Dernière édition : 26 novembre 2020

Notes prises par Téofil ADAMSKI

ALGÈBRE DE BASE ET THÉORIE DES NOMBRES

(ALGB)

Mark BAKER

M1 maths fonda Université de Rennes 1

Chapitre 1

RAPPELS SUR LES GROUPES ET LES ANNEAUX, CRITÈRES DE PRIMALITÉ

1.1 RAPPELS SUR LES GROUPES

THÉORÈME 1.1 (LAGRANGE). Soient G un groupe fini et $H < G$. Alors l'ordre de H divise celui de G.

DÉFINITION 1.2. Soit G un groupe. Un sous-groupe $H < G$ est *normal* (ou *distingué*) si

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

On note alors $H \triangleleft G$.

▷ EXEMPLES. – Si $f\colon G \to G'$ est un morphisme de groupes, alors son noyau $\operatorname{Ker} f < G$ est normal.
– Si G est un groupe abélien, alors tout sous-groupe de G est normal.

DÉFINITION-PROPOSITION 1.3. Soient G un groupe et $H < G$. On note G/H l'ensemble des classes $\{gH \mid g \in G\}$. Si H est normal, alors G/H est un groupe.

▷ EXEMPLE. Pour $n \geqslant 1$, l'ensemble $n\mathbf{Z}$ est un sous-groupe normal de $\mathbf{Z}$, donc le quotient $\mathbf{Z}/n\mathbf{Z}$ est un groupe.

THÉORÈME 1.4. Soit $\varphi\colon G \to G'$ un morphisme de groupes surjectif. On note $N := \operatorname{Ker}\varphi$. Alors $N \triangleleft G$ et l'application $\overline{\varphi}\colon G/N \to G'$ donnée par $\overline{\varphi}(gN) = \varphi(g)$ pour tout $g \in G$ est un isomorphisme.

NOTATION. Lorsque deux groupes G et G' sont isomorphes, on note $G \cong G'$.

▷ EXEMPLES. – L'application $x \in \mathbf{R} \longmapsto e^{2i\pi x} \in \mathbf{S}^1$ est un morphisme de groupes surjectif de noyau $\mathbf{Z}$, donc les groupes $\mathbf{R}/\mathbf{Z}$ et $\mathbf{S}^1$ sont isomorphes (et même homéomorphe).
– Le groupe $\mathbf{C}/\mathbf{Z}$ est homéomorphe à un cylindre, lui-même homéomorphe à $\mathbf{S}^1 \times \mathbf{R}$.
– On considère $\mathrm{GL}_n(\mathbf{C})$. L'application $\det\colon \mathrm{GL}_n(\mathbf{C}) \to \mathbf{C}^*$ est un homéomorphisme surjectif de noyau $\mathrm{SL}_n(\mathbf{C})$. On en déduit $\mathrm{GL}_n(\mathbf{C})/\mathrm{SL}_n(\mathbf{C}) \cong \mathbf{C}^*$.

THÉORÈME 1.5 (de structure des groupes abéliens finis). Soit G un groupe abélien fini. Alors il existe des nombres premiers $p_1, \ldots, p_k \in \mathbf{N}^*$ et des entiers $e_1, \ldots, e_k, p \in \mathbf{N}$ tels que

$$G \cong \frac{\mathbf{Z}}{p_1^{e_1}\mathbf{Z}} \times \cdots \times \frac{\mathbf{Z}}{p_k^{e_k}\mathbf{Z}} \times \mathbf{Z}^p.$$

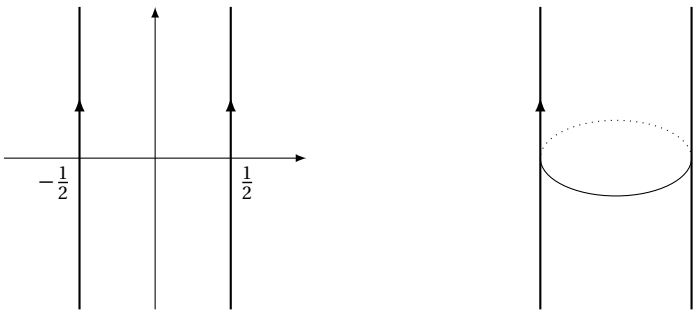


FIGURE 1.1 – Représentations du cylindre $\mathbf{C}/\mathbf{Z}$

1.2 RAPPELS SUR LES ANNEAUX

IMPORTANT. Dans la suite du cours, tous les anneaux sont supposés commutatifs, sauf éventuellement les anneaux de matrices.

▷ EXEMPLE. Pour tout anneau A, il existe un unique morphisme d'anneaux $\varphi\colon \mathbf{Z} \to A$ donné par

$$\varphi(n) = \begin{cases} n \cdot 1_A & \text{si } n \geqslant 0, \\ -(-n \cdot 1_A) & \text{sinon,} \end{cases} \qquad n \in \mathbf{Z}.$$

THÉORÈME 1.6. Soit $f\colon A \to B$ un morphisme d'anneaux surjectifs. Alors le noyau $\operatorname{Ker} f$ est un idéal de A et l'application $f\colon A/\operatorname{Ker} f \to B$ donnée par $\overline{f}(a + \operatorname{Ker} f) = f(a)$ pour tout $a \in A$ est un isomorphisme d'anneaux.

▷ EXEMPLES. – En considérant le morphisme d'anneaux $P \in \mathbf{R}[X] \longmapsto P(i) \in \mathbf{C}$, on obtient $\mathbf{R}[X]/\langle X^2+1\rangle \cong C$.
– On a $\mathbf{Z}[i]/\langle 1+3i\rangle \cong 10\mathbf{Z}$.

1.3 CRITÈRE DE PRIMALITÉ

THÉORÈME 1.7 (petit théorème de FERMAT). Soit $n \geqslant 1$ un entier. S'il existe $a \geqslant 1$ tel que $a^{n-1} \not\equiv 1 \mod p$, alors n n'est pas premier.

Un tel entier $a \in \mathbf{N}$ s'appelle un témoin de FERMAT de non-primalité de n.

LEMME 1.8. Soient $n \geqslant 1$ et $a \in [\![1, n]\!]$ des entiers premiers entre eux, *i. e.* $a \notin (\mathbf{Z}/n\mathbf{Z})^\times$. Alors l'entier a est un témoin de FERMAT de n

Ceci montrer que les éléments de $\mathbf{Z}/n\mathbf{Z} \setminus (\mathbf{Z}/n\mathbf{Z})^\times$ sont des témoins de FERMAT de n. Mais le test des éléments de $(\mathbf{Z}/n\mathbf{Z})^\times$ est rendu plus compliqué par l'existence des nombres de CARMICHAEL.

DÉFINITION 1.9. Un nombre de CARMICHAEL est un entier $n \geqslant 2$ non premier vérifiant $a^{n-1} \equiv 1 \mod n$ pour tout $a \in [\![2, n]\!]$ tel que $\operatorname{pgcd}(a, n) = 1$.

PROPOSITION 1.10. Soit $n \geqslant 2$ un nombre non premier. S'il n'est pas de CARMICHAEL, alors il y a au moins la moitié des nombres de $[\![1, n-1]\!]$ qui sont des témoins de FERMAT de n.

Preuve Comme n n'est pas de CARMICHAEL, il existe $a \in (\mathbf{Z}/n\mathbf{Z})^\times$ tel que $a^{n-1} \not\equiv 1 \mod n$. Or l'ensemble

$$\{a \in (\mathbf{Z}/n\mathbf{Z})^\times \mid a^{n-1} = 1\}$$

est un sous-groupe de $(\mathbf{Z}/n\mathbf{Z})^\times$, donc c'est un sous-groupe stricte, donc son cardinal est inférieur à $\frac{1}{2}\sharp(\mathbf{Z}/n\mathbf{Z})^\times$. Alors au moins la moitié des éléménts de $(\mathbf{Z}/n\mathbf{Z})^\times$ sont des témoins de FERMAT de n □

PRINCIPE DE MILLER-RABIN. Soient $n \geqslant 0$ un entier impair et $a \geqslant 1$ un entier tels que $\operatorname{pgcd}(a, n) = 1$.

1. Si $a^{n-1} \not\equiv \mod n$, alors l'entier n n'est pas premier d'après le théorème de FERMAT.
2. Supposons $a^{n-1} \equiv \mod n$. Alors n est impair, donc $n-1$ est pair, donc $a^{(n-1)/2}$ vérifie $x^2 - 1 \equiv 0 \mod n$. Si n est premier, alors $a^{(n-1)/2} \equiv \pm 1 \mod n$. Donc $a^{n-1} \equiv 1 \mod n$ et $a^{(n-1)/2} \not\equiv \pm 1 \mod n$ impliquent que n n'est pas premier.
3. Si $a^{(n-1)/2} \equiv -1 \mod n$, alors on abandonne. Si $a^{(n-1)/2} \equiv 1 \mod n$, alors $(n-1)/2$ est pair et on recommande l'étape 2. Si $a^{(n-1)/2} \equiv 1 \mod n$ et $a^{(n-1)/4} \not\equiv \pm 1 \mod n$, alors n n'est pas premier.

DÉFINITION 1.11. Soit $n \geqslant 2$ un entier. Un témoin de non-primalité de MILLER-RABIN est un entier $a \in [\![1, n-1]\!]$ vérifiant une des deux conditions suivantes :
– $a^{n-1} \not\equiv 1 \mod n$;
– il existe $k \geqslant 0$ tel que $2^{k+1} \mid n-1$ et $a^{(n-1)/2^k} \equiv 1 \mod n$ et $a^{(n-1)/2^{k+1}} \not\equiv \pm 1 \ [n]$.

THÉORÈME 1.12. Soit $n \geqslant 2$ un entier impair. S'il n'est pas premier, alors au moins trois quarts des entiers de l'ensemble $[\![1, n-1]\!]$ sont des témoins de non-primalité de MILLER-RABIN.

Chapitre 2
CORPS

2.1 EXTENSION DE CORPS

DÉFINITION 2.1. Une *extension* d'un corps K est un corps E tel que

(i) on ait $K \subset E$;

(ii) le corps K soit un sous-corps de E.

DÉFINITION 2.2. Une extension E d'un corps K est dite *finie* si sa dimension en tant que K-espace vectoriel est finie. La quantité $[E : K] := \dim_K E$ est appelée le *degré* de l'extension E de K.

PROPOSITION 2.3 (base télescopique). Soient K, L et E trois corps tels que $K \subset L \subset E$. Soient $(e_i)_{i\in I}$ une base du K-espace vectoriel L et $(f_j)_{j\in J}$ une base du L-espace vectoriel E. Alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base du K-espace vectoriel E. De plus, si les degrés sont finis, on a

$$[E : K] = [E : L][L : K].$$

DÉFINITION 2.4. Soient K un corps, E une extension de K et $\alpha \in E$. On note

– $K[\alpha]$ le sous-anneau de E engendré par K et α ;

– $K(\alpha)$ le sous-corps de E engendré par K et α.

On dit l'élément α est *algébrique* sur K s'il existe un polynôme non nul $P \in K[X]$ tel que $P(\alpha) = 0$. Dans le cas contraire, il est dit *transcendant* sur K.

◇ REMARQUE. Le corps $K(\alpha)$ est le corps des fractions de $K[\alpha]$.

LEMME 2.5. Soit K un corps. Alors tout élément d'une extension finie $K \subset E$ est algébrique sur K.

Preuve Soit $\alpha \in E$. On note $d := [E : K] < +\infty$. Alors les éléments $1, \alpha, \ldots, \alpha^d$ sont linéairement indépendants, donc il existe des éléments $a_0, \ldots, a_d \in K$ non tous nuls tels que $a_0 + \cdots + a_d\alpha^d = 0$. Cela montre que l'élément α est algébrique sur K. □

LEMME 2.6. Soient K un corps, E un extension de K et $\alpha_1, \ldots, \alpha_n \in K$. Alors $K[\alpha_1, \ldots, \alpha_n] = K(\alpha_1, \ldots, \alpha_n)$.

Preuve Il suffit de montrer que chaque élément non nul de l'anneau $B := K[\alpha_1, \ldots, \alpha_n]$ est inversible. On remarque que l'application

$$\theta_a : \left| \begin{array}{l} B \longrightarrow B, \\ x \longmapsto ax \end{array} \right.$$

est une transformation K-linéaire. Comme B est intègre, l'application θ_a est injective. Comme $\dim_K B < +\infty$, il s'agit d'un isomorphisme. Ainsi il existe un unique élément $b \in B$ tel que $ab = 1$. □

PROPOSITION 2.7. Soient K un corps, E un extension de K et $\alpha \in E$ un élément algébrique sur K. Alors il existe un unique polynôme $M \in K[X]$ irréductible et unitaire tel que $M(\alpha) = 0$. Un tel polynôme M est appelé le *polynôme minimal* de α sur K.

Preuve On considère le morphisme d'évaluation

$$h_\alpha : \left| \begin{array}{l} K[X] \longrightarrow E, \\ P \longmapsto P(\alpha). \end{array} \right.$$

Alors son noyau est un idéal de $K[X]$ et donc engendré par un unique polynôme unitaire $M \in K[X]$. De plus, ce dernier est irréductible car le quotient $K[X]/\langle M\rangle \cong \operatorname{Im} h_\alpha \subset E$ est intègre. □

PROPOSITION 2.8. Soient K un corps, E un extension de K et $\alpha \in E$ un élément algébrique sur K de polynôme minimal $M \in K[X]$. On note $n := \deg M$. Alors

1. on a $K(\alpha) \cong K[X]/\langle M\rangle$;
2. la famille $(1, \alpha, \dots, \alpha^{n-1})$ est une base du K-espace vectoriel $K[\alpha]$;
3. on a $[K(\alpha) : K] = n$;
4. on a $K[a] = K(\alpha)$.

Preuve 1. Le proposition ci-dessus assure $K[X]/\langle M\rangle \cong \operatorname{Im} h_\alpha = K[\alpha]$ qui est un corps, donc $K(\alpha) = K[a]$.
2. La preuve de ce point utilise principalement la division euclidienne. □

▷ EXEMPLES. – Comme $\sqrt{2}$ est algébrique sur $\mathbf{Q}$ de polynôme minimal $X^2 - 2$, on a

$$[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2.$$

– On considère $\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}, \sqrt{3})$. On veut montrer ue $\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\sqrt{2}, \sqrt{3})$ avec

$$[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}(\sqrt{2})] = 2 \qquad (*)$$

auquel cas on aura

$$[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}] = 4.$$

Montrons l'égalité $(*)$. Puisque $X^2 - 3$ annule $\sqrt{3}$, on a $[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}(\sqrt{2})] \in \{1, 2\}$. Raisonnons par l'absurde et supposons $[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}(\sqrt{2})] = 1$. Alors le polynôme $X^2 - 3$ est réductible dans $\mathbf{Q}(\sqrt{2})$, c'est-à-dire $\pm\sqrt{3} \in \mathbf{Q}(\sqrt{2})$. Ainsi il existe $a, b \in \mathbf{Q}$ tel que $\sqrt{3} = a + b\sqrt{2}$. En élevant au carré, on obtient $3 = a^2 + 2b^2 + 2ab\sqrt{2}$ et donc $\sqrt{2} \in \mathbf{Q}$ ce qui est absurde. On en déduit l'égalité $(*)$.

2.2 CORPS DE RUPTURE, CORPS DE DÉCOMPOSITION

POSITIONNEMENT DU PROBLÈME. Soit K un corps. On veut résoudre les deux problèmes suivants :
– étant donné un polynôme $P \in K[X]$ irréductible et de degré $d > 1$, on veut construire une extension de K dans laquelle P admet une racine ;
– étant donné un polynôme $P \in K[X]$, on veut construire une extension de K dans laquelle on peut décomposer P est en produit de facteurs de degré 1.

DÉFINITION 2.9. Soit $P \in K[X]$ un polynôme irréductible de degré $d > 1$. Une extension L de K est un *corps de rupture* de P sur K s'il existe une racine $\alpha \in L$ de P telle que $L = K[\alpha]$.

▷ EXEMPLES. – Le corps $\mathbf{C}$ est le corps de rupture de $X^2 + 1$ sur $\mathbf{R}$.
– Le corps $\mathbf{Q}(i)$ est le corps de rupture de $X^2 + 1$ sur $\mathbf{Q}$.
– le corps $\mathbf{Q}(\sqrt[3]{2})$ est un corps de rupture de $X^3 - 2$ sur $\mathbf{Q}$.

THÉORÈME 2.10. Soit $P \in K[X]$ un polynôme irréductible. Alors il existe un corps de rupture L de P sur K. De plus, ce corps L est unique à K-isomorphisme près.

Preuve • *Existence.* Posons $L := K[X]/\langle P\rangle$. Comme P est irréductible, le quotient L est un corps. De plus, le corps K s'injecte naturellement dans L, donc on considère L comme une extension de K. Enfin, si on note $\alpha \in L$ la classe de X dans L, alors $P(\alpha) = 0$ et $L = K[\alpha] = K(\alpha)$. Donc le corps L convient.
• *Unicité.* Soit L' un autre corps de rupture de P sur K. Alors il existe $\beta \in L'$ tel que $P(\beta) = 0$ et $L' = K[\beta]$. D'après la construction de L et L', il existe des isomorphismes $\varphi : K[X]/\langle P\rangle \longrightarrow K[\alpha]$ et $\psi : K[X]/\langle P\rangle \longrightarrow K[\beta]$. Alors le morphisme $\psi \circ \varphi^{-1} : L \longrightarrow L'$ est un isomorphisme. □

▷ EXEMPLE. Le polynôme $X^2 - 2$ est irréductibles dans $\mathbf{Q}[X]$ possédant trois racines α_i (pour $i \in \{1, 2, 3\}$), donc les corps $\mathbf{Q}(\alpha_i)$ sont ceux de ruptures de $X^3 - 2$ et ils sont tous isomorphes par les $\mathbf{Q}$-isomorphismes $\mathbf{Q}(\alpha_i) \longrightarrow \mathbf{Q}(\alpha_j)$ envoyant α_i sur α_j.

DÉFINITION 2.11. Soit $P \in K[X]$ un polynôme. Une extension L de K est un *corps de décomposition* de P sur K si vérifie les deux conditions suivantes :

(i) le polynôme P est scindé dans $L[X]$;

(ii) le corps L est engendré sur K par les racines de P.

THÉORÈME 2.12. Soit $P \in K[X]$ un polynôme. Alors il existe un corps de décomposition L de P sur K. De plus, ce corps L est unique à K-isomorphisme près.

Preuve L'unicité est laissée à titre d'exercice. Montrons l'existence. Soit $Q \in K[X]$ un facteur irréductible de P de degré supérieur ou égal à 2. Dans $L_1 := K[X]/\langle P\rangle$, il existe un polynôme $P_1 \in L[X]$ et $x_1 \in L$ tels que $P = (X - x_1)P_1$ et $\deg P_1 < \deg P$. En répétant ce processus, on obtient un corps L contenant toutes les racines $x_1, \ldots, x_d$ de P et tel que ce dernier soit scindé sur L. En fait, on a $L = K[x_1, \ldots, x_d]$. □

▷ EXEMPLES. – Trouvons le corps de décomposition du polynôme $X^4 - 2$ sur $\mathbf{Q}$. Les quatre racines de ce polynôme sont $\pm\sqrt[4]{2}$ et $\pm i\sqrt[4]{2}$. Donc son corps de rupture est $\mathbf{Q}(\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}) \cong \mathbf{Q}(\sqrt[4]{2}, i)$.

– De même, pour le polynôme $X^3 - 2$ sur $\mathbf{Q}$, son corps de rupture est

$$\mathbf{Q}(\sqrt[3]{2}, \sqrt[3]{2}j, \sqrt[3]{2}j^2) \cong \mathbf{Q}(\sqrt[3]{2}, j) \quad \text{avec} \quad j := e^{2i\pi/3}.$$

EXERCICE 2.1. Calculer les degrés $[\mathbf{Q}(\sqrt[4]{2}, i) : \mathbf{Q}]$ et $[\mathbf{Q}(\sqrt[3]{2}, j) : \mathbf{Q}]$.

2.3 CORPS FINIS

2.3.1 Préliminaire

DÉFINITION 2.13. Soit K un corps.

– Le *sous-corps premier* de K est le plus petit sous-contenant 1, *i. e.* c'est l'image de l'unique morphisme de $\mathbf{Z}$ dans K. Il s'agit de $\mathbf{Q}$ ou de $\mathbf{Z}/p\mathbf{Z}$ pour un nombre premier p.

– La *caractéristique* de K est soit p si son sous-corps premier est $\mathbf{Z}/p\mathbf{Z}$ soit 0 si son sous-corps premiers est $\mathbf{Q}$. On note $\mathrm{car}(K)$ sa caractéristique.

◇ REMARQUE. Si le corps K est fini, alors son sous-corps premier est $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$ et donc $\mathrm{car}(K) = p$.

PROPOSITION 2.14. Soit K un corps fini de caractéristique p. Alors il existe $n \geqslant 1$ tel que $|K| = p^n$.

Preuve Comme le corps est fini, le corps $\mathbf{F}_p$ est un sous-corps de K, donc le corps K est un $\mathbf{F}_p$-espace vectoriel. On a alors $|K| = p^n$ où $n := [K : \mathbf{F}_p]$. □

PROPOSITION 2.15. Soient K un corps et $\theta : K \to K$ un morphisme de corps. Alors l'ensemble $\mathrm{Fix}(\theta) \subset K$ des points fixes de θ est un sous-corps de K.

DÉFINITION-PROPOSITION 2.16. Soit K un corps de caractéristique $p > 0$. Alors l'application

$$\varphi : \left| \begin{array}{l} K \longrightarrow K, \\ x \longmapsto x^p \end{array} \right.$$

est un morphisme de corps, appelé *morphisme de* FROBENIUS. De plus, il s'agit d'un automorphisme de K si le corps K est fini. Pour $n \geqslant 1$, on note $\varphi^n : K \to K$ la composée n fois de φ par lui-même et alors l'ensemble $\mathrm{Fix}(\varphi^n)$ est l'ensemble des racines du polynôme $X^{p^n} - X$ dans K.

2.3.2 Propriétés des corps finis

THÉORÈME 2.17. Soient p un nombre premier et $n > 0$ un entier. Alors il existe un corps de cardinal $q := p^n$, unique à $\mathbf{F}_p$-isomorphisme près, on le note $\mathbf{F}_q$. C'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbf{F}_p$.

◇ REMARQUE. Attention, le notation $\mathbf{F}_q$ désigne l'unique corps, à $\mathbf{F}_p$-isomorphisme près, possédant q éléments et pas l'ensemble $\mathbf{Z}/q\mathbf{Z}$ qui n'est pas un corps.

Preuve • *Unicité.* Soit K un corps de cardinal q. Alors c'est le corps de décomposition du polynôme $X^q - X$ car tout élément de K est racine de ce polynôme (le neutre 0 est bien racine et cela se montre facilement en utilisant le théorème de LAGRANGE pour les éléments de $K^\times$) qui admet au plus q racines. Donc le corps K est le corps de décomposition du polynôme $X^q - X$ sur $\mathbf{F}_p$ et, de ce fait, il est unique à $\mathbf{F}_p$-isomorphisme près.

• *Existence.* Tout d'abord, remarquons que le polynôme $X^q - 1$ a des racines simples dans toute extension de $\mathbf{F}_p$. En effet, son polynôme dérivé $qX^{q-1} - 1 = -1$ est constant, donc il ne peut pas avoir de racines multiples.

On sait que le corps de décomposition K du polynôme $X^q - X$ sur $\mathbf{F}_p$ existe et qu'il est unique à $\mathbf{F}_p$-isomorphisme près. Montrons que $|K| = q$. Mais on sait que les racines de $X^q - X$ sont distinctes dans K et que l'ensemble des q-racines de $X^q - X$ est un sous-corps $K' \subset K$ de cardinal q puisque $K' = \mathrm{Fix}(\varphi^n)$. Comme $K' \subset K$ et le corps K' contient les racines du polynôme $X^q - X$, le corps K' est le corps de décomposition. Finalement, on en déduit $K = K'$ et $|K| = q$. □

THÉORÈME 2.18. Soit K un corps fini. Alors le groupe $K^\times$ est cyclique.

Preuve Comme le groupe $K^\times$ est abélien d'ordre fini, le théorème de structure assure qu'il existe une isomorphie

$$K^\times \cong \mathbf{Z}/p_1^{e_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p_k^{e_k}\mathbf{Z}$$

pour des nombres premiers p_i et des entiers $e_i \geqslant 1$. Si les nombres p_i sont distincts, alors le théorème des restes chinois assure

$$K^\times \cong \mathbf{Z}/(p_1^{e_1} \cdots p_k^{e_k})\mathbf{Z}$$

qui est cyclique. Raisonnons par l'absurde et supposons qu'il existe $i, j \in [\![1, k]\!]$ tels que $i \neq j$ et $p := p_i = p_j$. Quitte à renuméroter les nombres p_i, on suppose $i = 1$ et $j = 2$. Alors

$$K^\times \cong \mathbf{Z}/p^{e_1}\mathbf{Z} \times \mathbf{Z}/p^{e_2}\mathbf{Z} \times \mathbf{Z}/p_3^{e_3}\mathbf{Z} \times \cdots \times \mathbf{Z}/p_k^{e_k}\mathbf{Z}.$$

Mais le groupe $\mathbf{Z}/p^{e_1}\mathbf{Z} \times \mathbf{Z}/p^{e_2}\mathbf{Z}$ contient plus de p éléments d'ordre p et ceci n'est pas possible car ces éléments sont racines du polynômes $X^p - 1 \in K[X]$ qui admet au plus p racines dans K. Ainsi les nombres p_i sont distincts et on se ramène au cas précédent. D'où le théorème. □

◇ REMARQUES. – En général, le groupe $(\mathbf{Z}/n\mathbf{Z})^\times$ pour un entier $n \geqslant 1$ quelconque n'est pas cyclique. Par exemple, on a $(\mathbf{Z}/12\mathbf{Z})^\times \cong (\mathbf{Z}/2\mathbf{Z})^2$.

– Ce théorème donne $\mathbf{F}_q^\times \cong (\mathbf{Z}/(q-1)\mathbf{Z}, +)$. Cependant, cette isomorphisme est dur à expliciter.

2.3.3 Construction des corps $\mathbf{F}_p$

RAPPEL. Soient p un nombre premier et $P \in \mathbf{F}_p[X]$ un polynôme irréductible de degré $n \geqslant 1$. On a vu que le quotient $\mathbf{F}_p[X]/\langle P\rangle$ est un corps fini d'ordre p^n.

THÉORÈME 2.19. Soient $n \geqslant 1$ un entier et K un corps fini d'ordre p^n. Alors il existe un polynôme $P \in \mathbf{F}_p[X]$ irréductible, unitaire et de degré n tel que

$$K \cong \mathbf{F}_p[X]/\langle P\rangle.$$

Preuve Soit $\gamma \in K^\times$ un générateur du groupe cyclique $K^\times$. On considère le morphisme d'évaluation

$$h_\gamma : \left| \begin{array}{l} \mathbf{F}_p[X] \longrightarrow K, \\ \qquad P \longmapsto P(\gamma) \end{array} \right.$$

qui est surjectif. Le théorème d'isomorphisme assure

$$K \cong \mathbf{F}_p[X]/\operatorname{Ker} h_\gamma.$$

Par ailleurs, comme K est un corps, le noyau $\operatorname{Ker} h_\gamma \subset \mathbf{F}_p[X]$ est un idéal maximal. Comme $\mathbf{F}_p[X]$ est principal, il existe un polynôme $P \in \mathbf{F}_p[X]$ irréductible et unitaire tel que $\operatorname{Ker} h_\gamma = \langle P\rangle$. Ceci termine la preuve. □

COROLLAIRE 2.20. Soit $n \geqslant 1$ un entier. Alors il existe un polynôme de $\mathbf{F}_p[X]$ qui est irréductible et de degré n.

2.3.4 Plongements

LEMME 2.21. Soit K un corps et $m, n \geqslant 1$ deux entiers. Alors $X^n - 1 \mid X^m - 1$ dans $K[X]$ si et seulement si $n \mid m$.

Preuve Il suffit d'effectuer la division euclidienne de m par n et de travailler dans le quotient $K[X]/\langle X^n - 1\rangle$. □

THÉORÈME 2.22. Soient $k, \ell \geqslant 1$ deux entiers. Alors le corps $\mathbf{F}_{p^k}$ est un sous-corps de $\mathbf{F}_{p^\ell}$ si et seulement si $k \mid \ell$. Dans ce cas, on a

$$[\mathbf{F}_{p^\ell} : \mathbf{F}_{p^k}] = \ell/k.$$

Preuve $\Rightarrow$ On suppose que le corps $\mathbf{F}_{p^k}$ est un sous-corps de $\mathbf{F}_{p^\ell}$. Alors le corps $\mathbf{F}_{p^\ell}$ est un $\mathbf{F}_{p^k}$-espace vectoriel de dimension $d \geqslant 1$. On en déduit $p^\ell = (p^k)^d = p^{kd}$, donc $k \mid \ell$.

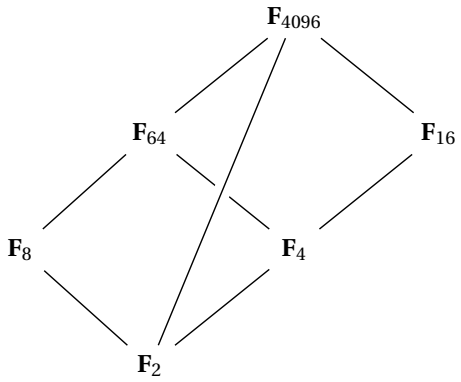
$\Leftarrow$ Réciproquement, on suppose $k \mid \ell$. Soit K un corps d'ordre p^ℓ. Alors c'est le corps de décomposition du polynôme $X^{p^\ell} - X$. Si $X^{p_k} - X \mid X^{p^\ell} - X$, alors il contient toutes les p^k racines du polynôme $X^{p^k} - X$ et ses racines forment une sous-corps $K' \subset K$ de cardinal p^k.

Il suffit alors de montrer $X^{p_k} - X \mid X^{p^\ell} - X$. Avec le lemme précédent, on a les équivalences

$$\begin{aligned} X^{p_k} - X \mid X^{p^\ell} - X &\iff X^{p_k-1} - 1 \mid X^{p^\ell-1} - 1 \\ &\iff p^k - 1 \mid p^\ell - 1 \\ &\iff k \mid \ell. \end{aligned}$$

Ceci permet de conclure. □

▷ EXEMPLES. Considérons le corps $\mathbf{F}_{4096}$. On remarque que $4096 = 2^{12}$ et les diviseurs de 12 sont 1, 2, 3, 4, 6, 12, donc les sous-corps de $\mathbf{F}_{4096}$ sont $\mathbf{F}_2$, $\mathbf{F}_4$, $\mathbf{F}_8$, $\mathbf{F}_{16}$, $\mathbf{F}_{64}$ et $\mathbf{F}_{4096}$.



2.4 POLYNÔMES IRRÉDUCTIBLES

2.4.1 Polynômes irréductibles sur $\mathbf{F}_p$

Pour un entier $d \geqslant 1$, on note $\mathscr{P}_d \subset \mathbf{F}_p[X]$ l'ensemble des polynômes irréductibles et unitaires de degré d à coefficients dans $\mathbf{F}_p$ et on pose $S_d := \prod_{P \in \mathscr{P}_d} P$.

THÉORÈME 2.23. Soit $n \geqslant 1$ un entier. Alors

$$X^{p^n} - 1 = \prod_{d \mid n} S_d.$$

Preuve Tout d'abord, remarquons que le polynôme $X^{p^n} - X$ admet uniquement des racines simples dans toute extension de $\mathbf{F}_p$ car son polynôme dérivé est constant dans $\mathbf{F}_p[X]$. Montrons maintenant le lemme suivant.

LEMME 2.24. Soit $A \in \mathbf{F}_p[X]$ un polynôme irréductible et unitaire de degré $d \geqslant 1$. Alors $A \mid X^{p^n} - X$ si et seulement si $d \mid n$.

Preuve $\Leftarrow$ On suppose $d \mid n$. Le corps $K := \mathbf{F}_p[X]/\langle P \rangle \cong \mathbf{F}_{p^d}$ est un corps de rupture de A sur $\mathbf{F}_p$. Puisque $d \mid n$, on a $\mathbf{F}_{p^d} \subset \mathbf{F}_{p^n}$. Le corps $\mathbf{F}_{p^n}$ étant un corps de décomposition de $P := X^{p^n} - X$ dans $\mathbf{F}_p$, la classe $\alpha \in K$ de X dans K est une racine de P. Maintenant, en faisant une division euclidienne de P par A et en évaluant en α, on montre que $A \mid P$.

$\Rightarrow$ Réciproquement, on suppose $A \mid P$. Alors la classe α est une racine de A et, comme $A \mid P$, c'est aussi une racine de P. Puisque $\mathbf{F}_{p^n}$ contient $\mathbf{F}_p$ et α, on a $\mathbf{F}_{p^d} \subset \mathbf{F}_{p^n}$ car $\mathbf{F}_{p^d} \cong K = \mathbf{F}_p(\alpha)$. D'où $d \mid n$. □

Ceci conclut la preuve. □

▷ EXEMPLE. Montrons que le polynôme $P := X^2 + X + 1 \in \mathbf{F}_p[X]$ est irréductible sur $\mathbf{F}_p$ lorsque $p \equiv 2 \mod 3$. On suppose $p \equiv 2 \mod 3$. Il suffit de montrer qu'il ne possède pas de facteur linéaire, *i. e.* il ne possède pas de racines dans $\mathbf{F}_p$. Raisonnons par l'absurde et supposons qu'il ait une racine $\alpha \in \mathbf{F}_p$. Alors $\alpha^3 = 1$ car $X^3 = (X-1)P$. De plus, comme $P(1) \neq 1$, on a $\alpha \neq 1$, donc $\alpha \in \mathbf{F}_p^\times$ et $o(\alpha) = 3$. Ceci est absurde car $3 \nmid p - 1 = |\mathbf{F}_p^\times|$.

2.4.2 Polynômes irréductibles sur Q ou Z

DÉFINITION 2.25. Un *corps de nombre* est une extension finie de $\mathbf{Q}$.

PROPOSITION 2.26. 1. Pour tout corps de nombre K, on a $\mathbf{Q} \subset K \subset \mathbf{C}$.
2. Pour tout entier $n > 0$, il existe un corps de nombres d'indice n dans $\mathbf{Q}$.

Preuve Pour le point 2, il suffit de considérer le corps $\mathbf{Q}[X]/\langle X^n + 2\rangle$ car le polynôme $X^n + 2$ est irréductible. □

THÉORÈME 2.27. Soit K un corps de nombre. Alors il existe $\alpha \in K$ tel que $K = \mathbf{Q}(\alpha)$.

Preuve Voir le polycopié de Tobias SCHMIDT (théorème 3.3.1). □

THÉORÈME 2.28. Soit K un corps de nombre. Alors il existe un polynôme irréductible $P \in \mathbf{Q}[X]$ de degré $[K : \mathbf{Q}]$ tel que $K \cong \mathbf{Q}[X]/\langle P\rangle$.

Preuve Soit $\alpha \in K$ un élément tel que $K = \mathbf{Q}(\alpha)$. Le morphisme d'évaluation

$$\left|\begin{array}{l}\mathbf{Q}[X] \longrightarrow K,\\ \quad S \longmapsto S(\alpha)\end{array}\right.$$

est surjectif et, comme $\mathbf{Q}[X]$ est principal, son noyau est engendré par un polynôme irréductible $P \in \mathbf{Q}[X]$. Le théorème d'isomorphisme donne alors $K \cong \mathbf{Q}[X]/\langle P\rangle$ qui est de degré $[K : \mathbf{Q}] = \deg P$. □

2.4.3 Critère d'EISENSTEIN

THÉORÈME 2.29 (EISENSTEIN). Soient $P := a_n X^n + \cdots + a_0 \in \mathbf{Z}[X]$ un polynôme et p un nombre premier tels que
(i) $p \nmid a_n$,
(ii) $p \mid a_i$ pour tout $i \in [\![0, n-1]\!]$;
(iii) $p^2 \nmid a_0$.
Alors le polynôme P est irréductible dans $\mathbf{Q}[X]$. De plus, si $\operatorname{pgcd}(a_1, \ldots, a_n) = 1$, alors il est irréductible dans $\mathbf{Z}[X]$.

▷ EXEMPLE. En prenant $p = 3$, le polynôme $2X^2 + 3X + 3$ est irréductible dans $\mathbf{Q}[X]$ et $\mathbf{Z}[X]$.

Preuve On le réduit modulo p et on obtient un polynôme $\overline{P} \in \mathbf{F}_p[X]$. Les conditions (i) et (ii) donne $\overline{P} = \overline{a_n} X$ avec $\overline{a_n} \neq 0$. Raisonnons par l'absurde et supposons qu'il soit réductible dans $\mathbf{Q}[X]$. Alors il existe $R, S \in \mathbf{Z}[X]$ tel que $P = RS$. Alors les polynômes $\overline{R}$ et $\overline{S}$ divisent $\overline{P}$ dans $\mathbf{F}_p[X]$, donc ce sont des monômes. On en déduit que tous les coefficients de R et S, sauf les coefficients dominants, sont divisibles par p. Soient $b_0, c_0 \in \mathbf{Z}$ les termes constants de R et S. Alors $a_0 = b_0 c_0$, donc $p^2 \mid a_0$ ce qui contredit la condition (iii). Donc le polynôme P est irréductible dans $\mathbf{Q}[X]$. □

2.4.4 Polynômes cyclotomiques

Soit $n \geqslant 1$. On considère $\mu_n \subset \mathbf{C}^*$ le groupe multiplicatif des racines n-ième de l'unité. Une racine $\zeta \in \mu_n$ est dite *primitive* si $\zeta^k \neq 1$ pour tout $k \in [\![1, k-1]\!]$. Le groupe des racines primitives est

$$\mu_n^\times = \{e^{2i\pi k/n} \mid k \in [\![1, n]\!], \operatorname{pgcd}(k, n) = 1\}$$

qui est donc de cardinal $\varphi(n)$. Le *n-ième polynôme cyclotomique* est le polynôme unitaire

$$\Phi_n := \prod_{\zeta \in \mu_n^\times} (X - \zeta).$$

▷ EXEMPLES. On a
– $\Phi_1 = X - 1$,
– $\Phi_2 = X + 1$,
– $\Phi_3 = X^2 + X + 1$,
– $\Phi_4 = X^2 + 1$.

PROPOSITION 2.30. On a

$$X^n - 1 = \prod_{d \mid n} \Phi_d \quad \text{et} \quad \Phi_n \in \mathbf{Z}[X].$$

Preuve La première égalité résulte du fait

$$\mu_n = \bigsqcup_{d|n} \mu_d^\times.$$

En effet, l'inclusion $\supset$ est claire. Réciproquement, soit $\zeta \in \mu_n$. Alors le théorème de LAGRANGE assure que l'ordre de ζ divise n. Par ailleurs, on a $\zeta \in \mu^\times_{o(\zeta)}$. Cela montre l'autre inclusion.

Par récurrence, montrons que le polynôme Φ_n est à coefficients entiers pour tout $n \geqslant 1$. L'initialisation est évidente. Soit $n \geqslant 2$. Supposons que $\Phi_d \in \mathbf{Z}[X]$ pour tout $d < n$. Alors $X^n - 1 = \Phi_n A$ où le polynôme

$$A := \prod_{\substack{d|n \\ d<n}} \Phi_d$$

est unitaire et à coefficients entiers. On peut alors en déduire que le polynôme Φ_n est à coefficients entiers. □

THÉORÈME 2.31. Le polynôme Φ_n est irréductible dans $\mathbf{Q}[X]$.

COROLLAIRE 2.32. 1. Le polynôme Φ_n est irréductible dans $\mathbf{Z}[X]$ car il est unitaire.

2. Soit $\zeta \in \mu_n^\times$. Alors le polynôme Φ_n est le polynôme minimal de ζ sur $\mathbf{Q}$. On en déduit $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \varphi(n)$. Ainsi le corps $\mathbf{Q}(\zeta)$ est le corps de décomposition de Φ_n.

2.5 RÉCIPROCITÉ QUADRATIQUE

2.5.1 Congruence quadratique

Soit p un nombre premier. On considère les congruences quadratiques de la forme $X^2 \equiv a \mod p$ pour un entier $a \in \mathbf{Z}$. Si $a = 0$, alors l'équation admet une solution $X \equiv 0$. Si $p \nmid a$, alors elle admet soit deux solutions soit aucun solution modula p.

DÉFINITION 2.33. On dit qu'un entier $a \in \mathbf{Z}$ est un *résidu quadratique modulo p* si l'équation $X^2 \equiv a \mod p$ admet une solution dans $\mathbf{Z}$.

THÉORÈME 2.34 (critère d'EULER). Soit $a \in \mathbf{Z}$ un entier premier avec p. Alors

1. l'entier a est un résidu quadratique modulo p si $a^{(p-1)/2} \equiv 1 \mod p$;
2. l'entier a est un non-résidu quadratique modulo p si $a^{(p-1)/2} \equiv -1 \mod p$.

Preuve Puisque les résidus et les non-résidus sont calculés modulo p, il suffit de considérer les éléments inversibles de $\mathbf{F}_p$. Notons que chaque élément de $\mathbf{F}_p^\times$ est soit un résidu soit un non-résidu. Montrons que $\mathbf{F}_p^\times$ est partagé en $(p-1)/2$ résidus et $(p-1)/2$ non résidus. Pour cela, considérons le morphisme

$$\theta : \begin{vmatrix} \mathbf{F}_p^\times \longrightarrow \mathbf{F}_p^\times, \\ x \longmapsto x^2. \end{vmatrix}$$

Son image est l'ensemble des résidus quadratiques et son noyau est réduit à ± 1. Comme $|\mathbf{F}_p^\times| = |\mathrm{Ker}\,\theta|\,|\mathrm{Im}\,\theta|$, on en déduit que $\mathbf{F}_p^\times$ contient $(p-1)/2$ résidus quadratique et autant de non-résidus quadratiques.

D'après le théorème de FERMAT, tous les éléments de $\mathbf{F}_p^\times$ sont racines du polynôme $X^{p-1} - 1$. Or dans $\mathbf{F}_p[X]$, on a $X^{p-1} - 1 = (X^{(p-1)/2} - 1)(X^{(p-1)/2} + 1)$. Ainsi, parmi les $p-1$ éléments de $\mathbf{F}_p^\times$, la moitié vérifie $X^{(p-1)/2} - 1 = 0$ et l'autre moitié vérifie $X^{(p-1)/2} + 1 = 0$. Et on remarque que cette première moitié sont les résidus quadratiques. □

2.5.2 Symbole de LEGENDRE

DÉFINITION 2.35. Soit $a \in \mathbf{Z}$. On définit le *symbole de* LEGENDRE associé au couple (a, p) la quantité

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \equiv 0 \mod p, \\ 1 & \text{si } a \text{ est un carré modulo } p, \\ -1 & \text{sinon} \end{cases}$$

Autrement dit, cette quantité vaut 1 (respectivement -1) si l'entier a est un (non-)résidu quadratique modulo p.

PROPOSITION 2.36. Soient $a, b \in \mathbf{Z}$. Alors

1. si $a \equiv b \mod p$, alors $(\frac{a}{p}) = (\frac{b}{p})$;

2. si $\text{pgcd}(a,p)=1$, alors $(\frac{a^2}{p})=1$;
3. si $p>0$, alors $(\frac{a}{p}) \equiv a^{(p-1)/2} \mod p$;
4. si $\text{pgcd}(a,p)=\text{pgcd}(b,p)=1$, alors $(\frac{ab}{p})=(\frac{a}{p})(\frac{b}{p})$

THÉORÈME 2.37 (de la réciprocité quadratique). Soient p et q deux nombres premiers impairs. Alors
1. $(\frac{-1}{p})=(-1)^{(p-1)/2}$, *i. e.* -1 est un résidu quadratique modulo p si et seulement si $p \equiv 1 \mod 4$;
2. $(\frac{2}{p})=(-1)^{(p^2-1)/8}$, *i. e.* 2 est un résidu quadratique modulo p si et seulement si $p \equiv \pm 1 \mod 8$;
3. $(\frac{p}{q})(\frac{q}{p})=(-1)^{(p-1)/2\cdot(q-1)/2}$.

◇ REMARQUE. Les points 1 et 2 s'appellent les lois complémentaires. Dû à GAUSS, le point 3 s'appelle la loi de la réciprocité quadratique. Ces trois lois permettent de calculer les résidus quadratiques modulo p.

▷ EXEMPLES. – L'équation $X^2 \equiv 17 \mod 97$ n'admet pas de solution car $(\frac{17}{97})=-1$.

– L'équation $X^2 \equiv 85 \ [17]$ admet des solutions car, comme $(\frac{17}{97})=-1$ et $(\frac{5}{97})=(\frac{97}{5})=(\frac{2}{5})=-1$, on a

$$\left(\frac{85}{97}\right)=\left(\frac{17\times 5}{97}\right)=\left(\frac{17}{97}\right)\left(\frac{5}{97}\right)=1.$$

– Calculer $(\frac{34}{71})$. Comme $71 \equiv 7 \mod 8$, la deuxième loi donne $(\frac{2}{71})=1$. De plus, on a

$$\left(\frac{17}{71}\right)=\left(\frac{71}{17}\right)=\left(\frac{3}{17}\right)=\left(\frac{17}{3}\right)=\left(\frac{-1}{3}\right)=-1.$$

D'où $(\frac{34}{71})=-1$.

Preuve du point 1 du théorème 2.37 D'après le critère d'EULER et comme p est impair, on a

$$\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2} \mod p=(-1)^{(p-1)/2}. \qquad \square$$

Preuve du point 2 du théorème 2.37 D'abord, on remarque que l'élément 2 est un résidu quadratique modulo p si et seulement si le polynôme X^2-1 admet une solution dans $\mathbf{F}_p^\times$ si et seulement si il est réductible sur $\mathbf{F}_p$. Ainsi l'élément 2 est un non-résidu quadratique modulo p si et seulement si le polynôme X^2-2 est irréductible sur $\mathbf{F}_p$. Comme $\mathbf{F}_{p^2} \cong \mathbf{F}_p[X]/\langle X^2-2\rangle$ est un corps de rupture pour X^2-2, ce polynôme admet une racine dans $\mathbf{F}_{p^2}$. Donc l'élément 2 est un résidu (respectivement non-résidu) quadratique modulo p si et seulement si le polynôme X^2-2 admet une racine dans $\mathbf{F}_p$ (respectivement dans $\mathbf{F}_{p^2}\setminus\mathbf{F}_p$).

D'après le TD, le groupe $\mathbf{F}_{p^2}^\times$ contient un élément α d'ordre 8 tel que $\alpha^4=-1$. Il vérifie donc $\alpha^2=-\alpha^{-2}$. On considère alors l'élément $\beta=\alpha+\alpha^{-1}\in\mathbf{F}_{p^2}^\times$ qui vérifie $\beta^2=2$. Ainsi l'élément 2 est un carré si et seulement si $\beta\in\mathbf{F}_p^\times$. Or comme $\text{Fix}\,\varphi=\mathbf{F}_p$, on a

$$\begin{aligned}\beta\in\mathbf{F}_p &\iff \beta^p\equiv\beta \mod p\\ &\iff (\alpha+\alpha^{-1})^p\equiv\alpha+\alpha^{-1} \mod p.\end{aligned}$$

Comme p est premier impair, il est congru à 1, 3, 5 ou 7 modulo 8.

– Si $p\equiv\pm1 \mod 8$, alors $(\alpha+\alpha^{-1})^p=\alpha^p+\alpha^{-p}=\alpha+\alpha^{-1}$.

– Si $p\equiv\pm3 \mod 8$, alors $(\alpha+\alpha^{-1})^p=\alpha^p+\alpha^{-p}=-(\alpha+\alpha^{-1})\neq\alpha+\alpha^{-1}$. En effet, comme $\alpha^8=1$, on a $\alpha^4=-1$, donc $\alpha^3=-\alpha^{-1}$. Ceci permet d'écrire

$$\beta^3=(\alpha+\alpha^{-1})^3=\alpha^3+\alpha^{-3}=-(\alpha+\alpha^{-1})=-\beta.$$

On en conclut que l'élément 2 n'est pas un carré si $p\equiv3 \mod 8$. De même si $p\equiv-3 \mod 8$.

Ceci conclut le point 2. $\square$

CAS DE RÉSIDUS QUADRATIQUE MODULO $p_1\cdots p_k$. Soient $p_1,\ldots,p_k$ des nombres premiers deux à deux distincts. On note $n:=p_1\cdots p_k$. Le théorème des restes chinois assure

$$(\mathbf{Z}/n\mathbf{Z})^\times\cong(\mathbf{Z}/p_1\mathbf{Z})^\times\times\cdots\times(\mathbf{Z}/p_k\mathbf{Z})^\times.$$

Donc un élément $a\in(\mathbf{Z}/n\mathbf{Z})^\times$ est un carré si et seulement si c'est un carré modulo p_i pour tout $i\in[\![1,k]\!]$.

▷ EXEMPLES. L'entier 85 n'est pas un carré modulo $403 = 13 \times 31$. En effet, on a

$$\left(\frac{85}{13}\right) = \left(\frac{7}{13}\right) = \left(\frac{13}{7}\right) = \left(\frac{-1}{7}\right) = -1,$$
$$\left(\frac{85}{31}\right) = \left(\frac{23}{31}\right) = (-1)\left(\frac{31}{23}\right) = -\left(\frac{8}{23}\right) = -\left(\frac{2}{23}\right) = -1.$$

2.5.3 Preuve de la loi de réciprocité quadratique

Soient p et q deux nombres premiers. On souhaite montrer la loi de réciprocité quadratique

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2\cdot(q-1)/2}.$$

On pose $\zeta_p := e^{2i\pi/p}$ une racine p-ième de l'unité. La *somme quadratique de* GAUSS est la quantité

$$g_p := \sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\zeta_p^k.$$

Cette somme vérifie $g_p^2 = p^*$ en notant $p^* := (\frac{-1}{p})p$. Maintenant, avec le critère d'EULER, on a

$$g_p^{q-1} = (g_p^2)^{(q-1)/2} = (p^*)^{(q-1)/2)} \equiv \left(\frac{p^*}{q}\right) \mod q,$$

donc

$$g_p^q \equiv \left(\frac{p^*}{q}\right) g_p \mod q. \tag{1}$$

Par ailleurs, le théorème de FERMAT assure

$$g_p^q \equiv \sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\zeta_p^{qk} \mod q.$$

Soit $a \in \mathbf{F}_p^\times$ l'inverse de q modulo p. En effectuant le changement de variables $t = qk$, on a

$$g_p^q \equiv \left(\frac{a}{p}\right)\sum_{t=1}^{p-1}\left(\frac{t}{p}\right)\zeta_p^t \mod q.$$

Comme $aq \equiv 1 \mod p$, on a $(\frac{a}{p}) = (\frac{q}{p})$ et on obtient

$$g_p^q \equiv \left(\frac{q}{p}\right) g_p \mod q. \tag{2}$$

Avec les relations (1) et (2), on obtient

$$\left(\frac{p^*}{q}\right) g_p \equiv \left(\frac{q}{p}\right) g_p \mod q.$$

En multipliant par g_p et en utilisant $g_p^2 = p^2$, on trouve

$$\left(\frac{p^*}{q}\right) p^* \equiv \left(\frac{q}{p}\right) p^* \mod q.$$

Puisque p^* est inversible modulo q et que les symboles de LEGENDRE valent ± 1, on obtient

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

Enfin, on a

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) = \left(\frac{(\frac{-1}{p})p}{q}\right) = \left(\frac{(-1)^{(p-1)/2}}{q}\right)\left(\frac{p}{q}\right) = ((-1)^{(p-1)/2})^{(q-1)/2}\left(\frac{p}{q}\right).$$

Ceci montre la loi de réciprocité quadratique.

Chapitre 3

MODULE SUR UN ANNEAU

3.1 NOTION DE MODULE

3.1.1 Définition

DÉFINITION 3.1. Soit A un anneau commutatif. Un *A-module* est un groupe abélien $(M,+)$ muni du multiplication scalaire

$$\left|\begin{array}{l} A\times M\longrightarrow M,\\ (a,x)\longmapsto a\cdot x\end{array}\right.$$

vérifiant les quatre points suivants :

(i) pour tout $x\in M$, on a $1_A\cdot x=x$;

(ii) pour tous $a,b\in A$ et $x\in M$, on a $(ab)\cdot x=a\cdot(b\cdot x)$;

(iii) pour tous $a,b\in A$ et $x\in M$, on a $(a+b)\cdot x=a\cdot x+b\cdot x$;

(iv) pour tous $a\in A$ et $x,y\in M$, on a $a\cdot(x+y)=a\cdot x+a\cdot y$.

DÉFINITION 3.2. Un *sous-module* d'un module M est un sous-groupe de $(M,+)$ stable par multiplication par un scalaire.

▷ EXEMPLES. – Soit K un corps. Alors tout K-module est un K-espace vectoriel.
– Les notions de **Z**-module et de groupe abélien coïncident (où la multiplication scalaire est alors définie naturellement).
– Tout idéal de A est un A-module pour la multiplication dans A. En particulier, l'anneau A est un A-module.

3.1.2 Morphisme de modules

DÉFINITION 3.3. Soient M et N deux A-modules. Une application $f\colon M\longmapsto N$ est un *morphisme de A-module* lorsque

$$f(ax+by)=af(x)+bf(y),\quad \forall x,y\in M,\ \forall a,b\in A.$$

On note $\mathrm{Hom}_A(M,N)$ l'ensemble des morphismes de M dans N.

◇ REMARQUE. Comme pour les espaces vectoriels, on définit le noyau et l'image d'un morphisme de A-module.

▷ EXEMPLE. L'application

$$\left|\begin{array}{l}\mathbf{Z}\times\mathbf{Z}\longrightarrow\mathbf{Z}\times\mathbf{Z},\\ (m,n)\longmapsto(2m,3n)\end{array}\right.$$

est un morphisme de **Z**-module.

3.1.3 Module quotient

THÉORÈME 3.4. Soient M un A-module et N un sous-module de M. Alors le quotient M/N est un A-module par rapport à la multiplication scalaire

$$\left|\begin{array}{l} A\times M/N\longrightarrow M/N,\\ (a,m+N)\longmapsto am+N.\end{array}\right.$$

De plus, la projection canonique

$$\pi : \begin{vmatrix} M \longrightarrow M/N, \\ m \longmapsto m+N \end{vmatrix}$$

est un morphisme surjectif de A-module vérifiant $\operatorname{Ker}\pi = N$.

PROPOSITION 3.5 (propriété universelle du module quotient). Soient $f : M \longrightarrow P$ un morphisme de A-module et N un A-module tel que $N \subset \operatorname{Ker} f$. Alors il existe une unique morphisme $\overline{f} : M/N \longrightarrow P$ tel que $f = \overline{f} \circ \pi$.

PROPOSITION 3.6 (premier théorème d'isomorphisme). Soient M et Q deux A-modules et $f : M \longrightarrow Q$ un morphisme surjectif de A-module. Alors le morphisme $\overline{f} : M/\operatorname{Ker} f \longrightarrow Q$ est un isomorphisme de A-module.

THÉORÈME 3.7 (de correspondance). Il y a une bijection entre les sous-modules de M/N et les sous-modules de M contenant N.

3.1.4 Produit direct et somme directe de modules

DÉFINITION 3.8. Soit $(M_i)_{i\in I}$ une famille de A-modules.

– Le *produit direct* de cette famille est le produit cartésien $\prod_{i\in I} M_i$ munit des opérations termes à termes.

– La *somme directe* de cette famille est le sous-module de $\prod_{i\in I} M_i$, noté $\bigoplus_{i\in I} M_i$, composé des familles presque nulles $(x_i)_{i\in I}$ de ce produit.

– Pour un ensemble I, on note $A^{(I)} \coloneqq \bigoplus_{i\in I} M_i$ et $A^I \coloneqq \prod_{i\in I} M_i$.

– Si $I = [\![1, n]\!]$, on a $\prod_{i=1}^n M_i = \bigoplus_{i=1}^n M_i$ et on note $A^n \coloneqq \prod_{i=1}^n A_i$.

3.1.5 Modules libres

DÉFINITION 3.9. Soit M un A-module. On dit qu'une partie $S \subset M$ est *génératrice* si tout élément de M est une combinaison linéaire finie d'éléments de S. Dans ce cas, les éléments de S sont appelés des *générateurs* de M. De plus, cette partie S est *libre* si toute combinaison linéaire finie nulle a ses coefficients nuls. Enfin, cette partie S est une *base* si elle est génératrice et libre. Si le A-module M admet une base, on dit qu'il est *libre*.

▷ EXEMPLE. Pour tout $n \geqslant 2$, le $\mathbf{Z}$-module $\mathbf{Z}/n\mathbf{Z}$ n'est pas libre.

DÉFINITION 3.10. Soit I un ensemble. Le A-module libre $A^{(I)}$ est appelé le *A-module libre standard de base I*. Une base de celui-ci est la famille $(e_i)_{i\in I}$ où on a posé $e_i \coloneqq (\delta_{i,j})_{j\in I}$ pour tout $i \in I$.

PROPOSITION 3.11. Soient M un A-module et $S \coloneqq (x_i)_{i\in I}$ une famille de M. Alors il existe une unique morphisme de A-module $\phi_S : A^{(I)} \longrightarrow M$ tel que $\phi_S(e_i) = x_i$ pour tout $i \in I$. De plus, la famille S est

– génératrice si et seulement si l'application ϕ_S est surjective ;

– libre si et seulement si l'application ϕ_S est injective ;

– une base si et seulement si l'application ϕ_S est bijective.

◇ REMARQUE. Un A-module est donc libre si et seulement s'il est isomorphe à A-module $A^{(I)}$ pour un certain ensemble I.

PROPOSITION 3.12. Tout A-module est un quotient d'un A-module libre.

Preuve Soient M un A-module et $S \coloneqq (x_i)_{i\in I} \subset M$ une partie génératrice. Alors le morphisme ϕ_S est surjectif ce qui assure

$$M \cong A^{(I)}/\operatorname{Ker}\phi_S$$

où le A-module $A^{(I)}$ est libre. □

3.1.6 Module de type fini

DÉFINITION 3.13. Un A-module est de *type fini* s'il admet une partie génératrice finie.

PROPOSITION 3.14. Soient $r, s \geqslant 1$ deux entiers. Si $A^r \cong A^s$, alors $r = s$.

Preuve On suppose $A^r \cong A^s$. D'après le théorème de KRULL, il existe un idéal maximal $\mathfrak{m}$ de A. Considérons le sous-module $\mathfrak{m}A^r$. Soit $\theta\colon A^r \longrightarrow A^s$ un isomorphisme de A-modules. Puisque celui-ci est A-linéaire, on obtient donc $\theta(\mathfrak{m}A^r) = \mathfrak{m}A^s$. Ainsi il induit un isomorphisme $\overline{\theta}\colon A^r/\mathfrak{m}A^r \longrightarrow A^s/\mathfrak{m}A^s$. Maintenant, comme $\mathfrak{m}$ est un idéal, on a $\mathfrak{m}A^r = \mathfrak{m}^r$ et $\mathfrak{m}A^s = \mathfrak{m}^s$. De plus, le quotient $K := A/\mathfrak{m}$ est un corps tel que $A^r/\mathfrak{m}^r = K^r$ et $A^s/\mathfrak{m}^s = K^s$. Or l'application $\overline{\theta}\colon K^r \longrightarrow K^s$ est un isomorphisme de K-espace vectoriel. D'où $r = s$. □

DÉFINITION 3.15. On appelle *rang* d'un A-module de type fini l'unique entier $r \geqslant 0$ vérifiant $M \cong A^r$.

3.2 ALGÈBRE LINÉAIRE DANS UN MODULE

Soient M et N deux A-modules. On peut munir l'ensemble $\mathrm{Hom}_A(M,N)$ d'une structure de A-module de manière naturelle. On suppose que les modules M et N sont libres. Il existe des bases $(v_1,\dots,v_m)$ et $(w_1,\dots,w_n)$ de M et N pour lesquelles les applications

$$\phi\colon \left|\begin{array}{l} A^m \longrightarrow M, \\ e_i \longmapsto v_i \end{array}\right. \quad \text{et} \quad \psi\colon \left|\begin{array}{l} A^n \longrightarrow N, \\ e_i \longmapsto w_i \end{array}\right. \quad \text{avec} \quad e_i := (\delta_{i,j})_{j\in[\![1,m]\!]}$$

sont des isomorphismes.

Par rapport à ces bases, il y a des morphismes de A-modules entre l'ensemble des morphismes $\mathrm{Hom}_A(M,N)$ et l'ensemble des matrices $\mathscr{M}_{n,m}(A)$.

3.2.1 Matrice

Pour tout morphisme $f \in \mathrm{Hom}_A(M,N)$, on note $[f] \in \mathscr{M}_{n,m}(A)$ sa matrice dans les bases choisies. On peut également définir la notion de déterminant dans un A-module.

PROPOSITION 3.16. Une matrice de $\mathscr{M}_n(A)$ est inversible si et seulement si son déterminant est inversible.

PROPOSITION 3.17. Soient $B \in \mathscr{M}_n(A)$ et $f_B\colon A \longrightarrow A$ l'endomorphisme associé. Alors

1. l'endomorphisme f_B est surjectif si et seulement si $\det B \in A^\times$;
2. si $\det B$ n'est pas un diviseur de 0 dans A, alors f_B est injectif.

3.2.2 Réduction de matrice à coefficients entiers

On souhaite simplifier une matrice $B \in \mathscr{M}_{m,n}(\mathbf{Z})$ à l'aide des opérateurs élémentaires sur les lignes et les colonnes. Comme pour les matrices de $\mathscr{M}_{m,n}(K)$, cela revient à multiplier à multiplier à droite ou à gauche la matrice B par des matrices élémentaires. Pour $i \in [\![1,m]\!]$, $j \in [\![1,n]\!]$ et $s \in \mathbf{Z}$, en notant $E_{i,j}(s) := I_k + sE_{i,j}$, l'opération $L_i \longrightarrow L_i + sL_j$ correspond à la multiplication $E_{i,j}(s)B$ et l'opération $C_i \longrightarrow C_i + sC_j$ correspond à la multiplication $BE_{i,j}(s)$. De même, pour $i \in [\![1,k]\!]$, on note $E_{i,i}(-1) := I_n - 2E_{i,i} \in \mathrm{GL}_k(\mathbf{Z})$ et, on considérant les bonnes dimensions, les multiplications $E_{i,i}(-1)B$ et $BE_{i,i}(-1)$ correspondent à la multiplication de la ligne L_i ou de la colonne C_i par -1. Cela constituent les opérations élémentaires.

PROPOSITION 3.18. Toute suite d'opérations élémentaires sur les lignes et colonnes d'une matrice $B \in \mathscr{M}_{m,n}(\mathbf{Z})$ peut-être décrit sous la forme $B' = PBQ$ avec $P \in \mathrm{GL}_m(\mathbf{Z})$ et $Q \in \mathrm{GL}_n(\mathbf{Z})$.

Maintenant, pour un corps K, une matrice $B \in \mathscr{M}_{m,n}(K)$ peut se réduire sous la forme

$$B = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}.$$

Mais ceci n'est pas toujours possible lorsque les coefficients sont entiers. Par exemple, la matrice $(2) \in \mathscr{M}_1(\mathbf{Z})$ ne peut être réduite sous cette forme.

THÉORÈME 3.19 (forme normale de SMITH, dans $\mathbf{Z}$). Soit $B \in \mathscr{M}_{m,n}(\mathbf{Z})$. Alors il existe $P \in \mathrm{GL}_m(\mathbf{Z})$ et $Q \in \mathrm{GL}_n(\mathbf{Z})$

telles que

$$PBQ = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & \mathbf{0} \end{pmatrix}$$

où les entiers $d_1, \dots, d_r \in \mathbf{N}^*$ vérifient $d_1 \mid d_2 \mid \cdots \mid d_r$.

Idée de la preuve À l'aide des opérations élémentaires, on transforme la matrice B en une matrice de la forme

$$\begin{pmatrix} d_1 & 0 \\ 0 & M \end{pmatrix}$$

avec $M \in \mathscr{M}_{m-1,n-1}(\mathbf{Z})$ et l'entier d_1 divise tous les coefficients de M. On peut alors procéder par récurrence. □

▷ EXEMPLE. Trouver la forme de SMITH de la matrice

$$\begin{pmatrix} 6 & -8 \\ -4 & 10 \end{pmatrix}.$$

Tout d'abord (étape 1), on met en premiers coefficients un entier positif plus petit que tous les autres en valeurs absolues :

$$\begin{pmatrix} 6 & -8 \\ -4 & 10 \end{pmatrix} \xrightarrow{L_1 \leftrightarrow L_2} \begin{pmatrix} -4 & 10 \\ 6 & -8 \end{pmatrix} \xrightarrow{L_1 \to -L_1} \begin{pmatrix} 4 & -10 \\ 6 & -8 \end{pmatrix}.$$

Ensuite (étape 2), on effectue la division $a_{2,1} = a_{1,1}q + r$. Si $r = 0$, on remplace $a_{2,1}$ par 0 ce qui n'est ici pas le cas. Sinon on refait l'étape 1 et on a

$$\begin{pmatrix} 4 & -10 \\ 6 & -8 \end{pmatrix} \xrightarrow{L_2 \to L_2 - L_1} \begin{pmatrix} 4 & -10 \\ 2 & 2 \end{pmatrix} \xrightarrow{L_1 \leftrightarrow L_2} \begin{pmatrix} 2 & 2 \\ 4 & -10 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 2 \\ 0 & -14 \end{pmatrix}.$$

Maintenant, on refait la division et le reste est ici nul : on obtient

$$\begin{pmatrix} 2 & 2 \\ 0 & -14 \end{pmatrix} \xrightarrow{C_2 \to C_2 - C_1} \begin{pmatrix} 2 & 0 \\ 0 & -14 \end{pmatrix} \xrightarrow{C_2 \to -C_2} \begin{pmatrix} 2 & 0 \\ 0 & 14 \end{pmatrix}.$$

On a ici terminé. Cependant (étape 3), si jamais une coefficient b de B n'est pas divisible par $a_{1,1}$, on ajoute la colonne C_j à la colonne C_1 et on refait l'étape 2. Par exemple, on a

$$\begin{pmatrix} 2 & 0 \\ 0 & 5 \end{pmatrix} \xrightarrow{C_1 \to C_1 + C_2} \begin{pmatrix} 2 & 0 \\ 5 & 5 \end{pmatrix} \xrightarrow{L_2 \to L_2 - 2L_1} \begin{pmatrix} 2 & 0 \\ 1 & 5 \end{pmatrix}$$
$$\longrightarrow \begin{pmatrix} 1 & 5 \\ 2 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 5 \\ 0 & -10 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -10 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -10 \end{pmatrix}.$$

THÉORÈME 3.20 (forme normale de SMITH). Soient A un anneau principal et $B \in \mathscr{M}_{m,n}(A)$. Alors il existe deux matrices $P \in \mathrm{GL}_m(A)$ et $Q \in \mathrm{GL}_n(A)$ telles que

$$PBQ = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & \mathbf{0} \end{pmatrix}$$

où les entiers $d_1, \dots, d_r \in A \setminus \{0\}$ vérifient $d_1 \mid d_2 \mid \cdots \mid d_r$.

Preuve Si l'anneau A est euclidien, il suffit de remplacer, dans la preuve précédente, les utilisations de la valeur absolue par le stathme $\nu \colon A \longrightarrow \mathbf{N}$. Si l'anneau A n'est pas euclidien, alors on admet le théorème : le procédé n'est pas algorithmique. □

THÉORÈME 3.21. Soient M et N deux $\mathbf{Z}$-modules libre de type fini et $f \colon M \to N$ un morphisme. Alors il existe deux bases de M et N pour lesquelles la matrice de f soit diagonale.

Preuve Soit B la matrice de f dans des bases quelconques. D'après le théorème précédente, on peut trouver deux matrices $P \in \mathrm{GL}_m(A)$ et $Q \in \mathrm{GL}_n(A)$ telle que la matrice PBQ soit une forme normale de SMITH. Mais les matrices P et Q sont des matrices de changements de bases. D'où le résultat. □

3.2.3 Générateurs et relations les Z-modules

Soit M un $\mathbf{Z}$-module de type fini. On note $(v_1,\dots,v_m)$ une famille génératrice de M. Alors le morphisme

$$\phi:\left|\begin{array}{c}\mathbf{Z}^m\longrightarrow M,\\ (r_1,\dots,r_m)\longmapsto r_1v_1+\cdots+r_mv_m\end{array}\right.$$

est injectif. On en déduit $M\cong\mathbf{Z}^m/\operatorname{Ker}\phi$ et les éléments du noyau $\operatorname{Ker}\phi$ donnent les relations entre les éléments générateurs v_i. Par exemple, le $\mathbf{Z}$-module $\mathbf{Z}/4\mathbf{Z}\times\mathbf{Z}/12\mathbf{Z}$ est le sous-module de $\mathbf{Z}^2$ engendré par les éléments $v_1:=(1,0)$ et $v_2:=(0,1)$ dans lequel on impose les relations $4v_1=0$ et $12v_2=0$.

3.3 THÉORÈMES DE STRUCTURES

3.3.1 Théorème de la base adaptée

Soient M un A-module et $N\subset M$ un sous-module. Dans la suite, on voudrait avoir une propriété qui dit que, si M est de type fini, alors N l'est aussi. Malheureusement, celle-ci n'est pas vraie si A n'est pas noethérien : dans cas cas, il existe un idéal $I\subset A$ qui n'est pas de type fini.

▷ EXEMPLE. On considère l'anneau des suites entières $A:=\mathbf{Z}^{\mathbf{N}}$. Alors le A-module A est de type fini, mais son sous-module des suites finies $\mathbf{Z}^{(\mathbf{N})}$ n'est pas de type fini.

DÉFINITION 3.22. Un A-module M est dit *noethérien* si tout sous-module de M est de type fini.

PROPOSITION 3.23. Soit A un anneau noethérien. Alors tout A-module de type fini est noethérien.

THÉORÈME 3.24 (de la base adaptée). Soient A un anneau principal, M un A-module libre de rang $m\geqslant 0$ et $N\subset M$ un sous-module. Alors il existe une base $(x_1,\dots,x_m)$ de M et une base $(y_1,\dots,y_n)$ de N telles que

(i) $n\leqslant m$;
(ii) pour tout $i\in[\![1,n]\!]$, il existe $d_i\in A\setminus\{0\}$ tel que $y_i=d_ix_i$;
(iii) $d_1\mid\cdots\mid d_n$ et $\langle d_1\rangle\supset\cdots\supset\langle d_n\rangle$.

Preuve Soient $X:=(v_1,\dots,v_m)$ une base de M et $Y:=(w_1,\dots,w_n)$ une partie génératrice minimale de N. Alors il existe un isomorphisme $\phi_X\colon A^m\longrightarrow M$ et un morphisme surjectif $\phi_Y\colon A^n\longrightarrow N$. On peut donc identifier ces familles comme respectivement des bases de A^m et A^n. On note $B\in\mathscr{M}_{m,n}(A)$ la matrice de Y dans X. Plus formellement, en notant $i\colon N\longrightarrow M$ l'inclusion, la matrice B est celle du morphisme $u:=\phi_X^{-1}\circ i\circ\phi_Y$ de sorte que la diagramme

$$\begin{array}{ccc}A^n & \xrightarrow{u} & A^m\\ {\scriptstyle\phi_Y}\downarrow & & \downarrow{\scriptstyle\phi_X}\\ N & \xhookrightarrow[i]{} & M\end{array}$$

commute. En utilisant le théorème de SMITH, il existe $P\in\mathrm{GL}_m(A)$ et $Q\in\mathrm{GL}_n(A)$ telles que

$$B':=PBQ=\operatorname{diag}(d_1,\dots,d_k,0).$$

Alors cette matrice B' est la matrice d'une nouvelle base $X':=(x_1,\dots,x_m)$ de M dans une nouvelle famille génératrice $Y':=(y_1,\dots,y_n)$ de N (*i. e.* $Y'=Q^{-1}Y$ et $X'=PX$). Alors pour $i\in[\![1,n]\!]$, on a $y_i=d_ix_i$ avec $d_i\neq 0$ sinon cela contredirait la minimalité de $(w_1,\dots,w_n)$. Montrons que la famille Y' est libre. Soient $a_1,\dots,a_n\in A$ tels que $a_1y_1+\cdots+a_ny_n=0$. Alors $a_1d_1x_1+\cdots+a_nd_nx_n=0$. Comme $(x_1,\dots,x_m)$ est libre, pour tout $i\in[\![1,n]\!]$, on a $a_id_i=0$, donc $a_i=0$ car l'anneau A est intègre. D'où la liberté de Y'. □

COROLLAIRE 3.25. Soient A un anneau principal et M un A-module libre de rang $m\geqslant 0$. Alors tout sous-module de M est libre et de rang inférieur ou égal à m.

3.3.2 Théorème de structure principal

THÉORÈME 3.26 (de structure principal). Soient A un anneau principal et M un A-module de type fini. Alors il

existe $d_1, \dots, d_r \in A \setminus (A^\times \cup \{0\})$ et $s \geqslant 0$ tels que

$$d_1 \mid \cdots \mid d_r \quad \text{et} \quad M \simeq A/\langle d_1 \rangle \oplus \cdots \oplus A/\langle d_r \rangle \oplus A^s.$$

L'entier s et la suite d'idéaux $\langle d_1 \rangle \supset \cdots \supset \langle d_r \rangle$ ne dépendent que de M

Preuve Soient $X := (x_1, \dots, x_m)$ une partie génératrice minimale de M et $\phi_X \colon A^m \longrightarrow M$ la surjection naturelle associée. Alors $M \simeq A^m / \operatorname{Ker} \phi_X$. De plus, le noyau $K := \operatorname{Ker} \phi_X$ est un sous-module libre de A^m de rang $n \leqslant m$, donc le théorème précédent assure qu'il existe une base $(v_1, \dots, v_n)$ de K, une base $(w_1, \dots, w_m)$ de M et des éléments $d_1, \dots, d_n \in A \setminus \{0\}$ tels que

$$d_1 \mid \cdots \mid d_n \qquad \text{et} \qquad v_i = d_i w_i, \quad \forall i \in [\![1, n]\!].$$

On a donc

$$\begin{aligned} M \simeq A^m / K &\simeq \bigoplus_{i=1}^{m} A w_i \Big/ \bigoplus_{i=1}^{n} A d_i w_i \\ &= A/\langle d_1 \rangle \oplus \cdots \oplus A/\langle d_n \rangle \oplus A^s \end{aligned}$$

avec $s := m - n \geqslant 0$. Montrons que les éléments d_i appartiennent à $A \setminus (A^\times \cup \{0\})$. Comme $(v_1, \dots, v_n)$ est une base de K ou $v_i = d_i w_i$ pour tout $i \in [\![1, n]\!]$, on a $d_i \neq 0$. De plus, comme $(w_1, \dots, w_m)$ est minimale, on a $d_i \notin A^\times$ car sinon $A/\langle d_i \rangle = \{0\}$, donc M peut-être engendré par moins de m générateurs ce qui est impossible. L'unicité est montrée dans le polycopié. □

◇ REMARQUE. En appliquant ce théorème pour $A = \mathbf{Z}$, on obtient le théorème de structure des groupes abéliens de type fini.

3.3.3 Groupes abéliens données par des générateurs et relations

▷ EXEMPLES. On considère le $\mathbf{Z}$-module M donné par trois générateurs x_1, x_2 et x_3 et les deux relations

$$2x_1 + 2x_2 + 8x_3 = 0 \quad \text{et} \quad -2x_1 + 2x_2 + 4x_3 = 0.$$

Intuitivement, ce module est le quotient de $\mathbf{Z}^3$, dont on note (x_1, x_2, x_3) une base, par le sous-module $K \subset \mathbf{Z}^3$ engendré par les éléments $r_1 := 2x_1 + 2x_2 + 8x_3$ et $r_2 := -2x_1 + 2x_2 + 4x_3$. Plus formellement, en notant $\phi \colon \mathbf{Z}^3 \longrightarrow M$ l'unique morphisme surjectif envoyant chaque élément e_i de la base canonique de $\mathbf{Z}^3$ sur x_i, on a $M \simeq \mathbf{Z}^3 / \operatorname{Ker} \phi$.

On considères la base canonique (x_1, x_2, x_3) de $\mathbf{Z}^2$. Alors la famille (r_1, r_2) est génératrice du noyau $\operatorname{Ker} \phi$. De plus, la matrice

$$B := \begin{pmatrix} 2 & -2 \\ 2 & 2 \\ 8 & 4 \end{pmatrix} \in \mathscr{M}_{3,2}(\mathbf{Z}).$$

définit une morphisme $B \colon \mathbf{Z}^2 \longmapsto \mathbf{Z}^3$ et il vérifie $\operatorname{Im} B = \operatorname{Ker} \phi$ et $\mathbf{Z}^3 / \operatorname{Im} B \simeq M$.

DÉFINITION 3.27. Le *conoyau* d'un morphisme de A-modules $h \colon P \longrightarrow Q$ est le quotient

$$\operatorname{Coker} h := Q / \operatorname{Im} h.$$

Si un module M s'écrit $M \simeq \operatorname{Coker} B$ pour un morphisme $B \colon P \longrightarrow Q$, on dit que ce module M est présenté par B ou que la matrice B est la matrice de présentation de M

PROPOSITION 3.28. Soit $B \in \mathscr{M}_{m,n}(\mathbf{Z})$ une matrice de présentation d'un $\mathbf{Z}$-module M. Alors les matrices suivantes présentent le même module M :

– la forme normale de SCHMIDT de B convient ;
– la matrice B à laquelle on a supprimé une colonne de zéros convient ;
– quelque soit $j \in [\![1, n]\!]$, si la j-ième colonne de B est $(\delta_{i,j})_{i \in [\![1,m]\!]}$, alors la matrice B à laquelle on a supprimé la i-ième ligne et la j-ième colonne convient.

▷ EXEMPLES. Reprenons l'exemple précédent et mettons B sous sa forme normale de SCHMIDT : on obtient

$$B \xrightarrow[L_3 \leftarrow L_2 - 5L_1]{L_2 \leftarrow L_2 - L_1} \begin{pmatrix} 2 & -2 \\ 0 & 4 \\ 0 & 12 \end{pmatrix} \xrightarrow{L_2 \leftarrow L_2 + L_1} \begin{pmatrix} 2 & -2 \\ 0 & 0 \\ 0 & 12 \end{pmatrix} \xrightarrow{L_3 \leftarrow L_3 - 3L_2} \begin{pmatrix} 2 & 0 \\ 0 & 4 \\ 0 & 0 \end{pmatrix}.$$

On en déduit $M \simeq \mathbf{Z}^3 / (2\mathbf{Z} \oplus 4\mathbf{Z} \oplus \{0\}) \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}$.

3.3.4 Preuve de la proposition 3.23

LEMME 3.29. Un A-module est noethérien M si et seulement si toute suite croissante de sous-modules de M est stationnaire, *i. e.* pour toute suite croissante $(M_n)_{n\in\mathbf{N}}$ de sous-modules de M, il existe un entier $n_0 \in \mathbf{N}$ tel que la suite $(M_n)_{n\geqslant n_0}$ soit constante.

LEMME 3.30. Soient M un A-module et $N \subset M$ un sous-module. Alors M est noethérien si et seulement si N et M/N sont noethériens.

Preuve Le sens direct est assez clair (cf. TD8). Réciproquement, on suppose que N et M/N sont noethériens. Notons $\pi\colon M \longrightarrow M/N$ la projection. Alors M est de type fini. Soit $M' \subset M$ un sous-module. Alors comme M/N est noethérien, le sous-module $\pi(M') \subset M/N$ est de type fini. De plus, le sous-module $M' \cap N \subset N$ est de type fini. Ainsi comme $\pi(M') \simeq M'/(M' \cap N)$, le sous-module M' est de type fini. On en déduit que M est noethérien. □

LEMME 3.31. Soient A un anneau noethérien et $n \geqslant 1$ un entier. Alors le A-module libre A^n est noethérien.

Preuve Procédons par récurrence sur l'entier $n \geqslant 1$. Par hypothèse, on a le résultat pour $n = 1$. Soit $n \geqslant 2$ un entier. Supposons que les A-modules $A, \ldots, A^{n-1}$ sont noethériens. Alors les modules $A \simeq A^n/A^{n-1}$ et A^{n-1} sont noethériens : on a bien un isomorphisme $A \simeq A^n/A^{n-1}$ car on a la suite exacte

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^{n-1} & \xrightarrow{\subset} & A^n & \xrightarrow{\pi} & A & \longrightarrow & 0 \\ & & & & (a_1,\ldots,a_n) & \longmapsto & a_n & & \\ & & (a_1,\ldots,a_{n-1}) & \longmapsto & (a_1,\ldots,a_{n-1},0) & & & & \end{array}$$

Par le lemme précédent, le module A^n est alors noethériens. □

◇ REMARQUE. Tout anneau euclidien est principal et donc noethérien.

Preuve de la proposition 3.23 Soient A un anneau noethérien et M un A-module de type fini. Montrons que M est noethérien. On sait qu'il existe un entier $n \geqslant 1$ et une surjection $\phi\colon A^n \longrightarrow M$. Par le deuxième lemme, le module M est noethérien. □

Chapitre 4
GÉOMÉTRIE DES NOMBRES

4.1 RÉSEAUX ET APPLICATIONS

4.1.1 Réseaux

Soit $n \geqslant 1$ un entier. On considère l'espace $\mathbf{R}^n$ muni du produit scalaire euclidien.

DÉFINITION 4.1. Un *réseau* de $\mathbf{R}^n$ est un sous-groupe additif $\Lambda \subset \mathbf{R}^n$ s'écrivant sous la forme $v_1\mathbf{Z} + \cdots + v_n\mathbf{Z}$ où la famille $(v_1, \ldots, v_n)$ est une base du $\mathbf{R}$-espace vectoriel $\mathbf{R}^n$.

▷ EXEMPLES. L'ensemble $\mathbf{Z}^n$ est un réseau de $\mathbf{R}^n$. En identifiant $\mathbf{C}$ et $\mathbf{R}^2$, les ensembles $\mathbf{Z}[i]$ et $\mathbf{Z}[e^{2i\pi/3}]$ sont des réseaux de $\mathbf{C}$.

DÉFINITION 4.2. Le *parallélépipède fondamental* d'un réseau Λ de $\mathbf{R}^n$ de base $(v_1, \ldots, v_n)$ est l'ensemble

$$\{a_1 v_1 + \cdots + a_n v_n \mid a_1, \ldots, a_n \in [0,1[\}.$$

Le *déterminant* du réseau Λ est le volume de son parallélépipède fondamental, on le note $\det \Lambda$. Autrement dit, on a $\det \Lambda = |\det(v_1 \quad \ldots \quad v_n)|$.

◇ REMARQUE. Cette définition ne dépend pas de la base choisie en utilisant les propriétés du déterminant.

DÉFINITION 4.3. Un sous-réseau d'un réseau Λ de $\mathbf{R}^n$ est un sous-groupe Λ' de Λ qui est un réseau.

▷ EXEMPLE. L'ensemble $2\mathbf{Z} \times 2\mathbf{Z}$ est un sous-réseau de $\mathbf{Z}^2$.

LEMME 4.4. Soient Λ un réseau de $\mathbf{R}^n$ et Λ' un sous-réseau de Λ. Alors

$$[\Lambda : \Lambda'] = \frac{\det \Lambda'}{\det \Lambda}.$$

4.1.2 Théorème de MINKOWSKI

THÉORÈME 4.5 (MINKOWSKI). Soient Λ un réseau de $\mathbf{R}^n$ et $S \subset \mathbf{R}^n$ une partie non vide, bornée, convexe et symétrique par rapport à 0. On suppose $\mathrm{vol}(S) > 2^n \det \Lambda$. Alors S contient un point non nul de Λ.

◇ REMARQUE. Le résultat est faux si on a uniquement l'inégalité large. En effet, il suffit de considérer le réseau $\mathbf{Z}^2$ et l'intérieur S du carré de sommets $(\pm 1, \pm 1)$.

Preuve On montre uniquement le cas où $\Lambda = \mathbf{Z}^2$. Considérons la projection $f : S \longrightarrow \mathbf{R}^2/(2\mathbf{Z})^2$. Alors on peut montrer $\mathrm{vol}\, f(S) \leqslant 4$. De plus, cette application n'est pas injective. En effet, comme elle préserve les volumes localement, si elle était injective, elle préserverait le volume de S et donc $\mathrm{vol}(f(S)) = \mathrm{vol}(S) > 4$ ce qui est impossible. Ainsi il existe deux points distincts $p_1, p_2 \in S$ tels que $f(p_1) = f(p_2)$ et on peut écrire $p_2 - p_1 = (2k, 2\ell)$ avec $(k, \ell) \in \Lambda$ tel que $(k, \ell) \neq (0,0)$. L'ensemble S étant symétrique par rapport à 0 et convexe, on obtient successivement $-p_1 \in S$ et $[-p_1, p_2] \subset S$, donc $(k, \ell) = \frac{1}{2}(-p_1 + p_2) \in S$ ce qui montre le théorème dans ce cas particuliers. □

4.1.3 Théorème des deux carrés

THÉORÈME 4.6. Un nombre premier p est le somme de deux carrés d'entiers si et seulement si

$$p = 2 \quad \text{ou} \quad p \equiv 1 \mod 4.$$

Preuve $\Rightarrow$ Modulo 4, les carrés sont 0 et 1, donc les sommes de deux carrés sont 0, 1 et 2. On suppose $p > 2$. Alors $p \equiv 1,3 \mod 4$. Donc si p est la somme de deux carrés, alors $p \equiv 1 \mod 4$.

$\Leftarrow$ On suppose $p \equiv 1 \mod 4$. D'après le critère d'EULER, l'entier -1 est un résidu quadratique modulo p, donc il existe $m \in \mathbf{N}$ tel que $m^2 \equiv -1 \mod p$. Maintenant, considérons le réseau $\Lambda \subset \mathbf{R}^2$ donné par la base (v_1, v_2) avec $v_1 := (m, 1)$ et $v_2 := (p, 0)$. Alors pour tous $a, b \in \mathbf{Z}$, on a

$$\begin{aligned} \|av_1 + bv_2\|^2 = (am + bp)^2 + a^2 &\equiv a^2m^2 + a^2 \mod p \\ &\equiv a^2(1 + m^2) \mod p \\ &\equiv 0 \mod p. \end{aligned}$$

Ceci montre que, pour tout $w \in \Lambda$, on a $p \mid \|w\|^2$. Par ailleurs, on a $\det \Lambda = p$. Soit $D \subset \mathbf{R}^2$ le disque de rayon $\sqrt{2p}$ centré en $(0,0)$. Alors $\mathrm{vol}(D) = 2p\pi > 4p = 4 \det \Lambda$. Comme D est borné, convexe et symétrique par rapport à 0, le théorème de MINKOWSKI assure l'existence d'un point $w \in D \cap \Lambda$ non nul. On a alors $\|w\|^2 < 2p$ et $p \mid \|w\|^2$, donc $p = \|w\|^2$ ce qui assure la conclusion. □

4.1.4 Représentation d'un nombre premier par une forme quadratique

PROPOSITION 4.7. Un nombre premier p est de la forme $p = x^2 + 2y^2$ avec $x, y \in \mathbf{Z}$ si et seulement si

$$p = 2 \quad \text{ou} \quad p \equiv 1,3 \mod 8.$$

◇ REMARQUE. L'application $(x, y) \longmapsto x^2 + 2y^2$ est une forme quadratique définie positive sur $\mathbf{Z}^2$.

Preuve $\Leftarrow$ On suppose qu'il existe $x, y \in \mathbf{Z}$ tels que $p = x^2 + 2y^2$. Alors $-2y^2 \equiv x^2 \mod p$ ce qui implique

$$1 = \left(\frac{-2y^2}{p}\right) = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right).$$

Distinguons les deux cas.

– Si $(\frac{-1}{p}) = (\frac{2}{p}) = +1$, alors $p \equiv 1 \mod 4$ et $p \equiv 1,7 \mod 8$, donc $p \equiv 1 \mod 8$.

– Si $(\frac{-1}{p}) = (\frac{2}{p}) = -1$, alors $p \equiv 3 \mod 4$ et $p \equiv 3,5 \mod 8$, donc $p \equiv 3 \mod 8$.

$\Leftarrow$ Le cas $p = 2$ est trivial. On suppose désormais $p \equiv 1,3 \mod 8$. Alors l'entier -2 est un résidu quadratique comme le montre le raisonnement ci-dessus, donc il existe $m \in \mathbf{N}$ tel que $m^2 \equiv -2 \mod p$. Considérons le même réseau $\Lambda \subset \mathbf{R}^2$ que dans la preuve précédente et l'ellipse ouverte

$$E := \{(x, y) \in \mathbf{R}^2 \mid x^2 + 2y^2 < 2p\}.$$

Alors $\mathrm{vol}(E) = \pi\sqrt{2}p > 4p = 4 \det \Lambda$ et, comme l'ellipse vérifie les bonnes propriétés, le théorème de MINKOWSKI assure l'existence d'un élément $(x_0, y_0) \in E \cap \Lambda \setminus \{(0,0)\}$. Alors $x_0^2 + 2y_0^2 < 2p$ et $p \mid x_0^2 + 2y_0$, donc $p = x_0^2 + 2y_0$. □

4.2 REPRÉSENTATION D'UN NOMBRE PAR UNE FORME QUADRATIQUE

4.2.1 Positionnement du problème et définition

PROBLÈME. Soient $a, b, c \in \mathbf{Z}$. On considère la forme quadratique binaire $q\colon (x, y) \in \mathbf{Z}^2 \longmapsto ax^2 + bxy + cy^2$. Quels entiers $n \in \mathbf{Z}$ s'écrit sous la forme $n = q(x, y)$ avec $(x, y) \in \mathbf{Z}^2$.

DÉFINITION 4.8. – Un entier $n \in \mathbf{Z}$ est dit

- *représenté* par q s'il existe $(x, y) \in \mathbf{Z}^2$ tel que $n = q(x, y)$;
- *proprement représenté* par q s'il existe $(x, y) \in \mathbf{Z}^2$ tel que $n = q(x, y)$ et $\mathrm{pgcd}(x, y) = 1$.

– Pour $a, b, c \in \mathbf{Z}$, la forme quadratique $q(x, y) = ax^2 + bxy + cy^2$ sera notée $q = (a, b, c)$ et son *discriminant* est l'entier $\mathrm{disc}\, q := b^2 - 4ac$.

LEMME 4.9. Un entier $n \in \mathbf{Z}$ est proprement représenté par une forme quadratique $q\colon \mathbf{Z}^2 \longrightarrow \mathbf{Z}$ si et seulement s'il existe une base (v_1, v_2) de $\mathbf{Z}^2$ vérifiant $q(v_1) = n$.

Preuve D'après la définition, il suffit de montrer qu'un vecteur $(x, y) \in \mathbf{Z}^2$ peut-être complété en une base de $\mathbf{Z}^2$ si et seulement si $\mathrm{pgcd}(x, y) = 1$. Pour cela, utilisons le résultat suivant, démontré dans la suite

LEMME 4.10. Soient $(\alpha,\gamma),(\beta,\delta)\in\mathbf{Z}^2$. Alors la famille $((\alpha,\gamma),(\beta,\delta))$ est une base de $\mathbf{Z}^2$ si et seulement si son déterminant vaut ±1.

Soit $(x,y)\in\mathbf{Z}^2$ un vecteur quelconque. Si $\operatorname{pgcd}(x,y)=1$, alors il existe $r,s\in\mathbf{Z}$ tels que $rx+sx=1$, donc le lemme assure que la famille $((x,y),(-s,r))$ est une base de $\mathbf{Z}^2$ car son déterminant vaut 1. Si $d:=\operatorname{pgcd}(x,y)>1$, alors pour tout $r,s\in\mathbf{Z}$, la déterminant de la famille $((x,y),(s,r))$ soit divisible par d et donc différent de 1, donc le vecteur (x,y) ne fait pas partie d'une base de $\mathbf{Z}^2$. □

Preuve du lemme 4.10 Le sens réciproque est évident. Directement, on suppose que la famille $((\alpha,\gamma),(\beta,\delta))$ est une base de $\mathbf{Z}^2$. Considérons l'endomorphisme $B\colon\mathbf{Z}^2\longrightarrow\mathbf{Z}^2$ canoniquement associé à la matrice

$$B:=\begin{pmatrix}\alpha&\beta\\\gamma&\delta\end{pmatrix}.$$

Alors l'image de B est $\mathbf{Z}^2$, donc son conoyau est triviale, donc cette matrice B présente le $\mathbf{Z}$-module trivial. Mettons cette matrice sous sa forme normale de SMITH

$$B'=\begin{pmatrix}d_1&0\\0&d_2\end{pmatrix}$$

avec $d_1>0$ et $d_1\mid d_2$. Alors cette matrice B' présente le même module que la matrice B, donc $d_1=d_2=1$. Mais comme $\det B=\pm\det B'$, on en déduit $\det B=\pm1$. □

4.2.2 L'action à droite de $\mathrm{SL}_2(\mathbf{Z})$

◇ REMARQUE. Pour toute forme quadratique $q\colon\mathbf{Z}^2\longrightarrow\mathbf{Z}$ et toute matrice $M\in\mathrm{SL}_2(\mathbf{Z})$, la composée $q\circ M$ est une forme quadratique.

LEMME 4.11. Soient $n\in\mathbf{Z}$ et $q\colon\mathbf{Z}^2\longrightarrow\mathbf{Z}$ une forme quadratique. Alors

1. pour toute $M\in\mathrm{SL}_2(\mathbf{Z})$, l'entier n est proprement représenté par q si et seulement s'il est proprement représenté par $q\circ M$;
2. l'entier n est proprement représenté par q si et seulement s'il existe $M\in\mathrm{SL}_2(\mathbf{Z})$ telle que $q\circ M(1,0)=n$.

Preuve 1. Soient $(x,y)\in\mathbf{Z}^2$ et $(x',y'):=M^{-1}(x,y)$. Alors $q\circ M(x',y')=q(x,y)$. De plus, on peut montrer que les entiers x et y sont premiers entre eux si et seulement si les entiers x' et y' le sont. Ceci assure le point 1.

2. Le sens réciproque est évident. On suppose que l'entier n est proprement représenté par q. Alors il existe deux entiers $\alpha,\gamma\in\mathbf{Z}$ premiers entre eux tels que $n=q(\alpha,\gamma)$. De plus, le théorème de BÉZOUT assure alors qu'il existe $\beta,\delta\in\mathbf{Z}$ tels que $\alpha\delta-\gamma\beta=1$. Il suffit alors de considérer la matrice

$$M:=\begin{pmatrix}\alpha&\delta\\\beta&\gamma\end{pmatrix}\in\mathrm{SL}_2(\mathbf{Z}).$$ □

DÉFINITION 4.12. Deux formes quadratiques $q,q'\colon\mathbf{Z}^2\longrightarrow\mathbf{Z}$ sont *équivalentes* s'il existe une matrice $M\in\mathrm{SL}_2(\mathbf{Z})$ telle que $q'=q\circ M$. On note alors $q\sim q'$.

◇ REMARQUE. Le relation $\sim$ définit une relation d'équivalence sur les formes quadratiques. De plus, par le lemme précédent, deux formes quadratiques équivalentes représentent les mêmes entiers.

ÉCRITURE SOUS FORME MATRICIELLE D'UNE FORME QUADRATIQUE. Soient $q:=(a,b,c)\colon\mathbf{Z}^2\longrightarrow\mathbf{Z}$ une forme quadratique. Alors pour tous $x,y\in\mathbf{Z}$, cette forme quadratique s'écrit sous la forme matricielle

$$q(x,y)=\begin{pmatrix}x&y\end{pmatrix}Q\begin{pmatrix}x\\y\end{pmatrix}\quad\text{avec}\quad Q:=\begin{pmatrix}a&b/2\\b/2&c\end{pmatrix}.$$

L'action de $\mathrm{SL}_2(\mathbf{Z})$ sur les formes quadratiques *via* l'application $(M,q)\longmapsto q\circ M$ peut alors se traduire par une action de $\mathrm{GL}_2(\mathbf{Z})$ sur les matrices symétriques *via* l'application $(M,Q)\longmapsto {}^tMQM$. En reprenant les notations précédent, le discriminant de q est $\operatorname{disc}q=-4\det Q$.

Ce discriminant est invariant sous l'action de $\mathrm{SL}_2(\mathbf{Z})$, c'est-à-dire qu'on a $\operatorname{disc}(q\circ M)=\operatorname{disc}q$ pour toute forme quadratique q et toute matrice $M\in\mathrm{SL}_2(\mathbf{Z})$.

Dans la suite du cours, on va considérer les formes quadratiques définies positives, *i. e.* les formes quadratiques $q:=(a,b,c)$ tels que $\operatorname{disc}q<0$ et $a,c>0$.

4.2.3 Réduction des formes quadratiques définies positives

OBJECTIF. On veut simplifier une forme quadratique définies positives (a,b,c) par l'action de $\mathrm{SL}_2(\mathbf{Z})$ afin de diminuer l'entier $|b|$ le plus possible.

DÉFINITION 4.13. Une forme quadratique (a,b,c) est une *forme réduite* si

$$\begin{cases} |b| \leqslant a \leqslant c, \\ |b| = a \text{ ou } a = c \quad \Longrightarrow \quad b \geqslant 0. \end{cases}$$

▷ EXEMPLES. Les formes quadratiques $(1,0,1)$ et $(1,1,4)$ sont réduites.

THÉORÈME 4.14. 1. Toute forme quadratique définie positive est équivalente à une unique forme réduite.
2. Étant donné un entier $\Delta < 0$, il n'existe qu'un nombre fini de formes réduites définies positives dont le discriminant vaut Δ.

Preuve Le point 1 sera démontré en TD. Le lemme suivant implique le point 2. □

ALGORITHME DE RÉDUCTION. Pour trouver une forme réduite équivalente à une forme quadratique définie positive $q := (a,b,c)$ donnée, on utilises les deux opérations suivantes qui diminuent les entiers a et $|b|$.

Opération n° 1 Si $c < a$, on remplace q par $q' := (c,-b,a) = q \circ M$ où

$$M := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Opération n° 2 Si $|b| \geqslant a$, on remplace q par $q' := (a,b',c')$ avec

$$b' = b + 2\delta a \quad \text{et} \quad c' := \frac{b'^2 - \operatorname{disc} q}{4}$$

pour un entier $\delta \in \mathbf{Z}$ bien choisi de telle sorte que $b' \in]-a,a]$. Ceci correspond à $q' = q \circ M$ avec

$$M := \begin{pmatrix} 1 & \delta \\ 0 & 1 \end{pmatrix}.$$

▷ EXEMPLE. Soit $q := (25,-14,2)$. Son discriminant vaut -4 et sa matrice associée est

$$Q := \begin{pmatrix} 25 & -7 \\ -7 & 2 \end{pmatrix}.$$

Alors

$$\begin{aligned} (25,-14,2) &\xrightarrow[M_1 := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)]{\text{opération n° 1}} (2,14,25) \\ &\xrightarrow[M_2 := \left(\begin{smallmatrix} 1 & -3 \\ 0 & 1 \end{smallmatrix}\right)]{\text{opération n° 2}} (2,2,1) \\ &\xrightarrow[M_3 := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)]{\text{opération n° 1}} (1,-2,2) \\ &\xrightarrow[M_4 := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)]{\text{opération n° 2}} (1,0,1). \end{aligned}$$

Alors sa forme réduite est $q' := q \circ M = (1,0,1)$ avec

$$M := M_1 M_2 M_3 M_4 = \begin{pmatrix} -1 & -1 \\ -3 & -4 \end{pmatrix}.$$

LEMME 4.15. Soit $q := (a,b,c)$ une forme quadratique définie positive et réduite. Alors

$$1 \leqslant a \leqslant \sqrt{\frac{|\operatorname{disc} q|}{3}}.$$

Preuve Comme $\operatorname{disc} q < 0$ et $|b| \leqslant a \leqslant c$, on a $-\operatorname{disc} q = 4ac - b^2 \geqslant 4a^2 - a^2 = 3a^2$ ce qui donne ensuite l'inégalité recherchée. □

▷ EXEMPLE. Il n'existe qu'une seule forme réduite de discriminant -4 : c'est x^2+y^2. En particulier, comme chaque forme quadratique définie positive sont équivalentes à une unique forme réduite, elles sont équivalentes entre elles.

4.2.4 Forme des discriminants représentant un entier

THÉORÈME 4.16. Soient $n, \Delta \in \mathbf{Z}$. Alors

1. il existe une forme quadratique de discriminant Δ représentant proprement n si et seulement si l'entier Δ est un carré modulo $4n$;

2. si Δ est un carré modulo $4n$ et $b_1, \dots, b_n \in]-n, n]$ sont les racines carrées de Δ modulo $4n$, alors toute forme quadratique représentant proprement n est équivalente à une forme quadratique (n, b_i, c_i) où l'entier $c_i \in \mathbf{Z}$ vérifie $b_i^2 - 4nc_i = \Delta$.

Preuve 1. D'après le lemme 4.11, l'entier n est proprement représenté par une forme quadratique $q := (a,b,c)$ si et seulement s'il existe une forme quadratique q' équivalente à q telle que $q'(1,0) = n$, c'est-à-dire $q' = (n,b,c)$. Donc une telle forme quadratique existe si et seulement si $\operatorname{disc}(n,b,c) = \Delta$ avec $\operatorname{disc}(n,b,c) = b^2 - 4nc$, c'est-à-dire que Δ est un carré modulo n.

2. Soit q une forme quadratique représentant n de discriminant Δ telle que $q(1,0) = n$. Alors $q = (n,b,c)$ pour des entiers $b, c \in \mathbf{Z}$ tels que $b^2 - 4nc = \Delta$, *i. e.* l'entier b est une racine carrée de Δ modulo $4n$. En effectuant une opération n° 2, on obtient l'équivalence $q \sim q' := (n, b+2\delta n, c')$ pour un entier $\delta \in \mathbf{Z}$ bien choisi de telle sorte à avoir $b + 2\delta_c \in]-n, n]$. Et il suffit de remarquer la congruence $(b+2\delta)^2 \equiv b^2 \mod 4n$. □

EXERCICE 4.1. Considérons la forme quadratique $q := (1,2,6)$ qui est équivalente à $q' := (1,0,5)$ et de discriminant -20. Les entiers 7 et 11 sont-ils proprement représentés par q ?

▷ Comme $-20 \equiv 0 \mod 4$ et $\left(\frac{-20}{7}\right) = \left(\frac{1}{7}\right) = 1$, l'entier -20 est un carré modulo $4 \times 7 = 20$. De plus, ce n'est pas un carré modulo 44 puisque $\left(\frac{-20}{11}\right) = \left(\frac{2}{11}\right) = -1$. Trouvons les racines carrées $b \in]-7, 7]$ de -20 modulo 28. Le théorème chinois donne $\mathbf{Z}/28\mathbf{Z} \simeq \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/7\mathbf{Z}$ et, pour tout $b \in [-7,7]$, on a

$$b^2 \equiv -20 \mod 28 \iff \begin{cases} b^2 \equiv -20 \mod 4, \\ b^2 \equiv -20 \mod 7 \end{cases} \iff \begin{cases} b \equiv 0,2 \mod 4, \\ b \equiv \pm 1 \mod 7 \end{cases} \iff b = \pm 6.$$

D'après le théorème précédent, les formes quadratiques $q_1 := (7,-6,2)$ et $q_2 := (7,6,2)$ représentent 7 et sont de discriminant -20. Or ces deux formes sont équivalentes à la même forme réduite $(2,2,3)$, donc $q_1 \sim q_2$. Maintenant, la forme quadratique $q \sim q'$ n'est pas équivalente à q_1, donc elle ne représente pas 7. De plus, elle ne représente pas non plus 11.

Chapitre 5

NOMBRES ET ENTIERS ALGÉBRIQUES, CORPS DE NOMBRES

5.1 NOMBRES ET ENTIERS ALGÉBRIQUES

DÉFINITION 5.1. Un nombre complexe $\alpha \in \mathbf{C}$ est un *entier algébrique* s'il existe un polynôme unitaire $P \in \mathbf{Z}[X]$ tel que $P(\alpha) = 0$.

PROPOSITION 5.2 (caractérisation des entiers algébriques). Soit $\alpha \in \mathbf{C}$. Alors les propositions suivantes sont équivalentes :

(i) le complexe α est un entier algébrique ;
(ii) le complexe α est un nombre algébrique et son polynôme minimal appartient à $\mathbf{Z}[X]$;
(iii) le $\mathbf{Z}$-module $\mathbf{Z}[\alpha]$ est de type fini.

Preuve Les implications (ii) $\Rightarrow$ (i) et (i) $\Rightarrow$ (ii) sont claires. On suppose (iii) et montrons (ii). Alors il existe un polynôme unitaire $P \in \mathbf{Z}[X]$ telle que $P(\alpha) = 0$, donc le complexe α est un nombre algébrique. De plus, prenons le polynôme unitaire $M \in \mathbf{Z}[X]$ de degré minimal tel que $M(\alpha) = 0$. Alors celui-ci est irréductible dans $\mathbf{Z}[X]$ et donc dans $\mathbf{Q}[X]$, donc c'est le polynôme minimal du complexe α. □

COROLLAIRE 5.3. L'ensemble B des entiers algébriques est un sous-anneau de l'ensemble des nombres algébriques.

Preuve Cela se démontre comme dans le cas des nombres algébriques. □

DÉFINITION 5.4. L'*anneau des entiers* d'un corps de nombre K, c'est-à-dire $\mathbf{Q} \subset K \subset \mathbf{C}$ et $[K : \mathbf{Q}] < +\infty$, est l'anneau $\mathcal{O}_K := K \cap B$, *i. e.* c'est les éléments de K qui sont des entiers algébriques.

▷ EXEMPLES. On a $\mathcal{O}_{\mathbf{Q}} = \mathbf{Z}$.

5.2 CORPS QUADRATIQUES

DÉFINITION 5.5. Un sur-corps K de $\mathbf{Q}$ est *quadratique* si $[K : \mathbf{Q}] = 2$.

PROPOSITION 5.6. Soient K un corps quadratique et $d \in \mathbf{Z} \setminus \{0, 1\}$ un entier sans facteur carré. Alors $K = \mathbf{Q}(\sqrt{d})$.

Preuve Soit $\alpha \in K \setminus \mathbf{Q}$. Alors le $\mathbf{Q}$-espace vectoriel $K = \mathbf{Q}[\alpha]$ admet pour base $(1, \alpha)$. Soit $M := X^2 + bX + c \in \mathbf{Q}[X]$ le polynôme minimal de α. Alors $2\alpha = -b \pm \sqrt{b^2 - 4ac}$, donc

$$K = \mathbf{Q}(\sqrt{b^2 - 4ac}) = \mathbf{Q}(\sqrt{u/v}) = \mathbf{Q}(\sqrt{uv}) = \mathbf{Q}(\sqrt{d}).$$

pour tous $u, v \in \mathbf{Z}^*$ car $\sqrt{b^2 - 4ac} \in \mathbf{Q}$ et $u/v = uv/v^2$. □

DÉFINITION 5.7. Soit $d \in \mathbf{Z}^*$. Le corps $\mathbf{Q}(\sqrt{d})$ est dit *quadratique réel* (respectivement *quadratique imaginaire*) si $d > 0$ (respectivement $d < 0$).

5.2.1 Conjugaison, trace et norme

DÉFINITION 5.8. Soient $K := \mathbf{Q}(\sqrt{d})$ un corps quadratique et $\alpha := x + y\sqrt{d}$. On pose

$$\overline{\alpha} := x - y\sqrt{d},$$
$$\mathrm{Tr}(\alpha) := \alpha + \overline{\alpha} \quad \text{et}$$
$$N(\alpha) := \alpha\overline{\alpha}$$

appelé respectivement le conjugué, la trace et la norme de α.

PROPOSITION 5.9. 1. La trace $\mathrm{Tr}\colon K \longrightarrow \mathbf{Q}$ est additive.
2. La norme $N\colon K \longrightarrow \mathbf{Q}$ est multiplicative.
3. Pour tous $a, b \in \mathbf{Q}$, on a $\mathrm{Tr}(a + b\sqrt{d}) = 2a$ et $N(a + b\sqrt{d}) = a^2 - db^2$.
4. Le polynôme minimal sur $\mathbf{Q}$ d'un élément $\alpha \in K \setminus \mathbf{Q}$ est le polynôme $X^2 - \mathrm{Tr}(\alpha)X + N(\alpha) \in \mathbf{Q}[X]$.

5.2.2 L'anneau des entiers d'un corps

PROPOSITION 5.10. Soit $K := \mathbf{Q}(\sqrt{d})$ un corps quadratique. Alors un élément de K est un entier algébrique si et seulement si sa trace et sa norme sont des entiers.

Preuve Il suffit d'appliquer le point 4 de la proposition 5.9 ainsi que le point (ii) de la proposition 5.2. □

THÉORÈME 5.11. Soit $d \in \mathbf{Z} \setminus \{0, 1\}$. On note $\mathcal{O}_d$ l'anneau des entiers du corps quadratique $\mathbf{Q}(\sqrt{d})$. Alors
1. si $d \equiv 2, 3 \mod 4$, alors $\mathcal{O}_d = \mathbf{Z}[\sqrt{d}]$;
2. si $d \equiv 1 \mod 4$, alors $\mathcal{O}_d = \mathbf{Z}[\omega]$ avec $\omega := \frac{1}{2}(1 + \sqrt{d})$.

Preuve Montrons d'abord que $\mathbf{Z}[\sqrt{d}] \subset \mathcal{O}_d$. Pour cela, on remarque que les éléments 1 et $\sqrt{d}$ sont des entiers algébriques puisqu'ils sont respectivement racines des polynômes $X - 1$ et $X^2 - d$. Or $\mathbf{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbf{Z}\}$. Ceci conclut l'inclusion. Ensuite, on remarque que

$$\omega \in \mathcal{O}_d \iff N(\omega) = \frac{1 - d}{4} \in \mathbf{Z} \iff d \equiv 1 \mod 4,$$

donc $\mathbf{Z}[\omega] \subset \mathcal{O}_d$ si $d \equiv 1 \mod 4$. On peut également montrer l'inclusion réciproque dans ce cas ce qui conclut le point 2. On montre de même le point 1. □

5.3 FACTORISATION DANS LES ANNEAUX $\mathcal{O}_d$

PROPOSITION 5.12. Soit $\alpha \in \mathcal{O}_d$. Alors
1. on a $\alpha \in \mathcal{O}_d^\times$ si et seulement si $N(\alpha) = \pm 1$;
2. si l'entier $|N(\alpha)|$ est premier, alors l'élément α est irréductible.

Preuve On montre ces deux points de la même manière que lorsque $d = -1$, *i. e.* $\mathbf{Z}[i] = \mathcal{O}_{-1}$. □

THÉORÈME 5.13. Tout élément $\alpha \in \mathcal{O}_d \setminus (\mathcal{O}_d^\times \cup \{0\})$ se factorise dans $\mathcal{O}_d$, *i. e.* se décompose en un produit d'éléments irréductibles de $\mathcal{O}_d$.

Preuve Procédons par récurrence sur l'entier $|N(\alpha)|$. Si $|N(\alpha)| = 2$, alors l'élément 2 est irréductible d'après la proposition précédente. Soit $n \geqslant 3$. Supposons que tout élément $\alpha \in \mathcal{O}_d \setminus (\mathcal{O}_d^\times \cup \{0\})$ tel que $1 < |N(\alpha)| < n - 1$ se factorise dans $\mathcal{O}_d$. Soit $\alpha \in \mathcal{O}_d \setminus (\mathcal{O}_d^\times \cup \{0\})$ un élément de norme absolue n. Si α est irréductible, c'est fini. On suppose alors qu'il existe deux éléments non inversibles $\beta, \gamma \in \mathcal{O}_d$ tels que $\alpha = \beta\gamma$. Alors $|N(\alpha)| = |N(\beta)||N(\gamma)|$, donc $1 < |N(\beta)|, |N(\gamma)| < n$. D'après l'hypothèse de récurrence, les éléments β et γ se factorisent dans $\mathcal{O}_d$ et il en va de même pour l'élément α ce qui termine la récurrence. □

QUESTION. Quels anneaux $\mathcal{O}_d$ sont factoriels ?

5.4 CORPS QUADRATIQUE IMAGINAIRE

5.4.1 Les anneaux $\mathcal{O}_d$ qui sont factoriels

On a vu que l'anneau $\mathcal{O}_{-1} = \mathbf{Z}[i]$ est euclidien et donc factoriel, mais que l'anneau $\mathcal{O}_{-4} = \mathbf{Z}[i\sqrt{5}]$ n'est pas factoriel. En fait, dans la plupart des cas, l'anneau $\mathcal{O}_d$ n'est pas factoriel.

THÉORÈME 5.14. Soit $d < 0$ un entier. Alors l'anneau $\mathcal{O}_d$ est factoriel si et seulement si

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

◇ REMARQUE. Le sens réciproque est dû à GAUSS. Le sens direct est un résultat montré par STARK et BAKER en 1966, il s'agit d'une preuve très difficile.

PROPOSITION 5.15. Soit $d < 0$ un entier congrus à 3 modulo 4. Alors $\mathcal{O}_d$ est factoriel si et seulement si $d = -1$. En particulier, les anneaux $\mathcal{O}_{-5}, \mathcal{O}_{-9}, \mathcal{O}_{-13}, \ldots$ ne sont pas factoriels.

Preuve Si $d < -1$, alors

$$1 - d = 2\frac{1-d}{2} \quad \text{et} \quad 1 - d = (1 + \sqrt{d})(1 - \sqrt{d}),$$

donc l'anneau $\mathcal{O}_d$ n'est pas factoriel. Réciproquement, on suppose que l'anneau $\mathcal{O}_d$ est factoriel. Remarquons que l'élément 2 est irréductible car sa norme vaut 2 et, dans $\mathcal{O}_d$, c'est l'élément de plus petite norme strictement supérieure à 1. Donc si $d \neq -1$, alors $2 \mid 1 \pm d$ ce qui est impossible car $\frac{1}{2}(1 \pm d) \notin \mathcal{O}_d$. Donc $d = -1$. □

PROPOSITION 5.16. L'anneau $\mathcal{O}_{-2} = \mathbf{Z}[i\sqrt{2}]$ est euclidien.

Preuve On procède comme pour l'anneau $\mathbf{Z}[i]$ en faisant d'abord une remarque d'ordre géométrique : on peut trouver un point de $\mathbf{Q}(i\sqrt{2})$ le plus proche d'un point de $\mathbf{Z}[i\sqrt{2}]$. □

◇ REMARQUE. En fait, dès que $d > 2$, l'anneau $\mathbf{Z}[i\sqrt{d}]$ n'est pas euclidien.

5.4.2 Les entiers d'EISENSTEIN

L'anneau des entiers d'EISENSTEIN est l'anneau $\mathcal{O}_{-3} = \mathbf{Z}[\omega]$. Le norme d'un élément $a + b\omega \in \mathbf{Z}[\omega]$ est égale à l'entier $a^2 - ab + b^2$. De plus, on a $\mathbf{Z}[\omega]^\times = \{\pm 1, \pm\omega, \pm(1+\omega)\}$.

PROPOSITION 5.17. L'anneau $\mathcal{O}_{-3}$ est euclidien.

Preuve Comme pour $\mathbf{Z}[i]$, l'anneau $\mathbf{Z}[\omega] \subset \mathbf{C}$ est le réseau hexagonal et, pour tout point $z \in \mathbf{C}$, on peut trouver un point de $\mathbf{Z}[\omega]$ à distance strictement inférieure à 1 de z. □

5.4.3 Une autre preuve du théorème des deux carrés

On souhaite ici montrer le théorème des deux carrés à l'aide de l'anneau $\mathbf{Z}[i]$ des entiers de GAUSS. Rappelons que ce théorème affirme qu'une nombre premier $p \geqslant 3$ est la somme de deux carrés d'entiers si et seulement s'il est congru à 1 modulo 4.

Preuve Le sens direct se fait comme dans la précédente preuve. Réciproquement, on suppose $p \equiv 1 \mod 4$. Alors -1 est un résidu quadratique modulo p par le critère d'EULER, *i. e.* il existe $m \in \mathbf{N}$ tel que $m^2 \equiv -1 \mod p$. On considère $p \in \mathbf{Z} \subset \mathbf{Z}[i]$. Comme $p \equiv 1 \mod 4$, l'élément p n'est pas irréductible dans $\mathbf{Z}[i]$. En effet, on a

$$m^2 + 1 = (m + i)(m - i).$$

Si l'élément p est irréductible dans $\mathbf{Z}[i]$, alors il serait premier car l'anneau $\mathbf{Z}[i]$ est euclidien, donc $p \mid m \pm i$ ce qui est impossible car l'élément p est réel. Donc il n'est bien pas irréductible dans $\mathbf{Z}[i]$. On peut donc trouver des entiers $a, b, c, d \in \mathbf{Z}$ tels que $p = (a + ib)(c + id)$ avec $N(a + ib) \neq 1$ et $N(c + id) \neq 1$. En appliquant la norme à cette égalité, on obtient $p^2 = N(a + ib)N(c + id)$. Mais comme $p \geqslant 3$ est premier, on obtient $p = N(a + ib) = a^2 + b^2$ ce qui conclut. □

5.5 FACTORISATION DANS $\mathcal{O}_d$

5.5.1 Propriété des idéaux de $\mathcal{O}_d$

PROBLÈME. Les anneaux $\mathcal{O}_d$ ne sont pas tours factoriels. Cependant, si on considère les idéaux de $\mathcal{O}_d$, on récupère la factorise unique à idéaux près. On veut donc avoir des informations sur ces idéaux.

NOTATION. Soit $d \in \mathbf{Z} \setminus \{0,1\}$ un entier non divisible par 4. On pose

$$\omega := \begin{cases} \sqrt{d} & \text{si } d \equiv 2,3 \mod 4, \\ \frac{1}{2}(1+\sqrt{d}) & \text{si } d \equiv 1 \mod 4 \end{cases}$$

de sorte que $\mathcal{O}_d = \mathbf{Z}[\omega]$.

PROPOSITION 5.18. Soient I et J deux idéaux de $\mathcal{O}_d$. Alors

1. l'idéal I est engendré par au plus deux générateurs ;
2. en notant $I = \langle \alpha_1, \beta_1 \rangle$ et $J = \langle \alpha_2, \beta_2 \rangle$, on a $IJ = \langle \alpha_1\alpha_2, \alpha_1\beta_2, \beta_1\alpha_2, \beta_1\beta_2 \rangle$ et on peut réduire son nombre de générateurs au nombre de deux ;
3. tout idéal premier et non nul I est maximal.

Preuve 1. Le $\mathbf{Z}$-module $\mathbf{Z}[\omega] \simeq \mathbf{Z}^2$ est libre et de rang 2, donc l'idéal I est un sous-module qui vaut 0, $\mathbf{Z}$ ou $\mathbf{Z}^2$. Donc il est engendré par au plus deux générateurs comme $\mathbf{Z}$-module et donc comme $\mathcal{O}_d$-module.
3. Soit $\alpha \in I \setminus \{0\}$. Alors $n := \alpha\overline{\alpha} \in I$, donc $\langle n \rangle = n\mathbf{Z} + n\omega\mathbf{Z} \subset I \subset \mathcal{O}_d = \mathbf{Z} + \omega\mathbf{Z}$, donc le $\mathbf{Z}$-module I est d'indice fini dans $\mathcal{O}_d$. Comme I est premier, le quotient $\mathcal{O}_d/I$ est intègre et fini, donc c'est un corps (cf. TD), donc l'idéal I est maximal. □

5.5.2 Norme d'un idéal de $\mathcal{O}_d$

DÉFINITION 5.19. La norme d'un idéal non nul I de $\mathcal{O}_d$ est l'entier $N(I) := [\mathcal{O}_d : I]$.

LEMME 5.20. Soit I un idéal non nul de $\mathcal{O}_d$. On note $\overline{I} := \{\overline{\alpha} \mid \alpha \in I\}$. Alors il existe $n \in \mathbf{Z}$ tel que $I\overline{I} = \langle n \rangle$. De plus, on a $N(I) = n$.

▷ EXEMPLE. On considère l'idéal $I := \langle 3, 1+\sqrt{-5} \rangle \subset \mathcal{O}_{-5}$. Alors

$$N(I) = \mathrm{Card}\left(\frac{\mathbf{Z}[\sqrt{-5}]}{\langle 3, 1+\sqrt{-5} \rangle}\right) = \mathrm{Card}\left(\frac{\mathbf{Z}}{3\mathbf{Z}}\right) = 3$$

et on a aussi

$$I\overline{I} = \langle 3, 1+\sqrt{-5} \rangle \langle 3, 1-\sqrt{-5} \rangle = \langle 9, 3+3\sqrt{-5}, 3-3\sqrt{-5}, 6 \rangle = \langle 3, 3+3\sqrt{-5} \rangle = \langle 3 \rangle.$$

PROPOSITION 5.21. 1. Le norme est multiplicative.
2. Pour tout $\alpha \in \mathcal{O}_d$, on a $N(\langle \alpha \rangle) = N(\alpha)$.
3. Tout idéal de $\mathcal{O}_d$ dont la norme est un nombre premier est premier.

Preuve Les deux premiers points se vérifient aisément avec le lemme 5.20. Pour le point 3, soit I un idéal dont la norme est un nombre premier. Alors le cardinal $\mathrm{Card}(\mathcal{O}_d/I)$ est premier, donc l'idéal I est maximal et donc premier d'après la proposition 5.18. □

5.5.3 Divisibilité d'idéaux

DÉFINITION 5.22. Un idéal I de $\mathcal{O}_d$ divise un autre idéal J de $\mathcal{O}_d$ s'il existe un idéal K de $\mathcal{O}_d$ tel que $J = IK$. On note alors $I \mid J$.

◇ REMARQUE. Si $I \mid J$, alors $J = IK \subset I\mathcal{O}_d \subset I$ pour un certain idéal K de $\mathcal{O}_d$. La réciproque est vraie comme le montre le lemme suivant.

LEMME 5.23. Soient I et J deux idéaux non nuls de $\mathcal{O}_d$. Alors $I \mid J$ si et seulement si $J \subset I$.

Preuve Montrons le sens réciproque et supposons $J \subset I$. Alors $J\overline{I} \subset I\overline{I} = \langle N(I) \rangle$. Alors l'idéal $K := N(I)^{-1}J\overline{I}$ est un idéal de $\mathcal{O}_d$ vérifiant $IK = J$. D'où $I \mid J$. □

LEMME 5.24. Soient I, J et K trois idéaux non nuls de $\mathcal{O}_d$ tels que $IJ = IK$. Alors $J = K$.

Preuve Comme $IJ = IK$, on a $\overline{I}IJ = \overline{I}IK$, donc $N(I)J = N(I)K$, donc $J = K$. □

LEMME 5.25. Soient I un idéal premier de $\mathcal{O}_d$ et J et K deux idéaux de $\mathcal{O}_d$ tels que $I \mid JK$. Alors $I \mid J$ ou $I \mid K$.

Preuve Supposons $I \nmid j$. Alors $J \not\subset I$, donc $I \subset I + J$. On a même $I \subsetneq I + J$ car sinon on aurait $I = I + J \supset J$ ce qui est impossible. Maintenant, comme I est premier, il est maximal, donc $I + J = \mathcal{O}_d$. En particulier, il existe $\alpha \in I$ et $\beta \in J$ tels que $1 = \alpha + \beta$. Ainsi pour tout $\gamma \in K$, on a $\gamma = \gamma\alpha + \gamma\beta \in I + JK \subset I$ puisque $I \mid JK$. D'où $K \subset I$ et cela conclut $I \mid K$. □

5.5.4 Factorisation d'idéaux

THÉORÈME 5.26. Tout idéal I de $\mathcal{O}_d$ tel que $\{0\} \subsetneq I \subsetneq \mathcal{O}_d$ admet une facteurs en produits d'idéaux premiers, *i. e.* il existe des idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ de $\mathcal{O}_d$ tels que $I = \mathfrak{p}_1 \cdots \mathfrak{p}_k$. Cette factorisation est unique à l'ordre des facteurs près.

Preuve On procède par récurrence sur le norme de l'idéal I. □

▷ EXEMPLE. L'anneau $\mathcal{O}_{-5}$ n'est pas factoriel. Par exemple, on a $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Mais au niveau des idéaux, cela marche bien. En effet, on a $\langle 6 \rangle = \langle 2 \rangle \langle 3 \rangle = \langle 2, 1 + \sqrt{-5} \rangle \langle 2, 1 - \sqrt{-5} \rangle \langle 3, 1 + \sqrt{-5} \rangle \langle 3, 1 - \sqrt{-5} \rangle$ où les idéaux apparaissant à droite sont tous premiers (leurs normes sont premières).

5.5.5 Caractérisation des anneaux $\mathcal{O}_d$ qui sont factoriels

THÉORÈME 5.27. L'anneau $\mathcal{O}_d$ est factoriel si et seulement s'il est principal.

Preuve Le sens réciproque est vrai dans un cas beaucoup plus général. On suppose que l'anneau $\mathcal{O}_d$ est factoriel. Remarquons d'abord que, pour tout élément irréductible $\alpha \in \mathcal{O}_d$, l'idéal $\langle \alpha \rangle$ est premier.

Soit I un idéal premier. Montrons qu'il est principal. Supposons $I \neq \{0\}$. Alors $\langle N(I) \rangle = I\overline{I} \subset I$, donc $I \mid \langle N(I) \rangle$. Notons $N(I) = u_1 \cdots u_k$ pour des éléments irréductibles $u_i \in \mathcal{O}_d$. Alors $\langle N(I) \rangle = \langle u_1 \rangle \cdots \langle u_k \rangle$ avec $I \mid \langle N(I) \rangle$, donc le lemme 5.25 assure qu'il existe un entier $i \in [\![1, k]\!]$ tels que $I \mid \langle u_i \rangle$. Mais comme les idéaux I et $\langle u_i \rangle$ sont premiers, on en déduit $I = \langle u_i \rangle$, donc l'idéal I est principal.

Soit I un idéal de $\mathcal{O}_d$. On peut l'écrire sur la forme $I = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ où les idéaux $\mathfrak{p}_i$ sont premiers. D'après ce qui précède, pour tout $i \in [\![1, k]\!]$, l'idéal $\mathfrak{p}_i$ est principal, donc il s'écrit $\mathfrak{p}_i = \langle u_i \rangle$. On en déduit que l'idéal $I = \langle u_1 \cdots u_k \rangle$ est principale qui termine la preuve. □

5.5.6 Structure des idéaux premiers de $\mathcal{O}_d$

LEMME 5.28. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_d$. Alors il existe un nombre premier p tels que $\langle p \rangle \subset \mathfrak{p}$ et $N(\mathfrak{p}) \in \{p, p^2\}$.

Preuve On écrit $N(\mathfrak{p}) = p_1 \cdots p_k$ où les entiers p_i sont premiers. Comme $\mathfrak{p} \mid \mathfrak{p}\overline{\mathfrak{p}} = \langle N(\mathfrak{p}) \rangle$, on a $\mathfrak{p} \mid \langle p_1 \rangle \cdots \langle p_k \rangle$, donc le lemme 5.25 assure qu'il existe un entier $i \in [\![1, k]\!]$ tels que $\mathfrak{p} \mid \langle p_i \rangle$, donc $\langle p_i \rangle \subset \mathfrak{p}$. Comme $N(\langle p_i \rangle) = p_i^2$, on a $N(\mathfrak{p}) \in \{p_i, p_i^2\}$. □

LEMME 5.29. Soit I un idéal non nul de $\mathcal{O}_d$. Alors il existe des entiers $n \in \mathbf{N}^*$ et $a, b \in \mathbf{Z}$ tels que $I = \langle n, a + b\omega \rangle$.

Preuve Puisque $I \neq \{0\}$, il existe $\alpha \in I$ tel que $\alpha\overline{\alpha} \in I \cap \mathbf{N}$. On note $n := \min(I \cap \mathbf{N})$. Soit $a + b\omega \in I$ où l'entier $b > 0$ est minimal. Alors $\langle n, a + b\omega \rangle \subset I$ et on peut montrer l'inclusion réciproque. □

LEMME 5.30. Soit I un idéal de $\mathcal{O}_d$ dont la norme p est première. Alors il existe $a \in [\![0, p-1]\!]$ tels que $I = \langle p, a + \omega \rangle$ et $p \mid N(a + \omega)$.

Preuve D'après le lemme 5, on peut écrire $I = \langle n, a + b\omega \rangle$ avec $n \in \mathbf{N}^*$ et $a, b \in \mathbf{Z}$. On sait que les vecteurs $(n, 0)$ et (a, b) génère I dans la base $(1, \omega)$ de $\mathcal{O}_d$, donc

$$\begin{vmatrix} n & a \\ 0 & b \end{vmatrix} = p.$$

On en déduit $nb = p$, donc $n = p$ et $b = 1$. En effet, si $n = 1$ et $b = p$, alors $1 \in I$, donc $I = \mathcal{O}_d$ ce qui est impossible car $N(\mathcal{O}_d) = d^2$. □

DÉFINITION 5.31. On dit qu'un nombre premier p est
– *inerte* s'il existe un idéal premier $\mathfrak{p}$ tel que $\langle p\rangle = \mathfrak{p}$, c'est-à-dire $N(\mathfrak{p}) = p^2$;
– *ramifié* s'il existe un idéal premier $\mathfrak{p}$ tel que $\langle p\rangle = \mathfrak{p}^2$, c'est-à-dire $\mathfrak{p} = \overline{\mathfrak{p}}$ et $N(\mathfrak{p}) = p$;
– *scindé* s'il existe un idéal premier $\mathfrak{p}$ tel que $\langle p\rangle = \mathfrak{p}\overline{\mathfrak{p}}$, c'est-à-dire $\mathfrak{p} \neq \overline{\mathfrak{p}}$ et $N(\mathfrak{p}) = p$.

▷ EXEMPLES. On se place dans l'anneau $\mathcal{O}_{-1} = \mathbf{Z}[i]$.
– Le nombre premier 2 est ramifié car

$$\langle 2\rangle = \langle 1+i\rangle^2 \quad \text{et} \quad N(\langle 1+i\rangle) = 2.$$

– Le nombre premier 3 est inerte car l'idéal $\langle 3\rangle$ est premier puisque, comme le polynôme X^2+3 est irréductible dans $\mathbf{F}_3$, le quotient

$$\frac{\mathbf{Z}[i]}{\langle 3\rangle} \simeq \frac{\mathbf{Z}[X]/\langle X^2+1\rangle}{\langle 3\rangle} = \frac{\mathbf{Z}[X]}{\langle 3, X^2+1\rangle} = \frac{\mathbf{F}_3[X]}{\langle X^2+1\rangle}$$

est un corps.
– Le nombre premier 5 est scindé car $\langle 5\rangle = \langle 2+i\rangle\langle 2-i\rangle$ avec $N(\langle 2+i\rangle) = N(\langle 2-i\rangle) = 5$.

THÉORÈME 5.32. Soit p un nombre premiers.
1. On suppose $p > 2$. Alors
– si $(\frac{d}{p}) = -1$, alors p est inerte dans $\mathcal{O}_d$;
– si $(\frac{d}{p}) = 0$, alors p est ramifié dans $\mathcal{O}_d$;
– si $(\frac{d}{p}) = 1$, alors p est scindé dans $\mathcal{O}_d$.
2. On suppose $p = 2$. Alors
– si $d \not\equiv 1 \mod 4$, alors 2 est ramifié dans $\mathcal{O}_d$;
– si $d \equiv 1 \mod 8$, alors 2 est scindé dans $\mathcal{O}_d$;
– si $d \equiv 5 \mod 8$, alors 2 est inert dans $\mathcal{O}_d$.

Preuve On a vu que, pour tout idéal premier $\mathfrak{p}$, il existe un nombre premier p tel que $\mathfrak{p} \mid \langle p\rangle$, *i. e.* $\langle p\rangle \subset \mathfrak{p}$. Donc le comportement de l'idéal $\langle p\rangle$ dépend de l'existence ou non d'idéaux de norme p.

Montrons uniquement le point 2. On suppose $p > 2$. Si $d \equiv 2,3 \mod 4$, alors $\omega = \sqrt{2}$ et $N(a+\sqrt{d}) = a^2 - d \equiv 0 \mod p$ qui admet 0, 1 ou 2 solutions a modulo p selon la valeur de $(\frac{d}{p})$.

Si $d \equiv 1 \mod 4$, alors $\omega = \frac{1}{2}(1+\sqrt{d})$ et, pour tout $a \in \mathcal{O}_d$, on a

$$\begin{aligned} N(a+\omega) \equiv 0 \mod p &\iff a^2 + a - \frac{d-1}{4} \equiv 0 \mod p \\ &\iff (2a+1)^2 \equiv d \mod p \\ &\iff b^2 \equiv d \mod p \end{aligned}$$

avec $b := 2a+1$, donc cette équation à $1+(\frac{d}{p})$ solutions b modulo p, donc elle est $1+(\frac{d}{p})$ solutions a modulo p. Ceci termine la preuve avec la remarque du début de cette preuve. □

5.5.7 Exemples de factorisation d'idéaux

(i) Premier exemple

On se place dans $\mathcal{O}_{-1} = \mathbf{Z}[i]$. Rappelons que, comme il est euclidien, il est principal, *i. e.* tous ses idéaux sont principaux. Trouvons la factorisation de l'idéal $\langle 5+3i\rangle$. Sa norme vaut $34 = 2\times 12$. L'entier 2 est ramifié puisque, comme $2 = (1+i)(1-i)$, on a $\langle 2\rangle = \langle 1+i\rangle^2$. De plus, l'entier 17 est scindé puisque $(\frac{-1}{17}) = 1$. On en déduit la factorisation

$$\langle 5+3i\rangle = \langle 1+i\rangle\langle 4-i\rangle.$$

(ii) Deuxième exemple

On se place dans $\mathcal{O}_{-13} = \mathbf{Z}[\sqrt{-13}]$. Trouvons la factorisation de l'idéal $\langle 42\rangle$. On a $42 = 2\times 3\times 7$. L'entier 2 est scindé puisque $\langle 2\rangle = \langle 2, 1+\sqrt{-13}\rangle\langle 2, 1-\sqrt{-13}\rangle$ où $\langle 2, 1+\sqrt{-13}\rangle = \langle 2, 1-\sqrt{-13}\rangle$. De plus, l'entier 3 est inerte puisque $(\frac{-13}{3}) = (\frac{2}{3}) = -1$. Enfin l'entier 7 est scindé puisque $\langle 7\rangle = \langle 7, 1+\sqrt{-13}\rangle\langle 7, 1-\sqrt{-13}\rangle$. On en déduit la factorisation

$$\langle 42\rangle = \langle 2, 1+\sqrt{-13}\rangle^2\langle 3\rangle\langle 7, 1+\sqrt{-13}\rangle\langle 7, 1-\sqrt{-13}\rangle.$$

5.6 CLASSES D'IDÉAUX ET GROUPE DES CLASSES

Soit $d<0$ un entier. On considère l'anneau $\mathcal{O}_d$. Pour tous idéaux I et J de $\mathcal{O}_d$, on note $I\sim J$ s'il existe deux entiers $\alpha,\beta\in\mathcal{O}_d$ tels que $\alpha I=\beta J$. On note $\mathrm{Cl}(\mathcal{O}_d)$ l'ensemble des classes d'équivalence pour la relation $\sim$. Pour tout idéal I de $\mathcal{O}_d$, on note $[I]\in\mathrm{Cl}(\mathcal{O}_d)$ sa classe d'équivalence. Pour tous idéaux I, I', J et J' de $\mathcal{O}_d$, on remarque que les relations $I\sim I'$ et $J\sim J'$ impliquent la relation $IJ\sim I'J'$. Ainsi la multiplication des idéaux induit une loi de composition interne dans $\mathrm{Cl}(\mathcal{O}_d)$. L'élément neutre est $[\mathcal{O}_d]$ et l'inverse d'un élément $[I]$ est $[\overline{I}]$.

DÉFINITION 5.33. L'ensemble $\mathrm{Cl}(\mathcal{O}_d)$ muni de la multiplication est le *groupe des classes* de $\mathcal{O}_d$.

◇ REMARQUE. On peut montrer que la classe $[\mathcal{O}_d]$ contient exactement les idéaux principaux.

THÉORÈME 5.34. Le groupe $\mathrm{Cl}(\mathcal{O}_d)$ est abélien et fini.

Preuve Ce théorème découle du lemme suivant qu'on va admettre provisoirement.

LEMME 5.35. Dans chaque classe de $\mathrm{Cl}(\mathcal{O}_d)$, il existe un idéal I tel que

$$N(I)\leqslant\begin{cases}\frac{4}{\pi}\sqrt{|d|} & \text{si } d\equiv 2,3 \mod 4,\\ \frac{2}{\pi}\sqrt{|d|} & \text{si } d\equiv 1 \mod 4.\end{cases}$$

Il est clair que ce groupe est abélien. Montrons qu'il est fini. D'après le lemme, il existe un entier $K\in\mathbf{N}$ tel que chaque classe $[I]$ contienne un idéal J vérifiant $N(J)\leqslant K$. Mais il y a seulement un nombre fini d'idéaux de norme inférieur ou égal à K (cf. paragraphe suivant), donc le nombre de classe est fini.

Justifions le fait qu'il existe qu'un nombre fini d'idéaux I tels que $N(I)\leqslant K$. Pour tout nombre premier $p\leqslant K$, selon les cas, il y a

– un idéal premier de norme p^2 si le nombre premier p est inerte ;
– un idéal premier de norme p si le nombre premier p est ramifié ;
– deux idéaux premiers de norme p si le nombre premier p est scindé.

Donc il y a un nombre fini d'idéaux premiers de norme inférieur ou égale à K. Maintenant, comme tout idéal se factorise en un produit unique d'idéaux premiers, on en déduit le résultat. □

Preuve du lemme On plonge l'anneau $\mathcal{O}_d$ dans $\mathbf{C}$ de sorte qu'il soit vu comme un réseau de $\mathbf{C}$. Le volume de son parallélogramme fondamental vaut

$$\mathrm{vol}\,P_{\mathcal{O}_d}=\begin{cases}\sqrt{|d|} & \text{si } d\equiv 2,3 \mod 4,\\ \frac{1}{2}\sqrt{|d|} & \text{si } d\equiv 2,3 \mod 4.\end{cases}\qquad(\star)$$

et le volume du parallélogramme fondamental d'un idéal I vaut $\mathrm{vol}\,P_I=N(I)\,\mathrm{vol}\,P_{\mathcal{O}_d}$. Appliquons le théorème de MINKOWSKI. Soit $r>0$. Considérons le disque ouvert

$$D_r:=\{x+iy\in\mathbf{C}\mid x^2+y^2<r^2\}\subset\mathbf{C}$$

qui est une partie non vide, bornée, convexe et symétrique par rapport à 0. Son volume vaut $\mathrm{vol}\,D_r=\pi r^2$. Soit I un idéal. On suppose $r^2>\frac{4}{\pi}\mathrm{vol}\,P_I$ de sorte que $\mathrm{vol}\,D_r>4\,\mathrm{vol}\,P_I$. Alors le théorème de MINKOWSKI assure qu'il existe un complexe $\alpha:=x+iy\in D_r\cap I$ tel que $\alpha\neq 0$. Ainsi pour tout $\varepsilon>0$, il existe un élément $\alpha\in I\setminus\{0\}$ tel que

$$|\alpha|^2<\frac{4}{\pi}\mathrm{vol}\,P_I+\varepsilon.$$

Comme le réseau $I\subset\mathbf{C}$ est discret, il existe donc un élément $\alpha\in I\setminus\{0\}$ tel que

$$|\alpha|^2\leqslant\frac{4}{\pi}\mathrm{vol}\,P_I.$$

En considérant l'idéal conjugué $\overline{I}$, il existe un élément $\alpha\in\overline{I}\setminus\{0\}$ tel que $N(\alpha)\leqslant\frac{4}{\pi}\mathrm{vol}\,P_{\overline{I}}$. On a $\overline{I}\mid\langle\alpha\rangle$, donc il existe un idéal J tel que $\overline{I}J=\langle\alpha\rangle$. On obtient alors

$$N(\overline{I})N(J)=N(\overline{I}J)=N(\langle\alpha\rangle)\leqslant\frac{4}{\pi}\mathrm{vol}\,P_{\overline{I}}=\frac{4}{\pi}N(\overline{I})\,\mathrm{vol}\,P_{\mathcal{O}_d}$$

ce qui permet de conclure $N(J)\leqslant\frac{4}{\pi}\mathrm{vol}\,P_{\mathcal{O}_d}$. En utilisant les inégalités $(\star)$, le lemme est donc démontré □

◇ REMARQUE. Lorsque $\mathcal{O}_d$ est euclidien, il est principal et le groupe $\mathrm{Cl}(\mathcal{O}_d)$ est trivial.