.2.

Suivons les premières étapes de cet algorithme sur un polynôme $P = \prod_{i=0}^{r} P_i^{a_i}$ qui n'est pas une puissance p-ième, $p \geqslant 3$.

2.1. $F \leftarrow \prod_{p \nmid a_i} P_i^{a_i - 1} \prod_{p \mid a_i} P_i^{a_i}$, $\quad V \leftarrow \prod_{p \nmid a_i} P_i$, $\quad k \leftarrow 0$.

2.3. $k \leftarrow 1$.

2.5. $W \leftarrow \prod_{\substack{p \nmid a_i \\ a_i \geqslant 2}} P_i$, $\quad A_1 \leftarrow \prod_{a_i = 1} P_i$.

2.7. $V = \prod_{\substack{p \nmid a_i \\ a_i \geqslant 2}} P_i$, $\quad F \leftarrow \prod_{\substack{p \nmid a_i \\ a_i \geqslant 2}} P_i^{a_i - 2} \prod_{p \mid a_i} P_i^{a_i}$.

...

2.3. $k \leftarrow p - 1$.

2.5. $W \leftarrow \prod_{\substack{p \nmid a_i \\ a_i \geqslant p}} P_i$, $\quad A_{p-1} \leftarrow \prod_{a_i = p-1} P_i$.

2.7. $V = \prod_{\substack{p \nmid a_i \\ a_i \geqslant p}} P_i$, $\quad F \leftarrow \prod_{\substack{p \nmid a_i \\ a_i \geqslant p}} P_i^{a_i - p} \prod_{p \mid a_i} P_i^{a_i}$.

2.3. $k \leftarrow p$.

2.4.1 $F \leftarrow \prod_{\substack{p \nmid a_i \\ a_i \geqslant p+1}} P_i^{a_i - p - 1} \prod_{p \mid a_i} P_i^{a_i}$, $\quad k \leftarrow p + 1$.

2.5. $W \leftarrow \prod_{\substack{p \nmid a_i \\ a_i \geqslant p+2}} P_i$, $\quad A_{p+1} \leftarrow \prod_{a_i = p+1} P_i$.

Le point-clef est que cet algorithme n'utilise que le calcul du pgcd.

7.4. Factorisation suivant les degrés

Il repose sur le lemme suivant :

Lemme 7.4.1. — *Soient P un polynôme unitaire sans facteur carré de $\mathbf{F}_q[T]$, et $P = \prod_{i=1}^{r} P_i$ sa décomposition en facteurs irréductibles. Alors*

$$\mathrm{pgcd}(T^{q^r} - T, P) = \prod_{\{i \mid \deg P_i \mid r\}} P_i$$

Démonstration. — Par la proposition 6.5.3,

$$T^{q^r} - T = \prod_{\{Q \in \mathscr{I} \mid \deg Q \mid r\}} Q. \quad \square$$

En tenant compte du fait que pour calculer le pgcd on peut utiliser la reste de la division de T^{p^r} par P, ceci nous donne l'algorithme suivant

Algorithme 7.4.2.

Entrée:

- P un polynôme unitaire sans facteur carré de $\mathbf{F}_q[T]$.

Sortie:

- Des paires (A_d, d) de sorte que :
  a. $P = \prod_d A_d$,
  b. Les composantes irréductibles de A_d sont toutes de degré d.

Algorithme:

1. $W \leftarrow T$, $d \leftarrow 0$.
2. Si $d+1 > \deg(P)$, alors
   2.1. Si P n'est pas constant, alors
      2.1.1 Ajouter $(P, \deg P)$ à la liste des résultats.
   2.2. Fin de l'algorithme.
3. $d \leftarrow d+1$, $W \leftarrow$ reste de la division de W^p par P.
4. $A_d \leftarrow \operatorname{pgcd}(W - T, P)$.
5. Si A_d n'est pas constant, alors
   5.1. Ajouter (A_d, d) à la liste des résultats.
   5.2. $P \leftarrow P/A_d$.
   5.3. $W \leftarrow$ reste de la division de W par P.
6. Retourner à l'étape 2.

7.5. Factorisation finale de Cantor-Zassenhaus

La dernière étape, qui est aussi le plus difficile est de décomposer les polynômes $A_{i,d}$ obtenus dans les étapes précédentes. Nous donnons successivement deux méthodes, l'une due à Cantor et Zassenhaus, l'autre a Berlekamp, cette dernière étant plus efficace pour les petites valeurs de q.

La méthode de Cantor-Zassenhaus est basée sur le lemme suivant :

Lemme 7.5.1. — *On suppose que $p \neq 2$. Soit P un polynôme unitaire sans facteur carré dont tous les facteurs irréductibles sont de degré d. Alors pour tout polynôme Q, on a la relation*

$$P = \operatorname{pgcd}(P, Q) \operatorname{pgcd}(P, Q^{\frac{q^d-1}{2}} + 1) \operatorname{pgcd}(P, Q^{\frac{q^d-1}{2}} - 1).$$

Démonstration. — Si $Q \in \mathbf{F}_q[T]$, alors pour tout $\alpha \in \mathbf{F}_{q^d}$, $Q(\alpha) \in \mathbf{F}_{q^d}$ et on a l'égalité $Q(\alpha)^{q^d} - Q(\alpha) = 0$ Donc $T^{q^d} - T \mid Q^{q^d} - Q$. Comme P est produit de facteur irréductibles unitaires distincts de degré d, P divise $T^{q^d} - T$ et donc $Q^{q^d} - Q$. Mais par Bezout, comme $p \neq 2$, les polynômes Q, $Q^{(q^d-1)/2} - 1$ et $Q^{(q^d-1)/2} + 1$ sont premiers entre eux deux à deux. En outre on a la relation

$$Q^{q^d} - Q = Q(Q^{\frac{q^d-1}{2}} - 1)(Q^{\frac{q^d-1}{2}} + 1)$$

En définitive

$$P = \operatorname{pgcd}(P, Q^{q^d} - Q) = \operatorname{pgcd}(P, Q) \operatorname{pgcd}(P, Q^{\frac{q^d-1}{2}} + 1) \operatorname{pgcd}(P, Q^{\frac{q^d-1}{2}} - 1) \quad \square$$

Ceci conduit à l'algorithme suivant

Algorithme 7.5.2.
Entrée:
- P un polynôme sans facteur carré dont les facteurs irréductibles sont de degré d.
Sortie:
- Facteurs irréductibles de P.
Algorithme:
1. Si $\deg P = d$, alors
   1.1. retourner P, fin de l'algorithme.
2. Choisir un polynôme unitaire aléatoire Q de degré $\leqslant 2d-1$.
3. $B \leftarrow \mathrm{pgcd}(P, Q^{\frac{q^d-1}{2}} - 1)$.
4. Si $\deg(B) = 0$ ou $\deg(B) = \deg(P)$, alors
   4.1 Retourner à l'étape 2.
5. Appliquer l'algorithme à B et P/B.

Il s'agit donc d'un algorithme basé sur une méthode aléatoire. On peut montrer que la probabilité que le polynôme $\mathrm{pgcd}(P, Q^{(q^d-1)/2} - 1)$ soit un facteur non trivial de P est proche de $1/2$.

Passons au cas $p = 2$. Dans ce cas on utilise le lemme suivant

Lemme 7.5.3. — *Si $p = 2$ et q une puissance de 2, On note U le polynôme*

$$U(T) = T + T^2 + T^4 + \cdots + T^{q^d/2}.$$

Si P est un polynôme sans facteur carré de $\mathbf{F}_q[T]$ dont tous les facteurs irréductibles sont de degré d et si $Q \in \mathbf{F}_q[T]$, alors

$$P = \mathrm{pgcd}(P, U(Q))\,\mathrm{pgcd}(P, U(Q) + 1)$$

Démonstration. — Comme le Frobenius Fr_2 définit un morphisme d'anneaux de $\mathbf{F}_q[T]$ dans $\mathbf{F}_q[T]$, on a les relations

$$U^2 = T^2 + T^4 + \cdots + T^{q^d}$$

et donc

$$U^2 + U = T + T^{q^d}.$$

Donc $U(Q)(U(Q) + 1) = U^{q^d}(Q) - U(Q)$. Comme dans la démonstration du lemme précédent, on montre que c'est un multiple de P. Et la fin de la démonstration est le même que pour le cas $p \neq 2$. □

Cela donne l'algorithme suivant pour $p = 2$:

Algorithme 7.5.4.

Entrée:

- Un polynôme P de $\mathbf{F}_2[T]$ tel que :
  a. P est sans facteur carré,
  b. les facteurs irréductibles de P sont de degré d.

Sortie:

- Les facteurs irréductibles de P.

Algorithme:

1. Si $d = \deg(P)$, alors
   1.1. retourner P, fin de l'algorithme.
2. $Q \leftarrow T$.
3. $C \leftarrow Q$, $D \leftarrow Q$.
4. Faire $d-1$ fois les opérations :
   4.1. $D \leftarrow$ reste de la division de D^2 par P,
   4.2. $C \leftarrow C + D$.
5. $B \leftarrow \mathrm{pgcd}(P, C)$.
6. Si $\deg(B) = 0$ ou $\deg(B) = \deg(P)$, alors
   6.1. $Q \leftarrow QT^2$.
   6.2. Retourner à l'étape 4.
7. Appliquer l'algorithme à B et P/B.

Il reste à montrer que cet algorithme ce termine.

Lemme 7.5.5. — *Si P est un polynôme non irréductible sans facteur carré dont tous les facteurs sont de degré d, alors il existe un nombre impair e tel que $1 \leqslant e \leqslant 2d-1$ tel que $\mathrm{pgcd}(P, U(T^e))$ soit un facteur non trivial de P.*

Démonstration. — Sinon, pour tout e impair compris entre 1 et $2d-1$, on a une des égalités $\mathrm{pgcd}(P, U(T^e)) = P$ ou $\mathrm{pgcd}(P, U(T^e)+1) = P$ et donc $U(T^e) \equiv 0$ ou 1 modulo P. Mais pour tout polynôme Q, P divise $U(Q^2) - U(Q)$, cette assertion vaut également pour les valeurs paires de e. D'un autre côté, l'application qui envoie Q sur $U(Q)$ est linéaire sur $\mathbf{F}_2$. Par conséquent pour tout polynôme Q de $\mathbf{F}_2[T]$ de degré inférieur ou égal à $2d-1$, on a $U(Q) \equiv 0$ ou 1 modulo P.

Le polynôme U de degré 2^{d-1} a au plus 2^{d-1} racines dans $\mathbf{F}_{2^d}$. Il existe donc $\alpha \in \mathbf{F}_{2^d}$ tel que $U(\alpha) \neq 0$. Soient P_1 et P_2 deux facteurs distincts de P. Les polynômes P_1 et P_2 sont scindés sur $\mathbf{F}_{2^d}$. Soit β une racine de P_2 sur $\mathbf{F}_{2^d}$. Comme P_2 est irréductible de degré d, $\mathbf{F}_{2d}$ est un corps de rupture pour P_2. Donc $\mathbf{F}_{2d} = \mathbf{F}_2[\beta]$ et il existe un polynôme R de $\mathbf{F}_2[T]$ tel que $\alpha = R(\beta)$. Par le lemme chinois, P_1 et P_2 étant irréductibles et distincts, il existe un polynôme Q tel que

$$Q \equiv 0 \pmod{P_1} \quad \text{et} \quad Q \equiv R \pmod{P_2}.$$

Quitte à remplacer Q par le reste de la division de Q par P_1P_2, on peut en outre supposer que $\deg(Q) \leqslant 2d-1$. En appliquant U on obtient que

$$U(Q) \equiv U(0) = 0 \pmod{P_1} \quad \text{et} \quad U(Q) \equiv U(R) \pmod{P_2}.$$

Mais $U(R)(\beta) = U(\alpha) \neq 0$. Comme on a un isomorphisme

$$\begin{array}{ccc} \mathbf{F}_2[T]/(P_2) & \xrightarrow{\sim} & \mathbf{F}_{2^d} \\ S & \mapsto & S(\beta) \end{array}$$

on obtient $U(Q) \not\equiv 0 \pmod{P_2}$. Comme $P_1 P_2 \mid P$, cela contredit $U(Q) \equiv 0$ ou 1 modulo P. □

Remarque 7.5.6. — La démonstration du fait qu'il suffit de considérer des polynômes de degré inférieur ou égal à $2d-1$ dans l'algorithme 7.5.2 est similaire.

7.6. *Factorisation de Berlekamp*

Une autre méthode, plus ancienne, existe pour le factorisation d'un polynôme sans facteur carré. Il s'agit de la factorisation de Berlekamp qui est basée sur le résultat suivant

***Lemme* 7.6.1**. — *Soit $P \in \mathbf{F}_q[T]$ un polynôme unitaire sans facteur carré, et soit $P = \prod_{i=1}^{r} P_i$ sa décomposition en facteurs irréductibles. Un polynôme Q de $\mathbf{F}_q[T]$ avec $\deg(Q) < \deg(P)$ vérifie*

$$Q^q \equiv Q \pmod{P}$$

si et seulement si, pour tout i compris entre 1 et r, il existe $s_i \in \mathbf{F}_q$ tel que

$$Q \equiv s_i \pmod{P_i}.$$

Démonstration. — $\Rightarrow$: On a la relation

$$T^q - T = \prod_{x \in \mathbf{F}_q} (T - x).$$

et donc $Q(T)^q - Q(T) = \prod_{x \in \mathbf{F}_q} (Q(T) - x)$. Donc si $Q^q - Q \equiv 0 \pmod{P}$, on a que pour tout i entre 1 et r, on a $P_i \mid \prod_{x \in \mathbf{F}_q} (Q(T) - x)$ et P_i étant irréductible divise un des facteurs.

$\Leftarrow$: Pour tout i entre 1 et r on a

$$Q(T)^q \equiv s_i^q \equiv s_i \equiv Q(T) \pmod{P_i}.$$

On obtient le résultat en appliquant le théorème des restes chinois. □

L'idée de l'algorithme est de résoudre l'équation $Q^q - Q \equiv 0 \pmod{P}$ puis de calculer le polynôme $\operatorname{pgcd}(P, Q - s_i)$. Mais si $Q = \sum_{i=0}^{d-1} q_i T^i$, comme le Frobenius Fr_q agit trivialement sur $\mathbf{F}_q$, on a $Q^q = \sum_{i=0}^{d-1} q_i T^{iq}$. On calcule donc d'abord la matrice $M = (m_{i,k})_{0 \leqslant i,k < d}$ de sorte que $\sum_{i=0}^{d-1} m_{i,k} T^i$ soit le reste de la division euclidienne de T^{qk} par P. Le noyau de $M - \mathrm{Id}$ correspond aux solutions de l'équation $Q^q - Q \equiv 0 \pmod{P}$. Notons qu'il y une solution triviale à savoir la constante 1, les autres solutions fournissent des facteurs non triviaux.

On obtient l'algorithme suivant

Algorithme 7.6.2.

Entrée:

- $P \in \mathbf{F}_q[T]$ polynôme de degré d sans facteur carré.

Sortie:

- L'ensemble E des facteurs irréductibles de P.

Algorithme:

1. Calculer pour $0 \leqslant i < d$ le reste $\sum_{i=0}^{d-1} m_{i,k} T^i$ de la division de T^{qk} par P.
2. $M \leftarrow (m_{i,k})_{0 \leqslant i,k < d}$.
3. Determiner une base $V_1,\ldots,V_r$ du noyau de $M - \mathrm{Id}$, de sorte que :
   a. $V_1 = (1, 0, \ldots, 0)$.
   b. r est le nombre de facteurs irréductibles de P.
4. $E \leftarrow P$, $k \leftarrow 1$, $j \leftarrow 1$.
5. Tant que $k < r$,
   5.1. $j \leftarrow j + 1$,
   5.2. $Q \leftarrow V_j$,
   5.3. Pour chaque élément U de E,
      5.3.1. $F < \emptyset$.
      5.3.2. Pour tout s de $\mathbf{F}_q$,
         5.3.1.1. $B \leftarrow \mathrm{pgcd}(U, Q - s)$,
         5.3.1.2. Si $\deg B > 0$, $F \leftarrow F \cup \{B\}$.
      5.3.3. $E \leftarrow (E - \{U\}) \cup F$, $k \leftarrow k - 1 + \sharp F$.
6. Retourner E.

CHAPITRE 8

BASES

8.1. *Base normale*

***Théorème* 8.1.1**. — *Soit p un nombre premier, $q = p^d$. Alors il existe un élément θ de $\mathbf{F}_q$ de sorte que $(\theta, \mathrm{Fr}_p(\theta), \dots \mathrm{Fr}_{p^{d-1}}(\theta))$ forme une base de $\mathbf{F}_q$ sur $\mathbf{F}_p$. Cette base est dite* normale.

Démonstration. — On considère le morphisme d'anneaux

$$\begin{array}{rccc} \varphi : & \mathbf{F}_p[T] & \to & \mathrm{End}_{\mathbf{F}_p}(\mathbf{F}_q) \\ & \sum_{i=0}^{n} a_i T^i & \mapsto & \sum_{i=0}^{n} a_i \,\mathrm{Fr}_p^i \end{array}$$

et on pose pour tout P de $\mathbf{F}_p[T]$ et tout x de $\mathbf{F}_q$, $P.x = \varphi(P)(x)$. On note $\mathfrak{a}$ le noyau de φ. Comme tout x de $\mathbf{F}_q$ est solution de $X^q - X = 0$, on a que $\mathrm{Fr}_q = \mathrm{Id}_{\mathbf{F}_q}$ et donc $X^d - 1$ appartient au noyau $\mathfrak{a}$. Inversement si $P = \sum_{i=0}^{m} a_i T^i$ appartient à ce noyau avec $m < d$, on a la relation

$$\sum_{i=0}^{m} a_i \,\mathrm{Fr}_{p^i} = 0.$$

Mais par le lemme 6.7.5 les automorphismes Id, Fr_p,…,$\mathrm{Fr}_{p^{d-1}}$ sont deux à deux distincts et par le lemme 6.7.6, cela implique que P est nul. On a donc obtenu que $\mathfrak{a} = (X^d - 1)$.

Pour tout y de $\mathbf{F}_q$, on note $\mathfrak{a}_y$ le noyau de l'application

$$\begin{array}{rccc} \varphi_y : & \mathbf{F}_p[T] & \to & \mathbf{F}_q \\ & \sum_{i=0}^{n} a_i T^i & \mapsto & \sum_{i=0}^{n} a_i \,\mathrm{Fr}_p^i(y) = P.y, \end{array}$$

$\mathfrak{a}_y$ est un idéal de $\mathbf{F}_p[T]$, on note Q_y un générateur unitaire de cet idéal.

Soit x_1,…,x_d une base de $\mathbf{F}_q$ sur $\mathbf{F}_p$. On a alors $\mathfrak{a} = \bigcap_{i=1}^{d} \mathfrak{a}_{x_i}$. Par conséquent,

$$\operatorname*{ppcm}_{1 \leqslant i \leqslant d} Q_{x_i} = X^d - 1. \tag{8.1.1}$$

Notons $\mathscr{I}$ l'ensemble des polynômes irréductibles unitaires sur $\mathbf{F}_p$ et

$$X^d - 1 = \prod_{P \in \mathscr{I}} P^{v_P(X^d-1)}$$

la décomposition de $X^d - 1$ en facteurs irréductibles. Par (8.1.1), pour chaque P de $\mathscr{I}$, il existe un i entre 1 et d tel que $P^{v_P(X^d-1)}$ divise Q_{x_i}. Mais si $R \mid Q_y$, on a $Q_{R.y} = Q_y/R$. On obtient donc que pour tout P de $\mathscr{I}$, il existe $y_P \in \mathbf{F}_q$ tel que $Q_{y_P} = P^{v_P(X^d-1)}$.

Or si y et z sont deux éléments de $\mathbf{F}_q$ tels que Q_y soit premier à Q_z, alors $Q_{y+z} = Q_y Q_z$. En effet, on a

$$Q_y Q_z.(y+z) = Q_z Q_y.y + Q_y Q_z.z = 0$$

Donc $Q_{y+z} \mid Q_y Q_z$. Mais par le théorème de Bezout, il existe des polynômes $U, V \in \mathbf{F}_p[T]$ tels qu'on ait l'égalité $UQ_y + VQ_z = 1$. Donc si P vérifie $P.(y+z) = 0$ alors $PQ_z.y = 0$ et donc $P.y = PVQ_z.y + PUQ_y.y = 0$, et donc $Q_y \mid P$ De même $Q_z \mid P$, d'où l'égalité. Posons

$$u = \sum_{\{\, P \in \mathscr{I} \mid\ P \mid X^d - 1 \,\}} y_P$$

alors $Q_u = X^d - 1$. Cela signifie que la famille u, $\mathrm{Fr}_p(u)$,...,$\mathrm{Fr}_{p^{d-1}}(u)$ est linéairement indépendante sur $\mathbf{F}_p$. Pour des raisons de dimension, c'est une base de $\mathbf{F}_q$ sur $\mathbf{F}_p$. □

***Remarque* 8.1.2**. — Pour les corps de caractéristique 2, les bases normales permettent de calculer les carrés et donc les puissances (cf. A.1.1). En effet si θ, θ^2,...$\theta^{2^{d-1}}$ est une base normale de $\mathbf{F}_{2^d}$ alors pour tout $(a_0, \ldots, a_{d-1}) \in \mathbf{F}_2^d$ on a

$$\begin{aligned}(a_0\theta + \cdots + a_{d-1}\theta^{2^{d-1}})^2 &= a_0^2\theta^2 + \cdots + a_{d-1}^2\theta^{2^d} \\ &= a_{d-1}\theta + a_0\theta^2 + \cdots + a_{d-2}\theta^{2^{d-1}}\end{aligned}$$

où la dernière égalité est obtenue en notant que $\theta^{2^d} = \theta$. Autrement dit le carré s'obtient par permutation circulaire des coordonnées. Pour un corps fini arbitraire, on a une expression similaire pour le calcul du Frobenius.

8.2. *Base normale gaussienne*

Dans ce paragraphe nous considérons uniquement des corps finis de caractéristique 2. Si elle sont bien adaptées au calcul des puissances, les bases normales sont en général mal adaptées pour le calcul du produit. Les bases normales gaussiennes sont des bases normales choisies de sorte à permettre un calcul efficace du produit. Le contenu de ce paragraphe est repris d'un article de Ash, Blake et Vanstone [**ABV**].

***Définition* 8.2.1**. — Soit q une puissance de 2 et $\theta, \ldots, \theta^{2^{d-1}}$ une base normale de $\mathbf{F}_q$ sur $\mathbf{F}_2$. En utilisant la relation

$$\theta^{2^{i+k}}\theta^{2^{j+k}} = (\theta^{2^i}\theta^{2^j})^{2^k}$$

on obtient que si $\lambda_{i,j}$ est la coordonnée de $\theta^{2^i}\theta^{2^j}$ en le vecteur de base θ, alors la coordonnée de $\theta^{2^i}\theta^{2^j}$ en θ^{2^k} est $\lambda_{i-k,j-k}$, les indices étant calculés modulo d. On en déduit qu'il existe une matrice symétrique $\lambda = (\lambda_{i,j}) \in \mathscr{M}_d(\mathbf{F}_2)$ telle que

$$\Big(\sum_{i=0}^{d-1} a_i\theta^{2^i}\Big)\Big(\sum_{i=0}^{d-1} b_i\theta^{2^i}\Big) = \sum_{k=0}^{d-1} \sum_{\substack{0 \leqslant i \leqslant d-1 \\ 0 \leqslant j \leqslant d-1}} \lambda_{i,j} a_{i+k} b_{j+k} \theta^{2^k}$$

où les indices sont calculés modulo d.

La *complexité* de la multiplication pour cette base normale est alors définie comme l'entier

$$C_\theta = \sharp\{\, (i,j) \mid \lambda_{i,j} \neq 0 \,\}.$$

L'objectif est donc de minimiser cette complexité. Une base normale est dite *optimale* si elle minimise cette complexité.

***Remarque* 8.2.2**. — Mullin, Onyszchuk et Vanstone ont montré dans [**MOV**] que C_θ est minorée par $2d - 1$.

***Théorème* 8.2.3**. — *Soit d un entier strictement positif et k un entier tel que $kd+1$ soit premier et tel que $\mathbf{F}_{kd+1}^{\times}$ soit engendré par $\{2\} \cup \mathbf{F}_{kd+1}^{\times d}$. On note β une racine primitive $(kd+1)$-ième de l'unité dans $\mathbf{F}_{2^{kd}}$ et on pose*

$$\alpha = \sum_{i=0}^{k-1} \beta^{\gamma^i}$$

où γ est un entier dont la classe dans $\mathbf{F}_{kd+1}$ est une racine primitive k-ième de l'unité. Alors α engendre une base normale de $\mathbf{F}_{2^d}$ dont la complexité vérifie

$$C_\alpha \leqslant \begin{cases} kd-1 & \textit{si } k \textit{ est pair}, \\ (k+1)d-k & \textit{sinon}. \end{cases}$$

Une telle base est dite gaussienne.

***Remarques* 8.2.4**. — (i) Comme $kd+1$ est premier, $2^{kd} \equiv 1 \pmod{kd+1}$ et $\mathbf{F}_{2^{kd}}$ contient effectivement une racine primitive $(kd+1)$-ième de l'unité.

(ii) Il est possible de montrer qu'un tel entier k existe si et seulement si 8 ne divise pas d.

8.3. *Quelques algorithmes associés*

Ce paragraphe s'inspire directement de l'annexe A du texte [**IEEE**]. Nous renvoyons le lecteur à cette référence pour plus de détails.

L'algorithme suivant teste l'existence d'une base gaussienne normale sur $\mathbf{F}_{2^d}$ pour l'entier k :

Algorithme 8.3.1.

Entrée:

- un entier $d > 1$ non divisible par 8,
- un entier k.

Sortie:

- renvoie *vrai* si la base du type voulu existe.

Algorithme:

1. $p \leftarrow kd+1$.
2. Si p n'est pas premier, renvoyer *faux*.
3. Calculer l'ordre n de 2 dans $\mathbf{F}_p$.
4. $h \leftarrow kd/n$.
5. $u = \mathrm{pgcd}(h, n)$.
6. Si $u = 1$, renvoyer *vrai*.

L'algorithme suivant permet de calculer le produit pour une base normale gaussienne. On se donne deux éléments

$$a_0\theta + \cdots + a_{d-1}\theta^{2^{d-1}} \quad \text{et} \quad b_0\theta + \cdots + b_{d-1}\theta^{2^{d-1}}$$

et on cherche à déterminer le produit $c_0\theta + \cdots + c_{d-1}\theta^{2^{d-1}}$. Par la remarque du paragraphe précédent, il suffit essentiellement d'écrire la formule pour c_0.

Algorithme 8.3.2.

Entrée:

- Un entier $d > 1$ non divisible par 8,
- Un entier k pour lequel il existe une base normale gaussienne.

Sortie:

- Expression pour c_0.

Algorithme:

1. $p \leftarrow\ kd + 1$.
2. Trouver à l'aide d'une méthode aléatoire un entier u d'ordre k dans $\mathbf{F}_p^\times$.
3. Calculer la suite $F(1),\ldots,F(p-1)$ de la façon suivante.
   3.1. $w \leftarrow 1$.
   3.2. Pour i variant de 0 à $k-1$,
      3.2.1. $n \leftarrow w$.
      3.2.2. Pour j variant de 0 à $d-1$,
         3.2.2.1. $F(n) \leftarrow i$.
         3.2.2.2. $n \leftarrow 2n$ modulo p.
      3.2.3. $w \leftarrow uw$ modulo p.
4. Si k est pair, alors $J = 0$, sinon
$$J = \sum_{i=1}^{d/2} a_{i-1}b_{d/2+i-1} + a_{d/2+i-1}b_{i-1}.$$
5. c_0 est donné par la formule :
$$c_0 = J + \sum_{i=1}^{p-2} a_{F(i+1)}b_{F(p-i)}.$$

Enfin pour obtenir le produit, on procède par permutations circulaires.

EXERCICES

8.1. On considère le corps $\mathbf{F}_{16}$.

1. Montrer qu'il existe une base normale gaussienne avec $k = 3$.
2. Ecrire les formules explicites de l'addition, du carré et du produit pour cette base.

8.2. Ecrire dans le langage de votre choix un programme qui réalise les algorithmes du paragraphe 8.3.

PARTIE II

COURBES ELLIPTIQUES

CHAPITRE 9

L'ESPACE PROJECTIF

9.1. Définitions

Définition 9.1.1. — Soit $\mathbf{K}$ un corps commutatif, et $n \in N$, un entier. L'*espace projectif* de dimension n sur $\mathbf{K}$ noté $\mathbf{P}^n(\mathbf{K})$ est défini par

$$\mathbf{P}^n(\mathbf{K}) = \{\, D \mid D \text{ droite vectorielle de } \mathbf{K}^{n+1} \,\}.$$

En associant à un élément x non nul de K^{n+1} la droite engendrée par cet élément, on définit une projection canonique

$$\begin{array}{rcl} \pi : \mathbf{K}^{n+1} - \{0\} & \to & \mathbf{P}^n(\mathbf{K}) \\ x & \mapsto & \mathbf{K}x. \end{array}$$

Deux vecteurs x et y ont la même image par π si et seulement s'ils appartiennent à la même droite, c'est à dire si et seulement s'ils sont colinéaires. On peut donc décrire également l'espace projectif comme un quotient

$$(\mathbf{K}^{n+1} - \{0\})/\sim \ \xrightarrow{\sim}\ \mathbf{P}^n(\mathbf{K})$$

où $\sim$ est la relation d'équivalence définie par

$$\forall x, y \in \mathbf{K}^{n+1} - \{0\}, \quad x \sim y \Leftrightarrow (\exists \lambda \in \mathbf{K}^\times, x = \lambda y).$$

On note $(x_0 : x_1 : \ldots : x_n)$ l'image par π de $(x_0, \ldots, x_n) \in \mathbf{K}^{n+1}$. Si $\boldsymbol{x} = (x_0 : \ldots : x_n)$, on dit que $(x_0, \ldots, x_n)$ sont des *coordonnées homogènes* pour $\boldsymbol{x}$. Notons que les coordonnées homogènes ne sont pas uniques : on a l'equivalence

$$(x_0 : \ldots : x_n) = (y_0 : \ldots : y_n) \Leftrightarrow (\exists \lambda \in \mathbf{K}^\times, \forall i \in \{0, \ldots, n\}, y_i = \lambda x_i).$$

Plus généralement, si E est un $\mathbf{K}$-espace vectoriel, l'espace projectif associé à E, noté $\mathbf{P}(E)$, est l'ensemble des droites vectorielles de E. La dimension de cet espace projectif est définie comme $\dim(E) - 1$. Si F est un sous-espace vectoriel de E on a une inclusion

$$\mathbf{P}(F) \subset \mathbf{P}(E).$$

Un sous-espace projectif est un sous-ensemble P de $\mathbf{P}(E)$ tel qu'il existe un sous-espace vectoriel F de E de sorte que $P = \mathbf{P}(F)$ Si F est de dimension 2, alors on parle de *droite projective*. Si F est un hyperplan de E, alors $\mathbf{P}(F)$ est appelé un *hyperplan* de $\mathbf{P}(E)$.

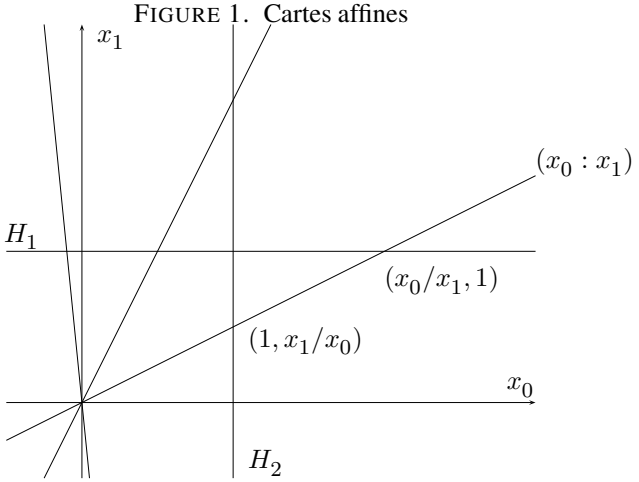
9.2. Cartes affines

Si $n \in \mathbf{N}$, notons $x_0, \ldots, x_n$ les coordonnées sur $\mathbf{K}^{n+1}$. Si $0 \leqslant i \leqslant n$, on considère l'hyperplan affine H_i d'équation $x_i = 1$. La restriction de π à H_i définit une application injective de $H_i \to \mathbf{P}^n(\mathbf{K})$. De façon géométrique, on associe à tout point de l'hyperplan la droite passant par ce point. L'image, qu'on notera U_i est donc formée des droites qui rencontrent H_i, c'est-à-dire des droites vectorielles non parallèles à H_i. On obtient donc que $U_i = \mathbf{P}^n(\mathbf{K}) - \mathbf{P}(E_i)$ où E_i est l'hyperplan vectoriel d'équation $T_i = 0$. En termes de coordonnées on obtient une bijection

$$\begin{array}{rcl} H_i & \to & \{\, (x_0 : \ldots : x_n) \in \mathbf{P}^n(\mathbf{K}) \mid x_i \neq 0 \,\} \\ (x_0, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) & \mapsto & (x_0 : \ldots : x_{i-1} : 1 : x_{i+1} : \ldots : x_n) \\ \left(\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}\right) & \leftarrow\!\shortmid & (x_0 : \ldots : x_n). \end{array}$$

Notons que $\mathbf{P}^n(\mathbf{K})$ est la réunion des U_i pour $1 \leqslant i \leqslant n$.

FIGURE 1. Cartes affines



On peut également voir l'espace projectif $\mathbf{P}^n(\mathbf{K})$ comme la réunion disjointe de U_0 et de $\mathbf{P}^n(E_0)$, où U_0 est identifié avec $\mathbf{K}^n$ via la bijection

$$\begin{array}{rcl} \mathbf{K}^n & \to & U_0 \\ (x_1, \ldots, x_n) & \mapsto & (1 : x_1 : \ldots : x_n). \end{array}$$

On dit alors que $\mathbf{P}(E_0)$ est *l'hyperplan à l'infini*. On peut identifier $\mathbf{P}(E_0)$ avec l'ensemble des directions des droites affines de $\mathbf{K}^n$.

Exemple 9.2.1. — En particulier en dimension 1, Le complémentaire de U_0 est le point $(0 : 1)$ appelé *point à l'infini* et noté ∞. Ensemblistement on a donc

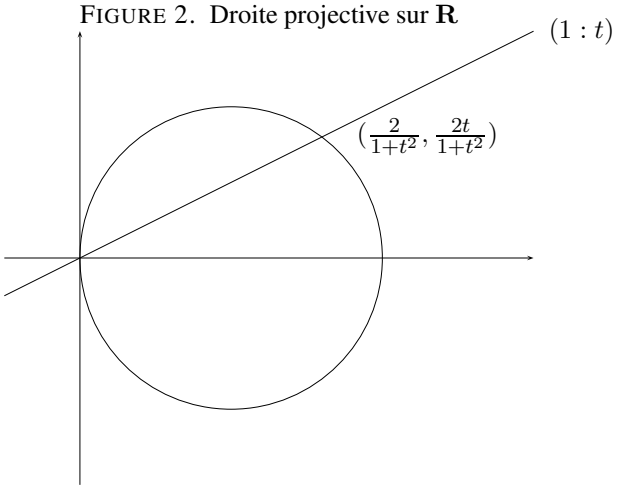
$$\mathbf{P}^1(\mathbf{K}) = \mathbf{K} \cup \{\infty\}.$$

Dans le cas où $\mathbf{K} = \mathbf{R}$, on obtient une bijection

$$\begin{array}{rcl} \mathbf{S}^1_{\mathbf{R}} & \to & \mathbf{P}^1(\mathbf{R}) \\ (x,y) & \mapsto & \begin{cases} (x+1:y) & \text{si } (x,y) \neq (-1,0), \\ (0:1) & \text{sinon.} \end{cases} \end{array}$$

où $\mathbf{S}^1_{\mathbf{R}} = \{(x,y) \in \mathbf{R}^2 \mid x^2+y^2 = 1\}$. Géométriquement, cela revient à considérer le cercle de centre $(1,0)$ et de rayon 1 et d'associer à chaque point de cercle distinct de $(0,0)$ la droite passant par ce point et à $(0,0)$ la droite tangente au cercle en ce point. On peut également

FIGURE 2. Droite projective sur $\mathbf{R}$



définir une bijection

$$\begin{array}{rcl} \mathbf{S}^2_{\mathbf{R}} & \to & \mathbf{P}^1(\mathbf{C}) \\ (x,y,z) & \mapsto & \begin{cases} (z+1:x+iy) & \text{si } (x,y,z) \neq (-1,0,0), \\ (0:1) & \text{sinon.} \end{cases} \end{array}$$

La droite projective complexe peut donc être vu comme une sphère réelle.

9.3. Sous-ensembles algébriques

Définition 9.3.1. — Dans la suite de ce chapitre, on note $\mathbf{K}$ un corps et $\overline{\mathbf{K}}$ une clôture algébrique de $\mathbf{K}$. Si $n \in \mathbf{N}$, on appelle *sous-ensemble algébrique* de $\overline{\mathbf{K}}^n$, toute partie X de $\overline{\mathbf{K}}^n$ telle qu'il existe une famille de polynômes $(P_i)_{i\in I}$ avec

$$P_i \in \overline{\mathbf{K}}[T_1, \ldots, T_n]$$

telle que

$$X = \{\, (x_1, \ldots, x_n) \in \overline{\mathbf{K}}^n \mid \forall i \in I,\ P_i(x_1, \ldots, x_n) = 0 \,\}.$$

On dit que X est défini sur $\mathbf{K}$ s'il existe une famille de polynômes $(P_i)_{i\in I}$ avec

$$P_i \in \mathbf{K}[T_1, \ldots, T_n]$$

telle que

$$X = \{\, (x_1, \ldots, x_n) \in \overline{\mathbf{K}}^n \mid \forall i \in I,\ P_i(x_1, \ldots, x_n) = 0 \,\}.$$

Si X est un sous-ensemble algébrique de $\overline{\mathbf{K}}^n$ défini sur $\mathbf{K}$, on définit

$$\begin{aligned} X(\mathbf{K}) &= \mathbf{K}^n \cap X \\ &= \{\, (x_1, \ldots, x_n) \in \mathbf{K}^n \mid \forall i \in I,\ P_i(x_1, \ldots, x_n) = 0 \,\}. \end{aligned}$$

Un élément de $X(\mathbf{K})$ est appelé un *point rationnel* de X.

Exemple 9.3.2. — En prenant $I = \emptyset$, on obtient que $\overline{\mathbf{K}}^n$ est un sous ensemble algébrique de $\overline{\mathbf{K}}^n$. En prenant un unique polynôme P constant égal à un, on voit qu'il en est de même de l'ensemble vide.

Remarque 9.3.3. — Si $\mathbf{K}$ est un corps fini de cardinal q et $\boldsymbol{x} = (x_1, \ldots, x_n)$ un élément de $\mathbf{K}^n$, alors le polynôme

$$P_{\boldsymbol{x}}(T_1, \ldots, T_n) = 1 - \prod_{i=1}^{n} (1 - (T_i - x_i)^{q-1})$$

vérifie

$$\forall \boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbf{K}^n, \quad P_{\boldsymbol{x}}(y_1, \ldots, y_n) = \begin{cases} 0 & \text{si } \boldsymbol{y} = \boldsymbol{x}, \\ 1 & \text{sinon.} \end{cases}$$

En conséquence, si X est une partie arbitraire de $\mathbf{K}^n$ le polynôme $Q_X = \prod_{\boldsymbol{x} \in X} P_{\boldsymbol{x}}$ vérifie

$$\forall \boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbf{K}^n, \quad Q_X(y_1, \ldots, y_n) = \begin{cases} 0 & \text{si } \boldsymbol{y} \in X, \\ 1 & \text{sinon.} \end{cases}$$

Toute partie X de $\mathbf{K}^n$ se décrit donc comme l'ensemble des solutions d'une équation polynômiale. Cela est faux dès que le corps $\mathbf{K}$ est infini. C'est une des raisons pour lesquelles il convient de se placer sur un corps algébriquement clos pour définir un sous-ensemble algébrique.

Remarque 9.3.4. — Si F est un polynôme homogène de $\mathbf{K}[T_0, \ldots, T_n]$, alors on a

$$\forall (x_0, \ldots, x_n) \in \mathbf{K}^{n+1}, \quad \forall \lambda \in \mathbf{K}, \quad P(x_0, \ldots, x_n) = 0 \Rightarrow P(\lambda x_0, \ldots, \lambda x_n) = 0.$$

Autrement dit, le sous-ensemble algébrique défini par l'annulation de P est un cône de sommet l'origine, c'est-à-dire une réunion de droites vectorielles. Il est alors naturel de considérer la partie de $\mathbf{P}^n(\overline{\mathbf{K}})$ ainsi définie

Définition 9.3.5. — Si $n \in \mathbf{N}$, on appelle *sous-ensemble algébrique* de $\mathbf{P}^n(\overline{\mathbf{K}})$ toute partie X telle qu'il existe une famille $(P_i)_{i \in I}$ de polynômes homogènes de $\overline{\mathbf{K}}[T_0, \ldots, T_n]$ tels que

$$X = \{\, (x_0 : \ldots : x_n) \in \mathbf{P}^n(\overline{\mathbf{K}}) \mid \forall i \in I,\ P_i(x_0, \ldots, x_n) = 0 \,\}.$$

On dit que X est défini sur $\mathbf{K}$ s'il existe une famille de polynômes homogènes $(P_i)_{i \in I}$ avec

$$P_i \in \mathbf{K}[T_0, \ldots, T_n]$$

telle que

$$X = \{\, (x_0 : \ldots : x_n) \in \mathbf{P}^n(\overline{\mathbf{K}}) \mid \forall i \in I,\ P_i(x_0, \ldots, x_n) = 0 \,\}.$$

Si X est un sous ensemble algébrique de $\overline{\mathbf{K}}$ défini sur $\mathbf{K}$, on définit

$$\begin{aligned} X(\mathbf{K}) &= \mathbf{P}^n(\mathbf{K}) \cap X \\ &= \{\, (x_0 : \ldots : x_n) \in \mathbf{P}^n(\mathbf{K}) \mid \forall i \in I,\ P_i(x_0, \ldots, x_n) = 0 \,\}. \end{aligned}$$

Un élément de $X(\mathbf{K})$ est appelé un *point rationnel* de X.

9.4. *Topologie de Zariski*

***Définition* 9.4.1**. — Une *Topologie* sur un ensemble X est un ensemble $\mathscr{U}$ de partie de X vérifiant les conditions suivantes

O1. $\emptyset \in \mathscr{U}$ et $X \in \mathscr{U}$,
O2. $\forall U, V \in \mathscr{U}, \quad U \cap V \in \mathscr{U}$,
O3. Pour toute famille $(U_i)_{i\in I} \in \mathscr{U}^I$, $\bigcup_{i\in I} U_i \in \mathscr{U}$.

Un élément de $\mathscr{U}$ est appelé un *ouvert* de la topologie et on dit qu'une partie F de X est *fermée* si et seulement si $X - F \in \mathscr{U}$. L'ensemble X muni d'une topologie est appelé espace topologique.

***Exemple* 9.4.2**. — La notion usuelle d'ouvert de $\mathbf{R}^n$ défini comme une partie U de $\mathbf{R}^n$ telle que

$$\forall \boldsymbol{x} = (x_1, \ldots, x_n) \in U, \quad \exists r > 0, \quad \forall \boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbf{R}^n, \quad \sum_{i=1}^{n} (x_i - y_i)^2 < r \Rightarrow \boldsymbol{y} \in U$$

munit $\mathbf{R}^n$ d'une structure d'espace topologique.

***Proposition* 9.4.3**. — *Les sous-ensembles algébriques de $\mathbf{P}^n(\overline{\mathbf{K}})$ (resp. $\overline{\mathbf{K}}^n$) vérifient les conditions suivantes :*

(i) *$\emptyset$ et $\mathbf{P}^n(\overline{\mathbf{K}})$ (resp. $\overline{\mathbf{K}}^n$) sont des sous-ensembles algébriques,*
(ii) *Si F et F' sont des sous-ensembles algébriques, il en est de même de $F \cup F'$,*
(iii) *Si $(F_i)_{i\in I}$ est une famille de sous-ensembles algébriques, alors $\bigcap_{i\in I} F_i$ est également un sous-ensemble algébrique.*

Ces propriétés assurent que les sous-ensembles algébriques de $\mathbf{P}^n(\overline{\mathbf{K}})$ (resp. $\overline{\mathbf{K}}^n$) sont les fermés d'une topologie sur $\mathbf{P}^n(\overline{\mathbf{K}})$ (resp. $\overline{\mathbf{K}}^n$). Cette topologie est appelée topologie de Zariski.

Démonstration. — Nous avons déja vu la première assertion.

Pour (ii), soit $(P_i)_{i\in I}$ est une famille d'équations pour F et $(Q_j)_{j\in J}$ une famille d'équations pour F'. Tout polynôme de la famille $(P_iQ_j)_{(i,j)\in I\times J}$ s'annule sur $F \cup F'$. D'un autre coté si x n'appartient pas à $F \cup F'$, il existe $i \in I$ tel que P_i ne s'annule pas en x et $j \in J$ tel que Q_j ne s'annule pas en x. Le produit P_iQ_j ne s'annule donc pas en x. Donc $F \cup F'$ est le sous-ensemble algébrique défini par la famille $(P_iQ_j)_{(i,j)\in I\times J}$.

En ce qui concerne (iii), soit $(P_j)_{j\in J_i}$ une famille de polynômes définissant F_i. Alors la concaténation des familles de polynômes $(P_j)_{j\in \cup_{i\in I} J_i}$ définit le sous-ensemble algébrique $\cap_{i\in I} F_i$. □

9.5. Equations homogènes et inhomogènes

Si X est un sous-ensemble algébrique de $\overline{\mathbf{K}}^n$ vu comme partie de $\mathbf{P}^n(\overline{\mathbf{K}})$, on souhaite trouver un sous-ensemble algébrique Y de $\mathbf{P}^n(\overline{\mathbf{K}})$ aussi petit que possible de sorte que X coïncide avec l'intersection $Y \cap \overline{\mathbf{K}}^n$. En termes imagés, on souhaite trouver « les points à l'infini de X ».

Remarque 9.5.1. — Si X est un sous-ensemble algébrique de $\mathbf{P}^n(\overline{\mathbf{K}})$ définit par des polynômes $(P_i)_{i\in I}$, alors $X \cap U_0$, vu comme partie de $\mathbf{K}^n$ est défini par les équations

$$P_i(1, T_1, \ldots, T_n) = 0$$

où i décrit l'ensemble I.

Notation 9.5.2. — Si $P \in \mathbf{K}[T_1, \ldots, T_n] - \{0\}$ est un polynôme non nul de degré total d s'écrivant

$$P = \sum_{\boldsymbol{\alpha}\in\mathbf{N}^n} a_{\boldsymbol{\alpha}} T^{\boldsymbol{\alpha}}.$$

On note $\widetilde{P}$ le polynôme homgène de degré d défini par

$$\widetilde{P} = \sum_{\boldsymbol{\alpha}\in\mathbf{N}^n} a_{\boldsymbol{\alpha}} T^{\boldsymbol{\alpha}} T_0^{d-|\boldsymbol{\alpha}|}$$

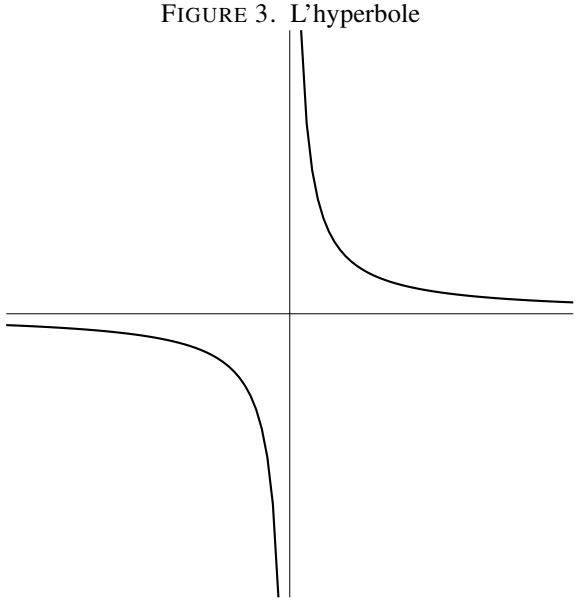
On pose également $\widetilde{0} = 0$.

Définition 9.5.3. — Si X est un sous-ensemble algébrique de $\overline{\mathbf{K}}^n$, défini par une famille $(P_i)_{i\in I}$ de polynômes de $\mathbf{K}[T_1, \ldots, T_n]$, on appelle adhérence de X et on note $\widetilde{X}$ le sous-ensemble algébrique de $\mathbf{P}^n(\overline{\mathbf{K}})$ défini par la famille de polynômes homogènes $(\widetilde{P}_i)_{i\in I}$.

***Remarque* 9.5.4**. — Il s'agit effectivement de l'adhérence de $X \subset \mathbf{P}^n(\overline{\mathbf{K}})$ pour la topologie de Zariski vue au paragraphe 9.4, l'adhérence d'une partie X d'un espace topologique de Y étant définie comme l'intersection des fermés de Y contenant X.

Exemple 9.5.5. — Considérons l'hyperbole affine d'équation $xy = 1$ (cf. figure 3). On

FIGURE 3. L'hyperbole



pose donc $P = XY - 1$. Le polynôme homogène en trois variables correspondant s'écrit $\widetilde{P} = XY - T^2$ Les points rajoutés sont ceux sur la droite projective d'équation $T = 0$ il s'agit donc de $(0 : 1 : 0)$ et de $(1 : 0 : 0)$. D'un point de vue géométrique, ils correspondent aux deux asymptotes de l'hyperbole.

Remarque 9.5.6. — De manière plus générale, les points à l'infini rajoutés à une courbe affine réelle définie par une équation polynômiale en deux variables peuvent être décrit comme les directions asymptotiques des branches infinies de la courbe (autrement dit si P_0 est un point fixée du plan on considère la limite de la direction de la droite P_0P lorsque la distance de P à P_0 tend vers l'infini, P restant sur la branche infinie considérée de la courbe).

9.6. Morphismes

Définition 9.6.1. — Soient E et F deux sous-ensembles algébriques de $\mathbf{P}^m(\overline{\mathbf{K}})$ et $\mathbf{P}^n(\overline{\mathbf{K}})$ respectivement. Un morphisme $\phi : E \to F$ est une application de E vers F telle que pour tout élément $\boldsymbol{x}$ de E, il existe un sous-ensemble algébrique $S_{\boldsymbol{x}}$ et une famille de $n+1$ polynômes homogènes $P_{\boldsymbol{x},0}, \ldots, P_{\boldsymbol{x},n}$ de $\overline{\mathbf{K}}[T_0, \ldots, T_m]$, de même degré d tels que $\boldsymbol{x} \notin S_{\boldsymbol{x}}$ et

$$\forall \boldsymbol{y} = (y_0 : \ldots : y_m) \in E - S_{\boldsymbol{x}},$$
$$\phi(y_0 : \ldots : y_m) = (P_{\boldsymbol{x},0}(y_0, \ldots, y_m) : \ldots : P_{\boldsymbol{x},n}(y_0, \ldots, y_m)).$$

On dit que ce morphisme est défini sur $\mathbf{K}$ si et seulement si les polynômes peuvent être choisis dans $\mathbf{K}[T_0, \ldots, T_m]$. Un isomorphisme est un morphisme bijectif.

Remarque 9.6.2. — Les polynômes homogènes $P_{\boldsymbol{x},0}, \ldots, P_{\boldsymbol{x},m}$ étant de même dégré d, le point

$$(P_{\boldsymbol{x},0}(y_0, \ldots, y_m) : \ldots : P_{\boldsymbol{x},n}(y_0, \ldots, y_m))$$

de $\mathbf{P}^n(\overline{\mathbf{K}})$ ne dépend pas du choix des coordonnées homogènes de $\boldsymbol{y}$.

Exemple 9.6.3. — On appelle *homographie* de $\mathbf{P}^n(\overline{\mathbf{K}})$ toute application

$$\overline{f} : \mathbf{P}^n(\overline{\mathbf{K}}) \to \mathbf{P}^n(\overline{\mathbf{K}})$$

telle qu'il existe une application linéaire bijective $f : \overline{\mathbf{K}}^{n+1} \to \overline{\mathbf{K}}^{n+1}$ de sorte que le diagramme

$$\begin{array}{ccc} \overline{\mathbf{K}}^{n+1} & \xrightarrow{f} & \overline{\mathbf{K}}^{n+1} \\ \pi \downarrow & & \pi \downarrow \\ \mathbf{P}^n(\overline{\mathbf{K}}) & \xrightarrow{\overline{f}} & \mathbf{P}^n(\overline{\mathbf{K}}) \end{array}$$

commute (i.e. $\pi \circ f = \overline{f} \circ \pi$). Toute homographie est un isomorphisme de $\mathbf{P}^n(\overline{\mathbf{K}})$ vers $\mathbf{P}^n(\overline{\mathbf{K}})$. Si $\overline{f}$ est une homographie et X un sous-ensemble algébrique de $\mathbf{P}^n(\overline{\mathbf{K}})$ alors $\overline{f}$ induit par restriction un isomorphisme de X vers $\overline{f}(X)$.

Exemple 9.6.4. — On suppose la caractéristique de $\mathbf{K}$ différente de deux. Soit C le sous-ensemble algébrique de $\mathbf{P}^2(\overline{\mathbf{K}})$ défini par l'équation $X^2+Y^2=T^2$. Alors C est isomorphe à la droite projective $\mathbf{P}^1(\overline{\mathbf{K}})$ via l'application

$$\begin{array}{rcl}\phi : \mathbf{P}^1(\overline{\mathbf{K}}) & \to & C \\ (x:y) & \mapsto & (x^2-y^2 : 2xy : x^2+y^2).\end{array}$$

La réciproque est donnée par

$$\begin{array}{rcl}\phi^{-1} : C & \to & \mathbf{P}^1(\overline{\mathbf{K}}) \\ (x:y:t) & \mapsto & \begin{cases}(x+t:y) & \text{si } (x:y:t)\neq(-1:0:1) \\ (-y:x-t) & \text{si } (x:y:t)\neq(1:0:1)\end{cases}\end{array}$$

En effet si $(x:y:t)\neq(-1:0:1)$ et $(x:y:t)\neq(1:0:1)$, la relation $x^2-t^2=-y^2$ implique que $(x+t:y)=(-y:x-t)$. On constate donc que pour définir l'inverse ϕ^{-1} comme un morphisme, on a besoin de deux familles de polynômes homogènes.

On utilisera également la notion, plus simple à définir, d'application rationnelle :

Définition 9.6.5. — Soient X et Y deux sous-ensembles algébriques de $\mathbf{P}^m(\overline{\mathbf{K}})$ et $\mathbf{P}^n(\overline{\mathbf{K}})$ respectivement. Une application rationnelle $\psi : X \dashrightarrow Y$ est la donnée d'une application $\psi : X - Z \to Y$, où Z est un sous-ensemble algébrique de $\mathbf{P}^m(\overline{\mathbf{K}})$ vérifiant $Z \subsetneq X$ telle qu'il existe une famille de $n+1$ polynômes homogènes $P_0,\dots,P_n$ de $\overline{\mathbf{K}}[T_0,\dots,T_m]$, de même degré d tels que pour tout $\boldsymbol{y}=(y_0:\dots:y_m)\in X-Z$,

$$\psi(y_0:\dots:y_m)=(P_0(y_0,\dots,y_m):\dots:P_n(y_0,\dots,y_m)).$$

EXERCICES

9.1. Montrer qu'on a une bijection de $\mathbf{S}^n_{\mathbf{R}}/\sim \to \mathbf{P}^n(\mathbf{R})$ où $\sim$ est la relation

$$\boldsymbol{x}=\boldsymbol{y} \quad \text{ou} \quad \boldsymbol{x}=-\boldsymbol{y}.$$

CHAPITRE 10

COURBES

10.1. Courbe plane

Dans la suite on s'intéressera surtout au cas des courbes planes

Définition 10.1.1. — Si $\mathbf{K}$ est corps, $\overline{\mathbf{K}}$ une clôture algébrique de $\mathbf{K}$, on appelle *courbe plane* un sous-ensemble algébrique C de $\mathbf{P}^2(\overline{\mathbf{K}})$ défini par un polynôme homogène non constant de $\mathbf{K}[T_0, T_1, T_2]$.

Remarque 10.1.2. — Soit C une courbe définie par un polynôme $P \in \mathbf{K}[T_0, T_1, T_2]$ et soit $P = \prod_{i=1}^{n} P_i^{m_i}$ une décomposition de P. On considérant les termes de plus bas degré de chaque P_i, on vérifie que chaque P_i est également homogène. Alors C est la réunion des courbes C_i définies par l'annulation de P_i. En particulier, on peut supposer que P est sans facteur carré.

10.2. La lissité dans le cadre analytique

Sur le corps $\mathbf{R}$ des réels, on dispose du théorème des fonctions implicites :

Théorème 10.2.1. — *Soit W un ouvert de $\mathbf{R}^2$ et $f : W \to \mathbf{R}$ une fonction de classe $\mathscr{C}^1$ sur W (c'est à dire différentiable, de différentielle continue sur W). Soit $(x_1, x_2) \in \mathbf{R}^2$ un point de W tel que $f(x_1, x_2) = 0$ et $df_{(x_1,x_2)} \neq 0$. Alors il existe un intervalle I de $\mathbf{R}$, un ouvert U de W contenant (x_1, x_2) et un entier $i \in \{1, 2\}$ de sorte que l'application*

$$\begin{array}{rcl} \{(y_1, y_2) \in U \mid f(x_1, x_2) = 0\} & \to & \mathbf{R} \\ (y_1, y_2) & \mapsto & y_i \end{array}$$

définisse une bijection de $\{(y_1, y_2) \in U \mid f(x_1, x_2) = 0\}$ sur I dont la réciproque est de classe $\mathscr{C}^1$.

Remarque 10.2.2. — On peut donc dire qu'en tout point en lequel la différentielle est non nulle, la courbe définie par $f(y_1, y_2) = 0$ ressemble localement à un intervalle. Inversement considérons la courbe d'équation

$$((X-2)^2 + Y^2 - 1)((X+2)^2 + Y^2 - 1) = 9$$

(cf. la figure 2). En le point $(0, 0)$, la différentielle est nulle.

FIGURE 1. Une courbe lisse

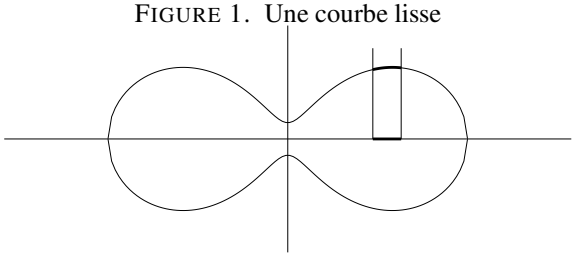
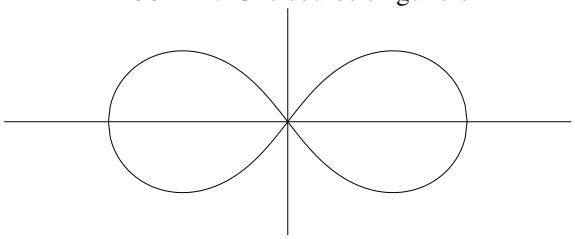


FIGURE 2. Une courbe singulière



10.3. Courbe non-singulière

Définition 10.3.1. — Soit C une courbe plane définie par un polynôme homogène P sans facteur carré, alors un point $\boldsymbol{x} = (x_0 : x_1 : x_2)$ de C est dit *singulier* si et seulement si

$$\frac{\partial P}{\partial X_i}(x_0, x_1, x_2) = 0 \quad \text{pour tout} \quad i \in \{1, 2, 3\}.$$

Le point x est dit *non-singulier* s'il n'est pas singulier. La courbe C est dite *non-singulière* si et seulement si tout point x de C est non-singulier.

10.4. Équivalence birationnelle entre courbes

Définition 10.4.1. — Soient C et C' deux courbes planes dans $\mathbf{P}^2(\overline{\mathbf{K}})$. Une équivalence birationnelle esr la donnée de parties finies $S \subset C$ et $S' \subset C'$ et d'une bijection

$$\phi : C - S \to C' - S'$$

telles qu'il existe des polynômes homogènes P_1, P_2 et P_3 de $\mathbf{K}[X, Y, T]$ de même degré d tels que pour tout $(x_1 : x_2 : x_3)$ de $C - S$,

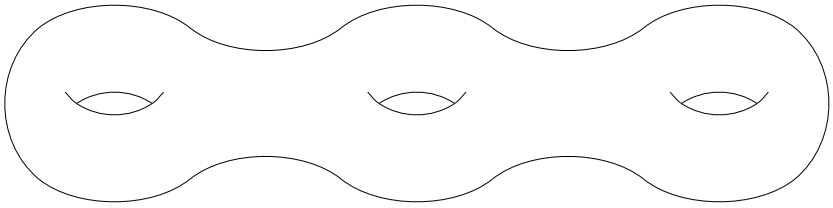
$$\phi(x_1 : x_2 : x_3) = (P_1(x_1, x_2, x_3) : P_2(x_1, x_2, x_3) : P_3(x_1, x_2, x_3)).$$

10.5. Notion de genre

Si C est une courbe non-singulière définie sur le corps des nombres complexes $\mathbf{C}$, alors en utilisant un analogue du théorème 10.2.1 sur le corps des complexes, tout point de C a un voisinage ouvert difféomorphe à un ouvert de $\mathbf{C}$. La courbe complexe C peut dont

être vue comme une surface réelle. Or les surfaces lisses orientées réelles sont classifiées à difféomorphisme près par leur genre. D'une façon imagée le genre est le nombre de « trous de la surface » (cf. la figure 3 pour une surface réelle de genre trois).

FIGURE 3. Tore à 3 trous

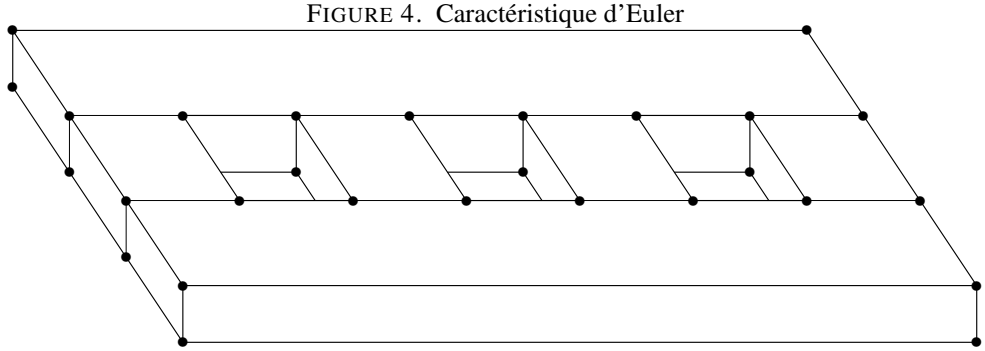


Pour déterminer le genre g d'une surface une possibilité est de recouvrir cette surface par des polygônes convexes (par exemple des triangles) et de compter le nombre s de sommets, a d'arêtes et f de faces de la figure. On a alors la relation

$$f - a + s = 2 - 2g.$$

Le nombre $f - a + s$ s'apelle caractéristique d'Euler de la surface. On peut vérifier cette formule pour le genre 3 sur la figure 4. On a effectivement $f = 32$, $a = 76$ et $s = 40$ donc $f - a + s = -4$ On

FIGURE 4. Caractéristique d'Euler



peut montrer le théorème suivant :

Théorème 10.5.1. — *Soit C une courbe non-singulière définie sur le corps des complexes $\mathbf{C}$ par un polynôme P irréductible et de degré d alors le genre de la courbe est donné par*

$$g(C) = \frac{(d-1)(d-2)}{2}.$$

Nous admettrons qu'il est possible de définir sur tout corps K le *genre* d'une courbe C de sorte que

Théorème 10.5.2. — *Soit C une courbe non-singulière définie sur un corps $\mathbf{K}$ par un polynôme P irréductible et de degré d alors le genre de la courbe C est donné par*

$$g(C) = \frac{(d-1)(d-2)}{2}.$$

La démonstration de ces résultats sortirait du cadre de ce texte.

Exemple 10.5.3. — Si C est une droite projective, alors d vaut 1 et $g(C) = 0$.

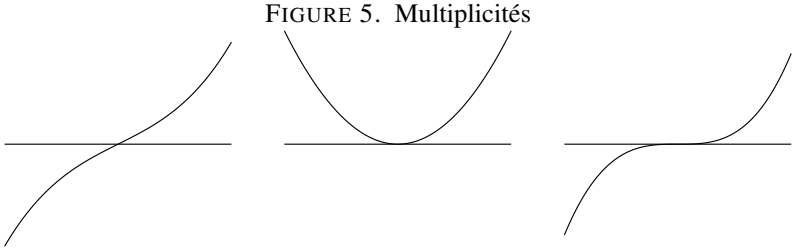
10.6. Multiplicités d'intersection

Définition 10.6.1. — Soit C une courbe plane définie par un polynôme P irréductible homogène de degré d, L une droite projective de $\mathbf{P}^2(\overline{\mathbf{K}})$ non contenue dans C et x un point de L. Quitte à faire un changement de coordonnées, on peut supposer que L est la droite à l'infini d'équation $T_0 = 0$ et que x est le point $(0 : 0 : 1)$. On appelle alors *multiplicité d'intersection* de L et de C en x l'ordre de 0 comme racine du polynôme $Q(T) = P(0, T, 1)$ en $T = 0$. On notera ici $m_x(L \cap C)$ cette multiplicité.

Exemple 10.6.2. — Considérons la courbe affine d'équation $Y = X^n$ correspondant à la courbe projective C d'équation $YT^{n-1} = X^n$. La multiplicité de l'intersection de C avec la droite $Y = 0$ en $(0, 0)$ est donné par l'ordre de 0 comme racine de X^n, c'est-à-dire n.

Remarque 10.6.3. — Les multiplicités d'intersection sur $\mathbf{R}$ ont également une interprétation géométrique. Ainsi la courbe est tangente à la droite en le point x si la multiplicité est supérieure ou égale à 2, la droite est osculatrice si la multiplicité est supérieure à trois (cf. la figure 5).

FIGURE 5. Multiplicités



1 : droite sécante 2 : droite tangente 3 : droite osculatrice

Remarque 10.6.4. — Si x est un point singulier de C et L une droite arbitraire passant par L, alors la multiplicité de l'intersection de L avec C en x est supérieure ou égale à 2. En effet, le fait que les dérivées partielles s'annulent en x entraîne que le polynôme Q défini ci-dessus vérifie $Q(0) = 0$ et $Q'(0) = 0$ par la propriété 3.7.7. L'ordre de la racine 0 est donc supérieure ou égale à deux.

Proposition 10.6.5. — *Soient C une courbe plane définie par un polynôme P irréductible homogène de degré d et L un droite projective de $\mathbf{P}^2(\overline{\mathbf{K}})$ non contenue dans C. Alors le nombre de points de L en lesquels la multiplicité d'intersection est non nulle est fini et*

$$\sum_{x\in L} m_x(L\cap C) = d.$$

Démonstration. — Quitte à faire un changement de coordonnées, on peut supposer que la droite L est d'équation $T_0 = 0$. La restriction de P à L est donc un polynôme $Q(T_1, T_2) = P(0, T_1, T_2)$, homogène de degré d. Ce polynôme est non nul puisque L n'est pas contenue dans C. On peut donc l'écrire $Q(T_1, T_2) = T_2^r R(T_1, T_2)$ où R est un polynôme homogène de degré $d - r$ tel que $R(1, 0) \neq 0$. Autrement dit,

$$R(T_1, T_2) = a_{r-d}T_1^{r-d} + \cdots + a_0 T_2^{r-d},$$

avec $a_{r-d} \neq 0$. Alors, r est la multiplicité d'intersection de L avec C en le point $(0 : 1 : 0)$ et pour tout $\boldsymbol{x} = (0 : x : 1)$ de $L - \{(0 : 1 : 0)\}$, $m_{\boldsymbol{x}}(L \cap C)$ est l'ordre de x comme racine du polynôme $R(T, 1)$. L'assertion de la proposition résulte alors du fait que ce polynôme, de degré $d - r$, est scindé sur le corps algébriquement clos $\overline{\mathbf{K}}$. □

Définition 10.6.6. — Si $m_1, \ldots, m_r \in L$ on dira que $m_1, \ldots, m_r$ sont des points d'intersection de C avec L comptés avec multiplicités si et seulement si

$$\forall x \in L, \quad \sharp\{i \mid m_i = x\} \leqslant m_x(L \cap C)$$

Si $r = d$, alors on dira que $m_1, \ldots, m_d$ sont les points d'intersection de C avec L comptés avec multiplicités.

Proposition 10.6.7. — *Soient C une courbe plane définie par un polynôme P homogène de degré d irréductible et L un droite projective de $\mathbf{P}^2(\overline{\mathbf{K}})$ non contenue dans C. Si $m_1, \ldots, m_{d-1}, m_d$ sont les points d'intersection de C avec L, alors*

(i) *Si les points m_1,…,m_{d-1} sont des points non-singuliers de C, alors il en est de même de m_d.*

(ii) *Si C et L sont définies sur $\mathbf{K}$ et si les points m_1,…,m_{d-1} sont définis sur $\mathbf{K}$, alors il en est de même de m_d.*

Démonstration. — La première assertion résulte du fait que si le point m_d est un des points $m_1, \ldots, m_{d-1}$, alors il est non-singulier. Dans le cas contraire, la multiplicité d'intersection en ce point vaut 1 et par la remarque 10.6.4, ce point est non singulier.

Par un changement de base de $\mathbf{K}^3$, on peut supposer que L est définie par $T_0 = 0$. On reprend alors les notations de la démonstration de la proposition 10.6.5. Le polynôme Q (resp. $S = Q(T, 1) = R(T, 1)$) appartient à $\mathbf{K}[T_1, T_2]$ (resp. $\mathbf{K}[T]$). Si $m_d = (0 : 1 : 0)$, alors l'assertion est vraie. Sinon, par hypothèse, il existe $(\alpha_1, \ldots, \alpha_{d-r-1})$ appartenant à $\mathbf{K}^{d-r-1}$ tel que

$$\prod_{i=1}^{r-d-1} (T - \alpha_i) \mid S.$$

Mais le quotient $S/\prod_{i=1}^{r-d-1}(T - \alpha_i)$ est un polynôme de degré un de $\mathbf{K}[T]$ qui s'écrit $a(T - b)$ et $m_d = (0 : b : 1)$ est défini sur $\mathbf{K}$. □

EXERCICES

10.1. Calculer la caractéristique d'Euler d'une sphère en utilisant le recouvrement donné par un ballon de football.

10.2. On considére le cube C de sommets les points de coordonnées $(\epsilon_1, \epsilon_2, \epsilon_3)$, avec $\epsilon_i \in \{-1, 1\}$. On note ∂C la réunion des faces du cube.

1. Montrer qu'on a une bijection

$$\partial C/\sim \to \mathbf{P}^2(\mathbf{R}),$$

où $\sim$ est la relation

$$\boldsymbol{x} = \boldsymbol{y} \quad \text{ou} \quad \boldsymbol{x} = -\boldsymbol{y}.$$

2. En considérant l'image des faces du cube, on obtient un découpage de $\mathbf{P}^2(\mathbf{R})$ en $f = 3$ carrés. Dénombrer le nombre s de sommets et le nombre a d'arêtes de ce découpage et calculer

$$e = f - a + s.$$

3. Que peut-on dire de la surface réelle $\mathbf{P}^2(\mathbf{R})$?

CHAPITRE 11

COURBES SUR LES CORPS FINIS

11.1. Le théorème de Chevalley-Warning

Pour ce paragraphe, le lecteur pourra se reporter avec profit à [**Se**].

Théorème 11.1.1. — *On note p un nombre premier et q une puissance de p. Soient $P_1, \dots, P_r$ des polynômes de $\mathbf{F}_q[T_1, \dots, T_n]$ tels que $\sum_{i=1}^r \deg(P_i) < n$ et soit V le sous-ensemble algébrique de $\overline{\mathbf{F}}_q^n$ qu'ils définissent. Alors*

$$\sharp V(\mathbf{F}_q) \equiv 0 \pmod{p}.$$

Démonstration. — On pose

$$P = \prod_{i=1}^{r} (1 - P_i^{q-1}).$$

Alors

$$\forall \boldsymbol{x} \in \mathbf{F}_q^n, \quad P(x) = \begin{cases} 1 & \text{si } x \in V(\mathbf{F}_q), \\ 0 & \text{sinon.} \end{cases}$$

On pose pour tout polynôme F de $\mathbf{F}_q[T_1, \dots, T_n]$

$$S(F) = \sum_{x \in \mathbf{F}_q^n} F(x).$$

On a donc que

$$\sharp V(\mathbf{F}_q) \equiv S(P) \pmod{p}.$$

Comme par hypothèse, $\sum_{i=1}^r \deg(P_i) < n$, on a $\deg P < n(q-1)$. L'application $F \mapsto S(F)$ étant linéaire sur $\mathbf{F}_q$, il suffit de montrer que pour tout monôme $T^{\boldsymbol{\alpha}}$ avec $|\alpha| < n(q-1)$, on a

$$S(T^{\boldsymbol{\alpha}}) = 0.$$

Mais on a la relation

$$S(T^{\boldsymbol{\alpha}}) = \sum_{(x_1, \dots, x_n) \in \mathbf{F}_q^n} \prod_{i=1}^{n} x_i^{\alpha_i} = \prod_{i=1}^{n} \sum_{x \in \mathbf{F}_q} x^{\alpha_i}.$$

Mais, comme $\sum_{i=1}^n \alpha_i = |\boldsymbol{\alpha}| < n(q-1)$, il existe i tel que $\alpha_i < q-1$. Il reste à montrer que si $\alpha < q-1$, alors

$$\sum_{x \in \mathbf{F}_q} x^{\alpha} = 0.$$

Si $\alpha = 0$, $\sum_{x\in\mathbf{F}_q} x^\alpha = q = 0$. Sinon le groupe $\mathbf{F}_q^\times$ est cyclique. Il existe donc $y \in \mathbf{F}_q$ tel que $\mathrm{ord}(y) = q-1$ et donc $y^\alpha \neq 1$. On a alors

$$\sum_{x\in\mathbf{F}_q} x^\alpha = \sum_{x\in\mathbf{F}_q^\times} x^\alpha = \sum_{x\in\mathbf{F}_q^\times} (xy)^\alpha = y^\alpha \sum_{x\in\mathbf{F}_q^\times} x^\alpha.$$

D'où $(1-y^\alpha)\sum_{x\in\mathbf{F}_q} x^\alpha = 0$, ce qui implique le résultat. □

Corollaire 11.1.2. — *Si $P_1,\dots,P_r$ sont des polynômes homogènes de $\mathbf{F}_q[T_0,\dots,T_n]$ tels que $\sum_{i=1}^r \deg(P_i) \leqslant n$, et V le sous-ensemble algébrique de $\mathbf{P}^n(\overline{\mathbf{F}}_q)$ qu'ils définissent, alors*

$$V(\mathbf{F}_q) \neq \emptyset.$$

11.2. Fonction zêta d'une courbe

Définition 11.2.1. — Si V est un sous-ensemble algébrique de $\mathbf{P}^n(\overline{\mathbf{F}}_q)$, alors on définit la série zêta de V comme la série formelle

$$Z(V,T) = \exp\Big(\sum_{n\geqslant 1} \frac{\sharp V(\mathbf{F}_{q^n})}{n}\, T^n\Big)$$

où $\exp$ est la série formelle $\sum_{n\in\mathbf{N}} \frac{1}{n!}T^n$.

Nous admettrons le résultat suivant

Théorème 11.2.2 (Weil). — *Si C est une courbe plane non-singulière de genre g définie sur un corps fini $\mathbf{F}_q$, alors il existe une extension L de $\mathbf{Q}$, un L-espace vectoriel H^1 de dimension $2g$ et une application linéaire bijective $\mathrm{Fr} : H^1 \to H^1$ telle que*

(i) *Les valeurs propres α_i de Fr sont racines de polynômes unitaires de $\mathbf{Z}[T]$ et pour tout plongement*

$$\sigma : \mathbf{Q}(\alpha_i) \hookrightarrow \mathbf{C}$$

on a $|\sigma(\alpha_i)| = \sqrt{q}$.

(ii) *Pour tout entier $n \geqslant 1$, $\sharp V(\mathbf{F}_{q^n}) = 1 - \mathrm{Tr}(\mathrm{Fr}^n) + q^n$.*

(iii) *La fonction zêta de C est donnée par*

$$Z(C,T) = \frac{\mathrm{Det}(1 - T\,\mathrm{Fr})}{(1-T)(1-qT)}$$

et appartient à $\mathbf{Q}(T)$.

Corollaire 11.2.3 (Estimation de Lang-Weil). — *On a des inégalités*

$$1 + q^n - 2gq^{\frac{n}{2}} \leqslant V(\mathbf{F}_{q^n}) \leqslant 1 + q^n + 2gq^{\frac{n}{2}}.$$

Démonstration. — En effet la condition (i) du théorème assure que

$$|\,\mathrm{Tr}(\mathrm{Fr}^n)| \leqslant 2gq^{\frac{n}{2}}.$$ □

EXERCICES

11.1. Quel est le cardinal de $\mathbf{P}^n(\mathbf{F}_q)$? Vérifier l'estimation de Lang-Weil dans le cas de $\mathbf{P}^1(\mathbf{F}_q)$.

CHAPITRE 12

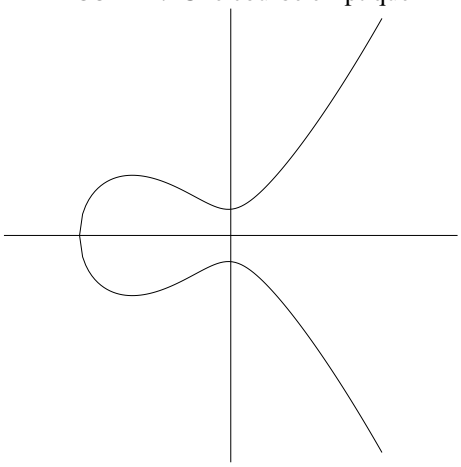
COURBES ELLIPTIQUES

Pour ce chapitre signalons deux bonnes références : le livre de Cassels [**Ca**] et celui de Knapp [**Kn**].

12.1. Définition

Définition 12.1.1. — Une *courbe elliptique* sur un corps $\mathbf{K}$ est une paire $(E, 0)$ où E est une courbe non-singulière plane de genre un et 0 un point rationnel de E.

FIGURE 1. Une courbe elliptique



Une courbe elliptique est donc définie par un polynôme de $\mathbf{K}[X, Y, T]$ qui est homogène de degré 3.

12.2. Forme de Weierstrass

Définition 12.2.1. — Une courbe elliptique $(E, 0)$ sur $\mathbf{K}$ est dite sous forme de Weierstrass si et seulement si son équation est de la forme

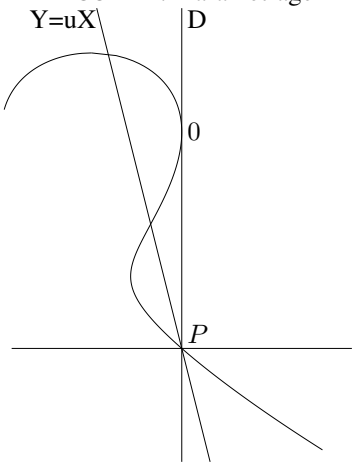
$$Y^2T + a_1XYT + a_3YT^2 = X^3 + a_2X^2T + a_4XT^2 + a_6T^3 \tag{12.2.1}$$

et $0 = (0 : 1 : 0)$. Si la caractéristique de $\mathbf{K}$ est différente de 2 on suppose que $a_1 = a_3 = 0$; si elle est différente de 3, on suppose en outre que $a_2 = 0$.

Théorème 12.2.2. — *Pour toute courbe elliptique* $(E, 0)$*, il existe une courbe* $(E', 0)$ *sous forme de Weierstrass et un isomorphisme* $\phi : E \xrightarrow{\sim} E'$ *tel que* $\phi(0) = 0$.

Démonstration. — La première étape consiste à rendre osculatrice la tangente D à E passant par 0. En effet la restriction à $T = 0$ du terme de gauche de (12.2.1), est le polynôme X^3 qui a une racine d'ordre 3 en $X = 0$. On suppose donc que cela n'est pas le cas. La multiplicité d'intersection de D avec E en 0 est alors égale à 2 et D rencontre E en un point P de $E(\mathbf{K})$. Quitte à faire une homographie, on peut supposer que $P = (0 : 0 : 1)$ et que D est la droit d'équation $X = 0$. L'idée est alors d'utiliser comme paramètre la pente de la droite passant par P (ce qui revient à faire un « éclatement en P »). Avec ce choix de coordonnées,

FIGURE 2. Paramétrage



l'équation de la courbe E est alors de la forme

$$F_1(X, Y)T^2 + F_2(X, Y)T + F_3(X, Y) = 0 \tag{12.2.2}$$

où F_i est un polynôme homogène de degré i en les deux variables X et Y. Le point 0 est alors le point de coordonnées $(0 : y : 1)$ avec

$$F_1(O, y) + F_2(0, y) + F_3(0, y) = 0$$

et $y \neq 0$. Comme F_i est homogène, cette équation se réécrit

$$F_1(O, 1) + F_2(0, 1)y + F_3(0, 1)y^2 = 0$$

En outre la multiplicité d'intersection étant 2, y est une racine double ce qui donne l'égalité

$$F_2(0, 1)^2 - 4F_1(0, 1)F_3(0, 1) = 0. \tag{12.2.3}$$

En effectuant les substitution $Y = UX$ et $T = 1$ dans l'équation (12.2.2) on arrive à l'équation affine suivante

$$F_1(1, U)X + F_2(1, U)X^2 + F_3(1, U)X^3 = 0.$$

Cette équation définit une courbe affine qui est réunion de la droite $X = 0$, correspondant pour cette substitution au point P, et de la courbe d'équation

$$F_1(1,U) + F_2(1,U)X + F_3(1,U)X^2 = 0. \tag{12.2.4}$$

Dans le cas où la caractéristique de $\mathbf{K}$ est différente de deux, on pose alors

$$V = 2F_3(1,U)X + F_2(1,U)$$

et on arrive à l'équation

$$V^2 = F_2(1,U)^2 - 4F_1(1,U)F_3(1,U).$$

Mais le coefficient de U^4 dans le terme de droite est $F_2(0,1)^2 - 4F_1(0,1)F_3(0,1)$ et en utilisant (12.2.3), ce terme de droite est un polynôme de degré trois qui peut donc se mettre sous la forme $\alpha_0U^3 + \alpha_2U^2 + \alpha_4U + \alpha_6$. En prenant $V' = \alpha_0V$ et $U' = \alpha_0U$, on se ramène à $\alpha_0 = 1$. En conséquence, la fonction

$$(x,y) \mapsto \Big(\alpha_0\frac{y}{x}, \alpha_0\Big(2F_3\Big(1,\frac{y}{x}\Big)x + F_2\Big(1,\frac{y}{x}\Big)\Big)\Big)$$

définit une équivalence birationnelle de E sur la courbe d'équation

$$Y^2T = X^3 + a_2X^2T + a_4XT^2 + a_6T^3,$$

avec $a_2 = \alpha_2$, $a_4 = \alpha_4\alpha_0$ et $a_6 = \alpha_4\alpha_0^2$. Si $\mathrm{car}(\mathbf{K}) \neq 3$, on peut faire un nouveau changement de variables $X' = X + a_2/3T$ qui permet de se ramener au cas $a_2 = 0$.

Si la caractéristique est égale à 2, on pose $V = F_3(1,U)X + F_3(0,1)yU^2$. L'équation (12.2.4) donne alors

$$V^2 = F_2(1,U)V + F_3(0,1)yU^2F_2(1,U) + F_1(1,U)F_3(1,U) + y^2F_3(0,1)^2U^4.$$

Comme $F_2(0,1) = 0$, le polynôme $F_2(1,U)$ est de degré 1. Mais on a également l'égalité $y^2 = F_1(0,1)/F_3(0,1)$ et le polynôme

$$F_3(0,1)yU^2F_2(1,U) + F_1(1,U)F_3(1,U) + y^2F_3(0,1)^2U^4$$

est de degré trois, ce qui fournit une équation de la forme

$$V^2 + \alpha_1UV + \alpha_3V = \alpha_0U^3 + \alpha_2U^2 + \alpha_4U + \alpha_6.$$

En prenant $V' = \alpha_0V$ et $U' = \alpha_0U$, on se ramène à $\alpha_0 = 1$, c'est à dire à une courbe d'équation

$$Y^2 + a_1XYT + a_3YT^2 = X^3 + a_2X^2T + a_4XT^2 + a_6T^3.$$

On peut enfin faire un nouveau changement de variables $X' = X + a_2/3T$ qui permet de se ramener au cas $a_2 = 0$. □

Proposition 12.2.3. — *Une courbe d'équation*

$$Y^2T + a_1XYT + a_3YT^2 = X^3 + a_2X^2T + a_4XT^2 + a_6T^3$$

est non-singulière si et seulement si

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \neq 0$$

où

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

L'élément Δ est appelé le discriminant *de la courbe E.*

Remarque 12.2.4. — Dans le cas où $a_1 = a_3 = a_2 = 0$, le discriminant se simplifie en

$$\Delta = -2^4(27a_6^2 + 4a_4^3)$$

12.3. Loi de groupe sur une courbe elliptique

Notations 12.3.1. — On se donne E une courbe définie par un polynôme homogène irréductible de degré trois sur $\mathbf{K}$ et 0 un point non-singulier de E. Si M et N sont deux points non-singuliers de E on note

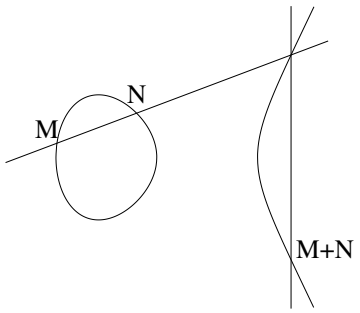
$$(MN) = \begin{cases} \text{la droite passant par } M \text{ et } N \text{ si } M \neq N, \\ \text{la tangente à } E \text{ en } M \text{ sinon.} \end{cases}$$

On note $(M.N)$ le troisième point d'intersection de la droite (MN) avec E. Par la proposition 10.6.7 ce point est un point non-singulier de E défini sur $\mathbf{K}$.

Définition 12.3.2. — Soit $U_0(\mathbf{K})$ l'ensemble des points non-singuliers de E définis sur $\mathbf{K}$. On définit une loi $+ : U_0(\mathbf{K}) \times U_0(\mathbf{K}) \to U_0(\mathbf{K})$ par

$$M + N = (0.(M.N)).$$

FIGURE 3. Loi de groupe



Théorème 12.3.3 (Poincaré). — *Si E est un courbe elliptique, la loi $+$ munit $E(\mathbf{K})$ d'une structure de groupe abélien.*

Remarque 12.3.4. — Cela est vrai plus généralement pour $U_0(\mathbf{K})$.

Remarque 12.3.5. — (i) 0 est bien l'élément neutre de E :

$$0 + M = (0.(0.M)) = M$$

puisque les trois points d'intersection comptés avec multiplicité de la droite $(0M)$ avec E sont 0, M et $(0.M)$.

(ii) De même, on vérifie que $(0.M)$ est l'opposé de M.

(iii) La difficulté est de montrer que la loi est associative.

12.4. Expression explicite de la loi de groupe

On suppose que la courbe est sous forme de Weierstrass. Son équation est donc de la forme

$$Y^2T + a_1XYT + a_3YT^2 = X^3 + a_2X^2T + a_4XT^2 + a_6T^3$$

Notons que $0 = (0 : 1 : 0)$ est l'unique point à l'infini de la courbe et que l'opposé d'un point de coordonnées affines (x, y) est donné par l'intersection de la droite verticale d'équation $X = x$ avec E. C'est donc le point de coordonnées $(x, -y - a_1x - a_3)$.

Proposition 12.4.1. — *Soient $M = (x_1, y_1)$ et $N = (x_2, y_2)$ deux points de la courbe. On suppose que $M \neq -N$. La somme $M + N$ est alors un point de coordonnées (x_3, y_3) donné par*

$$x_3 = p^2 + a_1p - a_2 - x_1 - x_2 \quad \textit{et} \quad y_3 = -(p + a_1)x_3 - q - a_3,$$

avec

$$p = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \textit{si } M \neq N, \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \textit{si } M = N, \end{cases}$$

et

$$q = \begin{cases} \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1} & \textit{si } M \neq N, \\ \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} & \textit{si } M = N. \end{cases}$$

Remarque 12.4.2. — La droite (MN) est la droite d'équation $Y = pX + q$.

Démonstration. — Posons

$$F(X, Y, T) = Y^2T + a_1XYT + a_3YT^2 - X^3 - a_2X^2T - a_4XT^2 - a_6T^3.$$

Si la droite (MN) est verticale, alors $0 \in (MN) \cap E$ et $0 = (M.N)$, donc

$$M + N = (0.(M.N)) = (0.0) = 0$$

cas exclu par hypothèse. Donc la droite (MN) n'est pas verticale et elle a une équation affine de la forme

$$Y = pX + q.$$

Calculons les coefficients p et q. Supposons $M \neq N$. Comme, par hypothèse, $M \neq -N$, on a $x_1 \neq x_2$ et

$$p = \frac{y_2 - y_1}{x_2 - x_1}$$
$$q = y_1 - px_1 = y_1 - \frac{y_2 - y_1}{x_2 - x_1}x_1 = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}.$$

Si $M = N$, l'équation de la tangente à E en $M = N$ s'écrit

$$\frac{\partial F}{\partial X}(x, y, 1)X + \frac{\partial F}{\partial Y}(x, y, 1)Y + \frac{\partial F}{\partial T}(x, y, 1) = 0,$$

c'est-à-dire

$$Y = -\frac{\frac{\partial F}{\partial X}(x, y, 1)}{\frac{\partial F}{\partial Y}(x, y, 1)}X - \frac{\frac{\partial F}{\partial T}(x, y, 1)}{\frac{\partial F}{\partial Y}(x, y, 1)}.$$

On en déduit les expressions suivantes pour p et q :

$$p = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$$
$$q = y_1 - px_1 = y_1 - \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}x_1$$
$$= \frac{2y_1^2 + a_1x_1y_1 + a_3y_1 - 3x_1^3 - 2a_1x_1^2 - a_4x_1 + a_1x_1y_1}{2y_1 + a_1x_1 + a_3}.$$

Mais le point (x_1, y_1) étant sur la courbe, on a

$$y_1^2 = x_1^3 + a_2x_1^2 + a_4x_1 + a_6 - a_1x_1y_1 - a_3y_1.$$

En définitive, on obtient

$$q = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

Le point $M+N$ a pour coordonnées (x_3, y_3). Comme $M+N = (0.(M.N))$, le point $(M.N)$ a pour coordonnées $(x_3 : y_3')$ avec

$$y_3 = y_3' - a_1x_3 - a_3. \tag{12.4.1}$$

On considère l'intersection de la droite (MN) avec E, donnée ensemblistement par les équations

$$\begin{cases} Y = pX + q \\ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6. \end{cases}$$

De manière plus précise, x_1, x_2 et x_3 sont les racines comptées avec multiplicité du polynôme $F(X, pX + q, 1)$. On a donc la relation

$$(pX + q)^2 + a_1(pX + q)X + a_3(pX + q) - X^3 - a_2X^2 - a_4X - a_6 = -(X - x_1)(X - x_2)(X - x_3).$$

En regardant le coefficient de X^2 dans cette égalité, on obtient

$$p^2 + a_1p - a_2 = x_1 + x_2 + x_3.$$

Donc

$$x_3 = p^2 + a_1 p - a_2 - x_1 - x_2$$

et, comme $y_3' = px_3 + q$, on obtient, compte tenu de (12.4.1), la relation

$$y_3 = -px_3 - q - a_1 x_3 - a_3. \quad \square$$

EXERCICES

12.1. Soit $\mathbf{K}$ un corps de caractéristique différente de 3. Soit E la courbe projective d'équation

$$X^3 + Y^3 + T^3 = 0$$

On note 0 le point $(1 : -1 : 0)$ de E.

1. Montrer que la courbe E est non-singulière. Pourquoi a-t-on supposé la caractéristique différente de 3 ?
2. Mettre la courbe elliptique $(E, 0)$ sous forme de Weierstrass.

12.2. Trouver tous les points de la courbe elliptique E

$$Y^2 = X^3 - X$$

sur $\mathbf{F}_3$ et écrire la table de multiplication de $E(\mathbf{F}_3)$ lorsque $0 = (0 : 1 : 0)$.

APPENDICES

APPENDICE A

A.1. Algorithmes de base

Pour ces exemples de programme nous avons voulu en même temps obtenir du code qui soit « prêt à l'emploi » et qui reflète directement les objets mathématiques présentés dans ce texte. Notre choix s'est donc porté sur le C++, qui permettait de satisfaire ces objectifs. Plus précisément nous utilisons le système `CWEB` de D. Knuth et S. Levy [**KL**]. Notre souhait de produire un code aisément compréhensible et pas trop long, tout en étant presque complet, a toutefois deux inconvénients majeurs : nous avons laissé de côté toute gestion des erreurs et des dépassements et toute optimisation.

A.1.1. Calcul d'une puissance.

Comme pour les entiers, l'idée de l'algorithme est d'écrire l'exposant en base 2, afin de se ramener à des calculs de carrés. La nombre d'étapes nécessaires est de l'ordre du logarithme de l'exposant.

Algorithme A.1.1.

Entrée:

- Entiers n,
- Elément a d'un anneau.

Sortie:

- a^n.

Algorithme:

1. Soit $n = n_r \dots n_0$ l'écriture de n en base 2.
2. $x \leftarrow a$.
3. *aux* $\leftarrow 1$.
3. Pour i variant de 0 à r,
   3.1. Si $n_i = 1$, *aux* $\leftarrow$ *aux* $* x$.
   3.2. $x \leftarrow x^2$.
4. Renvoyer *aux*.

En voici la réalisation en C++. Le type **long long** est défini pour certains compilateurs tel que `gcc`.

template⟨**class anneau**⟩
anneau *carre*(**anneau** a);

template⟨**class anneau**⟩
anneau *puissance*(**anneau** a, **long long** n)

```
{
  anneau aux, x;
  long long i;
  x = a;
  aux = (anneau) 1_L;
  if (n < 0) {
    exit(1);
  }
  for (i = n; i > 0; i = i/2) {
    if (i % 2 ≡ 1) aux = aux * x;
    x = carre(x);
  }
  return (aux);
}
```

A.1.2. Prenons par exemple les entiers

```
bool inversible(long a)
{
  return (a ≡ 1 ∨ a ≡ −1);
}
long inverse(long a)
{
  if (inversible(a)) return (a);
  else {
    cerr ≪ "Entier non inversible\n";
    exit(1);
  }
}
```

A.1.3. Calcul du pgcd.

Nous nous plaçons ici dans un anneau euclidien.

```
template⟨class euclidien⟩
euclidien pgcd(euclidien a, euclidien b)
{
  euclidien aux;
  while (b ≠ (euclidien) 0_L) {
    aux = b;
    b = a % b;
    a = aux;
  }
  return (a);
}
```

A.1.4. Coefficients de Bezout.

Voici un variante du même algorithme qui calcule en outre les coefficients pour le théorème de Bezout. (cf. l'algorithme 3.8.12) Les pointeurs u et v doivent pointer vers des valeurs accessibles.

```
template⟨class euclidien⟩
euclidien pgcdbezout(euclidien a, euclidien b, euclidien *u, euclidien *v)
{
  euclidien aux, q, u_0, u_1, u_2, v_0, v_1, v_2;
  u_0 = (euclidien) 1;
  u_1 = (euclidien) 0;
  v_0 = (euclidien) 0;
  v_1 = (euclidien) 1;
  while (b ≠ (euclidien) 0_L) {
    aux = b;
    q = a/b;
    b = a % b;
    a = aux;
    u_2 = u_0 − q * u_1;
    v_2 = v_0 − q * v_1;
    u_0 = u_1;
    u_1 = u_2;
    v_0 = v_1;
    v_1 = v_2;
  }
  *u = u_0;
  *v = v_0;
  return (a);
}
```

A.1.5. Détermination de l'ordre.

On suppose que a est un élément d'ordre fini dans $A^\times$ et on veut déterminer son ordre. On utilise pour cela la force brute

```
#define LIMITE_TEST 1000000
#define SHOW_PROGRESS
  template⟨class anneau⟩
  long ordre(anneau a)
  {
    anneau x;
    long aux;
    x = a;
    aux = 1;
    while (x ≠ (anneau) 1 ∧ aux < LIMITE_TEST) {
      x = x * a;
```

```
#ifdef SHOW_PROGRESS
      if (aux % 10000 ≡ 0)  cout ≪ aux ≪ "\n";
#endif
      aux++;
    }
    if (aux ≡ LIMITE_TEST) {
      cerr ≪ "Limite␣depassee\n";
      exit(1);
    }
    return (aux);
  }
```

A.1.6. En voici une deuxième version, qui ne vaut guère mieux, dans laquelle on suppose connaître un multiple de l'ordre.

```
  template⟨class anneau⟩
  long long ordre0(anneau a, long long multiple, long long bas)
  {
    long long aux;
    bool test = false;
    if (a ≡ (anneau) 1)  return (1);
    aux = bas;
    while (¬test ∧ aux ∗ aux ⩽ multiple) {
      if (multiple % aux ≡ 0) {
        test = puissance(a, aux) ≡ (anneau) 1;
        if (¬test ∧ puissance(a, multiple/aux) ≡ (anneau) 1) {
          multiple = multiple/aux;
          return (ordre0(a, multiple, aux));
        }
      }
#ifdef SHOW_PROGRESS
      if (aux % 10000000 ≡ 0)  cout ≪ aux ≪ "␣" ≪ multiple/aux ≪ "\n";
#endif
      aux++;
    }
    if (¬test)  aux = multiple + 1;
    return (aux − 1);
  }
  template⟨class anneau⟩
  long long ordre(anneau a, long long multiple)
  {
    if (puissance(a, multiple) ≠ (anneau) 1) {
      cerr ≪ "L'argument␣n'est␣pas␣multiple␣de␣l'ordre\n";
      exit(1);
    }
```

```
  return (ordre0(a, multiple, 2));
}
```

A.2. Les polynômes

A.2.7. Définition de la classe.

Notez que la description choisie n'est efficace ni en termes de temps ni de mémoire. La valeur statique *zero* sera utilisée pour les polynômes à coefficients dans un quotient.

```
template⟨class anneau⟩
class polynome;
template⟨class anneau⟩
void setzero(anneau a);
template⟨class anneau⟩
long ledegre(const polynome⟨anneau⟩ &a);
template⟨class anneau⟩
ostream &operator≪(ostream &stream, polynome⟨anneau⟩ a);
template⟨class anneau⟩
class polynome {
protected:
  long nombre;
  static anneau *zero;
  anneau *coeffs;
  void init(long n);
  void copy(const polynome⟨anneau⟩ &a);
public:
  friend void setzero <> (anneau a);
  void setsize(long n);
  polynome();
  polynome(int a);
  polynome(anneau a);
  polynome(long a, anneau b);
  polynome(const polynome⟨anneau⟩ &a);
  ~polynome();
  polynome⟨anneau⟩ operator=(const polynome⟨anneau⟩ &a);
  anneau &operator [](long i);
  polynome⟨anneau⟩ operator+(polynome⟨anneau⟩ a);
  polynome⟨anneau⟩ operator−(polynome⟨anneau⟩ a);
  polynome⟨anneau⟩ operator−();
  polynome⟨anneau⟩ operator * (polynome⟨anneau⟩ a);
  polynome⟨anneau⟩ operator/(polynome⟨anneau⟩ a);
  polynome⟨anneau⟩ operator%(polynome⟨anneau⟩ a);
  friend long ledegre <> (const polynome⟨anneau⟩ &a);
  long degre();
```

```
  bool inversible0( );
  polynome⟨anneau⟩ inverse0( );
  bool operator≡(polynome⟨anneau⟩ a);
  bool operator≠(polynome⟨anneau⟩ a);
  friend ostream &operator≪ <> (ostream &stream, polynome⟨anneau⟩ a);
};
template⟨class anneau⟩
polynome⟨anneau⟩ operator ∗ (anneau a, polynome⟨anneau⟩ b);
template⟨class anneau⟩
long ledegre(const polynome⟨anneau⟩ &a);
template⟨class anneau⟩
bool inversible(polynome⟨anneau⟩ a);
template⟨class anneau⟩
polynome⟨anneau⟩ inverse(polynome⟨anneau⟩ a);
template⟨class anneau⟩
ostream &operator≪(ostream &stream, polynome⟨anneau⟩ a);
```

A.2.8. Commençons par les constructeurs et destructeurs.

```
template⟨class anneau⟩
void setzero(anneau a)
{
  if (polynome⟨anneau⟩::zero ≡ ∅) polynome⟨anneau⟩::zero = new anneau;
  ∗polynome⟨anneau⟩::zero = a;
}
template⟨class anneau⟩
void polynome⟨anneau⟩::init(long n)
{
  long i;
  anneau nul = 0 L;
  if (zero ≠ ∅) nul = ∗zero;
  nombre = n;
  if (n > 0) coeffs = new anneau [n];
  else coeffs = ∅;
  for (i = 0; i < n; i++) coeffs[i] = nul;
}
template⟨class anneau⟩
polynome⟨anneau⟩::polynome( )
{
  nombre = 0;
  coeffs = ∅;
}
template⟨class anneau⟩
polynome⟨anneau⟩::polynome(int a)
{
```

```
  init(1);
  coeffs[0] = (anneau) a;
}
template⟨class anneau⟩
polynome⟨anneau⟩::polynome(anneau a)
{
  init(1);
  coeffs[0] = a;
}
template⟨class anneau⟩
polynome⟨anneau⟩::polynome(long a, anneau b)
{
  if (a < 0)  a = −1;
  nombre = a + 1;
  if (nombre > 0)  {
    init(nombre);
    coeffs[a] = b;
  }
  else  coeffs = ∅;
}
template⟨class anneau⟩
polynome⟨anneau⟩::∼polynome⟨anneau⟩ ()
{
  if (coeffs ≠ ∅)  delete [] coeffs;
  nombre = 0;
  coeffs = ∅;
}
```

A.2.9. Puis les opérateurs de copie :

```
template⟨class anneau⟩
void polynome⟨anneau⟩::copy(const polynome⟨anneau⟩ &a)
{
  long i;
  anneau *ancien, *nouveau;
  ancien = coeffs;
  nouveau = a.coeffs;
  nombre = ledegre(a) + 1;
  if (nombre > 0)  coeffs = new anneau [nombre];
  else  coeffs = ∅;
  for (i = 0; i < nombre; i++)  coeffs[i] = nouveau[i];
  if (ancien ≠ ∅)  delete [] ancien;
}
template⟨class anneau⟩
```

```
void polynome⟨anneau⟩::setsize(long n)
{
  long i, ancienn;
  anneau *ancien;
  if (n < 0) n = 0;
  ancienn = nombre;
  if (ancienn > n) ancienn = n;
  ancien = coeffs;
  nombre = n;
  if (nombre > 0) init(nombre);
  else coeffs = ∅;
  for (i = 0; i < ancienn; i++) coeffs[i] = ancien[i];
  if (ancien ≠ ∅) delete [] ancien;
}
template⟨class anneau⟩
polynome⟨anneau⟩::polynome(const polynome⟨anneau⟩ &a)
{
  nombre = 0;
  coeffs = ∅;
  copy(a);
}
template⟨class anneau⟩
polynome⟨anneau⟩ polynome⟨anneau⟩::operator=(const polynome⟨anneau⟩ &a)
{
  copy(a);
  return (*this);
}
```

A.2.10. Extraction du degré, d'un coefficient :

```
template⟨class anneau⟩
anneau &polynome⟨anneau⟩::operator [ ](long i)
{
  if ((i ⩾ 0) ∧ (i < nombre)) return (coeffs[i]);
  else if (i < 0) {
    cerr ≪ "Coefficient negatif\n";
    exit(1);
  }
  else {
    setsize(i + 1);
    return (coeffs[i]);
  }
}
template⟨class anneau⟩
long ledegre(const polynome⟨anneau⟩ &a)
```

```
{
  long aux;
  aux = a.nombre − 1;
  while (aux ⩾ 0) {
    if (a.coeffs[aux] ≡ 0 L) aux−−;
    else return (aux);
  }
  return (aux);
}
template⟨class anneau⟩
long polynome⟨anneau⟩::degre( )
{
  return (ledegre(∗this));
}
```

A.2.11. et les opérations d'anneaux :

```
template⟨class anneau⟩
polynome⟨anneau⟩ polynome⟨anneau⟩::operator+(polynome⟨anneau⟩ a)
{
  long n, m, i;
  polynome⟨anneau⟩ aux;
  n = nombre;
  m = a.nombre;
  if (a.nombre > n) {
    n = a.nombre;
    m = nombre;
  }
  aux.init(n);
  for (i = 0; i < m; i++) aux.coeffs[i] = coeffs[i] + a.coeffs[i];
  for (i = m; i < nombre; i++) aux.coeffs[i] = coeffs[i];
  for (i = m; i < a.nombre; i++) aux.coeffs[i] = a.coeffs[i];
  return (aux);
}
template⟨class anneau⟩
polynome⟨anneau⟩ polynome⟨anneau⟩::operator−( )
{
  long i;
  polynome⟨anneau⟩ aux;
  aux.init(nombre);
  for (i = 0; i < nombre; i++) aux.coeffs[i] = −coeffs[i];
  return (aux);
}
template⟨class anneau⟩
```

```
polynome⟨anneau⟩ polynome⟨anneau⟩::operator−(polynome⟨anneau⟩ a)
{
  return ((∗this) + (−a));
}
template⟨class anneau⟩
polynome⟨anneau⟩ polynome⟨anneau⟩::operator ∗ (polynome⟨anneau⟩ a)
{
  long n, i, j;
  polynome⟨anneau⟩ aux;
  n = nombre + a.nombre − 1;
  aux.init(n);
  for (i = 0; i < nombre; i++)
    for (j = 0; j < a.nombre; j++)
      aux.coeffs[i + j] = aux.coeffs[i + j] + coeffs[i] ∗ a.coeffs[j];
  return (aux);
}
template⟨class anneau⟩
polynome⟨anneau⟩ operator ∗ (anneau a, polynome⟨anneau⟩ b)
{
  polynome⟨anneau⟩ temp = a;
  return (temp ∗ b);
}
```

A.2.12. Division euclidienne des polynômes.

```
template⟨class anneau⟩
polynome⟨anneau⟩ polynome⟨anneau⟩::operator/(polynome⟨anneau⟩ a)
{
  long i, d, dr;
  polynome⟨anneau⟩ reste = ∗this;
  polynome⟨anneau⟩ quotient;
  anneau coeff, c;
  d = a.degre( );
  dr = degre( );
  if (d > dr) return (quotient);
  if (¬inversible(a[d])) {
    cerr ≪ "Coefficient␣dominant␣non␣inversible\n";
    exit(1);
  }
  c = inverse(a[d]);
  quotient.setsize(dr − d + 1);
  while (dr ⩾ d) {
    coeff = reste.coeffs[dr] ∗ c;
    reste = reste
```

```
        −polynome⟨anneau⟩ (dr − d, coeff)∗a;
    quotient.coeffs[dr − d] = coeff;
    dr = reste.degre();
  }
  return (quotient);
}
template⟨class anneau⟩
polynome⟨anneau⟩ polynome⟨anneau⟩::operator%(polynome⟨anneau⟩ a)
{
  long i, d, dr;
  polynome⟨anneau⟩ reste = ∗this;
  polynome⟨anneau⟩ quotient;
  anneau coeff, c;
  d = a.degre();
  dr = degre();
  if (d > dr) return (reste);
  if (¬inversible(a.coeffs[d])) {
    cerr ≪ "Coefficient dominant non inversible\n";
    exit(1);
  }
  c = inverse(a[d]);
  quotient.setsize(dr − d + 1);
  while (dr ⩾ d) {
    coeff = reste.coeffs[dr] ∗ c;
    reste = reste
        −polynome⟨anneau⟩ (dr − d, coeff)∗a;
    quotient.coeffs[dr − d] = coeff;
    dr = reste.degre();
  }
  return (reste);
}
```

A.2.13. Les inversibles dans $A[T]$ sont les inversibles de A.

```
template⟨class anneau⟩
bool polynome⟨anneau⟩::inversible0()
{
  if (degre() ≡ 0) return (inversible(coeffs[0]));
  else return (false);
}
template⟨class anneau⟩
bool inversible(polynome⟨anneau⟩ a)
{
  return (a.inversible0());
```

```
}
template⟨class anneau⟩
polynome⟨anneau⟩ polynome⟨anneau⟩::inverse0( )
{
  if (inversible0( )) return (inverse(coeffs[0]));
  else {
    cerr ≪ "Polynome non inversible\n";
    exit(1);
  }
}
template⟨class anneau⟩
polynome⟨anneau⟩ inverse(polynome⟨anneau⟩ a)
{
  return (a.inverse0( ));
}
```

A.2.14. Le carré :

```
template⟨class anneau⟩
anneau carre(anneau a)
{
  return (a ∗ a);
}
```

A.2.15. Test d'égalité.

```
template⟨class anneau⟩
bool polynome⟨anneau⟩::operator≡(polynome⟨anneau⟩ a)
{
  long i, d;
  bool aux;
  d = degre( );
  if (d ≠ a.degre( )) return (false);
  aux = true;
  for (i = 0; i ⩽ d; i++) aux = aux ∧ coeffs[i] ≡ a.coeffs[i];
  return (aux);
}
template⟨class anneau⟩
bool polynome⟨anneau⟩::operator≠(polynome⟨anneau⟩ a)
{
  return (¬((∗this) ≡ a));
}
```

A.2.16. Enfin une sortie rudimentaire pour les tests.

```
char variable ;
template⟨class anneau⟩
ostream &operator≪(ostream &stream , polynome⟨anneau⟩ a)
{
  long i, d;
  bool first ;
  d = a.degre( );
  if (d < 0) stream ≪ "0";
  else {
    first = true;
    for (i = 0; i ⩽ d; i++) {
      if (a.coeffs[i] ≠ 0_L) {
        if (¬first) stream ≪ "+";
        first = false;
        variable++;
        stream ≪ "(" ≪ a.coeffs[i] ≪ ")";
        variable−−;
        stream ≪ (char) variable ≪ "^" ≪ i;
      }
    }
  }
  return (stream);
}
```

A.3. Les quotients d'un anneau euclidien

A.3.17. Définition de la classe.

```
template⟨class euclidien⟩
class quotient ;
template⟨class euclidien⟩
void setmodulodef (euclidien a);
template⟨class euclidien⟩
ostream &operator≪(ostream &stream , quotient⟨euclidien⟩ a);
template⟨class euclidien⟩
class quotient {
protected :
  euclidien modulo ;
  euclidien x;
  static euclidien ∗modulodef ;
public :
  friend void setmodulodef <> (euclidien a);
  void reduce( );
```

```
  quotient( );
  quotient(euclidien a);
  quotient(euclidien m, euclidien a);
  quotient⟨euclidien⟩ operator+(quotient⟨euclidien⟩ a);
  quotient⟨euclidien⟩ operator−(quotient⟨euclidien⟩ a);
  quotient⟨euclidien⟩ operator−( );
  quotient⟨euclidien⟩ operator ∗ (quotient⟨euclidien⟩ a);
  bool inversible0( );
  quotient⟨euclidien⟩ inverse0( );
  bool operator≡(quotient⟨euclidien⟩ a);
  bool operator≠(quotient⟨euclidien⟩ a);
  friend ostream &operator≪ <> (ostream &stream, quotient⟨euclidien⟩ a);
};
template⟨class euclidien⟩
bool inversible(quotient⟨euclidien⟩ a);
template⟨class euclidien⟩
quotient⟨euclidien⟩ inverse(quotient⟨euclidien⟩ a);
template⟨class euclidien⟩
quotient⟨euclidien⟩ carre(quotient⟨euclidien⟩ a);
template⟨class euclidien⟩
ostream &operator≪(ostream &stream, quotient⟨euclidien⟩ a);
```

A.3.18. Tout d'abord les constructeurs :

```
template⟨class euclidien⟩
void setmodulodef(euclidien a)
{
  if (quotient⟨euclidien⟩::modulodef ≡ ∅)
    quotient⟨euclidien⟩::modulodef = new euclidien;
  ∗quotient⟨euclidien⟩::modulodef = a;
}
template⟨class euclidien⟩
quotient⟨euclidien⟩::quotient( )
{
  if (modulodef ≠ ∅) modulo = ∗modulodef;
  else modulo = (euclidien) 0;
  x = (euclidien) 0;
}
template⟨class euclidien⟩
quotient⟨euclidien⟩::quotient(euclidien a)
{
  if (modulodef ≠ ∅) modulo = ∗modulodef;
  else modulo = (euclidien) 0;
  x = a;
}
```

```
template⟨class euclidien⟩
quotient⟨euclidien⟩::quotient(euclidien m, euclidien a)
{
  modulo = m;
  x = a;
}
```

A.3.19. Nous utilisons la réduction :

```
template⟨class euclidien⟩
void quotient⟨euclidien⟩::reduce( )
{
  x = x % modulo;
}
```

A.3.20. Voici les opérations d'anneaux :

```
template⟨class euclidien⟩
quotient⟨euclidien⟩ quotient⟨euclidien⟩::operator+(quotient⟨euclidien⟩ a)
{
  quotient⟨euclidien⟩ aux;
  aux.modulo = pgcd(modulo, a.modulo);
  aux.x = x + a.x;
  aux.reduce( );
  return (aux);
}
template⟨class euclidien⟩
quotient⟨euclidien⟩ quotient⟨euclidien⟩::operator−(quotient⟨euclidien⟩ a)
{
  return ((*this) + (−a));
}
template⟨class euclidien⟩
quotient⟨euclidien⟩ quotient⟨euclidien⟩::operator−( )
{
  quotient⟨euclidien⟩ aux;
  aux.modulo = modulo;
  aux.x = −x;
  return (aux);
}
template⟨class euclidien⟩
quotient⟨euclidien⟩ quotient⟨euclidien⟩::operator * (quotient⟨euclidien⟩ a)
{
  quotient⟨euclidien⟩ aux;
  aux.modulo = pgcd(modulo, a.modulo);
  aux.x = x * a.x;
```

```
  aux.reduce( );
  return (aux);
}
```

A.3.21. Calcul de l'inverse.

Passons à l'inverse et au quotient dans l'anneau quotient

```
template⟨class euclidien⟩
bool quotient⟨euclidien⟩::inversible0( )
{
  return (inversible(pgcd(x, modulo)));
}
template⟨class euclidien⟩
bool inversible(quotient⟨euclidien⟩ a)
{
  return (a.inversible0( ));
}
template⟨class euclidien⟩
quotient⟨euclidien⟩ quotient⟨euclidien⟩::inverse0( )
{
  quotient⟨euclidien⟩ aux;
  euclidien u, v, d;
  aux.modulo = modulo;
  d = pgcdbezout(x, modulo, &u, &v);
  if (inversible(d)) {
    aux.x = inverse(d) * u;
    aux.reduce( );
    return (aux);
  }
  else {
    cerr ≪ "Element non inversible\n";
    exit(1);
  }
}
template⟨class euclidien⟩
quotient⟨euclidien⟩ inverse(quotient⟨euclidien⟩ a)
{
  return (a.inverse0( ));
}
```

A.3.22. Le carré :

```
template⟨class euclidien⟩
quotient⟨euclidien⟩ carre(quotient⟨euclidien⟩ a)
{
```

```
  return (a * a);
}
```

A.3.23. Les tests d'égalités

```
template⟨class euclidien⟩
bool quotient⟨euclidien⟩::operator≡(quotient⟨euclidien⟩ a)
{
  return (modulo ≡ a.modulo ∧ ((x − a.x) % modulo) ≡ (euclidien) 0);
}
template⟨class euclidien⟩
bool quotient⟨euclidien⟩::operator≠(quotient⟨euclidien⟩ a)
{
  return (¬((∗this) ≡ a));
}
```

A.3.24. Un affichage rudimentaire pour les essais.

```
template⟨class euclidien⟩
ostream &operator≪(ostream &stream, quotient⟨euclidien⟩ a)
{
  stream ≪ a.x ≪ " mod " ≪ a.modulo;
  return (stream);
}
```

A.3.25. Exemples d'utilisation.

Un corps fini peut être construit comme un quotient d'un anneau de polynômes sur $\mathbf{F}_p$.

```
typedef polynome⟨long⟩ polentier;
template⟨⟩
long ∗polentier::zero = ∅;
typedef quotient⟨long⟩ modm;
template⟨⟩
long ∗modm::modulodef = ∅;
typedef polynome⟨modm⟩ polmodm;
template⟨⟩
modm ∗polmodm::zero = ∅;
typedef quotient⟨polmodm⟩ objfini;
template⟨⟩
polmodm ∗objfini::modulodef = ∅;
```

A.3.26. Symbole de Legendre.

On suppose que p est un nombre premier.

```
template⟨class entier⟩
int legendre(entier n, entier p)
{
```

```
  if (p ≡ 2) {
    if (n % 2 ≡ 0) return (0);
    else return (1);
  }
  setmodulodef(p);
  quotient⟨entier⟩ x(p, n);
  x = puissance(x, (p − 1)/2);
  if (x ≡ 0) return (0);
  else if (x ≡ 1) return (1);
  else return (−1);
}
```

A.3.27. Et voici pour travailler sur le corps $\mathbf{F}_{823\,543}$ ou $\mathbf{F}_{285\,311\,670\,611}$:

```
void corps823543init( )
{
  setmodulodef((long) 7);
  setzero((modm) 0);
  polmodm U(1, 1);
  polmodm P;
  P = puissance(U, 7) − U + (polmodm) 1;
  setmodulodef(P);
}
void corps285311670611init( )
{
  setmodulodef((long) 11);
  setzero((modm) 0);
  polmodm U(1, 1);
  polmodm P;
  P = puissance(U, 11) − U + (polmodm) 1;
  setmodulodef(P);
}
```

A.3.28. Terminons avec des exemples de calculs sur ces corps :

```
void exemple1( )
{
  corps823543init( );
  objfini g;
  g = polmodm(1, 1);
  cout ≪ ordre(g, 823542) ≪ "\n";
}
void exemple2( )
{
```

```
  corps285311670611init( );
  objfini g;
  g = polmodm(1, 1);
  cout << ordre(g, puissance((long long) 11, 11) − 1) << "\n";
}
```

EXERCICES

A.1.

1. Justifier la description des corps $\mathbf{F}_{823\,543}$ et $\mathbf{F}_{285\,311\,670\,611}$ utilisées.
2. On fait l'hypothèse hardie que les algorithmes précédents fonctionnent. Sachant que la fonction *exemple1* affiche la valeur $274\,514$, trouver un générateur de $\mathbf{F}_{823\,543}^{\times}$.
3. Toujours sous la même hypothèse, sachant que la fonction *exemple2* décrite ci-dessus affiche la valeur $57\,062\,334\,122$, trouver un générateur de $\mathbf{F}_{285\,311\,670\,611}^{\times}$.

A.4. Polynômes sur $\mathbf{F}_2$

Dans cette annexe nous nous concentrons sur les polynômes sur $\mathbf{F}_2$. D'une part, ils constituent un exemple utile d'anneau euclidien ; d'autre part nous implémentons dans ce contexte le test de primalité décrit dans l'algorithme 6.5.6.

La classe est basée sur une classe de chaînes compressées de valeur booléennes. Pour la lisibilité nous avons à nouveau omis les questions de dépassements et d'optimisations.

A.4.1. Référence à une valeur booléenne.

Nous conservons ces suites de 0 ou 1 sous forme compactée. Cela signifie que si c est une telle chaîne et i un entier, $c[i]$ ne peut pas être un référence standard **bool** $\&$. Nous introduisons donc une classe particulière pour cela :

```
class ref_bool {
public :
  unsigned long *ptr;
  unsigned int offset ;
  ref_bool(unsigned long *nptr, unsigned int noffset);
  operator bool ();
  bool operator=(const bool &a);
  bool operator=(const ref_bool &a);
  bool operator++( );
};
```

A.4.2. Dans la création, *ptr* pointe sur une entier long, *offset* indiquant la position à l'intérieur de cet entier.

```
ref_bool ::ref_bool(unsigned long *nptr, unsigned int noffset)
{
  ptr = nptr;
  offset = noffset;
}
```

A.4.3. La valeur booléenne associée s'obtient à l'aide d'un opérateur de transtypage :

```
ref_bool ::operator bool ()
{
  unsigned long t;
  t = *ptr;
  t = t >> offset;
  return (t % 2);
}
```

A.4.4. Nous voulons pouvoir changer une valeur dans un telle chaîne avec des expressions telles que $c[i] = 0$ ou $c[i] = d[j]$.

```
bool ref_bool ::operator=(const bool &a)
{
  *ptr = (*ptr & ~(1L << offset)) + ((unsigned long) a << offset);
  return (a);
}
bool ref_bool ::operator=(const ref_bool &a)
{
  unsigned long t;
  t = *a.ptr;
  t = t >> a.offset;
  *ptr = (*ptr & ~(1L << offset)) + ((t % 2) << offset);
  return (t % 2);
}
```

A.4.5. Nous définissons maintenant les classes de chaînes de bits. Le nombre `LB` est le nombre de bits par entier long.

```
#define LB 32
  class bitstring {
  protected :
    long size ;
    long nombre ;
    unsigned long *data;
    void init(long n);
    void copy(const bitstring &a);
    void dolshift(long a);
    void dorshift(long a);
  public :
    void setsize(long n);
    bitstring( );
    bitstring(long a);
    bitstring(bool a);
    bitstring(long a, bool b);
    bitstring(const bitstring &a);
    ~bitstring( );
    bitstring operator=(const bitstring &a);
    ref_bool operator [ ](long i);
    bitstring operator+(bitstring a);
    bitstring operator+=(bitstring a);
    bitstring operator-(bitstring a);
    bitstring operator-( );
    bitstring operator<<(long a);
```

```
  bitstring operator≫(long a);
  bitstring operator≪=(long a);
  bitstring operator≫=(long a);
  bool operator≡(bitstring a);
  bool operator≠(bitstring a);
  friend ostream&operator≪(ostream & stream, bitstring a);
};
```

A.4.6. Voici les différentes initialisations. Notons que celle à partir d'un entier long correspond au morphisme d'anneaux $\mathbf{Z} \to \mathbf{F}_2[T]$. Si on veut allouer un espace à la chaîne, on peut utiliser **bitstring**(a, b).

```
void bitstring ::init(long n)
{
  long i;
  size = n;
  nombre = (n + LB − 1)/LB;
  if (nombre > 0) data = new unsigned long [nombre];
  else data = ∅;
  for (i = 0; i < nombre; i++) data[i] = 0;
}
bitstring ::bitstring( )
{
  size = 0;
  nombre = 0;
  data = ∅;
}
bitstring ::bitstring(long a)
{
  init(1);
  data[0] = a % 2;
}
bitstring ::bitstring(bool a)
{
  init(1);
  data[0] = a;
}
bitstring ::bitstring(long a, bool b)
{
  if (a < 0) init(0);
  else {
    init(a + 1);
    data[a/LB] = ((long) b) ≪ (a % LB);
  }
```

```
}
```

A.4.7. Nous passons ensuite au destructeur qui libère la place allouée

```
bitstring::~bitstring( )
{
  if (data ≠ ∅) delete [ ] data ;
  data = ∅;
  size = 0;
  nombre = 0;
}
```

A.4.8. Pour la copie il faut encore une fois envisager le cas où ∗**this** et a coïncident.

```
void bitstring : :copy(const bitstring &a)
{
  long i ;
  unsigned long ∗ancien, ∗nouveau;
  ancien = data;
  nouveau = a.data;
  nombre = a.nombre;
  size = a.size;
  if (nombre > 0) data = new unsigned long [nombre];
  else data = ∅;
  for (i = 0; i < nombre; i++) data[i] = nouveau[i];
  if (ancien ≠ ∅) delete [ ] ancien ;
}
```

A.4.9. Ceci nous donne les opérations de copie et d'égalité usuels :

```
bitstring : :bitstring(const bitstring &a)
{
  init(0);
  copy(a);
}
bitstring bitstring : :operator=(const bitstring &a)
{
  copy(a);
  return (∗this);
}
```

A.4.10. La fonction suivante tronque la chaîne perdant éventuellement des données.

```
void bitstring : :setsize(long n)
{
  long i, ancienn, nouveaun ;
  unsigned long ∗ancien;
```

```
  if (n < 0)  n = 0;
  ancienn = nombre;
  ancien = data;
  size = n;
  nombre = (n + LB − 1)/LB;
  if (ancienn > nombre)  ancienn = nombre;
  init(n);
  for (i = 0; i < ancienn; i++)  data[i] = ancien[i];
  if (nombre > 0 ∧ size % LB ≠ 0)
    data[nombre − 1] &= #ffffffff ≫ (LB − size % LB);
  if (ancien ≠ ∅)  delete [] ancien;
}
```

A.4.11. L'opérateur d'adressage retourne comme annoncé une référence à un booléen du type **ref_bool**.

```
ref_bool bitstring ::operator [](long i)
{
  if (i ⩾ size ∨ i < 0)  {
    cerr ≪ "Index␣hors␣de␣portee\n";
    exit(1);
  }
  return (ref_bool(&data[i/LB], i % LB));
}
```

A.4.12. Pour la somme nous considérons qu'il s'agit d'un espace vectoriel sur $\mathbf{F}_2$. Il s'agit donc d'un ou exclusif. Notez que dans un tel espace addition et soustraction coïncident : tout élément est son propre opposé.

```
bitstring bitstring ::operator+(bitstring a)
{
  long n, i;
  bitstring aux;
  n = size;
  if (a.size > n)  n = a.size;
  aux.init(n);
  for (i = 0; i < nombre; i++)  aux.data[i] = data[i];
  for (i = 0; i < a.nombre; i++)
    aux.data[i] = (aux.data[i] | a.data[i]) & ∼(aux.data[i] & a.data[i]);
  return (aux);
}
bitstring bitstring ::operator+=(bitstring a)
{
  long n, i;
  n = size;
  if (a.size > n)  {
```

```
    n = a.size;
    setsize(n);
  }
  for (i = 0; i < a.nombre; i++)
    data[i] = (data[i] | a.data[i]) & ~(data[i] & a.data[i]);
  return (*this);
}
bitstring bitstring::operator-(bitstring a)
{
  return ((*this) + a);
}
bitstring bitstring::operator-()
{
  return (*this);
}
```

A.4.13. Les opérateurs de décalage viennent en deux variantes. L'une à usage interne, tronque éventuellement à droite et à gauche. L'opérateur proprement dit, à usage externe, augmente la taille dans les décalages vers la gauche.

```
bitstring bitstring::operator<<(long a)
{
  bitstring aux;
  long i, delta, r;
  unsigned long long t;
  if (a == 0) aux = *this;
  else if (a > 0) {
    aux.init(size + a);
    delta = a/LB;
    r = a % LB;
    if (aux.nombre > nombre + delta) {
      t = data[nombre - 1];
      t <<= r;
      aux.data[nombre + delta] = t >> LB;
    }
    for (i = nombre - 1; i > 0; i--) {
      t = (((long long) data[i]) << LB) + data[i - 1];
      t <<= r;
      aux.data[i + delta] = t >> LB;
    }
    t = data[0];
    t <<= r;
    aux.data[delta] = t;
  }
  return (aux);
```

```
}
void bitstring ::dolshift(long a)
{
  long i, delta, r;
  unsigned long long last;
  unsigned long long t;
  if (a > 0) {
    delta = a/LB;
    r = a % LB;
    if (nombre > delta) last = data[nombre - 1 - delta];
    for (i = nombre - 1; i > delta; i--) {
      t = last << LB;
      last = data[i - delta - 1];
      t += last;
      t <<= r;
      data[i] = t >> LB;
    }
    if (delta < nombre) {
      t = data[0];
      t <<= r;
      data[delta] = t;
    }
    for (i = 0; i < delta ∧ i < nombre; i++) data[i] = 0;
  }
}
bitstring bitstring ::operator<<=(long a)
{
  setsize(size + a);
  dolshift(a);
  return (*this);
}
bitstring bitstring ::operator>>(long a)
{
  bitstring aux;
  long i, delta, r, n;
  unsigned long long t;
  if (a ≡ 0) aux = *this;
  else if (a ⩾ size) aux.init(0);
  else if (a > 0) {
    aux.init(size - a);
    delta = a/LB;
    r = a % LB;
    t = data[nombre - 1];
    t >>= r;
```

```
      aux.data[nombre − 1 − delta] = t;
      for (i = nombre − 2; i ⩾ delta; i−−) {
        t = (((long long) data[i + 1]) ≪ LB) + data[i];
        t ≫= r;
        aux.data[i − delta] = t;
      }
    }
    return (aux);
  }
  void bitstring ::dorshift(long a)
  {
    long i, delta, r;
    unsigned long long last, next;
    unsigned long long t;
    if (a > 0) {
      delta = a/LB;
      r = a % LB;
      if (delta < nombre) last = data[delta];
      for (i = delta; i < nombre − 1; i++) {
        next = data[i + 1];
        t = next ≪ LB;
        t += last;
        last = next;
        t ≫= r;
        data[i − delta] = t;
      }
      if (delta < nombre) {
        t = data[nombre − 1];
        data[nombre − 1 − delta] = t ≫ r;
      }
      for (i = nombre − delta; i < nombre; i++) data[i] = 0;
    }
  }
  bitstring bitstring ::operator≫=(long a)
  {
    dorshift(a);
    setsize(size − a);
    return (∗this);
  }
```

A.4.14. Les tests d'égalités ne prennent pas la différence de taille en compte.

```
  bool bitstring ::operator≡(bitstring a)
  {
    bool aux;
```

```
  long i, n;
  aux = true;
  n = nombre;
  if (n > a.nombre) n = a.nombre;
  for (i = nombre − 1; i > n − 1 ∧ aux; i−−) aux = data[i] ≡ 0;
  for (i = a.nombre − 1; i > n − 1 ∧ aux; i−−) aux = a.data[i] ≡ 0;
  for (i = 0; i < n ∧ aux; i++) aux = data[i] ≡ a.data[i];
  return (aux);
}
bool bitstring : :operator≠(bitstring a)
{
  return (¬((∗this) ≡ a));
}
```

A.4.15. Nous terminons avec un opérateur pour les flux sortant, pour les tests.

```
ostream & operator≪(ostream & stream, bitstring a)
{
  long i;
  for (i = a.size − 1; i ⩾ 0; i−−) stream ≪ (a[i] ? "1" : "0");
  return (stream);
}
```

A.4.16. Polynômes sur $\mathbf{F}_2$.

La classe des polynômes sur $\mathbf{F}_2$ est dérivée de la précédente. Notons que cette classe n'ayant pas de données supplémentaires, les constructeurs reprennent ceux de **bitstring**.

```
class F2_pol : public bitstring {
public :
  F2_pol( ) : bitstring( ) { };
  F2_pol(long a) : bitstring(a) { };
  F2_pol(bool a) : bitstring(a) { };
  F2_pol(long a, bool b) : bitstring(a, b) { };
  F2_pol(const bitstring &a) : bitstring(a) { };
  F2_pol operator ∗ (F2_pol a);
  F2_pol operator/(F2_pol a);
  F2_pol operator%(F2_pol a);
  long degre( );
  F2_pol carre( );
  bool isprime( );
  friend ostream&operator≪(ostream & stream, F2_pol a);
};
```

A.4.17. Nous définissons le degré du polynôme :

```
long F2_pol ::degre()
{
  long aux;
  aux = size - 1;
  while (aux >= 0) {
    if (¬(*this)[aux]) aux--;
    else return (aux);
  }
  return (aux);
}
```

A.4.18. Les opérateurs supplémentaires pour ces polynômes sont la multiplication et les opérateurs donnés par la division euclidienne des polynômes. La multiplication utilise l'algorithme 3.5.3

```
F2_pol F2_pol ::operator * (F2_pol a)
{
  long i, last;
  F2_pol aux, t;
  t = *this;
  last = 0;
  t.setsize(degre() + a.degre() + 1);
  for (i = 0; i <= a.degre(); i++)
    if (a[i]) {
      t.dolshift(i - last);
      aux += t;
      last = i;
    }
  return (aux);
}
```

A.4.19. Pour la division euclidienne nous reprenons l'algorithme 3.5.15.

```
F2_pol F2_pol ::operator/(F2_pol a)
{
  F2_pol r, aux, t, x;
  long d = degre(), ad = a.degre(), last;
  if (ad < 0) {
    cerr << "Division par le polynome nul\n";
    exit(1);
  }
  r = (*this);
  if (d >= ad) {
    aux.init(d - ad);
```

```
    t.init(d);
    t = a ≪ (d − ad);
    x.init(d − ad);
    x = F2_pol(1, 1) ≪ (d − ad);
    last = d;
  }
  while (d ⩾ ad) {
    t.dorshift(last − d);
    r += t;
    x.dorshift(last − d);
    aux += x;
    last = d;
    d = r.degre( );
  }
  return (aux);
}
F2_pol F2_pol ::operator%(F2_pol a)
{
  F2_pol aux, t;
  char c;
  long d = degre( ), ad = a.degre( ), last;
  if (ad < 0) {
    cerr ≪ "Division par le polynome nul\n";
    exit(1);
  }
  aux = (∗this);
  if (d ⩾ ad) {
    t.init(d);
    t = a ≪ (d − ad);
    last = d;
  }
  while (d ⩾ ad) {
    t.dorshift(last − d);
    aux += t;
    last = d;
    d = aux.degre( );
  }
  aux.setsize(ad);
  return (aux);
}
```

A.4.20. Pour le carré, nous utilisons le fait que le Frobenius est un morphisme d'anneaux.

```
F2_pol F2_pol ::carre( )
{
```

```
  long i, n;
  F2_pol aux;
  n = degre();
  aux.init(2 * n + 1);
  for (i = 0; i ⩽ n; i++) aux[2 * i] = (*this)[i];
  return (aux);
}
F2_pol carre(F2_pol a)
{
  return (a.carre());
}
```

A.4.21. Pour le calcul de puissance, nous devons définir une fonction inverse.

```
bool inversible(F2_pol a)
{
  return (a.degre() ≡ 0);
}
F2_pol inverse(F2_pol a)
{
  if (inversible(a)) return (a);
  else {
    cerr ≪ "polynome␣sur␣F_2␣non␣inversible\n";
    exit(1);
  }
}
```

A.4.22. Puis nous donnons un opérateur pour les flux de sortie pour les essais.

```
ostream & operator≪(ostream & stream, F2_pol a)
{
  long i;
  bool first = true;
  for (i = a.size − 1; i ⩾ 0; i−−)
    if (a[i]) {
      if (¬first) stream ≪ "+";
      if (i ≡ 0) stream ≪ "1";
      else if (i ≡ 1) stream ≪ "T";
      else stream ≪ "T^" ≪ i;
      first = false;
    }
  if (first) stream ≪ "0";
  return (stream);
}
```

A.4.23. La dernière fonction teste si le polynôme P est premier en utilisant l'algorithme 6.5.6.

```
bool F2_pol ::isprime()
{
  long i, j, l, m;
  F2_pol T(1,1), P, Q, one;
  bool aux = true;
  l = degre();
  P = T;
  one = 1_L;
  m = 1;
  for (i = 1; i <= l ∧ aux; i++) {
    P = P.carre() % (*this);
    if (i * i <= l ∧ l % i ≡ 0 ∧ pgcd(i,m) ≡ 1) {
      Q = P + T;
      aux = pgcd((*this), Q) ≡ one;
      m *= i;
    }
    if (i ≡ l) {
      Q = P + T;
      aux = Q ≡ 0_L;
    }
  }
  return (aux);
}
```

A.4.24. Pour terminer, donnons un exemple élémentaire de calcul :

```
void test_isprime(F2_pol P)
{
  cout << P << (P.isprime() ? " est premier" : " est decomposable") << "\n";
}
void test_F2_pol()
{
  F2_pol P, T;
  long i;
  T = F2_pol(1,1);
  P = T;
  P = puissance(T,8) + puissance(T,4) + T*T*T + T + 1_L;
  test_isprime(P);
  for (i = 1; i < 8; i++) {
    P = (T << 7) + (T << (i-1)) + 1_L;
    test_isprime(P);
  }
  P = F2_pol(397,1) + F2_pol(12,1) + F2_pol(7,1) + F2_pol(6,1) + 1_L;
```

```
    test_isprime(P);
}
```

APPENDICE B

B.1. Annales d'examen

U.J.F. (Grenoble I) DESS Cryptologie 2002/2003

Examens du 4 octobre 2002

Durée totale : 2 heures

Calculatrices non autorisées

Il sera tenu compte de la clarté des justifications données. Tous les exercices sont indépendants les uns des autres.

Module A1A

- Exercice 1 -

1. Effectuer la division euclidienne de $3T^4 + 8T^3 + 2T^2 + T + 2$ par $3T^2 + 2T + 1$ dans $\mathbf{Q}[T]$.
2. Effectuer la division euclidienne de $2T^4 - 8T^3 + 5T^2 - 4T + 2$ par $T^2 - 3T - 1$ dans $\mathbf{Z}[T]$.
3. Effectuer la division euclidienne de $3T^4 - 5T^3 + 3T^2 - 2T + 1$ par $T^2 + 2T - 1$ dans $\mathbf{Z}[T]$.

- Exercice 2 -

Soit A un anneau commutatif. Quel est le reste de la division euclidienne de $P(X, Y)$ par $Y - X$ dans l'anneau $A[X][Y]$, vu comme anneau de polynômes sur $A[X]$?

- Exercice 3 -

1. Quel est le dernier chiffre du nombre $(378\,753)^{2\,783}$?
2. Calculer le reste de la division par 11 de $(378\,755)^{2\,783}$?
3. Quel est le reste de la division par 9 de $(13\,571)^{1\,257}$?

- Exercice 4 -

Trouver un générateur des groupes $\mathbf{F}_5^\times$, $\mathbf{F}_7^\times$, $\mathbf{F}_{11}^\times$.

T.S.V.P.

- Exercice 5 -

Donner, en la justifiant, une description des corps $\mathbf{F}_{49}$, $\mathbf{F}_{121}$, $\mathbf{F}_{169}$.

- Exercice 6 -

Donner une description de $\mathbf{F}_4$ puis écrire la table d'addition et de multiplication pour ce corps.

- Exercice 7 -

1. À quelle condition $\mathbf{Z}/m\mathbf{Z}$ contient-il un élément d'ordre 3 ?
2. Montrer que T^2+T+1 est irréductible sur $\mathbf{F}_q$ si et seulement si $q \equiv 2 \pmod 3$.
3. Factoriser T^2+T+1 dans $\mathbf{F}_3[T]$.
4. Montrer que si $q \equiv 1 \pmod 3$, alors le cardinal de l'ensemble des cubes dans $\mathbf{F}_q$:

$$\mathbf{F}_q^3 = \{\, x^3, x \in \mathbf{F}_q \,\}$$

est égal à $(q+2)/3$.
5. Donner une construction de $\mathbf{F}_{13^3}$.

Module A1B

- Exercice 1 -

On considère la courbe E sur $\mathbf{F}_5$ d'équation affine

$$Y^2 = X^3 - X$$

1. Donner l'équation de la courbe projective $\widetilde{E}$ associée. La courbe $\widetilde{E}$ est-elle non-singulière ?

On pose $0 = (0 : 1 : 0)$.

2. Donner tous les éléments de $\widetilde{E}(\mathbf{F}_5)$.

3. A quel groupe $\widetilde{E}(\mathbf{F}_5)$ est-il isomorphe ?

- Exercice 2 -

1. Si E est une courbe elliptique sur $\mathbf{F}_7$, donner une majoration du nombre de points de $E(\mathbf{F}_7)$.

On considère la courbe E sur $\mathbf{F}_7$ d'équation affine

$$Y^2 = X^3 + 1$$

2. Donner l'équation de la courbe projective $\widetilde{E}$ associée. La courbe $\widetilde{E}$ est-elle non-singulière ?

En pose $0 = (0 : 1 : 0)$.

3. Donner tous les éléments de $\widetilde{E}(\mathbf{F}_7)$.

4. Calculer la multiplicité d'intersection de la courbe avec sa tangente en le point M de coordonnées homogènes $(0 : 1 : 1)$. Calculer $(M.M)$. En déduire l'ordre de M.

5. Construire un isomorphisme de groupes

$$(\mathbf{Z}/2\mathbf{Z})^2 \times \mathbf{Z}/3\mathbf{Z} \to \widetilde{E}(\mathbf{F}_7)$$

en précisant l'image de $(1, 0, 0)$, $(0, 1, 0)$ et $(0, 0, 1)$.

- Exercice 3 -

Soit $\mathbf{K}$ un corps de caractéristique différente de 2 et de 3. Soit $\overline{\mathbf{K}}$ une clôture algébrique de $\mathbf{K}$. On considère la courbe C sur $\mathbf{K}$ d'équation affine

$$Y^2 = X^3$$

1. Donner l'équation de la courbe projective $\widetilde{C}$ associée.

2. Quels sont les points à l'infini de $\widetilde{C}$?

3. Quels sont les points singuliers de $\widetilde{C}$?

4. On considère la droite projective D_p d'équation $Y = pX$ avec $p \in \overline{\mathbf{K}}$. Donner les coordonnées des points d'intersection de D avec $\widetilde{C}$.

T.S.V.P.

5. En déduire un morphisme $\psi : \mathbf{P}^1(\overline{\mathbf{K}}) \to \widetilde{C}$ envoyant $(0:1)$ sur $(0:1:0)$ qu'on explicitera.
6. Que peut-on dire de $\mathbf{P}^1(\overline{\mathbf{K}})$ et $\widetilde{C}$?
7. On note $0 = (0:1:0)$ et $\widetilde{C}_0$ l'ensembles des points non-singuliers de $\widetilde{C}$. Déterminer $\psi^{-1}(\psi(a:1) + \psi(b:1))$. (Indication : On pourra se placer dans le plan affine $\overline{\mathbf{K}}^2$ vu comme $\{\,(x:1:t) \in \mathbf{P}^2(\overline{\mathbf{K}})\,\}$ et écrire $T = pX + q$ l'équation d'une droite passant par des points $M_1 = (x_1:1:t_1)$ et $M_2 = (x_2:1:t_2)$. On pourra également poser $(x_3:1:t_3) = (M_1.M_2)$ et $(x_4:1:t_4) = M_1 + M_2$.)
8. A quel groupe $(\widetilde{C}_0(\overline{\mathbf{K}}), +)$ est-il isomorphe ?

BIBLIOGRAPHIE

[ABV] D. W. Ash, I. F. Blake, and S. A. Vanstone, *Low complexity bases*, Discrete Appl. Math. **25** (1989), 191–210.

[Ca] J. W. S. Cassels, *Lectures on elliptic curves*, London math. society student texts, vol. 24, Cambridge university press, Cambridge, 1991.

[Co] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Math., vol. 138, Springer-Verlag, Berlin, Heidelberg and New York, 1993.

[DH] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Trans. Information Theory **22** (1976), n° 6, 644–654.

[EG] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Trans. Inform. Theory **31** (1985), n° 4, 469–472.

[IEEE] IEEE, *Standard specifications for public key cryptography*, Tech. Report P1363, IEEE Standards Department, 1999.

[Kn] A. W. Knapp, *Elliptic curves*, Math. notes, vol. 40, Princeton university press, Princeton, 1993.

[KL] D. E. Knuth and S. Levy, *The CWEB System of structured documentation*, Addison Wesley, Baltimore, 1994.

[Me] A. Meyer, *Illustrations*, Science et Vie Junior, Dossier Hors Série **53** (2002), 85.

[MOV] R. C. Mullin, I. M. Onyszchuk, and S. A. Vanstone, *Optimal normal basis in* $GF(p^n)$, Discrete Appl. Math. **22** (1988), n° 2, 149–161.

[Per] D. Perrin, *Cours d'algèbre*, ENS, Paris, 1988.

[RDO] E. Ramis, C. Deschamps, et J. Odoux, *Cours de mathématiques spéciales 1. Algèbre*, Masson, Paris, 1985.

[RSA] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems.*, Comm. ACM **21** (1978), n° 2, 120–126.

[Se] J.-P. Serre, *Cours d'arithmétique*, Le mathématicien, PUF, Paris, 1988.

Glossaire

$\mathbf{Z}$: anneau des entiers 8
$\mathbf{N}$: entiers positifs ou nuls 8
$\mathbf{Q}$: nombres rationnels 8
$\mathbf{R}$: nombres réels 8
$\mathbf{C}$: nombres complexes 8
$\sharp X$: cardinal de X 8
$|a|$: valeur absolue de a 8
$a \mid b$: a divise b 8
$a\mathbf{Z}$: multiples de l'entier a 8
$\mathscr{P}$: ensemble des nombres premiers 8
$a\%b$: reste de la division euclidienne 8
$a \equiv b \pmod m$: a congru à b modulo m . . . 11
$\overline{x}$: classe d'équivalence de x 12
$E/\mathscr{R}$: quotient de E pour la relation d'équivalence $\mathscr{R}$ 12
$\mathbf{Z}/n\mathbf{Z}$: entiers modulo n 13
G^X : applications de X vers G 17
$\mathfrak{S}_X$: groupe des permutations de X 17
$\mathfrak{S}_n$: groupe des permutations de $\{1, \ldots, n\}$ 17
$\langle X \rangle$: sous-groupe engendré par X 18
$\mathrm{Ker}(\phi)$: Noyau de ϕ 18
$\mathrm{Im}(\phi)$: Image de ϕ 18
G/H : classes à gauche 18
$(G : H)$: Indice de H dans G 19
$H \lhd G$: sous groupe distingué 20
$\mathrm{ord}(g)$: ordre de g 20
G_{p^∞} : composante p-primaire 22
$A^\times$: éléments inversibles de A 26
$\mathscr{M}_{m,n}(A)$: matrices $m \times n$ 27
$\mathscr{M}_n(A)$: $\mathscr{M}_{n,n}(A)$ 28
$\mathrm{car}(A)$: caractéristique de A 28
$\mathrm{Fr}(A)$: Corps des fractions de A 28
$B[X]$: sous-anneau engendré par $B \cup X$. . . . 29
$\mathbf{K}(X)$: sous-corps engendré par X 29
$\mathbf{K}(x_1, \ldots, x_n)$: sous corps engendré par les x_i 29
$(x_1, x_2, \ldots, x_n)$: idéal engendré 30
$\sum_{i=1}^n I_i$: somme des idéaux I_i 30
$a \sim b$: a et b sont associés 31
pgcd : plus grand commun diviseur 32
ppcm : plus petit commun multiple 32
$A[T]$: anneau de polynômes 32
$\deg(P)$: degré de P. 33
$\mathbf{K}(T)$: corps des fractions rationnelles 33
$A[[T]]$: séries formelles sur A 36
$v_0(F)$: ordre de F 36
$P(Q) = P \circ Q$: série formelle composée . . . 37
$A[T_1, \ldots, T_n]$: polynômes à n variables . . . 37
$T^{\boldsymbol{\alpha}}$: le produit $\prod_{i=1}^n T_i^{\alpha_i}$ 37
$\frac{\partial P}{\partial T_i}$: dérivée partielle de P. 37
$\mathscr{I}$: système de représentants des irréductibles de A 41
φ : fonction indicatrice d'Euler 44
$\mathscr{L}(M, N)$: applications linéaires de M vers N 48
$E^\vee$: dual de E 48
$\dim E$: dimension de E 49
$(e_1^\vee, \ldots, e_n^\vee)$: base duale de $(e_1, \ldots, e_n)$ . . 49
$P_{\boldsymbol{e}}^{\boldsymbol{e}'}$: matrice de changement de bases de $\boldsymbol{e}$ à $\boldsymbol{e}'$ 50
$X^*(G)$: caractères de G 50
$\mathbf{L}/\mathbf{K}$: extension de corps 56
$\mathrm{Irr}_{\mathbf{K}}^{\alpha}(T)$: polynôme minimal de α sur $\mathbf{K}$ . . . 58
$\overline{\mathbf{K}}$: clôture algébrique de $\mathbf{K}$ 60
$\mu_n(\mathbf{K})$: racines n-ième de l'unité dans $\mathbf{K}$ . . 63
$\mu_n^*(\mathbf{K})$: racines primitives n-ièmes de l'unité 63
$\phi_n(T)$: n-ième polynôme cyclotomique 63
C_p^i : facteur binômial 65
$\mathbf{F}_q$: corps à $q = p^d$ éléments 65
$\mathbf{P}^n(K)$: espace projectif de dimension n sur $\mathbf{K}$ 90
$\mathbf{P}(E)$: ensemble des droites de E 90
$g(C)$: genre de la courbe C 101
$Z(V, T)$: série zêta associée à V 105
Δ : discriminant 110

INDEX

A

Algorithme
- addition mod n 14
- Bezout 40, 118
- division euclidienne 35, 125
- factorisation
  - de Berlekamp 84
  - de Cantor-Zassenhaus 81
  - de Cantor-Zassenhaus pour $\mathbf{F}_2$ 81
  - sans facteur carré 78
  - stratégie 77
  - suivant les dégrés 79
- inverse dans un quotient 131
- pgcd 117
- puissance 14, 116

Anneau 26
- commutatif 26
- de matrices 28
- de polynômes 32
- euclidien 38
- factoriel 41
- intègre 26
- morphisme 28
- nul 27
- principal 38
- produit 27
- quotient 29
- unifère 26

Application linéaire 48

Automorphisme 28

B

Base
- d'un espace vectoriel 49
- duale 49
- polynômiale 67

Base normale 85
- gaussienne 87
- optimale 86

Bezout 9, 39, 118

C

Caractéristique 28
- d'un corps 45

Caractère
- d'un groupe 50

Cardinal d'un sous-groupe 19

Clôture algébrique 60
- relative 59

Classe
- à droite 18
- à gauche 18

Classe d'équivalence 12

Coefficient dominant 33

Compléxité 86

Composante p-primaire 22

Congruence 11

Coordonnées
- de l'opposé sur une courbe elliptique 111
- de la somme sur une courbe elliptique . . . 111
- homogènes 90

Corps 26
- algébriquement clos 60
- de décomposition 61
- des fractions 28
- des fractions rationnelles en une variable . . 33
- parfait 76

Corps finis
- structure 65

Courbe
- elliptique 107
  - critère de lissité 110
  - loi de groupe 110
- non-singulière 99

Cryptographie
- El Gamal 73
- RSA 45

D

Décomposition en facteurs irréductibles . . 11, 41
Degré
  d'un polynôme 33
  total d'un polynôme 37
Degré de l'extension 56
Dérivée
  d'un polynôme 32
  partielle d'un polynôme 37
Dimension
  d'un espace projectif 90
  d'un espace vectoriel 49
Discriminant d'une courbe elliptique 110
Diviseur 8
  strict de 0 26
Divisibilité 31
  dans les entiers 8
Division euclidienne 34
  dans les entiers 8
Droite projective 90
Dual d'un espace vectoriel 48

E

Élément
  algébrique 58
  inversible 26
    dans un anneau de polynômes 34
  irréductible 31
  sans facteur carré 76
Éléments associés 31
Ensemble-quotient 12
Espace projectif 90
  dimension 90
  droite 90
  hyperplan 90
  sous-espace 90
Espace vectoriel 47
  dual 48
  sous-espace vectoriel 48
Euclide 10
Extension
  algébrique 59
  d'Artin-Schreier 72
  de corps 56
  de Kummer 70
  finie 56

F

Factorisation
  de Berlekamp 83
  de Cantor-Zassenhaus 80
  sans facteur carré 78
  suivant les degrés 79
Famille
  génératrice 48
  libre 48, 49
  presque-nulle 48
Fonction indicatrice d'Euler 44
Fonction zêta 105
Formule d'inversion de Fourier 52
Frobenius 65

G

Gauss 9, 40
Générateur d'un groupe 18
Genre
  d'une courbe 101
  d'une surface réelle 100
Groupe 16
  abélien 16
  commutatif 16
  courbe elliptique 110
  cyclique 18
  monogène 18
  produit 16
  quotient 20
  sous-groupe 17

H

Hilbert 90 . . . . . 71, 72
Homographie 96
Hyperplan
  à l'infini 91
  projectif 90

I

Idéal 29
  d'un anneau-quotient 30
  engendré 30
  maximal 30
  premier 30
  principal 38
Image
  d'un morphisme de groupes 18
Indice d'un sous-groupe 19
Interpolation de Lagrange 55
Inverse
  dans un anneau 26
  dans un groupe 16
  dans un quotient 40
Isomorphisme
  d'anneaux 28
  de corps 28
  de groupes 17

L
Legendre 69, 132
Lemme
d'Euclide 10, 39
de Gauss 9, 40
Logarithme discret 73
M
Matrice 27
de changement de bases 50
Module 47
sous-module 48
sur $\mathbf{Z}$ 47
Morphisme
d'anneaux 28
de A-modules 48
de corps 28
de groupes 17
Frobenius 65
Multiple 8, 31
Multiplicativité des degrés 56
Multiplicité d'intersection 101
N
Noyau
d'un morphisme de groupes 18
O
Ordre
d'un élément d'un groupe 20
Ordre d'une série formelle 36
P
pgcd 8, 32, 117
Point
non-singulier 99
singulier 99
point rationnel 93
Polynôme
cyclotomique 63
d'interpolation 55
dérivé 32
minimal 58
scindé 55
Polynômes 32
à n variables 37
unitaires 33
ppcm 8, 32
Premier 8
Produit
d'anneaux 27
de groupes 16
Propriété universelle des polynômes 33, 37
Q
Quotient
d'un anneau 29
d'un ensemble 12
d'un groupe 20
de $A[T]$ 35
R
Racine
d'un polynôme 54
primitive n-ième de l'unité 63
Racine n-ième de l'unité 63
Relation d'équivalence 12
Représentant d'une classe d'équivalence 12
Reste d'une division euclidienne 8
S
Série formelle 36
composée 37
ordre 36
Somme
d'idéaux 30
Sous-anneau 29
engendré 29
Sous-corps 29
engendré 29
premier 45
Sous-ensemble algébrique 92
de l'espace projectif 93
Sous-espace projectif 90
Sous-espace vectoriel 48
Sous-groupe 17
de $\mathbf{Z}$ 18
de $\mathbf{Z}/n\mathbf{Z}$ 21
distingué 20
d'un groupe-quotient 21
engendré 18
Sous-module 48
Stathme 38
Symbole de Legendre 69, 132
T
Théorème
d'Hilbert 90 additif 72
d'Hilbert 90 multiplicatif 71
de Bezout 9, 39
de Dedekind 71
des fonctions implicites 98
Topologie 94
de Zariski 94
fermé 94
ouvert 94
Transformée de Fourier
discrète 52
rapide 52
V
Valuation p-adique 41