Cours de Bachelor

Semestre d'été 2004-2005

INTRODUCTION À LA THÉORIE DES NOMBRES

Cours du Professeur EVA BAYER FLUCKIGER

Notes de cours par Caroline Lassueur

Ecole Polytechnique Fédérale de Lausanne
Section de mathématiques
CH-1015 Lausanne

Note.

Ce document n'est pas un support de cours officiel. Il s'agit de notes de cours personnelles et partiellement adaptées. De ce fait certaines banalités ou rappels énoncés durant le cours n'y figurent pas, alors que d'autres choses non-énoncées y figurent.

Table des matières

Table des notations

$\mathrm{Aut}(K/F)$	Ensemble des automorphisme du corps K qui sont l'identité sur F
$\mathbb{C}$	Les nombres complexes
C_d	Groupe cyclique d'ordre d
$\mathrm{car}(A)$	La caractéristique de l'anneau A
$Cl(K)$	Groupe des classes d'idéaux
det	Déterminant
D	Discriminant
D_P	Groupe de décomposition de l'idéal P
E_n	Courbe cubique $y \leq= x \geq -n \leq x$
$E(\mathbb{Q})$	Groupe des points rationnels de la courbe E
$\mathbb{F}_p$	Corps fini a p éléments $\mathbb{Z}/p\mathbb{Z}$
$\mathbb{F}_q$	Corps fini a $q = p^n$ éléments
$\mathrm{Gal}(K/F)$	Groupe de Galois de l'extension K/F
h_K	Nombre de classe
Id_S	Application identité de l'ensemble E
Im	Image d'une application
$\mathcal{I}(K)$	Groupe des idéaux fractionnaires de $\mathcal{O}_K$
I_P	Groupe d'inertie de l'idéal P
m_x	Application de multiplication par x
ker	Noyau
K^H	Sous-corps invariant du sous-groupe H
$K(\alpha)$	Extension du corps K par l'élément α
K^n	$\{x^n \mid x \in K\}$
$\mathbb{N}$	Les nombres naturels, 0 compris
$\mathbb{N}_n$	$\{1, 2, 3, \ldots, n\}$
N	La norme
$\mathcal{O}_K$	Anneau des entiers sur $\mathbb{Z}$ de K
$\mathbb{P}$	Ensemble des éléments premiers de l'anneau $\mathbb{Z}$
$pgdc(a, b)$	Plus grand diviseur commun de a et b
$\mathcal{P}(K)$	Groupe des idéaux principaux de $\mathcal{O}_K$
$\mathbb{Q}(\sqrt{d})$	Corps quadratique
$\mathbb{Q}(\zeta_p)$	Corps cyclotomique
$\mathbb{Q}$	Les nombres rationnels
$\mathbb{R}$	Les nombres réels
$R[X]$	Anneau de polynôme à coefficient dans l'anneau R
R^*	Groupe des unités de l'anneau R
Tr	La trace
$\mathbb{Z}$	Les nombres entiers
Δ_x	Le polynôme carctéristique de x
φ	Indicatrice d'Euler
ζ_p	Racine primitive p-ième de l'unité dans $\mathbb{C}$

$a \mid b$	a divise b
$a \nmid b$	a ne divise pas b
(a, b)	Plus grand diviseur commun de a et b
$a \equiv b \mod m$	a est congrus à b modulo m
$[a]_m$	Classe de a modulo m
$[X^n]$	Coefficient de X^n
$[K : F]$	Degré de l'extension K/F
$\#A$	Cardinalité de l'ensemble A
$i = \overline{m, n}$	$m \leq i \leq n$
$\left(\frac{a}{p}\right)$	Symbole de Legendre
$\left(\frac{K/F}{p}\right)$	Automorphisme de Froebenius
$< f >$	Idéal principal engendré par l'élément f
$\|.\|$	Module complexe/valeur absolue
$\oplus$	La somme directe
$\sum$	Symbole de sommation
$\times$	Le produit cartésien
$\prod$	Produit/produit cartésien
$\circ$	La composition des applications
$\cap$	L'intersection
$\cup$	L'union
$\neq$	La non égalité
$\cong$	Isomorphisme de structure algébrique
$\subset$	L'inclusion
$\subseteq$	L'inclusion
$\subsetneq$	L'inclusion stricte
$\not\subset$	La non inclusion
$<$	Sous-groupe
$\hookrightarrow$	Flèche injective
$\twoheadrightarrow$	Flèche surjective
$\forall$	Symbole universel "pour tout"
$\exists$	Symbole universel "il existe"

CHAPITRE 1

Rappels d'arithmétique

Divisibilité

Définition 1.1.
Soit $a, b \in \mathbb{Z}$, $b \neq 0$. On dit que b **divise** a s'il existe $c \in \mathbb{Z}$ tel que $a = bc$. On note $b \mid a$ (sinon $b \nmid a$).

Si $a \neq 0 \neq b$, on dit que $d \in \mathbb{N}$ est **le plus grand diviseur commun** de a et de b si :

- $d \mid a$ et $d \mid b$;
- s'il existe $c \in \mathbb{N}$ tel que $c \mid a$ et $c \mid b$, alors $c \leq d$.

Notations : $\text{pgdc}(a, b) = d$ $\qquad$ $(a, b) = d$.

En particulier, si $(a, b) = 1$, on dit que a et b sont **premiers entre eux**.

Remarque 1.2.
Pour trouver le pgdc on utilise l'**algorithme d'Euclide**. Il est basé sur l'observation suivante :

Division euclidienne : si $a, b \in \mathbb{Z}$, $b \neq 0$, alors il existe $q, r \in \mathbb{Z}$ tels que $a = qb + r$ et $|r| < |b|$.
Variante : si $a, b \in \mathbb{Z}$, $b \neq 0$, alors il existe $q, r \in \mathbb{Z}$ tels que $a = qb + r$ et $0 \leq r < |b|$. le couple (q, r) est alors unique.

Identité de Bézout.
Soit $a, b \in \mathbb{Z}$, $a \neq 0 \neq b$. Alors il existe $r, s \in \mathbb{Z}$ tels que $ar + bs = (a, b)$.

Idée de la preuve. On utilise l'algorithme d'Euclide pour trouver $\text{pgdc}(a, b)$ et on remonte les divisions successives pour l'exprimer en fonction de a et b. □

Nombres premiers et factorisation

Définition 1.3.
On dit que $p \in \mathbb{Z} \setminus \{0, \pm 1\}$ est **premier** si $p = ab$ entraîne que soit $a \in \mathbb{Z}^* = \{\pm 1\}$, soit $b \in \mathbb{Z}^*$.

Notation : L'ensemble des premiers de $\mathbb{Z}$ sera noté $\mathbb{P}$.

Proposition 1.4.
Soit $a, b \in \mathbb{Z}$ et $p \in \mathbb{P}$, alors :

$$\textit{Si } p \mid ab \textit{ alors } p \mid a \textit{ ou } p \mid b.$$

Démonstration. Supposons que $p \mid ab$ et $p \nmid a$, i.e $(p, a) = 1$.
Par Bézout : $\exists r, s \in \mathbb{Z}$ tels que $rp + sa = 1$, ainsi en multipliant par b, on obtient :

$$\underbrace{rpb}_{p|} + \underbrace{sab}_{p|} = b \qquad \Rightarrow \qquad p \mid b$$

□

Théorème fondamental de l'arithmétique.
Soit $n \in \mathbb{N}$, $n \neq 0$, $n \neq 1$. Alors il existe des premiers distincts $p_1, \ldots, p_r > 0$ et des entiers positifs $e_1, \ldots, e_r$ tels que :

$$n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$$

Cette décomposition est unique à ordre près des facteurs.

Démonstration.
Existence : Procédons par récurrence sur n.
Les cas $n = 2$ et $n = 3$ sont triviaux puisque 2 et 3 sont premiers.
Supposons alors le théorème vrai pour tous les entiers jusqu'à $n > 3$ et montrons qu'il est vérifié pour $n + 1$.
Si $n + 1$ est premier, alors il n'y a rien à montrer. Sinon, il existe $a, b \in \mathbb{N}_n \setminus \{1\}$ tels que $n + 1 = ab$.
Par hypothèse de récurrence, le théorème est vrai pour a et pour b. Il suffit alors de regrouper les facteurs de a et de b et le théorème est vrai pour $n + 1$.

Unicité : Supposons que n admette deux décompositions premières

$$p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} = q_1^{f_1} \cdot \ldots \cdot q_s^{f_s}.$$

Alors $p_1 \mid q_1^{f_1}, \ldots, q_s^{f_s}$. Ainsi, on peut renuméroter les q_i de telle sorte que $p_1 \mid q_1$. Or q_1 est premier, donc $p_1 = q_1$.
On simplifie les deux côtés de l'équation :

$$p_1^{e_1 - 1} \cdot \ldots, p_r^{e_r} = q_1^{f_1 - 1} \cdot \ldots, q_s^{f_s}.$$

En itérant le raisonnement précédent, on obtient $\{p_i\}_{i=1}^r = \{q_j\}_{j=1}^s$. En particulier, $r = s$ et $\{e_i\}_{i=1}^r = \{f_j\}_{j=1}^s$.

□

Remarques 1.5.

(1) On peut étendre ce théorème à $\mathbb{Z}$. L'unicité de la décompostion première est alors à comprendre à ordre et signe près des facteurs.

(2) Les anneaux intègres possédant la propriété de factorisation unique sont appélés anneaux **factoriels**.

Théorème 1.6 (Euclide)**.**
Il existe une infinité de nombres premiers.

Démonstration. Supposons *ab absurdo* qu'il existe un nombre fini de nombres premiers distincts $p_1 < \ldots < p_s$.
Posons :

$$N := p_s! + 1$$

Ainsi $p_i \nmid N$ pour tout $i = \overline{1,s}$.
Or , d'après le théorème précédent, il existe au moins un premier p tel que $p \mid N$, mais $p \neq p_i$ pour tout $i = \overline{1,s}$. $\lightning$ □

Congruences

Soit $m \in \mathbb{N} \setminus \{0,1\}$.

Définition 1.7.
Soit $a, b \in \mathbb{Z}$. On dit que a et b sont **congrus modulo m** si $m \mid (b-a)$.
Notation : $a \equiv b \mod m$.

La relation "$\equiv \mod m$" est une relation d'équivalence sur $\mathbb{Z}$ (elle est réflexive, symétrique et transitive).
On note $\mathbb{Z}/m\mathbb{Z}$ l'ensemble des classes d'équivalence, aussi appelées **classes de congruences modulo** m.

Propriété 1.8.
Si $a, a', b, b' \in \mathbb{Z}$ sont tels que

$$a \equiv a' \mod m \quad \textit{et} \quad b \equiv b' \mod m$$

alors

$$a + b \equiv a' + b' \mod m \quad \textit{et} \quad ab \equiv a'b' \mod m.$$

Démonstration. $a \equiv a' \mod m \Rightarrow m \mid a' - a$ et
$b \equiv b' \mod m \Rightarrow m \mid b' - b$.
Ainsi, $m \mid [(a' - a) + (b' - b)] = (a' + b') - (a + b)$. D'où $a + b \equiv a' + b' \mod m$.
En outre,

$$m \mid [a' \underbrace{(b' - b)}_{m\mid} + \underbrace{(a' - a)}_{m\mid} b] = a'b' - a'b + a'b - ab = a'b' - ab$$

d'où $ab \equiv a'b' \mod m$. □

Pour tout $a \in \mathbb{Z}$, on note $[a] = [a]_m = m\mathbb{Z} + a$ la classe de a dans $\mathbb{Z}/m\mathbb{Z}$.
On définit alors les deux opérations suivantes :

$$[a]_m + [b]_m := [a+b]_m \quad \forall a, b \in \mathbb{Z}/m\mathbb{Z}$$

$$[a]_m \cdot [b]_m := [ab]_m \quad \forall a, b \in \mathbb{Z}/m\mathbb{Z}$$

La propriété précédente nous assure que ces deux opérations sont bien-définies. En outre, on vérifie facilement que, muni de ces deux lois, $\mathbb{Z}/m\mathbb{Z}$ est élevé au rang d'anneau commutatif.

Définition 1.9.
Soit A un anneau commutatif.

- Un élément $u \in A$ est une **unité** s'il existe $v \in A$ tel que $uv = 1_A$.
  On note A^* l'ensemble des unité de A. Il s'agit d'un groupe ! !
- Un élément $a \in A \setminus \{0\}$ est un **diviseur de zéro** s'il existe $b \in A \setminus \{0\}$ tel que $ab = 0_A$.
- On dit que A est **intègre** s'il n'admet pas de diviseur de zéro.

Théorème 1.10.
Soit $m \in \mathbb{N}$, $m > 1$, et $a \in \mathbb{Z}$. Alors,

(1) *si $m \mid a$, alors $[a] = [0]$ dans $\mathbb{Z}/m\mathbb{Z}$;*
(2) *$(m, a) = 1$ si et seulement si $[a] \in (\mathbb{Z}/m\mathbb{Z})^*$;*
(3) *si $1 < (m, a) < m$, alors $[a]$ est un diviseur de $[0]_m$.*

Démonstration.

(1) $m \mid a \;\Leftrightarrow\; m \mid (a - 0) \;\Leftrightarrow\; a \equiv 0 \mod m$.
(2) Si $(m, a) = 1$, alors par Bézout il existe $r, s \in \mathbb{Z}$ tels que $1 = mr + as$. Ainsi
$$[1]_m = [mr + as]_m = [mr]_m + [as]_m = [0]_m + [a]_m[s]_m = [a]_m[s]_m .$$
D'où $[a] \in (\mathbb{Z}/m\mathbb{Z})^*$.
La réciproque est banale puisque si $[a]_m$ est une unité, alors il existe $s \in \mathbb{Z}$ tel que $[1]_m = [a]_m[s]_m$ et donc il existe $r \in \mathbb{Z}$ tel que $1 = as + rm$, i.e $(a, m) = 1$.
(3) Remarquons d'abord que si $1 < (m, a) < m$, alors a est nécessairement non-nul. Soit donc $d = (a, m)$. Alors il existe $r, s \in \mathbb{Z}$ tels que $ar + ms = d$. En outre, il existe $e, f \in \mathbb{Z} \setminus \{0\}$ tels que $m = ed$ et $a = fd$. Par conséquent,
$$[a]_m[e]_m = [fde]_m = [f]_m[m]_m = [f]_m[0]_m = [0]_m.$$
Ainsi $[a]_m$ est un diviseur de zéro dans $\mathbb{Z}/m\mathbb{Z}$.

□

Corollaire 1.11.
L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier.

Démonstration. L'ensemble $\mathbb{Z}/p\mathbb{Z}$ étant un anneau commutatif, il reste à montrer que tout élément non-nul est une unité si et seulement si p est premier.
Soit $[a] \in \mathbb{Z}/p\mathbb{Z}$, $[a] \neq [0]_p$. Alors $p \nmid a$ et p étant premier on a $(p, a) = 1$ si et seulement si $[a]$ est une unité dans $\mathbb{Z}/p\mathbb{Z}$.
Réciproquement si tout élément $[a] \neq [0]$ dans $\mathbb{Z}/p\mathbb{Z}$ est une unité alors tout entier $a \in \mathbb{N}$ tel que $1 \leq a < p$ est premier à p, donc p est premier. □

Notation : On note $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Définition 1.12 (Indicatrice d'Euler)**.**
Soit $m \in \mathbb{Z}$, $m > 1$. L'**indicatrice d'Euler** de m est par définition le nombre :
$$\varphi(m) := \#(\mathbb{Z}/m\mathbb{Z})^*$$

Proposition 1.13.
Soit p un nombre premier. Alors $\varphi(p) = p - 1$.

Démonstration. Banal, $\mathbb{F}_p$ étant un corps, on a $\#\mathbb{F}_p^* = \#\mathbb{F}_p - 1 = p - 1$. □

Proposition 1.14.
Soit p un nombre premier et $r \geq 1$ un entier. Alors $\varphi(p^r) = p^r - p^{r-1}$.

Démonstration. D'après le point (2) du théorème 1.10 calculer $\varphi(p^r)$ revient à compter le nombre d'éléments premiers à p^r parmi les nombres $1, \ldots, p^r$. Il est en fait plus simple de compter les éléments non premiers à p^r.
Posons $P := \{n \in \mathbb{N} \mid n < p^r \text{ et } p \mid n\}$. Alors $n \in P$ si et seulement si $n = pm < p^r$ pour un certain $m \in \mathbb{Z}$ si et seulement si $n = pm$ avec $m < p^{r-1}$.
D'où :

$$\varphi(p^r) = \#(\mathbb{Z}/p^r\mathbb{Z})^* = \#(\mathbb{Z}/p^r\mathbb{Z}) - \#P = p^r - p^{r-1}$$

□

Proposition 1.15.
Soit $m_1, m_2 \in \mathbb{N}$, $m_1, m_2 > 1$ tels que $(m_1, m_2) = 1$.
Alors :

$$\varphi(m_1 m_2) \;=\; \varphi(m_1)\varphi(m_2)$$

Pour montrer cette proposition, nous aurons besoin du lemme des restes chinois.

Lemme des restes chinois.
Soit $m_1, m_2 \in \mathbb{N}$, $m_1, m_2 > 1$ tels que $(m_1, m_2) = 1$. Posons $m := m_1 m_2$. Alors l'application naturelle

$$\begin{array}{rccc} f: & \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \\ & [a]_m & \longmapsto & ([a]_{m_1}, [a]_{m_2}) \end{array}$$

est un isomorphisme d'anneaux.

Démonstration. L'application f est bien-définie puisque si $[a]_{m_1 m_2} = [b]_{m_1 m_2}$ alors il existe $s \in \mathbb{Z}$ tel que $a = b + sm_1 m_2 = b + (sm_1)m_2 = b + (sm_2)m_1$, ie. $[a]_{m_2} = [b]_{m_2}$ et $[a]_{m_1} = [b]_{m_1}$. Il s'agit clairement aussi d'un homorphisme d'anneaux. Montrons qu'il est bijectif.

Injectivité. Soit $a \in \mathbb{Z}$ tel que $([0]_{m_1}, [0]_{m_2}) = ([a]_{m_1}, [a]_{m_2})$.
Donc $m_1 \mid a$ et $m_2 \mid a$. Ainsi $(m_1, m_2) = 1$ entraîne que $m \mid a$. Par conséquent, $[a]_m = [0]_m$ et f est de ce fait injectif.

Surjectivité. $\#(\mathbb{Z}/m\mathbb{Z}) = m = m_1 m_2 = \#[\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}]$. Ainsi f injectif implique que f est aussi surjectif.

□

Corollaire 1.16.
Soit $m_1, \ldots, m_r \in \mathbb{N}$, $m_i > 1 \; \forall\, i = \overline{1, r}$, avec $(m_i, m_j) = 1$ si $i \neq j$. Posons $m := \prod_{i=1}^{r} m_i$.
Alors :

$$\mathbb{Z}/m\mathbb{Z} \cong \prod_{i=1}^{r} (\mathbb{Z}/m_i\mathbb{Z})$$

Démonstration. On applique le lemme des restes chinois de façon successive à des paires de facteurs de $\prod_{i=1}^{r}(\mathbb{Z}/m_i\mathbb{Z})$. □

Reformulation du lemme des restes chinois. (Enoncé traditionnel).
Soit $m_1, \ldots, m_r \in \mathbb{N}$, $m_i > 1 \; \forall\, i = \overline{1, r}$, avec $(m_i, m_j) = 1$ si $i \neq j$. Soit $a_1, \ldots, a_r \in \mathbb{Z}$.

Alors, il existe un unique $a \in \mathbb{Z}$ tel que

$$a \equiv \begin{cases} a_1 & \mod m_1 \\ \cdots & \\ a_r & \mod m_r. \end{cases}$$

Exemple 1.17.
Prenons $m_1 = 7$, $m_2 = 11$, $m_3 = 13$ ainsi que $a_1 = -1$, $a_2 = -1$ et $a_3 = -1$. On cherche $a \in \mathbb{Z}$ tel que

$$a \equiv \begin{cases} -1 & \mod 7 \\ -1 & \mod 11 \\ -1 & \mod 13. \end{cases}$$

On trouve

$$1000 \equiv \begin{cases} -1 & \mod 7 \\ -1 & \mod 11 \\ -1 & \mod 13. \end{cases}$$

Ainsi $a \equiv 1000 \mod 7 \cdot 11 \cdot 13 = 1001$.

Proposition 1.18.
Soit A, B deux anneaux commutatifs ainsi que A^* et B^* leurs groupes des unités respectifs. Soit $f : A \longrightarrow B$ un homomorphisme d'anneaux. Alors f induit un homomorphisme de groupes $f|_{A^*} : A^* \longrightarrow B^*$.

Démonstration. Découle du fait que l'image d'une unité par un homomorphisme d'anneaux est encore une unité. □

En particulier, $f : \mathbb{Z}/m\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$ induit un isomorphisme de groupes :

$$f : (\mathbb{Z}/m\mathbb{Z})^* \longrightarrow (\mathbb{Z}/m_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/m_r\mathbb{Z})^*$$

Nous sommes maintenant ainsi en mesure de démontrer la proposition 1.15.

Proposition 1.19.
Soit $m_1, \ldots, m_r \in \mathbb{N}$, $m_i > 1$ $\forall\, i = \overline{1, r}$, avec $(m_i, m_j) = 1$ si $i \neq j$. Alors :

$$\varphi(m_1 \cdots m_r) = \varphi(m_1) \cdot \cdots \cdot \varphi(m_r)$$

Démonstration. En effet, en se basant sur la remarque ci-dessus on peut écrire

$$\begin{aligned} \varphi(m_1 \cdots m_r) &= \#(\mathbb{Z}/(m_1 \cdots m_r)\mathbb{Z})^* \\ &= \#(\mathbb{Z}/m_1\mathbb{Z})^* \cdot \cdots \cdot \#(\mathbb{Z}/m_r\mathbb{Z})^* \\ &= \varphi(m_1) \cdot \cdots \cdot \varphi(m_r)\,. \end{aligned}$$

□

Remarque 1.20.
Ce dernier résultat permet de calculer $\varphi(a)$ pour tout $a \in \mathbb{N}$, $a > 1$. En effet, $a = p_1^{e_1} \cdots p_r^{e_r}$ pour des premiers distincts $p_1, \ldots, p_r$ et des entiers naturels $e_1, \ldots, e_r$. Etant donné que $(p_i^{e_i}, p_j^{e_j}) = 1$ si $i \neq j$, il vient

$$\varphi(a) = \varphi(p_1^{e_1}) \cdots \varphi(p_r^{e_r}) = p_1^{e_1 - 1}(p_1 - 1) \cdots p_r^{e_r - 1}(p_r - 1)\,.$$

Théorème d'Euleur et petit théorème de Fermat

Théorème 1.21 (Euler)**.**
Soit $m \in \mathbb{N}$, $m > 1$, et soit $a \in \mathbb{Z}$ tel que $(a, m) = 1$. Alors :

$$a^{\varphi(m)} \equiv 1 \mod m$$

Démonstration. Considérons le groupe $G := (\mathbb{Z}/m\mathbb{Z})^*$. Sa cardinalité est $\varphi(m)$. Or d'après le théorème de Lagrange, l'ordre de tout élément de G divise l'ordre, $\varphi(m)$, de ce dernier. Ainsi

$$[a^{\varphi(m)}]_m = [a]_m^{\varphi(m)} = 1_G \,.$$

D'où $a^{\varphi(m)} \equiv 1 \mod m$. □

Corollaire 1.22 (Petit théorème de Fermat)**.**
Soit $p \in \mathbb{N}$ un nombre premier et $a \in \mathbb{Z}$ tel que $p \nmid a$.
Alors :

$$a^{p-1} \equiv 1 \mod p$$

Remarque 1.23.
Le petit théorème de Fermat est utilisé dans les tests de primalité. On choisit un $n \in \mathbb{N}$ et on souhaite savoir si n est premier ou non. En effet, s'il existe $a \in \mathbb{Z}$ tel que $a^{n-1} \not\equiv 1 \mod n$ alors n n'est pas premier.

Définition 1.24.
Un entier $n \in \mathbb{N}$ est dit **2-pseudo-premier** s'il est composé et si $2^{n-1} \equiv 1 \mod n$.

On constate qu'il n'existe que très peu de nombres 2-pseudo-premiers.

CHAPITRE 2

Corps finis

Rappels algébriques

1. La caractéristique d'un anneau

Rappelons que pour tout anneau A, il existe un unique homomorphisme d'anneau :

$$\begin{array}{rccl} \eta_A : & \mathbb{Z} & \longrightarrow & A \\ & n & \longmapsto & \eta_A(n) = n_A := \begin{cases} n \cdot 1_A := \underbrace{1_A + \ldots + 1_A}_{n \text{ fois}} & \text{si } n > 0 \\ 0_A & \text{si } n = 0 \\ n \cdot 1_A := \underbrace{(-1_A) + \ldots + (-1_A)}_{-n \text{ fois}} & \text{si } n < 0 \end{cases} \end{array}$$

Son noyau est un idéal de $\mathbb{Z}$: $\ker \eta_A := m\mathbb{Z}$ pour un certain $m \in \mathbb{N}$ appelé la **caractéristique** de A et on note $\operatorname{car}(A) := m$.

En outre si A est un anneau intègre, sa caractéristique est soit nulle soit un nombre premier. En effet, si η_A est injectif alors $\ker \eta_A = \{0\} = 0\mathbb{Z}$, i.e $\operatorname{car}(A) = 0$. Par contre si η_A n'est pas injectif, alors $\ker \eta_A \neq \{0\}$ et donc $m \neq 0$. Supposons alors *ab absurdo* que $m \notin \mathbb{P}$, alors il existe $u, v \in \mathbb{N}$, $1 < u, v < m$, tels que $m = u \cdot v$. Ainsi,

$$0_A = m \cdot 1_A = (u \cdot v) \cdot 1_A = (u \cdot 1_A) \cdot (v \cdot 1_A) = \underbrace{u_A}_{\neq 0_A} \cdot \underbrace{v_A}_{\neq 0_A}.$$

Autrement dit, A n'est pas intègre. $\lightning$ Donc $m \in \mathbb{P}$.

2. Extensions de corps

Soit $\mathbb{E}$ un corps. Si $\mathbb{F}$ est un sous-corps de $\mathbb{E}$, alors $\mathbb{E}$ est appelé une **extension** du corps $\mathbb{F}$, et l'on note $\mathbb{F} \subseteq \mathbb{E}$.

Alors $\mathbb{E}$ est un $\mathbb{F}$-espace vectoriel. (Les axiomes d'espaces vectoriels découlent immédiatement des axiomes d'anneaux de $\mathbb{E}$ et du fait que $\mathbb{F}$ est un sous-anneau de $\mathbb{E}$.)

On appelle **degré** d'une extension de corps $\mathbb{F} \subseteq \mathbb{E}$, noté $[\mathbb{E} : \mathbb{F}]$, la dimension de $\mathbb{E}$ en tant que $\mathbb{F}$-espace vectoriel :

$$[\mathbb{E} : \mathbb{F}] := \dim_{\mathbb{F}} \mathbb{E}$$

Si $\mathbb{F} \subseteq \mathbb{E}$ est une extension de corps et $\alpha \in \mathbb{E}$, alors on définit l'**extension de** $\mathbb{F}$ **par** α, notée $\mathbb{F}(\alpha)$, comme étant le plus petit sous-corps de $\mathbb{E}$ contenant à la fois $\mathbb{F}$ et α :

$$\mathbb{F}(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} \mid f, g \in \mathbb{F}[X] \text{ et } g(\alpha) \neq 0 \in \mathbb{E}\}$$

En particulier, si α est algébrique sur $\mathbb{F}$ alors :

$$\mathbb{F}(\alpha) = \mathbb{F}[\alpha]$$

Nous avons en fait le critère d' "algébritude" pour les éléments de $\mathbb{E}$ suivant :

$$a \in \mathbb{E} \text{ algébrique sur } \mathbb{F} \quad \Leftrightarrow \quad [\mathbb{F}(\alpha) : \mathbb{F}] < \infty$$

Par ailleurs, si $a \in \mathbb{E}$ est effectivement algébrique sur $\mathbb{F}$, alors en appliquant le 1^{er} théorème d'isomorphie à l'homomorphisme $ev_a : \mathbb{F}[X] \longrightarrow \mathbb{F}(a)$ on obtient l'isomorphisme suivant :

$$\mathbb{F}[X]/ < \mu_a(X) > \cong \mathbb{F}(\alpha)$$

où $\mu_a(X) \in \mathbb{F}[X]$ est le polynôme minimal de a.
Par suite, on obtient,

$$[\mathbb{F}(\alpha) : \mathbb{F}] = \deg \mu_a(X).$$

Définitions et propriétés

Définition 2.1.
Un **corps fini** est un corps de cardinalité finie.

Proposition 2.2.
Soit K un corps fini. Alors il existe $p \in \mathbb{P}$ et $n \in \mathbb{N}$ tels que $\#K = p^n$.

Démonstration. Tout corps est intègre, ainsi par ce qui précède, $\text{car}(K) = p$ pour un certain $p \in \mathbb{P}$. Ainsi $\mathbb{F}_p$ s'injecte dans K :

$$\begin{array}{ccc} \mathbb{F}_p & \hookrightarrow & K \\ [n]_p & \mapsto & n_K \end{array}$$

En d'autres termes, K est une extension de degré fini $n \in \mathbb{N}$ de $\mathbb{F}_p$ et donc $\#K = p^n$. □

Scholie 2.3.
La caractéristique d'un corps fini à p^n éléments est p.

Théorème 2.4.
Soit $p \in \mathbb{P}$, $n \in \mathbb{N}$ et posons $q := p^n$. Alors :

(a) *Il existe un corps fini à q éléments ;*

(b) *Si K et K' sont deux corps avec $\#K = q = \#K'$, alors $K \cong K'$. Autrement dit, à isomorphisme près, il existe un unique corps à q éléments.*
On le notera $\mathbb{F}_q$.

(c) *Soit K un corps à q éléments. Alors, le groupe multiplicatif K^* est cyclique d'ordre $q - 1$.*

(d) *Soit K un corps à q éléments. Alors, tout élément de K est racine du polynôme*

$$F(X) = X^q - X \in \mathbb{F}_p[X].$$

De plus, F se décompose en facteurs linéaires sur K :

$$F(X) := \prod_{\alpha \in K} (X - \alpha) \quad \in K[X].$$

Démonstration.

(a) Soit $F(X) = X^q - X \in \mathbb{F}_p[X]$. Soit L une extension de $\mathbb{F}_p$ contenant toutes les racines de F, par exemple le corps de rupture de F. Posons $K := \{\alpha \in L \,|\, \alpha^q = \alpha\}$ l'ensemble des racines de F dans L.
Montrons que K est un corps. Il suffit, en fait, de voir que K est un sous-corps de L.

- $1 \in K$, banal.
- Soit $x, y \in K$, alors $(xy)^q = x^q y^q = xy$, i.e $xy \in K$.
  De plus $(x+y)^q = x^q + p(...) + y^q = x^q + y^q = x + y$ puisque la caractéristique de L est p. Ainsi $x + y \in K$.
- Soit $x \in K$ et z son inverse dans L. Alors $xz = 1 = zx$ et de ce fait $z^q = z^q \cdot 1 = z^q xz = z^q x^q z = (zx)^q z = 1 \cdot z = z$, i.e $z \in K$.

Il reste à voir que la cardinalité de K est q.
Comme tout élément de K est racine de F, on a $\#K \leq q = \deg f$. Pour montrer l'égalité, il suffit de voir que F ne possède pas de racine multiple. Observons,

$$F'(X) = \underbrace{qX^{q-1}}_{=0} - 1 = -1 \ \in \mathbb{F}_p[X].$$

Ainsi, F' n'a aucune racine, ce qui implique que toutes les racines de F sont distinctes[1].
D'où $\#K = q$.

(b) Soit K et K' deux corps tels que $\#K = q = \#K'$.
Par (c) nous savons que K^* est cyclique. Soit donc $\alpha \in K$ un générateur de ce groupe cyclique : $K^* =< \alpha >$.
Par conséquent $K = \mathbb{F}_p(\alpha)$. En effet :

- $'' \subseteq'' :$ $K = \{0, \alpha^1, \ldots, \alpha^{q-1}\} \subseteq \mathbb{F}_p(\alpha)$.
- $'' \supseteq'' :$ $\mathbb{F}_p(\alpha)$ est le plus petit corps qui contient $\mathbb{F}_p$ et α. Or $\mathbb{F}_p \subseteq K$ et $\alpha \in K$ entraîne que $\mathbb{F}_p(\alpha) \subseteq K$.

Soit $f_\alpha \in \mathbb{F}_p[X]$ le polynôme minimal de α. Ainsi

$$K = \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[X]/ < f_\alpha > \ .$$

Par ailleurs, α est une racine commune de $F(X) = X^q - X \in \mathbb{F}_p[X]$ et de $f_\alpha \in \mathbb{F}_p[X]$, qui est irréductible. Donc $f_\alpha \,|\, F$.
Maintenant, K' est aussi un corps à q éléments, ainsi, par le point (d), les éléments de K' sont racines de F. Or $f_\alpha \,|\, F$, il existe donc un élément $\alpha' \in K'$ qui soit racine de f_α. Comme f_α est irréductible, il s'agit aussi du polynôme minimal de α'. Il vient :

$$K' \supseteq \mathbb{F}_p(\alpha') \cong \mathbb{F}_p[X]/ < f_\alpha > \cong \mathbb{F}_p(\alpha) = K$$

Finalement $\#K = q = \#K'$ implique que $K \cong K'$.

(c) Soit K un corps à q éléments. Alors K^* est un groupe à $q - 1$ éléments. Montrons qu'il est cyclique. En fait, il s'agit d'un cas particulier du lemme suivant :

1. Soit F un corps et $f \in F[X]$. Alors, f à une racine multiple si et seulement s'il existe $g(X)$ tel que $\deg g > 0$ et $g(X) | f(X)$ et $g(X) | D(f(X))$.

Lemme 2.5.
Soit F un corps et H un sous-groupe fini de F^*. Alors H est cyclique.

Démonstration. Tout corps étant commutatif, H est abélien. Ainsi d'après le théorème de décomposition des groupes abéliens finis, on a

$$H \cong C_{d_1} \times \cdots \times C_{d_m} \qquad \text{où} \quad d_1 | \ldots | d_m.$$

Par conséquent, $\#H = d_1 \cdots d_m$.
Or, si $\alpha \in H$, alors l'ordre de α $o(\alpha) | d_m$.
$\Rightarrow \alpha$ est une racine du polynôme X^{d_m}, qui possède au plus d_m racines.
$\Rightarrow \#H = d_1 \cdots d_m \leq d_m$.
$\Rightarrow d_1 = \ldots = d_{m-1} = 1$.
Ainsi $H \cong C_{d_m}$, qui est cyclique. □

(d) Soit $\alpha \in K^*$. Alors $\alpha^{\#K^*} = \alpha^{q-1} = 1_K$ par le théorème de Lagrange.
Ainsi tout $\alpha \in K$ satisfait $\alpha^q = \alpha$, i.e tout $\alpha \in K$ est racine de $F(X) = X^q - X$.
Donc $(X - \alpha) | F(X)$ pour tout $\alpha \in K$. Ainsi $\prod_{\alpha \in K}(X - \alpha) | F(X)$.
Les deux polynômes étant de degré q et unitaires, on obtient que

$$F(X) := \prod_{\alpha \in K}(X - \alpha) \quad \in K[X].$$

□

Proposition 2.6.
Soit $f \in \mathbb{F}_p[X]$ un polynôme irréductible de degré $n \geq 1$ et posons $q = p^n$.
Alors f divise $X^q - X$.

Démonstration. Soit α une racine de f. Il existe une extension L de $\mathbb{F}_p$ contenant α. On a alors $\mathbb{F}_p(\alpha) \subseteq L$.
Comme f est irréductible, il s'agit du polynôme minimal de α, par conséquent :

$$\mathbb{F}_p[X]/ < f > \cong \mathbb{F}_p(\alpha) =: K \qquad \text{et} \qquad [K : \mathbb{F}_p] = \deg f = n.$$

Ainsi K est un corps fini a q éléments et par le point (d) du théorème précédent on obtient que α est une racine de $F(X) = X^q - X \in \mathbb{F}_p[X]$. Ainsi F et f ont une racine en commun et donc f étant irréductible, on obtient que $f | F$. □

Exemple 2.7.
Posons $p = 2$ et $n = 3$, alors $p^n = 2^3 = 8$.
$F(X) = X^8 - X \in \mathbb{F}_8[X]$.
Sur $\mathbb{F}_2$ on a $F(X) = X(X + 1)(X^3 + X \leq +1)(X \geq +X + 1)$. On a alors

$$K = \mathbb{F}_2[X]/ < X^3 + X \leq +1 > \cong \mathbb{F}_2(\alpha) = \{0, 1, \alpha, \alpha + 1, \alpha \leq, \alpha \leq +1, \alpha \leq +\alpha, \alpha \leq +\alpha + 1\}$$

pour α une racine de $X^3 + X \leq +1$.
De faÁon similaire, on obtient

$$K' = \mathbb{F}_2[X]/ < X^3 + X + 1 > \cong \mathbb{F}_2(\beta)$$

pour β une racine de $X^3 + X + 1$.
Ainsi :

$$K \cong \mathbb{F}_8 \cong K'$$

Automorphisme de Frobenius

Soit K un corps et $n \in \mathbb{N}$. Notons alors $K^n = \{x^n \mid x \in K\}$.

Proposition-Définition 2.8.
Supposons que $\mathrm{car}(K) = p \neq 0$. *Alors l'application*

$$\begin{array}{rccc} \varphi : & K & \longrightarrow & K^p \\ & x & \longmapsto & x^p \end{array}$$

est un isomorphisme du corps K sur son sous-corps K^p.
Si K est un corps fini, alors φ *est un automorphisme de K, appelé* **automorphisme de Frobenius**.

Démonstration.

- $\varphi(1) = 1$
- $\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y)$
- $\varphi(x + y) = (x + y)^p = x^p + p(...) + y^p = x^p + y^p = \varphi(x) + \varphi(y)$ puisque $\mathrm{car}(K) = p$.

L'application φ est donc bien d'un homomorphisme de corps. Elle est clairement surjective par définition de K^p. Elle est aussi injective puisque tout homomorphisme de corps non nul est injectif. (En effet, le noyau est un idéal, donc dans le cas d'un corps il est soit nul soit égal au corps tout entier.)
A supposer que K soit un corps fini, on obtient $K \cong K^p$ et donc $\#K = \#K^p$. D'où $K^p = K$. □

Racines primitives mod p et conjecture d'Artin

Si p est un nombre premier, on sait que $\mathbb{F}_p^*$ est un groupe cyclique.

Définition 2.9.
Soit $a \in \mathbb{Z}$ et $p \in \mathbb{P}$ tels que $p \nmid a$.
On dit que a est une **racine primitive modulo** p si $[a]_p$ engendre $\mathbb{F}_p^*$.

Exemple 2.10.
2 racine primitive mod 11 mais pas mod 7.
3 racine primitive mod 7.

Conjecture d'Artin. *Il existe une infinité de premiers p tels que* 2 *soit une racine primitive modulo p.*

Généralisation. *Tout* $a \in \mathbb{N}$ *qui n'est pas un carré est une racine primitive modulo p pour une infinité de premiers p.*

Remarque 2.11.
Hypothèse de Riemann $\Longrightarrow$ Conjecture d'Artin.

Définition 2.12.
Soit K un corps et soit $n \in \mathbb{N}$.
On dit que $\alpha \in K$ est une **racine n-ième de l'unité** si $\alpha^n = 1_K$.

Exemples 2.13.

(1) $K = \mathbb{C}$, alors $\alpha = e^{2i\pi/n}$ est une racine n-ième de l'unité.

(2) $K = \mathbb{F}_q$, alors tout $\alpha \neq 0$ est une racine $(q-1)$-ième de l'unité puisque $\#\mathbb{F}_q^* = q - 1$.

(3) K corps quelconque, $H < K^*$ tel que H fini quelqconque, alors tout $\alpha \in H$ est une racine de l'unité puisque H est cyclique.

Définition 2.14.
Soit K un corps et soit $n \in \mathbb{N}$.
On dit que $\alpha \in K$ est une **racine primitive n-ième de l'unité** si $\alpha^n = 1_K$ mais $\alpha^m \neq 1_K \; \forall \, m \in \mathbb{N}_{n-1}$.

Exemples 2.15.

(1) $K = \mathbb{C}$, alors $e^{2i\pi k/n}$ est une racine n-ième primitive de l'unité $\Leftrightarrow (k, n) = 1$.

(2) $K = \mathbb{F}_p$. Soit $a \in \mathbb{Z}$ tel que $p \nmid a$.
Alors a est une racine primitive mod $p \Leftrightarrow [a]_p$ est une racine primitive $(p-1)$-ième de l'unité dans $\mathbb{F}_p$.

CHAPITRE 3

La loi de la réciprocité quadratique

Symbole de Legendre

Soit p un nombre premier et $a \in \mathbb{Z}$ un entier.

Définition 3.1.
On dit que a est un **résidu quadratique mod p** ou plus simplement un **carré mod p** si $[a]_p \in \mathbb{F}_p^2 := \{x^2 \mid x \in \mathbb{F}_p\}$.

Symbole de Legendre.
Soit $p \in \mathbb{P}$, $p \neq 2$. Soit $a \in \mathbb{Z}$ tel que $p \nmid a$. On définit le symbole de Legendre comme suit :

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

Remarque 3.2.
Si $p = 2$ alors tout $a \in \mathbb{Z}$ est un carré modulo 2.

Remarque 3.3.
Soit $p \neq 2$ un premier et $a, b \in \mathbb{Z}$ tels que $p \nmid a$ et $p \nmid b$. Alors

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Le symbole de Legendre induit une application

$$\begin{array}{ccc} \mathbb{F}_p^* & \longrightarrow & \{\pm 1\} \\ [a]_p & \longmapsto & \left(\frac{a}{p}\right) \end{array}$$

que l'on peut étendre à tout $\mathbb{F}_p$ en posant $\left(\frac{a}{p}\right) := 0$ si $p \mid a$.

Loi de la réciprocité quadratique (Gauss 1796)**.**
Soit $p, l \neq 2$ deux nombres premiers distincts. Alors :

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

Notation 3.4.
Pour tout $n \in \mathbb{N}$ impaire, posons

$$\varepsilon(n) := [\frac{n-1}{2}] \mod 2 = \begin{cases} 0 & \text{si } n \equiv 1 \mod 4\,, \\ 1 & \text{si } n \equiv 3 \mod 4\,. \end{cases}$$

En effet, si $n \equiv 1 \mod 4$, on peut écrire $n = 4m + 1$ et $\frac{n-1}{2} = 2m \equiv 0 \mod 2$. Si $n \equiv 3 \mod 4$ alors on peut écrire $n = 4m + 3$ et $\frac{n-1}{2} = 2m + 1 \equiv 1 \mod 2$.
Avec cette notation la loi de la réciprocité quadratique devient :

$$\left(\frac{p}{l}\right) = (-1)^{\varepsilon(p)\varepsilon(l)} \left(\frac{l}{p}\right) = \begin{cases} \left(\frac{l}{p}\right) & \text{sinon}\,, \\ -\left(\frac{l}{p}\right) & \text{si } p \equiv l \equiv 3 \mod 4. \end{cases}$$

.

Exemple 3.5.
Est-ce que 7 est un carré modulo 17 ?
Calculons à l'aide de la réciprocité quadratique :

$$\left(\frac{7}{17}\right) = (-1)^{1\cdot 0}\left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = (-1)^{1\cdot 1}\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

($\varepsilon(7) = 1$, $\varepsilon(17) = 0$, $\varepsilon(3) = 1$, $17 \equiv 3 \mod 7$ et $7 \equiv 1 \mod 3$).
Ainsi 7 n'est pas un carré modulo 17.

Première loi supplémentaire.

$$\left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$$

Autrement dit, -1 est un carré mod p si et seulement si $p \equiv 1 \mod 4$.
(Où $p \neq 2$ est un premier).

Notation 3.6.
Pour tout $n \in \mathbb{N}$ impaire, posons

$$\omega(n) := [\frac{n^2-1}{8}] \mod 2 = \begin{cases} 0 & \text{si } n \equiv \pm 1 \mod 8\,, \\ 1 & \text{si } n \equiv \pm 3 \mod 8\,. \end{cases}$$

Deuxième loi supplémentaire.

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

Autrement dit, 2 *est un carré mod p si et seulement si* $p \equiv \pm 1 \mod 8$.
(Où $p \neq 2$ *est un premier).*

Théorème 3.7.
Soit q une puissance d'un nombre premier p.

(1) *Si* $p = 2$ *tout élément de* $\mathbb{F}_q$ *est un carré.*

(2) *Si* $p \neq 2$, *l'ensemble* $\mathbb{F}_q^{*2}$ *est un sous-groupe d'indice* 2 *de* $\mathbb{F}_q^*$, *qui n'est autre que le noyau de l'homomorphisme (de groupes) :*

$$\begin{array}{rccc} \phi : & \mathbb{F}_q^* & \longrightarrow & \{\pm 1\} \\ & x & \longmapsto & x^{\frac{q-1}{2}} \end{array}.$$

Démonstration.

(1) Soit $x \in \mathbb{F}_q$ avec $q = 2^n$, $n \geq 1$. Alors, d'après le théorème 2.4, on a $x^{2^n} - x = 0$, ainsi $x = x^{2^n} = (x^{2^{n-1}})^2$ est un carré.

(2) Commenç ons par montrer que $\mathbb{F}_q^{*2} = \ker \phi$. Soit $x \in \mathbb{F}_q^*$ et y dans une extension de $\mathbb{F}_q$ tel que $y^2 = x$.
Alors $x \in \mathbb{F}_q^{*2} \Leftrightarrow y \in \mathbb{F}_q^* \Leftrightarrow y^{q-1} = 1$.
Maintenant $y^{q-1} = x^{\frac{q-1}{2}} = \pm 1$ puisque $x^{q-1} = 1$ (en effet, $\mathbb{F}_q^*$ est cyclique d'ordre $q-1$).
En résumé, $x \in \mathbb{F}_q^{*2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$. En d'autres termes, $\mathbb{F}_q^{*2} = \ker \phi$.
Calculons son indice. $\mathbb{F}_q^*$ est un groupe cyclique d'ordre $q-1$.

$$\mathbb{F}_q^* = \{x, x^2, \ldots, x^{q-1}\} \text{pour un certain } x \in \mathbb{F}_q \,.$$

$$\mathbb{F}_q^{*\,2} = \{x^2, x^4, \ldots, x^{q-1}\} \;\Rightarrow\; \#\mathbb{F}_q^{*\,2} = \frac{q-1}{2}\,.$$

Ainsi $[\mathbb{F}_q^* : \mathbb{F}_q^{*2}] = \frac{\#\mathbb{F}_q^*}{\#\mathbb{F}_q^{*\,2}} = \frac{(q-1)2}{q-1} = 2$.

□

Corollaire 3.8 (Critère d'Euler)**.**
Soit $p \neq 2$ *un nombre premier et* $a \in \mathbb{Z}$. *Alors :*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$

Démonstration.

· Si $p \mid a$ la formule est banale puisque les deux côtés sont zéro.

· Si $p \nmid a$, alors $a \neq 0$. Considérons $[a] \in \mathbb{F}_p$.

$$\begin{aligned}\left(\frac{a}{p}\right) = 1 &\overset{\text{déf}}{\Leftrightarrow} a \text{ est un carré} \mod p \\ &\Leftrightarrow [a]_p \in \mathbb{F}_p^{*\,2} \\ &\Leftrightarrow ([a]_p)^{\frac{p-1}{2}} = 1 \\ &\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \mod p\end{aligned}$$

□

Remarques 3.9.

(1) On peut aussi définir le symbole de Legendre pour $x \in \mathbb{F}_p$. Si $a \in \mathbb{Z}$ tel que $[a]_p = x$ on pose

$$\left(\frac{x}{p}\right) := \left(\frac{a}{p}\right).$$

C'est bien définit puisque $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$ si $a \equiv a' \mod p \Leftrightarrow [a]_p = [a']_p$.
D'après la démonstration du corollaire on trouve que

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

(2) Ce corollaire montre la multiplicativité du symbole de Legendre :

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \mod p \equiv (a^{\frac{p-1}{2}})(b^{\frac{p-1}{2}}) \mod p \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Sommes de Gauss

Soit $p, l \neq 2$ deux nombres premiers distincts et ω une racine primitive l-ième de l'unité dans une extension Ω de $\mathbb{F}_p$.
Si $x \in \mathbb{F}_l$, l'élément ω^x a un sens puisque $\omega^l = 1$. On choisit $r \in \mathbb{Z}$ tel que $[r]_l = x$ et on pose $\omega^x := \omega^r$. (Cette opération est clairement bien-définie).

Définition 3.10.
On peut ainsi définir la **somme de Gauss** :

$$y := \sum_{x \in \mathbb{F}_l} \left(\frac{x}{l}\right) \omega^x \in \Omega$$

Lemme 3.11.
Soit y la somme de Gauss définie ci-dessus. Alors :

$$y^2 = (-1)^{\varepsilon(l)} l$$

Démonstration.

$$y^2 = (\sum_{t\in\mathbb{F}_l} \left(\frac{t}{l}\right)\omega^t)(\sum_{z\in\mathbb{F}_l} \left(\frac{z}{l}\right)\omega^z)$$

$$= \sum_{t\in\mathbb{F}_l}\sum_{z\in\mathbb{F}_l} \left(\frac{tz}{l}\right)\omega^{t+z}$$

Posons $u := t + z$, alors $z = u - t$ et on obtient

$$y^2 = \sum_{u\in\mathbb{F}_l} \omega^u \sum_{t\in\mathbb{F}_l} \left(\frac{t(u-t)}{l}\right)$$

Maintenant si $t \neq 0$, il vient

$$\left(\frac{t(u-t)}{l}\right) = \left(\frac{-t^2(1-ut^{-1})}{l}\right) = \underbrace{\left(\frac{-1}{l}\right)}_{(-1)^{\varepsilon(l)}} \underbrace{\left(\frac{t^2}{l}\right)}_{1} \left(\frac{1-ut^{-1}}{l}\right) = (-1)^{\varepsilon(l)} \left(\frac{1-ut^{-1}}{l}\right).$$

Par conséquent,

$$(-1)^{\varepsilon(l)} y^2 = \sum_{u\in\mathbb{F}_l} c_u \omega^u \quad \text{où } c_u = \sum_{t\in\mathbb{F}_l^*} \left(\frac{1-ut^{-1}}{l}\right).$$

Maintenant, si $u = 0$ alors

$$c_0 = \sum_{t\in\mathbb{F}_l^*} \underbrace{\left(\frac{1}{l}\right)}_{1} = l - 1\,.$$

Si $u \neq 0$, en posant $s := 1 - ut^{-1} \in \mathbb{F}_l^* \setminus \{1\}$ on obtient

$$c_u = [\sum_{s\in\mathbb{F}_l^*} \left(\frac{s}{l}\right)] - \left(\frac{1}{l}\right).$$

Or d'après le théorème 3.7 #{carrés de $\mathbb{F}_l^*$}=#{non carrés de $\mathbb{F}_l^*$}, ainsi

$c_u = -\left(\frac{1}{l}\right) = -1.$

Revenons au calcul de y^2, il vient

$$(-1)^{\varepsilon(l)} y^2 = \sum_{u\in\mathbb{F}_l} c_u \omega^u = l - 1 + \sum_{u\in\mathbb{F}_l^*} (-\omega^u)$$

or,

$$\sum_{u\in\mathbb{F}_l^*} (\omega^u) = (\sum_{k=1}^{l} \omega^k) - \omega^l = \omega\frac{1-\omega^l}{1-\omega} - \omega^l = \omega\frac{1-1}{1-\omega} - 1 = -1$$

ainsi $(-1)^{\varepsilon(l)} y^2 = l - 1 + 1 = l$. D'où $y^2 = (-1)^{\varepsilon(l)} l$. □

Lemme 3.12.
Soit y la somme de Gauss définie ci-dessus. Alors :

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

Démonstration. En utilisant le fait que Ω est de caractéristique p, on obtient :

$$y^p = (\sum_{x\in\mathbb{F}_l}\left(\frac{x}{l}\right)\omega^x)^p = \sum_{x\in\mathbb{F}_l}\left(\frac{x}{l}\right)^p \omega^{xp}$$
$$= \sum_{x\in\mathbb{F}_l}\left(\frac{x}{l}\right)\omega^{xp}$$

Posons $z := xp$ alors :

$$y^p = \sum_{z\in\mathbb{F}_l}\left(\frac{zp^{-1}}{l}\right)\omega^z = \left(\frac{p^{-1}}{l}\right)\underbrace{\sum_{z\in\mathbb{F}_l}\left(\frac{z}{l}\right)\omega^z}_{y}$$

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

puisque $\left(\frac{p^{-1}}{l}\right)\left(\frac{p}{l}\right) = \left(\frac{p^{-1}p}{l}\right) = \left(\frac{1}{l}\right) = 1$. Ainsi

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

□

Preuve de la réciprocité quadratique

Preuve de la formule de la réciprocité quadratique.

$$\left(\frac{p}{l}\right) \overset{lem.2}{=} y^{p-1} = (y^2)^{\frac{p-1}{2}} \overset{Euler}{=} \left(\frac{y^2}{p}\right)$$
$$\overset{lem.1}{=} \left(\frac{(-1)^{\varepsilon(l)}l}{p}\right)$$
$$\overset{Euler}{=} (-1)^{\varepsilon(l)\frac{p-1}{2}}\left(\frac{l}{p}\right)$$
$$= (-1)^{\varepsilon(l)\varepsilon(p)}\left(\frac{l}{p}\right).$$

□

Lois supplémentaires.

$$(1) \quad \left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)} = \begin{cases} 1 & si\ p \equiv 1 \mod 4 \\ -1 & si\ p \equiv 3 \mod 4 \end{cases}$$

$$(2) \quad \left(\frac{2}{p}\right) = (-1)^{\omega(p)} = \begin{cases} 1 & si\ p \equiv \pm 1 \mod 8 \\ -1 & si\ p \equiv \pm 3 \mod 8 \end{cases}$$

Démonstration.

(1) Claire par le critère d'Euler puisque $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\varepsilon(p)}$.

(2) Soit α une racine primitive 8-ième de l'unité dans une extension de $\mathbb{F}_p$. Alors

$$\alpha^8 = 1 \ \Rightarrow\ \alpha^4 = -1 \ \Rightarrow\ \alpha^2 = -\alpha^{-2} \ \Rightarrow\ \alpha^2 + \alpha^{-2} = 0.$$

Posons $y := \alpha + \alpha^{-1}$, alors $y^2 = \underbrace{\alpha^2 + \alpha^{-2}}_{0} + 2\underbrace{\alpha\alpha^{-1}}_{1} = 2$ et puisque α est dans un corps de caractéristique p, on a $y^p = \alpha^p + \alpha^{-p}$.

Si $p \equiv \pm 1 \mod 8$ alors $y^p = \alpha + \alpha^{-1} = y$, i.e. $y^{p-1} = 1$. Donc :

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

Si $p \equiv \pm 3 \mod 8 \equiv \pm 5 \mod 8$, alors $y^p = \alpha^5 + \alpha^{-5} = \alpha^4\alpha + (\alpha^4\alpha)^{-1} = -\alpha - \alpha^{-1} = -y$. D'où $y^{p-1} = -1$. Ainsi :

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

□

CHAPITRE 4

Corps quadratiques

Définitions et caractérisation

Définition 4.1.
Un **corps quadratique** K est une extension de degré 2 de $\mathbb{Q}$.

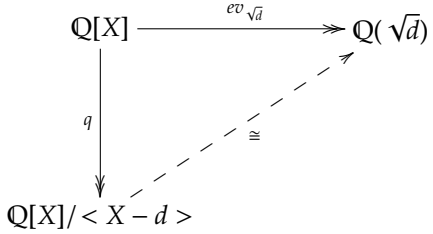
$$[K : \mathbb{Q}] = 2.$$

Exemple 4.2.
$\mathbb{Q}(i) \cong \mathbb{Q}[X]/ < X + 1 >$ extension de degré 2 de $\mathbb{Q}$.

De façon générale, on peut considérer d un entier sans facteur carré. Alors,

$$K_d := \mathbb{Q}[X]/ < X - d > \cong \mathbb{Q}(\sqrt{d}).$$

Ainsi $[K_d : \mathbb{Q}] = 2$, c'est donc un corps quadratique.
Plus précisément, cet isomorphisme est obtenu par application du premier théorème d'isomorphisme à l'homomorphisme d'évaluation en $\sqrt{d}$:



L'homomorphisme $ev_{\sqrt{d}}$ est surjectif car pour tout $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ on a $a + b\sqrt{d} = ev_{\sqrt{d}}(a + bX)$.
En outre $\ker ev_{\sqrt{d}} =< X - d >$:

- "$\supseteq$" Soit $f \in < X - d >$, alors il existe $g \in \mathbb{Q}[X]$ tel que $f(X) = g(X)(X - d)$, de telle sorte que $ev_{\sqrt{d}}(f) = ev_{\sqrt{d}}(f)(d - d) = 0$, i.e $f \in \ker ev_{\sqrt{d}}$.
- "$\subseteq$" Soit $f \in \ker ev_{\sqrt{d}}$, alors $f(\sqrt{d}) = 0$. Dond il existe $g \in \mathbb{C}[X]$ tel que $f(X) = g(X)(X - \sqrt{d})$ et $deg f \geq 2$. Ainsi, comme f est à coefficients rationnels, $-\sqrt{d}$ est aussi racine de f et donc $f(X) = h(X)(X + \sqrt{d})(X - \sqrt{d}) = h(X)(X - d)$ avec $h(X) \in \mathbb{Q}[X]$, i.e $f \in < X - d >$.

Proposition 4.3.
Soit K un corps quadratique, alors il existe un entier d sans facteur carré tel que $K \cong K_d$.

Démonstration. Soit K une extension de $\mathbb{Q}$ de degré 2, alors il existe un polynôme irréductible $f \in \mathbb{Q}[X]$ de degré 2 avec $K \cong \mathbb{Q}[X]/ < f >$.
Soit α une racine de f, alors $K \cong \mathbb{Q}(\alpha)$. Puisque α est racine d'un polynôme de degré 2 la formule du discriminant (pour les équations du second degré) nous assure qu'il existe un entier d sans facteur carré et des rationnels $a, b \in \mathbb{Q}$ tels que $\alpha = a + b\sqrt{d}$.
Par conséquent $\alpha \in \mathbb{Q}(\sqrt{d})$ et donc $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{d})$. Ce dernier étant le plus petit corps contenant $\mathbb{Q}$ et $\sqrt{d}$ et qu'en outre $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ et $\sqrt{d} \in \mathbb{Q}(\alpha)$ ($\sqrt{d} = \frac{1}{b}(\alpha - a)$), il vient $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\alpha)$. D'où $K \cong \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d}) \cong K_d$. □

Définition 4.4.
Si $d < 0$ on dit que que $\mathbb{Q}(\sqrt{d})$ est un **corps quadratique imaginaire**.
Si $d > 0$ on dit que que $\mathbb{Q}(\sqrt{d})$ est un **corps quadratique réel**.

Nous avons un automorphisme de corps défini par :

$$\begin{array}{rccc} \sigma : & \mathbb{Q}(\sqrt{d}) & \longrightarrow & \mathbb{Q}(\sqrt{d}) \\ & a + b\sqrt{d} & \longmapsto & a - b\sqrt{d} \end{array}$$

En effet, $\sigma(1) = 1$;

$$\begin{aligned} \sigma[(a + b\sqrt{d}) + (a' + b'\sqrt{d})] &= \sigma[(a + a') + (b + b')\sqrt{d}] \\ &= (a + a') - (b + b')\sqrt{d} \\ &= (a - b\sqrt{d}) + (a' - b'\sqrt{d}) \\ &= \sigma(a + b\sqrt{d}) + \sigma(a' + b'\sqrt{d}); \end{aligned}$$

$$\begin{aligned} \sigma[(a + b\sqrt{d})(a' + b'\sqrt{d})] &= \sigma[(aa' + bb'd) + (ab' + ba')\sqrt{d}] \\ &= (aa' + bb'd) - (ab' + ba')\sqrt{d} \\ &= (a - b\sqrt{d})(a' - b'\sqrt{d}) \\ &= \sigma(a + b\sqrt{d})\sigma(a' + b'\sqrt{d}). \end{aligned}$$

Ainsi σ est un homomorphisme de corps injectif (car non nul).
Il est aussi clairement surjectif puisque pour tout $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ on a $a + b\sqrt{d} = \sigma(a - b\sqrt{d})$ avec $a - b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. Il s'agit donc bien d'un automorphisme du corps quadratique $\mathbb{Q}(\sqrt{d})$.

A l'aide de σ, nous pouvons définir les applications **trace** et **norme** d'un corps quadratique comme suit :

$$\begin{array}{rccc} \mathrm{Tr} : & \mathbb{Q}(\sqrt{d}) & \longrightarrow & \mathbb{Q} \\ & x & \longmapsto & \mathrm{Tr}(x) := x + \sigma(x) \\ & a + b\sqrt{d} & \longmapsto & a + b\sqrt{d} + a - b\sqrt{d} = 2a \end{array}$$

$$\begin{array}{rccc} \mathrm{N} : & \mathbb{Q}(\sqrt{d}) & \longrightarrow & \mathbb{Q} \\ & x & \longmapsto & \mathrm{N}(x) := x\sigma(x) \\ & a + b\sqrt{d} & \longmapsto & (a + b\sqrt{d})(a - b\sqrt{d}) = a - bd \end{array}$$

La trace est additive :

$$\begin{aligned}\mathrm{Tr}[(a+b\sqrt{d})+(a'+b'\sqrt{d})] &= \mathrm{Tr}[(a+a')+(b+b')\sqrt{d}]\\ &= 2(a+a') = 2a+2a'\\ &= \mathrm{Tr}(a+b\sqrt{d})+\mathrm{Tr}(a'+b'\sqrt{d}) \qquad \forall\,(a+b\sqrt{d}),(a'+b'\sqrt{d})\in\mathbb{Q}(\sqrt{d})\end{aligned}$$

La norme est multiplicative :

$$\begin{aligned}\mathrm{N}[(a+b\sqrt{d})(a'+b'\sqrt{d})] &= \mathrm{N}[(aa'+bb'd)+(ab'+ba')\sqrt{d}]\\ &= (aa'+bb'd)-(ab'+ba')d = (a-bd)(a'-b'd)\\ &= \mathrm{N}(a+b\sqrt{d})\,\mathrm{N}(a'+b'\sqrt{d}) \qquad \forall\,(a+b\sqrt{d}),(a'+b'\sqrt{d})\in\mathbb{Q}(\sqrt{d})\end{aligned}$$

Anneau des entiers

Définition 4.5.
Un élément $x \in \mathbb{Q}(\sqrt{d})$ est dit **entier** sur $\mathbb{Z}$ s'il existe un polynôme unitaire $f \in \mathbb{Z}[X]$ tel que $f(x) = 0$. Pour $K = \mathbb{Q}(\sqrt{d})$, on note $\mathcal{O}_K$ l'ensemble des entiers de K.

Théorème 4.6 (Admis sans preuve)**.**
$\mathcal{O}_K$ est un anneau et $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$.

Esquisse de preuve. Pour la première assertion, se référrer soit au cours d'algèbre commutative, soit au cours de représentation des groupes où la démonstration est donnée dans le cas plus général d'un anneau factoriel quelconque. La deuxième assertion vient du fait que les entiers de $\mathbb{Q}$ sur $\mathbb{Z}$ sont exactement $\mathbb{Z}$ et que $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d})$. □

Conséquence 4.7.
Soit $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d}) = K$.
Alors, z est un entier de $\mathbb{Q}(\sqrt{d}) \Leftrightarrow \mathrm{Tr}(z) \in \mathbb{Z}$ et $\mathrm{N}(z) \in \mathbb{Z}$.
Autrement dit, on peut caractériser les entiers de $\mathbb{Q}(\sqrt{d})$ sur $\mathbb{Z}$ par :

$$\mathcal{O}_K = \{a + b\sqrt{d} \in K \mid 2a \in \mathbb{Z} \text{ et } a - bd \in \mathbb{Z}\}.$$

Démonstration.

" $\Leftarrow$" Supposons que $\mathrm{Tr}(z) \in \mathbb{Z}$ et $\mathrm{N}(z) \in \mathbb{Z}$. Alors z est racine du polynôme à coefficients entiers

$$X - \mathrm{Tr}(z)X + \mathrm{N}(z) = X - 2aX + a - db = (X - (a + b\sqrt{d}))(X - (a - b\sqrt{d})).$$

Autrement dit $z \in \mathcal{O}_K$.

" $\Rightarrow$" Si $z \in \mathcal{O}_K$, alors il est racine d'un certain polynôme du deuxième degré $f(X) = X+AX+B$ avec $A, B \in \mathbb{Z}$. Il suit de la formule de résolution des équations du second degré que l'autre racine de f est $a - b\sqrt{d} = \sigma(z)$. Ainsi par stabilité de l'addition et de la multiplication dans $\mathcal{O}_K$, on obtient que $z + \sigma(z) = \mathrm{Tr}(z) \in \mathcal{O}_K$ et $z\sigma(z) = \mathrm{N}(z) \in \mathcal{O}_K$. Or $\mathrm{Tr}(z), \mathrm{N}(z) \in \mathbb{Q}$. Par conséquent, $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$ entraîne que la norme et la trace de z sont des éléments de $\mathbb{Z}$.

□

Théorème 4.8.
Soit $K = \mathbb{Q}(\sqrt{d})$. Alors,

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & si\ d \equiv 2,3 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & si\ d \equiv 1 \mod 4\,. \end{cases}$$

Démonstration. Soit $x = a + b\sqrt{d}$ un entier de $\mathbb{Q}(\sqrt{d})$. Alors $2a \in \mathbb{Z}$ et $a - bd \in \mathbb{Z}$.
En particulier, $2a \in \mathbb{Z} \Rightarrow$ soit $a \in \mathbb{Z}$, soit $a + \frac{1}{2} \in \mathbb{Z}$.

$$\begin{aligned} \text{Si } a \in \mathbb{Z} &\Rightarrow a \in \mathbb{Z} \\ &\Rightarrow \underbrace{a}_{\in\mathbb{Z}} - \underbrace{(a - bd)}_{\in\mathbb{Z}} = bd \in \mathbb{Z} \\ &\Rightarrow b \in \mathbb{Z} \qquad \text{puisque } d \text{ est supposé sans facteur carré} \\ &\Rightarrow b \in \mathbb{Z}. \end{aligned}$$

D'autre part, si $a + \frac{1}{2} \in \mathbb{Z}$ (i.e. $2a$ est impaire), alors $(2a) = (2m+1) = 4m + 4m + 1 \equiv 1 \mod 4$.
Ainsi,

$$\begin{aligned} a - bd \in \mathbb{Z} &\Rightarrow (2a) - (2b)d \in 4\mathbb{Z} \\ &\Rightarrow (2a) \equiv (2b)d \equiv 1 \mod 4 \qquad \text{puisque } (2a) \equiv 1 \mod 4 \\ &\Rightarrow \text{soit } d \equiv 1 \mod 4 \text{ et } (2b) \equiv 1 \mod 4, \\ &\quad \text{soit } d \equiv 3 \mod 4 \text{ et } (2b) \equiv 3 \mod 4 \\ &\Rightarrow d \equiv 1 \mod 4 \text{ et } (2b) \equiv 1 \mod 4 \\ &\quad \text{car } (2b) \equiv 3 \mod 4 \text{ n'est pas possible} \\ &\Rightarrow d \equiv 1 \mod 4 \text{ et } 2b \equiv 1 \mod 2 \\ &\Rightarrow d \equiv 1 \mod 4 \text{ et } b + \frac{1}{2} \in \mathbb{Z}. \end{aligned}$$

Par conséquent, si $d \not\equiv 1 \mod 4$, i.e $d \equiv 2,3 \mod 4$ alors $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$. D'où $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.
Par contre, si $d \equiv 1 \mod 4$ soit $a, b \in \mathbb{Z}$, alors $a + b\sqrt{d} = a - b + 2b(\frac{1+\sqrt{d}}{2}) \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, soit $a + \frac{1}{2}, b + \frac{1}{2} \in \mathbb{Z}$, auquel cas $a + b\sqrt{d} = \underbrace{(a-b)}_{\in\mathbb{Z}} + \underbrace{2b}_{\in\mathbb{Z}} \frac{1+\sqrt{d}}{2} \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Donc $\mathcal{O}_K \subseteq \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.
Pour l'autre inclusion, considérons $x \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ alors il existe $l, m \in \mathbb{Z}$ tels que :

$$x = l + m\frac{1+\sqrt{d}}{2} = (l + \frac{m}{2}) + \frac{m}{2}\sqrt{d}$$

Il suffit alors de voir que la norme et la trace sont des éléments de $\mathbb{Z}$. En effet,
$\mathrm{Tr}(x) = 2l + m \in \mathbb{Z}$ et $\mathrm{N}(x) = l + lm + \frac{m}{4}(1-d) \in \mathbb{Z}$ puisque $(1-d) \equiv 0 \mod 4$. Par conséquent, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. □

Lemme 4.9.
Soit $K = \mathbb{Q}(\sqrt{d})$ et $x \in \mathcal{O}_K$. Alors, x est une unité de $\mathcal{O}_K \Leftrightarrow \mathrm{N}(x) = \pm 1$.

Démonstration.

" $\Rightarrow$" Si x est une unité de $\mathcal{O}_K$, alors il existe $y \in \mathcal{O}_K$ tel que $xy = 1$. Par suite, on calcule $1 = \mathrm{N}(1) = \mathrm{N}(xy) = \mathrm{N}(x)\,\mathrm{N}(y)$. D'où $\mathrm{N}(x) = \pm 1$.

" $\Leftarrow$" Supposons que $N(x) \pm 1 = N(x) = x\sigma(x)$. Ainsi soit $\sigma(x)$ soit $-\sigma(x)$ est l'inverse de x, qui est de ce fait une unité.

□

Exemple 4.10.
$K = \mathbb{Q}(i)$ alors $\mathcal{O}_K = \mathbb{Z}[i]$ et $\mathcal{O}_K^* = \{1, i, -1, -i\}$.
$(i = \sqrt{(-1)} \Rightarrow d = -1 \equiv 3 \mod 4 \Rightarrow \mathcal{O}_K = \mathbb{Z}[\sqrt{d}] = \mathbb{Z}[i])$

Remarque 4.11.
L'anneau $\mathcal{O}_K$ n'est pas toujours factoriel.

Exemple 4.12.
Pour $K = \mathbb{Q}(\sqrt{-6})$, l'anneau des entiers $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$ n'est pas factoriel. $(-6 \equiv 2 \mod 4)$
En effet, posons $z = \sqrt{-6}$, alors $(-\sqrt{-6})\sqrt{-6} = 6 = 2 \cdot 3$.
Montrons que $\sqrt{-6}, 2$ et 3 sont indécomposables dans $\mathbb{Z}[\sqrt{-6}]$.

- Supposons qu'il existe $x, y \in \mathbb{Z}[\sqrt{-6}]$ tels que $xy = 2$, alors
$$4 = \mathrm{N}(2) = \mathrm{N}(x)\,\mathrm{N}(y).$$
Comme $d = -6 < 0$, la norme est positive, et entière d'après la conséquence ci-dessus. Ainsi on a nécessairement $\mathrm{N}(x) = \mathrm{N}(y) = 2$, car si $\mathrm{N}(x) = 1$, alors [1] $x \in \mathcal{O}_K^*$.
Or $x \in \mathbb{Z}[\sqrt{-6}] \Rightarrow \exists a, b \in \mathbb{Z}$ tels que $x = a + b\sqrt{-6} \Rightarrow 2 = \mathrm{N}(x) = a + 6b$. Mais il n'existe pas de tels éléments dans $\mathbb{Z}$. $\lightning \Rightarrow 2$ est indécomposable dans $\mathcal{O}_K$.
- Supposons qu'il existe $x, y \in \mathbb{Z}[\sqrt{-6}]$ tels que $xy = 3$, alors
$$9 = \mathrm{N}(3) = \mathrm{N}(x)\,\mathrm{N}(y).$$
Ainsi $\mathrm{N}(x) = \mathrm{N}(y) = 3$. Or $x \in \mathbb{Z}[\sqrt{-6}] \Rightarrow \exists a, b \in \mathbb{Z}$ tels que $x = a + b\sqrt{-6} \Rightarrow 3 = \mathrm{N}(x) = a + 6b$. Mais il n'existe pas de tels éléments dans $\mathbb{Z}$. $\lightning \Rightarrow 2$ est indécomposable dans $\mathcal{O}_K$.
- Supposons qu'il existe $x, y \in \mathbb{Z}[\sqrt{-6}]$ tels que $xy = \sqrt{-6}$, alors
$$6 = \mathrm{N}(\sqrt{-6}) = \mathrm{N}(x)\,\mathrm{N}(y).$$
Ainsi on peut supposer spdg. que $\mathrm{N}(x) = 2$ et $\mathrm{N}(y) = 3$. Mais on sait déjà que ce cas de figure n'est pas possible $\Rightarrow \sqrt{-6}$ est indécomposable dans $\mathcal{O}_K$.

Par conséquent, puique 6 admet deux décompositions premières distinctes, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$ ne peut pas Ítre factoriel.

Théorème 4.13 (Sans preuve)**.**
Soit $d < 0$ un entier sans facteur carré et $K = \mathbb{Q}(\sqrt{d})$.
Alors, $\mathcal{O}_K$ est factoriel $\Leftrightarrow$ $d = -1, -2, -3, -7, -11, -19, -43, -67$ ou -163.

Probléme ouvert (Problème de Gauss)**.**
Montrer qu'il existe une infinité de $d > 0$ tels que $\mathcal{O}_K$ soit factoriel.

1. Rappelons qu'un élément premier n'est ni nul, ni une unité.

CHAPITRE 5

Corps de nombres et anneaux d'entiers

Définitions

Définition 5.1.
Un **corps de nombres** (algébrique) est une extension de degré fini de $\mathbb{Q}$.

Exemple 5.2.
Un corps quadratique est un corps de nombres de degré 2.

Contre-exemple 5.3.
Le corps $\mathbb{R}$ n'est pas un corps de nombres puisqu'il s'agit d'un $\mathbb{Q}$-espace vectoriel de dimension infinie.

Définition 5.4.
Soit K un corps de nombres. On dit que $x \in K$ est un élément **entier** sur $\mathbb{Z}$ s'il existe $f \in \mathbb{Z}[X]$ unitaire tel que $f(x) = 0$.
On note $\mathcal{O}_K$ l'ensemble des entiers de K.

Théorème 5.5 (Sans démonstration)**.**
$\mathcal{O}_K$ est un anneau et $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$.
De plus, si $[K : \mathbb{Q}] = n$ alors $\mathcal{O}_K$ est un $\mathbb{Z}$-module libre de rang n.

Idéaux fractionnaires

Définition 5.6.
On dit que $I \subseteq K$ est un **idéal fractionnaire** de $\mathcal{O}_K$ si :

- I est un $\mathcal{O}_K$-module,
- il existe $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$, tel que $I \subseteq \alpha^{-1}\mathcal{O}_K$.

En particulier, si $\alpha = 1$, alors I est un idéal au sens usuel. (Appelé **idéal entier**).

Théorème 5.7 (Sans démonstration)**.**
L'ensemble des idéaux fractionnaires de $\mathcal{O}_K$ forme un groupe pour la multiplication.

Théorème de décomposition unique (Sans démonstration)**.**
Soit I un idéal fractionnaire de $\mathcal{O}_K$.
Alors il existe des idéaux premiers $P_1, \dots, P_r$ de $\mathcal{O}_K$ et des entiers $m_1, \dots, m_r \in \mathbb{Z}$ tels que :

$$I = P_1^{m_1} \cdots P_r^{m_r}$$

Cette décomposition est unique à ordre près des facteurs.

Ramification et autres

Soit K un corps de nombre et $\mathcal{O}_K$ l'anneau des entiers de K. Soit $p \in \mathbb{P}$ et appliquons le théorème de décomposition unique à l'idéal engendré par p :

$$p\mathcal{O}_K = P_1^{e_1} \cdots P_r^{e_q}$$

où les P_i sont des idéaux premiers de $\mathcal{O}_K$ distincts 2 à 2 et les e_i sont des entiers positifs.

On appelle e_i l'**indice de ramification** de P_i dans $\mathbb{Z}$.

Le quotient $\mathcal{O}_K/P_i$ est un anneau intègre fini, il s'agit donc d'un corps [1]. En fait il s'agit d'une extension finie du corps $\mathbb{F}_p$ et on appelle $f_i := [\mathcal{O}_K/P_i : \mathbb{F}_p]$ le **degré résiduel** de P_i sur $\mathbb{Z}$. Ainsi $\#(\mathcal{O}_K/P_i) = p^{f_i}$.

Si l'idéal $p\mathcal{O}_K =< p >_{\mathcal{O}_K}$ est premier, on dit que p est **inerte** dans K.

Si $q \geq 2$ et $e_1 = \ldots = e_q = 1$ on dit que p est **décomposé** dans K.

Si $e_i \geq 2$ pour un i, on dit que p **se ramifie** dans K.

Théorème 5.8.
Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique. ($d \in \mathbb{Z}$ sans facteur carré).

(1) *Sont **décomposés** dans K les $p \in \mathbb{P}$ impairs tels que* $\left(\frac{d}{p}\right) = 1$ *et* $p = 2$ *si* $d \equiv 1 \mod 8$.
($q = 2, e_1 = e_2 = 1, f_1 = f_2 = 1$).

(2) *Sont **inertes** dans K les $p \in \mathbb{P}$ impairs tels que* $\left(\frac{d}{p}\right) = -1$ *et* $p = 2$ *si* $d \equiv 5 \mod 8$.
($q = 1, e_1 = 1, f_1 = 2$).

(3) *Sont **ramifiés** dans K les $p \in \mathbb{P}$ impairs tels que* $\left(\frac{d}{p}\right) = 0$ *et* $p = 2$ *si* $d \equiv 2, 3, 6, 7 \mod 8$
($\Leftrightarrow d \equiv 2, 3 \mod 4$).
($q = 1, e_1 = 2, f_1 = 1$).

1. Tout anneau fini et intègre est un corps.

Lemme 5.9.
Soit f un polynôme de $\mathbb{Z}[X]$ et $\overline{f}$ son image dans $\mathbb{F}_p[X]$, où p est un nombre premier. Soit $A = \mathbb{Z}[X]/<f>$. Alors :

$$A/pA \cong \mathbb{F}_p[X]/<\overline{f}>$$

Démonstration. Considérons les deux projections canoniques succéssives

$$\mathbb{Z}[X] \overset{\pi_1}{\twoheadrightarrow} \mathbb{F}_p[X] \overset{\pi_2}{\twoheadrightarrow} \mathbb{F}_p[X]/<\overline{f}> \ .$$

L'idéal $<f>\subseteq \ker(\pi_2 \circ \pi_1)$ donc par la propriété universelle du quatient on obtient un homomorphisme surjectif

$$\mathbb{Z}[X]/<f> \overset{\pi}{\twoheadrightarrow} \mathbb{F}_p[X]/<\overline{f}>$$

tel que $\ker(\pi) = p \cdot \mathbb{Z}[X]/<f>$. Ainsi par le premier théorème d'isomorphie il vient :

$$(\mathbb{Z}[X]/<f>)/p(\mathbb{Z}[X]/<f>) \cong \mathbb{F}_p[X]/<\overline{f}>$$

□

Preuve du théorème. Soit $2 \neq p \in \mathbb{P}$.

Si $d \equiv 2 \, ou \, 3 \mod 4$ alors $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ donc $\mathcal{O}_K/p\mathcal{O}_K = (\mathbb{Z} + \mathbb{Z}\sqrt{d})/<p>$.

Si $d \equiv 1 \mod 4$ alors $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}$.

$a + b\frac{1+\sqrt{d}}{2} \equiv a + (b+p)\frac{1+\sqrt{d}}{2} \mod <p>, a, b \in \mathbb{Z}$, b impair.

Ainsi de toute façon

$$\mathcal{O}_K/p\mathcal{O}_K \cong (\mathbb{Z} + \mathbb{Z}\sqrt{d})/<p> \ .$$

De plus on sait déjà que

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{d} \cong \mathbb{Z}[X]/<X^2 - d>$$

ainsi par le lemme il vient

$$(\mathbb{Z}[X]/<X^2 - d>)/p(\mathbb{Z}[X]/<X^2 - d>) \cong \mathbb{F}_p[X]/<X^2 - [d]_p> \ .$$

D'où

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_p[X]/<X^2 - [d]_p> \ .$$

Alors :

p est décomposé $\Leftrightarrow$ $p\mathcal{O}_K = P_1P_2$ est produit de deux idéaux premiers distincts
$\Leftrightarrow$ $\mathcal{O}_K/p\mathcal{O}_K = \mathcal{O}_K/P_1P_2 \cong \mathcal{O}_K/P_1 \times \mathcal{O}_K/P_2$ produit de deux corps
$\Leftrightarrow$ $X^2 - [d]_p$ est produit de deux facteurs distincts dans $\mathbb{F}_P[X]$
$\Leftrightarrow$ $[d]_p \in \mathbb{F}_p^{*\,2}$
$\Leftrightarrow$ $\left(\frac{d}{p}\right) = 1$

p est inerte $\Leftrightarrow$ $\mathcal{O}_K/p\mathcal{O}_K$ est un corps
$\Leftrightarrow$ $X^2 - [d]_p$ est irréductible sur $\mathbb{F}_P[X]$
$\Leftrightarrow$ $[d]_p$ n'est pas un carré dans $\mathbb{F}_p$
$\Leftrightarrow$ $\left(\frac{d}{p}\right) = -1$

$$\begin{aligned} \text{p se ramifie} &\Leftrightarrow X^2 - [d]_p \text{ est un carré dans } \mathbb{F}_p[X] \\ &\Leftrightarrow [d]_p = [0]_p \\ &\Leftrightarrow \left(\frac{d}{p}\right) = 0 \end{aligned}$$

Considérons maintenant le cas $p = 2$.

Si $d \equiv 2$ ou $3 \mod 4$ alors $\mathcal{O}_K/2\mathcal{O}_K \cong \mathbb{F}_2[X]/ < X^2 - [d]_2 >$. Ainsi soit $X^2 - [d]_2 = X^2$, soit $X^2 - [d]_2 = X^2 - 1 = (X+1)^2$ qui est un carré dans les deux cas. Donc 2 se ramifie. Si $d \equiv 1 \mod 4$ (i.e $d \equiv 1$ ou $5 \mod 8$) alors $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ et le polynôme minimal de $\frac{1+\sqrt{d}}{2}$ est $X^2 - X - \frac{d-1}{4}$ et donc

$$\mathcal{O}_K/2\mathcal{O}_K \cong \mathbb{F}_2[X]/ < X^2 - X - [\frac{d-1}{4}]_2 > .$$

Si $d \equiv 1 \mod 8$ alors $[\frac{d-1}{4}]_2 = 0$ et $X^2 - X - [\frac{d-1}{4}]_2 = X^2 - X = X(X-1)$, i.e 2 est décomposé.

Si $d \equiv 5 \mod 8$ alors $[\frac{d-1}{4}]_2 = 1$ et $X^2 - X - [\frac{d-1}{4}]_2 = X^2 - X - 1$ est irréductible sur $\mathbb{F}_2[X]$, i.e 2 est inerte. □

CHAPITRE 6

Unités dans un corps quadratique réel

Soit d un entier sans facteur carré.
Considérons alors l'**équation de Pell** : $x - dy = 1$.

Proposition 6.1.
L'équation de Pell admet une solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ avec $y \neq 0$.

Pour prouver cette proposition, nous aurons besoin des deux lemmes suivants, le premier étant basé sur le principe des trous de pigeons de Dirichlet.

Lemme 6.2 (Dirichlet)**.**
Soit $a \in \mathbb{R} \setminus \mathbb{Q}$. Alors il existe une infinité de nombres rationnels $\frac{x}{y}$, $(x, y) = 1$, tels que

$$|\frac{x}{y} - a| < \frac{1}{y}.$$

Démonstration. On divise $[0, 1) = [0, \frac{1}{n}) \cup [\frac{1}{n}, \frac{2}{n}) \cup \cdots \cup [\frac{n-1}{n}, 1)$ avec $n \in \mathbb{N}$ $n > 1$.
Pour $\beta \in \mathbb{R}$ on dnote par $[\beta]$ sa partie entière inférieure :

$$0 \leq \beta - [\beta] < 1$$

Considérons les $n + 1$ nombres $ka - [ka]$, $k = \overline{0, n}$. Par le 'pigeonhole principle' de Dirichlet il existe au moins un interrvalle de la division ci-dessus qui contient deux de ces nombres. Donc il existe $r, s \in \mathbb{Z}$, $0 \leq r < s \leq n$ tels que

$$|(sa - [sa]) - (ra - [ra])| < \frac{1}{n}.$$

On pose $y := s - r > 0$ et $x := [sa] - [ra]$ $(x, y \in \mathbb{Z})$. Ainsi

$$|x - ya| = |[sa] - [ra] - (s - r)a| = |(sa - [sa]) - (ra - [ra])| < \frac{1}{n}.$$

Alors de $0 < y < n$ on tire :

$$|\frac{x}{y} - a| < \frac{1}{ny} < \frac{1}{y}$$

Si $x = x'c$ et $y = y'c$, on simplifie par c et on obtient

$$|\frac{x'}{y'} - a| < \frac{1}{y} < \frac{1}{y'}$$

On peut donc supposer s.p.d.g. que $(x, y) = 1$. On note que $|\frac{x}{y} - a| \neq 0$ et on choisit $m \in \mathbb{Z}$ tel que $m > \frac{1}{|\frac{x}{y} - a|}$.

Comme précédemment, il existe $x_1, y_1 \in \mathbb{Z}$ $(x_1, y_1) = 1$ tels que

$$|\frac{x_1}{y_1} - a| < \frac{1}{my_1} < |\frac{x}{y} - a| \quad \Rightarrow (x_1, y_1) \neq (x, y)$$

et

$$|\frac{x_1}{y_1} - a| < \frac{1}{my_1} < \frac{1}{y_1}\,.$$

Et ainsi de suite.

□

Lemme 6.3.
Il existe une constante $M \in \mathbb{N}$ telle que $|x - dy| < M$ admet une infinité de solutions $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.

Démonstration. Comme $\sqrt{d} \in \mathbb{R} \setminus \mathbb{Q}$, en vertu du lemme précédent, il existe une infinité de $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, $(x, y) = 1$ et $y > 0$ tels que $|\frac{x}{y} - \sqrt{d}| < \frac{1}{y}$ et donc que $|x - \sqrt{d}y| < \frac{1}{y}$.
Par suite,

$$|x + \sqrt{d}y| = |x - \sqrt{d}y + 2\sqrt{d}y| \leq |x + \sqrt{d}y| + 2\sqrt{d}|y| < \frac{1}{y} + 2\sqrt{d}y.$$

D'où :

$$\begin{aligned} |x - dy| = |x - \sqrt{d}y||x + \sqrt{d}y| &< \frac{1}{y}(\frac{1}{y} + 2\sqrt{d}y) \\ &= \frac{1}{y} + 2\sqrt{d} \\ &\leq 1 + 2\sqrt{d} \qquad \text{puisque } 0 < y \in \mathbb{Z}\,. \end{aligned}$$

On pose alors $M := [1 + 2\sqrt{d}] + 17$[1]. □

Preuve de la proposition 6.1.
Par le lemme précédent, il existe $M \in \mathbb{N}$ tel que $-M < \underbrace{x - dy}_{\in\mathbb{Z}} < M$ pour une infinité de $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, $y > 0$.
Il existe alors nécessairement, par le "Dirichlet's pigeonhole principle", un $m \in \mathbb{Z}$, $-M < m < M$, tel que $x - dy = m$ pour une infinité de $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.
Parmi ceux-ci on peut trouver une paire de couples $(x_1, y_1), (x_2, y_2) \in \mathbb{Z} \times \mathbb{Z}$ avec $x_1 \neq x_2$ tels que $x_1 \equiv x_2 \mod |m|$ et $y_1 \equiv y_2 \mod |m|$, puisque $\#\{[(x, y)]mod|m|\} = m < \infty$. (Dirichlet's pigeonhole principle, encore.)
Posons $a := x_1 - \sqrt{d}y_1$, $b := x_2 - \sqrt{d}y_2 \in \mathbb{Q}(\sqrt{d})$ et notons $b' := x_2 + \sqrt{d}y_2$ le conjugué de b. On a alors

$$ab' = (x_1 - \sqrt{d}y_1)(x_2 + \sqrt{d}y_2) = x_1x_2 - y_1y_2d + (x_1y_2 - x_2y_1)\sqrt{d}$$

où $x_1x_2 - y_1y_2d \equiv \underbrace{x_1 - y_1^2d}_{m} \equiv 0 \mod |m|$ et $x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 \equiv 0 \mod |m|$.
Ainsi, il existe $u, v \in \mathbb{Z}$ tels que $ab' = m(u + v\sqrt{d})$. Donc $\mathrm{N}(ab') = m(u - vd)$.
Or $\mathrm{N}(ab') = \mathrm{N}(a)\,\mathrm{N}(b') = \underbrace{(x_1 - y_1^2d)}_{m}\underbrace{(x_2 - y_2^2d)}_{m} = m$.
D'où $u - vd = 1$.
Autrement dit, on a trouvé une solution à l'équation de Pell.

1. les crochets dénotent ici la partie entière inférieure.

Il reste à voir que $v \neq 0$. En effet, supposons *ab absurdo* que $v = 0$, alors,
$u = \pm 1 \Rightarrow ab' = \pm m \Rightarrow \pm mb = ab'b = a\,\mathrm{N}(b) = am \Rightarrow b = \pm a \Rightarrow b = a$
$\Rightarrow x_1 = x_2$ ↯. □

Théoréme-Définition 6.4.
Soit $K = \mathbb{Q}(\sqrt{d})$ où $d \geq 2$ sans facteur carré.
*Il existe une unique unité $\varepsilon > 1$ telle que $\mathcal{O}_K^* = \{\pm\varepsilon^n \mid n \in \mathbb{Z}\}$. On appelle ε l'**unité fondamentale** de K.*

Démonstration. D'après la proposition, il existe $x, y \in \mathbb{Z}, x > 0, y > 0$, tels que $(x - y\sqrt{d})(x + y\sqrt{d}) = x - dy = 1$.
Soit $M \in \mathbb{R}$ fixé, $M > u$.
Soit c une unité de $\mathcal{O}_K$, $1 < c < M$. D'après le lemme 4.9 $\pm 1 = \mathrm{N}(c) = cc'$.
$c' = -c^{-1} \Rightarrow -M < -c^{-1} < M$
$c' = c^{-1} \Rightarrow -M < c^{-1} < M$
Donc $|c|, |c'| < M$.
Il existe un nombre fini de $c \in \mathcal{O}_K^*$, $1 < c < M$ avec $|c|, |c'| < M$. De plus il existe au moins une unité, à savoir u. Soit donc ε la plus petite de ces unité, $\varepsilon > 1$.
Si $\delta \in \mathcal{O}_K^*$ est positif alors il existe $k \in \mathbb{Z}$ unique tel que $\varepsilon^k \leq \delta < \varepsilon^{k+1}$.
D'où $1 \leq \delta\varepsilon^{-k} < \varepsilon$, donc $\delta\varepsilon^{-k} = 1$ par minimalité et donc $\delta = \varepsilon^k$.
Si $\delta \in \mathcal{O}_K^*$ est négatif alors $-\delta$ est positif et $-\delta = \varepsilon^k$ et $\delta = -\varepsilon^k$.

□

Exemple 6.5.

- $K = \mathbb{Q}(\sqrt{5})$, alors $\varepsilon = \frac{1+\sqrt{5}}{2}$.
- $K = \mathbb{Q}(\sqrt{94})$, alors $\varepsilon = 2143295 + 221064\sqrt{94}$.

CHAPITRE 7

Groupes de classes d'idéaux

Soit K un corps de nombres et $\mathcal{O}_K$ son anneau des entiers.
Notons $\mathcal{I}(K)$ le groupe des idéaux fractionnaires de $\mathcal{O}_K$ (ou de K par abus de langage).
Notons $\mathcal{P}(K)$ le sous-groupe des idéaux principaux.
L'ensemble des idéaux principaux est en effet clos pour la multiplication :

$$< x >< y >=< xy > \qquad \forall\, x, y \in \mathcal{O}_K$$

- $x\mathcal{O}_K y\mathcal{O}_K \subseteq xy\mathcal{O}_K$ (banal vu la commutativité).
- $\forall\, c \in \mathcal{O}_K$ on a $xyc = x \cdot 1 \cdot yc \in x\mathcal{O}_K y\mathcal{O}_K$, ainsi $xy\mathcal{O}_K \subseteq x\mathcal{O}_K y\mathcal{O}_K$.

De plus $< x >^{-1}=< x^{-1} >$ par unicité. Donc $\mathcal{P}(K)$ est muni d'une structure de groupe.

Finalement, posons $Cl(K) = \mathcal{I}(K)/\mathcal{P}(K)$. C'est un groupe, appelé **groupe des classes d'idéaux de** $\mathcal{O}_K$.

Remarque 7.1.
Soit $I, J \in \mathcal{I}(K)$. Alors I et J sont dans la mÍme classe de $Cl(K) \Leftrightarrow$ il existe $x \in K^*$ tel que $xI = J$.
Ceci découle du fait que $< x > I = xI$. Clairement $< x > I \supseteq xI$. En outre, si $z \in< x > I$ alors z s'écrit comme $\sum_a xc_a i_a = x(\sum_a c_a i_a) \in xI$ avec $c_a \in \mathcal{O}_K$ et $i_a \in I\, \forall a = \overline{1,n}$. D'où $< x > I \subseteq xI$.

Théorème 7.2 (Sans démonstration)**.**
$Cl(K)$ est un groupe fini.

Terminologie.
On appelle le **nombre de classes** de $\mathcal{O}_K$, le nombre $h_K := \#Cl(K)$.

Remarque 7.3.
$h_K = 1 \Leftrightarrow \mathcal{O}_K$ est principal $\Leftrightarrow \mathcal{O}_K$ est factoriel.
(L'implication "$\mathcal{O}_K$ factoriel $\Rightarrow \mathcal{O}_K$ principal" est une particularité des anneaux d'entiers !)

Probléme ouvert.
Existe-t-il une infinité de corps de nombres K tels que $h_K = 1$?
Le cas particulier des corps quadratiques réels se raméne au Probléme de Gauss par la remarque ci-dessus.

Remarque 7.4.
Le nombre h_K peut-Ítre arbitrairement grand. En particulier, pour tout premier p, il existe un corps de nombres K tel que $p|h_K$.

Probléme ouvert.
Déterminer la structure de groupe de $Cl(K)$.

CHAPITRE 8

Corps quadratiques et formes binaires

Formes bilinéaires symétriques et quadratiques entières

Soit $K = \mathbb{Q}(\sqrt{d})$, d sans facteur carré, un corps quadratique. Le but est de ce chapitre est d'étudier $Cl(K)$. Nous l'atteindrons par l'intermédiaire des formes binaires.

Définition 8.1.

- Une **forme bilinéaire symétrique entière** est une paire (L, B) où :
  1. L est $\mathbb{Z}$-module de rang fini n,
  2. $B : L \times L \longrightarrow \mathbb{Z}$ est une forme bilinéaire telle que $B(x, y) = B(y, x)\ \forall\, x, y \in L$.

  On dit que (L, B) est **paire** si $B(x, x) \equiv 0 \mod 2\ \forall\, x \in L$.
- Une **forme quadratique entière** est une paire (L, Q) où :
  1. L est $\mathbb{Z}$-module de rang fini,
  2. $Q : L \longrightarrow \mathbb{Z}$ est telle que :
     - $Q(\lambda x) = \lambda \leq Q(x)\ \forall\, x \in L, \forall\, \lambda \in \mathbb{Z}$,
     - $$\begin{array}{rccc} B_Q : & L \times L & \longrightarrow & \mathbb{Z} \\ & (x, y) & \longmapsto & B_Q(x, y) := Q(x + y) - Q(x) - Q(y) \end{array}$$ soit bilinéaire.

  ($\Rightarrow B_Q$ est symétrique est paire :
  $B_Q(x, x) = Q(2x) - 2Q(x) = 4Q(x) - 2Q(x) \equiv 0 \mod 2$.)

Remarque 8.2.
Si (L, B) est une forme bilinéaire symétrique entière et paire alors on peut lui associer la forme quadratique entière suivante :

$$\begin{array}{rccc} Q_B : & L & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & \frac{1}{2}B(x, x) \end{array}$$

Vérifions que Q_B est une forme quadratique entière :

- $Q_B(\lambda x) = \frac{1}{2}B(\lambda x, \lambda x) = \lambda \leq (\frac{1}{2}B(x, x))\ \forall\, x \in L, \forall\, \lambda \in \mathbb{Z}$;
- La forme B_{Q_B} est bilinéaire :

$$\begin{aligned} B_{Q_B}(ax + z, y) &= Q_B(ax + z + y) - Q_B(ax + z) - Q_B(y) \\ &= \frac{1}{2}B(ax + z + y, ax + z + y) - \frac{1}{2}B(ax + z, ax + z) - Q_B(y) \\ &= B(ax + z, y) = aB(x, y) + B(z, y) \qquad \forall\, a \in \mathbb{Z}\ \forall\, x, y, z \in L. \end{aligned}$$

D'autre part,

$$\begin{aligned} aB_{Q_B}(x,y) + B_{Q_B}(z,y) &= a[Q_B(x+y) - Q_B(x) - Q_B(y)] + Q_B(z+y) - Q_B(z) - Q_B(y) \\ &= a[\frac{1}{2}B(x+y,x+y) - \frac{1}{2}B(x,x) - \frac{1}{2}B(y,y)] \\ &\quad + \frac{1}{2}B(z+y,z+y) - \frac{1}{2}B(z,z) - \frac{1}{2}B(y,y) \\ &= aB(x,y) + B(z,y) \qquad\qquad \forall\, a \in \mathbb{Z}\ \forall\, x,y,z \in L. \end{aligned}$$

La linéarité dans la deuxième variable est évidente par symétrie, ainsi B_{Q_B} est bilinéaire.

Nous obtenons ainsi une bijection entre :

$$\begin{pmatrix}\text{Formes bilinéaires}\\ \text{symétriques paires}\end{pmatrix} \longleftrightarrow \begin{pmatrix}\text{Formes quadratiques}\\ \text{entières}\end{pmatrix}$$

$$B \longmapsto Q_B$$

$$B_Q \longleftarrow Q$$

En effet, soit B une forme bilinéaires symétrique paire et Q une forme quadratique entière et soit encore $x, y \in L$ alors :

- $Q_{B_Q}(x) = \frac{1}{2}B_Q(x,x) = \frac{1}{2}[Q(2x) - Q(x) - Q(x)] = \frac{1}{2}[4Q(x) - 2Q(x)] = Q(x)$.
- $B_{Q_B}(x,y) = Q_B(x+y) - Q_B(x) - Q_B(y) = \frac{1}{2}B(x+y,x+y) - \frac{1}{2}(x,x) - \frac{1}{2}(y,y) = \frac{1}{2}B(x,y) + \frac{1}{2}B(y,x) = B(x,y)$.

Définition 8.3.
Soit (L,B) une forme bilinéaire symétrique entière et $(e_1,\dots,e_n)$ une base de L. Alors on associe à B la matrice M_B définie par

$$(M_B)_{ij} := B(e_i,e_j)\,.$$

Cette matrice est symétrique (puisque B l'est).
Alors :

1. le **déterminant** de (L,B) est : $\det(M_B)$;
2. le **discriminant** est $\operatorname{disc}(L,B) = \operatorname{disc}(B) := (-1)^{\frac{n(n-1)}{2}} \det(L,B)$;
3. on dit que (L,B) est **non-dégénérée** si $\operatorname{disc}(L,B) \neq 0$;
4. on dit que (L,B) est **définie-positive** si $B(x,x) > 0\ \forall\, x \in L \setminus \{0\}$;
5. on dit que (L,B) est **définie-négative** si $B(x,x) < 0\ \forall\, x \in L \setminus \{0\}$;
6. on dit que (L,B) est **indéfinie** si elle n'est ni définie-positive ni définie-négative.

Définition 8.4.
Soit (L,Q) une forme quadratique entière. Alors on pose :

1. $\det(L,Q) := \det(L,B_Q)$ le **déterminant** de (L,Q) ;
2. $\operatorname{disc}(L,Q) := \operatorname{disc}(L,B_Q)$ le **discriminant** de (L,Q).

On dit que (L,Q) est **non-dégénérée**, **définie-positive**, **définie-négative** ou **indéfinie**, respectivement, si $(L;B_Q)$ l'est .

Revenons au corps quadratique $K = \mathbb{Q}(\sqrt{d})$, avec d sans facteur carré. Rappelons que :

$$\mathscr{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{si } d \equiv 2,3 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{si } d \equiv 1 \mod 4\,. \end{cases}$$

On peut donc voir l'ensemble $\mathscr{O}_K$ comme un $\mathbb{Z}$-module de rang 2.

► Supposons d'abord $d \equiv 2,3 \mod 4$ et posons :

$$\begin{array}{rccc} B: & \mathbb{Z}[\sqrt{d}] \times \mathbb{Z}[\sqrt{d}] & \longrightarrow & \mathbb{Z} \\ & (x,y) & \longmapsto & \mathrm{Tr}_{K/\mathbb{Q}}(x\sigma(y)) \end{array}$$

Il s'agit d'une forme bilinéaire symétrique entière :

$$\begin{aligned} \textit{Symétrie}: \ B(a+b\sqrt{d}, c+e\sqrt{d}) &= \mathrm{Tr}[(a+b\sqrt{d})(c-e\sqrt{d})] \\ &= \mathrm{Tr}[(ac-ebd)+(bc-ae)\sqrt{d}] = 2(ac-ebd) \\ &= \mathrm{Tr}[(ac-ebd)+(ae-bc))\sqrt{d}] \\ &= \mathrm{Tr}[(c+e\sqrt{d})(a-b\sqrt{d})] \\ &= B(c+e\sqrt{d}, a+b\sqrt{d}) \quad \forall\, a+b\sqrt{d}, c+e\sqrt{d} \in \mathbb{Z}[\sqrt{d}] \end{aligned}$$

$$\begin{aligned} \textit{Bilinéarité}: \ B(ax+z,y) &= \mathrm{Tr}[(ax+z)\sigma(y)] = \mathrm{Tr}[ax\sigma(y)+z\sigma(y)] \\ &= a\,\mathrm{Tr}[x\sigma(y)] + \mathrm{Tr}[z\sigma(y)] \\ &= aB(x,y)+B(z,y) \qquad\qquad \forall\, x,y,z \in \mathbb{Z}[\sqrt{d}], \forall\, a \in \mathbb{Z} \end{aligned}$$

alors, la symétrie entraîne la linéarité dans la deuxième variable.
Dans la base $(1, \sqrt{d})$, nous avons :

$$\begin{aligned} &B(1,1) = \mathrm{Tr}(1) = 2 \\ &B(1,\sqrt{d}) = B(\sqrt{d},1) = \mathrm{Tr}(\sqrt{d}) = \sqrt{d} + \sigma(\sqrt{d}) = 0 \\ &B(\sqrt{d},\sqrt{d}) = \mathrm{Tr}(-d) = -2d. \end{aligned}$$

Ainsi la matrice de B est :

$$M_B = \begin{pmatrix} 2 & 0 \\ 0 & -2d \end{pmatrix}$$

Il est alors évident que B est paire et on calcule :

$$\det B = -4d \qquad \text{et} \qquad \mathrm{disc}\, B = (-1)^{\frac{2(2-1)}{2}} \det B = -\det B = 4d\,.$$

► Supposons maintenant $d \equiv 1 \mod 4$ et posons :

$$\begin{array}{rccc} B: & \mathbb{Z}[\frac{1+\sqrt{d}}{2}] \times \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \longrightarrow & \mathbb{Z} \\ & (x,y) & \longmapsto & \mathrm{Tr}_{K/\mathbb{Q}}(x\sigma(y)) \end{array}$$

Choisissons la base $(1, \frac{1+\sqrt{d}}{2})$, il vient :

$$\begin{aligned} &B(1,1) = \mathrm{Tr}(1) = 2 \\ &B(1,\tfrac{1+\sqrt{d}}{2}) = B(\tfrac{1+\sqrt{d}}{2},1) = \mathrm{Tr}(\tfrac{1}{2}+\tfrac{1}{2}\sqrt{d}) = 2\cdot\tfrac{1}{2} = 1 \\ &B(\tfrac{1+\sqrt{d}}{2},\tfrac{1+\sqrt{d}}{2}) = \mathrm{Tr}(\tfrac{1}{4}-\tfrac{1}{4}d) = 2(\tfrac{1}{4}-\tfrac{1}{4}d) = \tfrac{1-d}{2}. \end{aligned}$$

Ainsi la matrice de B est :

$$M_B = \begin{pmatrix} 2 & 1 \\ 1 & \frac{1-d}{2} \end{pmatrix}$$

On calcule alors :

$$\det B = 1-d-1 = -d \qquad \text{et} \qquad \mathrm{disc}\, B = (-1)^{\frac{2(2-1)}{2}} \det B = -\det B = d\,.$$

Définition 8.5.
Le **discriminant** d'un corps quadratique $K = \mathbb{Q}(\sqrt{d})$ est par définition :

$$D_K = D := \begin{cases} 4d & \text{si } d \equiv 2,3 \mod 4 \\ d & \text{si } d \equiv 1 \mod 4\,. \end{cases}$$

Théorème 8.6.
Soit p un nombre premier.
Alors p se ramifie dans $K \Leftrightarrow p \mid D_K$.

Démonstration. Découle du théorème de classification et de la définition de D_K ci-dessus. □

En résumé, nous avons

$$\begin{array}{rccc} B: & \mathscr{O}_K \times \mathscr{O}_K & \longrightarrow & \mathbb{Z} \\ & (x,y) & \longmapsto & \mathrm{Tr}(x\sigma(y)) \end{array}$$

qui est une forme bilinéaire symétrique entière et paire de discriminant $disc(K)$. La forme quadratique associée est

$$\begin{array}{rccc} Q: & \mathscr{O}_K & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & Q(X) = \mathrm{N}(x) \end{array}$$

En effet par définition on a $Q(x) = \frac{1}{2}B(x,x) = \frac{1}{2}\,\mathrm{Tr}(x\sigma(x))\frac{1}{2}\,\mathrm{Tr}(\mathrm{N}(x)) = \frac{2}{2}\,\mathrm{N}(x) = \mathrm{N}(x) \in \mathbb{Z}$.

Définition 8.7.
Soit $I \subseteq \mathscr{O}_K$ un idéal. La **norme** de I est par définition :

$$\mathrm{N}(I) \;=\; \#(\mathscr{O}_K/I)$$

Remarque 8.8.

(1) Si $I = x\mathscr{O}_K$, avec $x \in \mathscr{O}_K$ alors $\mathrm{N}(I) = \mathrm{N}(x)$. (C.f. proposition 9.5)

(2) Soit $I \subseteq \mathscr{O}_K$ un idéal. Posons

$$\begin{array}{rccc} B_I: & I \times I & \longrightarrow & \mathbb{Z} \\ & (x,y) & \longmapsto & B_I(x,y) := \mathrm{Tr}(\frac{1}{\mathrm{N}(I)}x\sigma(y)) \end{array}$$

alors la forme quadratique associée est

$$\begin{array}{rccc} Q_I: & I & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & \frac{\mathrm{N}(x)}{\mathrm{N}(I)} \end{array}$$

en effet, $Q_I(x) = \frac{1}{2}B_I(x,x) = \frac{1}{2}\,\mathrm{Tr}(\frac{1}{\mathrm{N}(I)}x\sigma(x)) = \frac{1}{2}\frac{1}{\mathrm{N}(I)}2\,\mathrm{N}(x) = \frac{\mathrm{N}(x)}{\mathrm{N}(I)}$.

Proposition 8.9.
La forme B_I est une forme bilinéaire symétrique entière et paire de discriminant $disc(K)$.

Formes binaires

Soit L un $\mathbb{Z}$-module de rang 2 et (e_1, e_2) une base de L. Soit $B : L \times L \longrightarrow \mathbb{Z}$ une forme bilinéaire symétrique paire. Alors la matrice de B dans cette base est de la forme

$$\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$$

pour des éléments $a, b, c \in \mathbb{Z}$.

Soit $Q : L \longrightarrow \mathbb{Z}$ la forme quadratique entière associée. On a alors

$$Q(xe_1 + ye_2) = \frac{1}{2}B(xe_1 + ye_2) = \frac{1}{2}\begin{pmatrix} x & y \end{pmatrix}\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = ax \leq +bxy + cy \leq .$$

On note aussi $Q = (a, b, c)$.

On dit que Q est **primitive** si a, b, c sont premiers entre eux deux à deux.
Soit (L, Q) et (L, Q') deux formes quadratiques. On dit que Q et Q' sont dans la mÍme **classe propre** s'il existe un isomorphisme $f : L \longrightarrow L$ tel que $\det(f) = 1$ et $Q'(f(x)) = Q(x)\ \forall\, x \in L$.
Notons $\mathscr{Q}^+(D)$ l'ensemble des classes propres de formes quadratiques entières binaires primitives définies-positives de discriminant D.

Théorème 8.10.
Soit K un corps quadratique imaginaire de discriminant D. Alors on a une bijection

$$\begin{array}{ccc} Cl(K) & \longrightarrow & \mathscr{Q}^+(D) \\ I & \longmapsto & Q_I \end{array}$$

Remarque 8.11.
La bijection ci-dessus permet de munir $\mathscr{Q}^+(D)$ d'une structure de groupe par transport de la structure de groupe de $Cl(K)$. On obtient ainsi la "**composition des formes quadratiques**".

CHAPITRE 9

Trace, norme et discriminant

Norme et trace d'un élément d'un corps

Définition 9.1.
Soit K/F une extension de corps de degré n. Soit $x \in K$. On note

$$\begin{array}{rccc} m_x : & K & \longrightarrow & K \\ & y & \longmapsto & xy \end{array}$$

la multiplication par x. Cette application est F-linéaire.
On définit alors la **trace**, la **norme** et le **polynôme caractéristique** de x comme étant, respectivement, la **trace**, le **déterminant** et le **polynôme caractéristique** de m_x.
Notations : $\mathrm{Tr}_{K/F}(x) = \mathrm{Tr}(x)$, $\mathrm{N}_{K/F}(x) = \mathrm{N}(x)$ et $\Delta_{K/F,x} \in F[X]$.

Propriétés 9.2.

- $\mathrm{Tr}(x + x') = \mathrm{Tr}(x) + \mathrm{Tr}(x') \quad \forall\, x, x' \in K.$
- $\mathrm{Tr}(ax) = a\,\mathrm{Tr}(x) \quad \forall\, x \in K\ \forall a \in F.$
- $\mathrm{Tr}(a) = na \quad \forall\, a \in F$ *(n=degré de l'extension).*
- $\mathrm{N}(xx') = \mathrm{N}(x)\,\mathrm{N}(x') \quad \forall\, x, x' \in K.$
- $\mathrm{N}(ax) = a^n\,\mathrm{N}(x) \quad \forall\, x \in K\ \forall a \in F.$
- $\mathrm{N}(a) = a^n \quad \forall\, a \in F.$
- $\Delta_x \in F[X]$ *et* $\Delta_x(X) = X^n - \mathrm{Tr}(x)X^{n-1} + \ldots + (-1)^n\,\mathrm{N}(x) \quad \forall\, x \in K.$

Proposition 9.3.
Soit $x \in K$ et $x_1, \ldots, x_n$ les racine du polynôme minimal de x avec multiplicité $[K : F(x)]$. Alors :

(1) $\mathrm{Tr}(x) = x_1 + ... + x_n$

(2) $\mathrm{N}(x) = x_1 \cdots x_n$

(3) $\Delta_x(X) = (X - x_1) \cdots (X - x_n)$.

Démonstration. Supposons que $K = F(x)$. Alors $(1, x, \ldots, x^{n-1})$ est une base de K sur F.
Soit $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ le polynôme minimal de x.
Remarquons que $f(X) = (X - x_1) \cdots (X - x_n)$. Soit $m_x : K \longrightarrow K$ la multiplication par x. La matrice

de m_x dans la base $(1, x, \dots, x^{n-1})$ est :

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

Puisque $x^n = -a_0 - a_1 x - \ldots - a_{n-1}x^{n-1}$ il vient

$$\begin{aligned} \Delta_x(X) &= \det(XId - m_x) \\ &= \begin{vmatrix} X & 0 & \cdots & 0 & a_0 \\ -1 & X & \cdots & 0 & a_1 \\ 0 & -1 & \ddots & 0 & a_2 \\ \vdots & \vdots & \ddots & X & \vdots \\ 0 & 0 & \cdots & -1 & X + a_{n-1} \end{vmatrix} \\ &= X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \\ &= f(X) = (X - x_1) \cdots (X - x_n)\,. \end{aligned}$$

On a donc $\mathrm{Tr}(x) = -a_{n-1}$ et $\mathrm{N}(x) = (-1)^n a_0$.
Mais on sait que $X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 = (X - x_1) \cdots (X - x_n)$. Donc $a_{n-1} = -x_1 - ... - x_n$ et $a_0 = (-1)^n x_1 \cdots x_n$.
Finalement on obtient $\mathrm{Tr}(x) = x_1 + ... + x_n$ et $\mathrm{N}(x) = x_1 \cdots x_n$.
Il reste à traiter le cas général $K \neq F(x)$. (Cf. exercices). □

Théorème de la base adaptée

Théorème de la base adaptée.
Soit R un anneau principal, L un R-module libre de type fini et de rang n, ainsi que M un sous-R-module de L.
Alors, il existe une base $(e_1, \dots, e_n)$ de L et des éléments non-nuls $r_1, \dots, r_q \in R$, avec $1 \leq q \leq n$ tels que :

(1) *M est un module libre de base $(r_1 e_1, \dots, r_q e_q)$;*

(1) *r_i divise r_{i+1} , i.e. $r_1 | r_2 | \dots | r_q$.*

En particulier, cette proposition nous assure que tout sous-module d'un module libre de type fini est libre et de type fini.

Démonstration. La preuve se déroule en deux étapes. Nous montrons d'abord que tout sous-module de L est libre et ensuite les deux assertions de la proposition.
Supposons $M \neq \{o\}$ car sinon $q = 0$.

· Soit $\mathcal{F} = \{f_1 \dots, f_n\}$ une base de L. Considérons $\mathrm{Hom}_R(L, R)$. C'est un R-module à droite d'après le paragraphe 1.2.1. Notons alors $\{\phi_1, \dots, \phi_n\}$ la base duale de $\mathcal{F}$, $(\phi_k(f_j) = \delta_{ij})$.

· Pour tout $\varphi \in \mathrm{Hom}_R(L,R)$, on a que $\varphi(M) \subseteq R$ est un sous-R-module de ${}_RR$, donc un idéal à gauche de R. Posons alors $\mathcal{G} = \{\varphi(M) | \varphi \in \mathrm{Hom}_R(L,R)\}$ qui est une famille non-vide d'idéaux à gauche de R puisqu'elle contient l'image de M par l'application qui envoie tous les éléments sur 1_R.
Or, R principal implique que tous les sous-R-modules de ${}_RR$ sont de type fini (puique ce sont les idéaux à gauches qui sont engendrés par un seul élément), ce qui revient à dire que R est noethérien. Ainsi, vu la proposition **??** $\mathcal{G}$ posséde un élément maximal $\pi(M)$ avec $\pi \in \mathrm{Hom}_R(L,R)$ et on peut écrire $\pi(M) =< r_\pi >$ pour un certain $r_\pi (\neq 0) \in R$ étant donné que R est principal et différent du module nul. Alors, il existe $m \in M$ tel que $r_\pi = \pi(m)$.

· Montrons que r_π divise $\varphi(m)$ pour tout $\varphi \in \mathrm{Hom}_R(L,R)$.
Soit $\varphi \in \mathrm{Hom}_R(L,R)$ et $d = pgdc(r_\pi, \varphi(m))$. Par Bézout, il existe $u, v \in R$ tels que $d = ur_\pi + v\varphi(m) = u\pi(m) + v\varphi(m) = (u\pi + v\varphi)(m)$. De plus d divise r_π, ainsi $< r_\pi > \subseteq < d > = < (u\pi + v\varphi)(m) > \subseteq (u\pi + v\varphi)(M)$. Alors, par maximalité de $\pi(M) =< r_\pi >$ on a nécessairement égalité. Par conséquent, $< r_\pi > = < d >$ et donc $< \varphi(m) > \subseteq < r_\pi >$. Autrement dit, il existe $r \in R$ tel que $\varphi(m) = rr_\pi$, i.e. r_π divise $\varphi(m)$.
En particulier, r_π divise les les images de m par les éléments de la base duale, c'est-à-dire qu'il existe $s_i \in R$ telq que $\phi_i(m) = r_\pi s_i$ pour tout $i \in \mathbb{N}_n$.

· Posons $n = \sum_{i=1}^{n} s_i f_i \in L$, ce qui implique que $\phi_i(r_\pi n) = r_\pi s_i = \phi_i(m)$ pour tou $i \in \mathbb{N}_n$, donc $m = r_\pi n$ et $\pi(n) = 1_R$ puisque $\pi(m) = r_\pi$.

· Soit $l \in L$, alors $l = \pi(l)n + (l - \pi(l)n)$ avec $\pi(l)n \in Rn$ et $l - \pi(l)n \in \ker(\pi)$ car $\pi(l - \pi(l)n = \pi(l) - \pi(l)\pi(n) = \pi(l) - \pi(l) = 0$. Ainsi $L = Rn + \ker(\pi)$. De plus $Rn \cap \ker(\pi) = \{0\}$, car si l est un élément de cette intersection alors $l = rn$ pour un $r \in R$ et $\pi(l) = 0$, ainsi $0 = \pi(l) = \pi(rn) = r\pi(n) = r \cdot 1 = r$ et $l = o$.
Par conséquent, on a la somme directe $L = Rn \oplus \ker(\pi)$.

· Prenons maintenant un $x \in M$, alors $\pi(x) \in \pi(M) =< r_\pi >$. Donc $\pi(x) = br_\pi$ avec $b \in R$, ainsi $\pi(x)n = br_\pi n = bm \in Rm \subseteq M$ et $x - \pi(x)n \in (M \cap \ker(\pi)$ car $\pi(x - \pi(x)n) = \pi(x) - \pi(x)\pi(n) = \pi(x) - \pi(x) \cdot 1 = 0$ et $\pi(x)n = bm \in M$.
Par conséquent, on a aussi la somme directe $M = Rm \oplus (M \cap \ker(\pi))$.

· Nous pouvons alors montrer que M est libre, par récurrence sur $p = rang(M)$.
Si $rang(M) = 0$ alors $M = \{0\}$ qui est libre de base vide.
Pour $rang(M) \geq 1$, on a $M \neq \{0\}$ et $M = Rm \oplus (M \cap \ker(\pi))$ avec $rang(Rm) = 1$. Ainsi si $rang(M) = p$, alors $rang(M \cap \ker(\pi)) = p - 1$ qui est libre par hypothèse de récurrence et donc M est libre.

· Nous pouvons maintenant montrer que les points (1) et (2) sont vérifiés ; par récurrence sur le rang p de L.
Si $p = 0$ alors $L = \{0\} = M$ et les résultats sont triviaux.
Soit $p \geq 1$, alors si $M = \{0\}$, on peut prendre n'importe quelle base de L et $q = 0$.
Supposons donc $M \neq \{0\}$. Le noyau $\ker(\pi)$ est un sous-module de M. De plus, comme $L = Rn \oplus \ker(\pi)$, il vient $rang(\ker(\pi)) = p - 1$. On peut donc appliquer l'hypothèse de récurrence à $\ker(\pi)$ et à son sous-module $M \cap \ker(\pi)$: il existe une base $(e_2, \ldots, e_p)$ de $\ker(\pi)$ telle que $(r_2 e_2, \ldots, r_q e_q)$ est une base de $M \cap \ker(\pi)$ avec $r_i \in R$ pour tout $i = 2, \ldots, q$ et $r_2 | \ldots | r_q$.

De plus, en posant $e_1 := n$ et $a_1 := r_\pi$, on obtient une base $(e_1, \dots, e_p)$ de L (comme $L = Rn \oplus \ker(\pi)$) et une base $(r_1 e_1, \dots, r_q e_q)$ de $M \cap \ker(\pi)$ (comme $M = Rr_\pi n \oplus (M \cap \ker(\pi))$).

· Il reste à voir que r_1 divise r_2, i.e $r_\pi | r_2$. (Pour autant que r_2 existe, i.e si $M \cap \ker(\pi) \neq \{o\}$). Comme précédemment, on pose $d := pgdc(r_1, r_2)$. Puisque R est principal, on a $d = ur_1 + vr_2$ pour certains $u, v \in R$. Par la propriété universelle des modules libres, il existe un homomorphisme $\psi : L \to_R R$ tel que $\psi(e_1) = \psi(e_2) = 1$ et $\psi(e_i) = 0$ pour tout $i > 2$. Alors $ur_1 e_1 + vr_2 e_2 \in M$ et $\psi(ur_1 e_1 + vr_2 e_2) = ur_1 + vr_2 = d$; donc $Rr_\pi = Rr_1 \subseteq Rd \subseteq \psi(M)$. Par maximalité de Rr_π, on a nécessairement égalité : $Rr_1 = Rd = \psi(M)$ et donc $r_1 | r_2$ puisque $d = ur_1 + vr_2$.

□

Remarque 9.4.
On se base sur ce théorème pour démontrer le théorème de classification des groupes abéliens finis.

Norme d'un idéal d'un corps de nombres

Soit K un corps de nombres et $\mathscr{O}_K$ son anneau des entiers.

Proposition 9.5.
Soit $x \in \mathscr{O}_K$, $x \neq 0$. *Alors* $|\mathrm{N}(x)| = \#(\mathscr{O}_K / x\mathscr{O}_K)$.

Démonstration. La multiplication par x, $m_x : K \longrightarrow K$ est un isomorphisme de $\mathbb{Q}$-espaces vectoriels pisque $x \neq 0$. Ainsi $\mathrm{rang}_{\mathbb{Z}}(\mathscr{O}_K) = \mathrm{rang}_{\mathbb{Z}}(x\mathscr{O}_K)$. Alors par le théorème de la base adaptée, il existe une base $(e_1, \dots, e_n)$ de $\mathscr{O}_K$ et $a_1, \dots, a_n \in \mathbb{Z}_+$ tels que $(a_1 e_1, \dots, a_n e_n)$ soit une base de $x\mathscr{O}_K$. Ceci implique que

$$\mathscr{O}_K / x\mathscr{O}_K \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}\,.$$

D'où $\#(\mathscr{O}_K / x\mathscr{O}_K) = a_1 \cdots a_n$.

$$\text{Soit } f : \begin{array}{ccc} \mathscr{O}_K & \longrightarrow & x\mathscr{O}_K \\ e_i & \longmapsto & a_i e_i \end{array}$$

Alors $\det(f) = a_1 \cdots a_n$.
Remarquons que $(xe_1, \dots, xe_n)$ est aussi une base de $x\mathscr{O}_K$.

$$\text{Soit } g : \begin{array}{ccc} x\mathscr{O}_K & \longrightarrow & x\mathscr{O}_K \\ a_i e_i & \longmapsto & xe_i \end{array}$$

C'est un $\mathbb{Z}$-isomorphisme. Donc $\det(g)$ = une unité de l'anneau $\mathbb{Z} = \pm 1$. Mais

$$g \circ f : \begin{array}{ccc} \mathscr{O}_K & \longrightarrow & x\mathscr{O}_K \\ e_i & \longmapsto & xe_i \end{array} \text{ est la multiplication par } x,\ m_x.$$

D'où $\mathrm{N}(x) = \det(m_x) = \det(g) \cdot \det(f) = \pm 1 \cdot a_1 \cdots a_n$ et donc

$$|\mathrm{N}(x)| = a_1 \cdots a_n = \#(\mathscr{O}_K / x\mathscr{O}_K)\,.$$

□

Définition 9.6.
Soit $I \subseteq \mathscr{O}_K$ un idéal. On pose $\mathrm{N}(I) := \#(\mathscr{O}_K / I)$.

Proposition 9.7 (Admis sans démonstration)**.**
Soit $I, J \subseteq \mathscr{O}_K$ deux idéaux. Alors :

$$\mathrm{N}(IJ) = \mathrm{N}(I)\,\mathrm{N}(J)$$

Soit I un idéal entier de $\mathscr{O}_K$, alors il existe des idéaux premiers $P_1, \dots, P_m$ et $n_1, \dots, n_m \in \mathbb{N}$ tels que

$$I = P_1^{n_1} \cdots P_m^{n_m}.$$

Alors $\mathrm{N}(I) = \mathrm{N}(P_1)^{n-1} \cdots \mathrm{N}\,{P_m}^{n_m}$.

Soit P un idéal premier de $\mathscr{O}_K$. Alors $P \cap \mathbb{Z} = p\mathbb{Z}$ pour un certain $p \in \mathbb{P}$. Alors $\mathscr{O}_K/P$ est une extension de degré fini de $\mathbb{F}_P$.
On note $f := [\mathscr{O}_K/P : \mathbb{F}_p]$ le degrérésiduel de P. Il vient $\mathrm{N}(P) = \#(\mathscr{O}_K/P) = p^f$.

Discriminant

Soit K/F une extension de corps de degré n.
Soit $x_1, \dots, x_n \in K$. Posons $D_{K/F}(x_1, \dots, x_n) := \det(\mathrm{Tr}_{K/F}(x_i x_j))$ le **discriminant** de $(x_1, \dots, x_n)$.

Proposition 9.8 (Cf. Exercices)**.**
Soit $y_1, \dots, y_n \in K$ tels que $y_j = \sum_{i,j} a_{i,j} x_i$. Alors :

$$D(y_1, \dots, y_n) = [\det(a_{ij})]^2 D(x_1, \dots, x_n)$$

Proposition 9.9 (Cf. Exercices)**.**
Supposons que $K = F(x)$ et soit f le polynôme minimal de x. Alors :

$$D(1, x, , \dots, x^{n-1}) = (-1)^{\frac{n(n-1)}{2}}\,\mathrm{N}(f'(x))$$

Trace, norme et discriminant d'un corps de nombres

Soit K un corps de nombres et $\mathscr{O}_K$ son anneau des entiers.

Théorème 9.10 (Sans preuve)**.**
Soit $x \in \mathscr{O}_K$. Alors $\mathrm{Tr}(x), \mathrm{N}(x) \in \mathbb{Z}$.
Plus généralement, tous les coefficients du polynôme caractéristique de x sont des entiers.

Définition 9.11.
Soit $(e_1, \dots, e_n)$ une $\mathbb{Z}$-base de $\mathscr{O}_K$. Alors le **discriminant** du corps de nombre K est par définition

$$D(K) := D(e_1, \dots, e_n) \in \mathbb{Z}\,.$$

Remarque 9.12.
Par la proposition 9.8, $D(K)$ est indépendant du choix de la base puisque si A est la matrice du changement de base alors son déterminant est ± 1 qui élevé au carré est 1.

Théorème 9.13 (Admis sans démonstration)**.**
Soit p un premier.
Alors p se ramifie dans $K \Leftrightarrow p \mid D(K)$.

Corollaire 9.14.
Il n'y a qu'un nombre fini de p premiers qui se ramifient dans K

Exemple 9.15.
On a déjà défini les notions de norme, trace et discriminant pour les corps quadratiques. On vérifie que ces définitions coÔncident avec celles que nous venons d'introduire.

Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique.

Norme et trace. Soit $x = a + b\sqrt{d} \in K$. Il faut regarder $m_x : K \longrightarrow K$. On choisit la $\mathbb{Q}$-base $(1, \sqrt{d})$ de K, alors la matrice de m_x est

$$\begin{pmatrix} a & bd \\ b & a \end{pmatrix}$$

On a donc $\mathrm{Tr}(x) = 2a = x + \sigma(x)$ et $\mathrm{N}(x) = a^2 - b^2 d = x\sigma(x)$, ce qui correspond aux définitions du chapitre 4.
Remarquons encore que les racines du polynôme minimal de x $(X^2 - 2aX + a^2 - b^2 d)$ sont : $x_1 = a + b\sqrt{d}$ et $x_2 = a - b\sqrt{d}$.
On a donc bien $\mathrm{Tr}(x) = x_1 + x_2$ et $\mathrm{N}(x) = x_1 x_2$.

Discriminant.

- Cas 1 : $d \equiv 2$ ou $3 \mod 4$.
  Alors $(1, \sqrt{d})$ est une base de $\mathcal{O}_K$.
  $\mathrm{Tr}(1 \cdot 1) = 2$, $\mathrm{Tr}(1 \cdot \sqrt{d}) = 0$ et $\mathrm{Tr}(\sqrt{d} \cdot \sqrt{d}) = 2d$, donc
  $$D(K) = D(1, \sqrt{d}) = \det\begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d\,.$$
  Soit $x = \sqrt{d}$. Le polynôme minimal de x est $f(X) = X^2 - d$. Donc $f'(X) = 2X$ et
  $$D(K) = (-1)^{\frac{2\cdot 1}{2}} \mathrm{N}(f'(\sqrt{d})) = (-1)2\sqrt{d}(-2\sqrt{d}) = 4d\,.$$
- Cas 2 : $d \equiv 1 \mod 4$.
  Alors $(1, \frac{1-\sqrt{d}}{2})$ est une base de $\mathcal{O}_K$.
  On a $\mathrm{Tr}(1 \cdot 1) = 2$, $\mathrm{Tr}(1 \cdot \frac{1-\sqrt{d}}{2}) = 1$ et $\mathrm{Tr}(\frac{1-\sqrt{d}}{2} \cdot \frac{1-\sqrt{d}}{2}) = \frac{1+d}{2}$, ainsi
  $$D(K) = D(1, \frac{1-\sqrt{d}}{2}) = \det\begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} = 1 + d - 1 = d\,.$$
  De plus, le polynôme minimal de $\frac{1-\sqrt{d}}{2}$ est $f(X) = X^2 - X + \frac{1-d}{2}$, donc $f'(X) = 2X - 1$ et
  $$D(K) = (-1)^{\frac{2\cdot 1}{2}} \mathrm{N}(f'(\frac{1-\sqrt{d}}{2})) = -\mathrm{N}(-\sqrt{d}) = d\,.$$

Ceci correspond bien au calcul du discriminant que nous avons effectuer au chapitre 8.

Remarque 9.16.
Remarquons que p se ramifie dans $K = \mathbb{Q}(\sqrt{d}) \Leftrightarrow p \mid D$.

De plus, p est inerte dans $K \Leftrightarrow \left(\frac{D}{p}\right) = -1$

et p est décomposé dans $K \Leftrightarrow \left(\frac{D}{p}\right) = 1$.

CHAPITRE 10

Corps cyclotomiques

Définition et propriétés

Soit p un nombre premier et soit ζ_p une racine primitive p-ième de l'unité dans $\mathbb{C}$.

Exemple 10.1.
$\zeta_p = e^{\frac{2i\pi}{p}}$. On a $\zeta_p^p = 1$ et $\zeta_p^m \neq 1$ si $0 < m < p$.

Définition 10.2.
Posons $K = \mathbb{Q}(\zeta_p)$. Ce corps de nombre s'appelle le **p-ième corps cyclotomique** ou **le corps cyclotomique des racines de p-ièmes de l'unité**.

La racine de l'unité ζ_p est une racine du polynôme $X^p - 1$, mais

$$X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \ldots + X + 1)$$

il ne s'agit donc pas d'un polynôme irréductible.
Posons $\phi_p := X^{p-1} + X^{p-2} + \ldots + X + 1 \in \mathbb{Z}[X]$.

Proposition 10.3 (Critère d'Eisenstein)**.**
Soit R un anneau factoriel et $p \in R$ un premier. Soit $f(X) = \sum_{k=0}^{n} a_k X^k \in R[X]$ un polynôme primitif. Si $p \nmid a_n$, $p \mid a_k$ $\forall\, k < n$ et $p^2 \nmid a_0$, alors $f(X)$ est irréductible sur $R[X]$ (et donc dans son corps des fractions).

Démonstration. Procédons par l'absurde. Supposons que $f(X)$ soit réductible, i.e. il existe $g(X), h(X) \in R[X]$ de degré > 0 tels que $f(X) = g(X)h(X)$.
Ecrivons $g(X) = \sum_{i=0}^{l} b_i X^i$ et $h(X) = \sum_{j=0}^{m} c_j X^j$ avec $m, l > 0$ et $a_j = \sum_{k=0}^{j} b_k c^{j-k}$.
Donc $a_n = b_l c_m$ et $a_0 = b_0 c_0$. Donc $p \nmid a_n$ entraîne que $p \nmid b_l$ et $p \nmid c_m$. Et $p \mid a_0$ implique que soit $p \mid b_0$, soit $p \mid c_0$ car p est premier et R factoriel.
Mais $p^2 \nmid a_0$ implique que l'on peut supposer s.p.d.g. que $p \nmid b_0$ et $p \mid c_0$.
Posons $r = \min\{j \mid p \nmid c_j\} < m$, donc $p \nmid c_r$ et $p \nmid b_0$, par conséquent $p \nmid b_0 c_r$.
Or par hypothèse, $p \mid a_r$, ainsi $p \mid b_i c_{r-i}$ pour $i \geq 1$ car $j < r$ implique que $p \mid c_j$ par définition de r.
On obtient donc une cobtradiction, car on a alors $p \mid b_0 c_r$ car

$$b_0 c_r = \underbrace{a_r}_{p\mid} - \underbrace{\sum_{j=1}^{r} b_j c_{r-j}}_{p\mid} .$$

□

Corollaire 10.4.
Le polynôme ϕ_p est irréductible.

Démonstration. On a $\phi_p(X) = \frac{X^p-1}{X-1}$. Posons $Y := X - 1$ alors

$$\frac{X^p - 1}{X - 1} = \frac{(Y+1)^p - 1}{Y} =: f(Y)\,.$$

Donc

$$f(Y) = Y^{p-1} + \sum_{i=p-1}^{1} C_i^p Y^{i-1} \in \mathbb{Z}[Y]$$

On a alors $p \mid C_i^p$ pour tout $i = \overline{1, p-1}$ et le terme constant est $C_1^p = p$ qui n'est pas divisble par $p \leq$. Ainsi le critère d'Eisenstein assure que $f(Y)$ est irréductible. D'où ϕ_p est irréductible. □

Corollaire 10.5.
Le corps cyclotomique $\mathbb{Q}(\zeta_p)$ est de degré $p - 1$.

Démonstration. Le polynôme ϕ_p étant irréductible, il s'agit alors du polynôme minimal de ζ_p. Ainsi

$$\mathbb{Q}(\zeta_p) \cong \mathbb{Q}[X]/ < \phi_p >$$

et donc $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = deg(\phi_p) = p - 1$. □

Remarque 10.6.
On a $\phi_p := X^{p-1} + X^{p-2} + \ldots + X + 1$, ainsi $\mathrm{Tr}(\zeta_p) = -[X^{p-}] = -1$ et $\mathrm{N}(\zeta_p) = [X^0] = 1$.

Supposons maintenant $p \neq 2$.

Proposition 10.7.
L'anneau des entiers de $\mathbb{Q}(\zeta_p)$ est $\mathbb{Z}[\zeta_p]$.

Proposition 10.8.
Pour tout $i = 1, \ldots, p-1$ on a

- $\mathrm{Tr}(\zeta_p^i) = -1$
- $\mathrm{N}(\zeta_p^i) = 1$
- $\mathrm{N}(\zeta_p^i - 1) = p$.

Démonstration. Le polynôme minimal de ζ_p^i est ϕ_p. D'où $\mathrm{Tr}(\zeta_p^i) = -1$ et $\mathrm{N}(\zeta_p^i) = 1$.
Le polynôme minimal de $\zeta_p^i - 1$ est $\phi_p(X+1)$, dont le terme constant est p. D'où $\mathrm{N}(\zeta_p^i - 1) = p$. □

Posons $P := (\zeta_p^i - 1)\mathbb{Z}[\zeta_p] =< \zeta_p^i - 1 >_{\mathcal{O}_K}$. Alors

$$\mathbb{Z}[\zeta_p]/P \cong \mathbb{F}_p\,.$$

Par conséquent P est un idéal maximal, donc premier. (Puisque $\mathbb{F}_p$ est un corps).

Remarque 10.9.
$(\zeta_p^i - 1) = (\zeta_p - 1)(\zeta_p^{i-1} + \ldots + 1) \in (\zeta_p - 1)\mathbb{Z}[\zeta_p]$.
Donc $(\zeta_p^i - 1)\mathbb{Z}[\zeta_p] \subseteq (\zeta_p - 1)\mathbb{Z}[\zeta_p]$.
Mais $(\zeta_p^i - 1)\mathbb{Z}[\zeta_p]$ est maximal, on a donc

$$(\zeta_p^i - 1)\mathbb{Z}[\zeta_p] = (\zeta_p - 1)\mathbb{Z}[\zeta_p]\,.$$

Proposition 10.10.
Le discriminant de $K = \mathbb{Q}(\zeta_p)$ *est* $(-1)^{\frac{p(p-1)}{2}} p^{p-2}$.

Démonstration. Une base de $\mathbb{Q}(\zeta_p)$ est $(1, \zeta_p, \ldots, \zeta_{p-2})$, ainsi

$$D(\mathbb{Q}(\zeta_p)) = D(1, \zeta_p, \ldots, \zeta_{p-2}) = (-1)^{\frac{p-1}{p}} \mathrm{N}(\phi_p(\zeta_p)),\,.$$

On a $X^p - 1 = \phi_p(X)(X-1)$ donc en dérivant on obtient

$$pX^{p-1} = \phi_p'(X)(X-1) + \phi_p(X)\,.$$

Par suite,

$$p\zeta_p^{p-1} = \phi_p'(\zeta_p)(\zeta_p - 1) + \underbrace{\phi_p(\zeta_p)}_{0} = \phi_p'(\zeta_p)(\zeta_p - 1)\,.$$

Donc

$$\mathrm{N}(p)\,\mathrm{N}(\zeta_p)^{p-1} = \mathrm{N}(\phi_p'(\zeta_p))\,\mathrm{N}(\zeta_p - 1)\,.$$

Or $\mathrm{N}(p) = p^{p-1}$ puisque on est dans une extension de degré $p-1$, $\mathrm{N}(\zeta_p) = 1$ puisque ζ_p est une unité de $\mathscr{O}_K$ et $\mathrm{N}(\zeta_p - 1) = \mathrm{N}(P) = \#\mathbb{F}_p = p$.
D'où $\mathrm{N}(\phi_p'(\zeta_p)) = p^{p-2}$ et $D(K) = (-1)^{\frac{p(p-1)}{2}} p^{p-2}$. □

Corollaire 10.11.
Le seul nombre premier qui se ramifie dans $\mathbb{Q}(\zeta_p)$ *est* p.

Démonstration. Immédiat puisque q se ramifie dans $\mathbb{Q}(\zeta_p) \Leftrightarrow q$ divise le discriminant de $\mathbb{Q}(\zeta_p)$, qui est $(-1)^{\frac{p(p-1)}{2}} p^{p-2}$. Par conséquent, la seule possibilité est $q = p$. □

Proposition 10.12 (Admise sans démonstration)**.**

$$p\mathbb{Z}[\zeta_p] = P^{p-1}\,.$$

Automorphismes de $\mathbb{Q}(\zeta_p)$

Notons

$$\mathrm{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) := \{\sigma : \mathbb{Q}(\zeta_p) \longrightarrow \mathbb{Q}(\zeta_p) \text{ automorphismes de corps} \,|\, \sigma|_{\mathbb{Q}} = \mathrm{Id}\}\,.$$

Il s'agit d'un groupe pour la composition des applications.

Soit $\sigma \in \mathrm{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Que vaut $\sigma(\zeta_p)$?
Le polynôme minimal de $\sigma(\zeta_p)$ est ϕ_p, donc $\sigma(\zeta_p) = \zeta_p^i$, $1 \leq i \leq p-1$.

Posons $\sigma(\zeta_p) := \zeta_p^{x(\sigma)}$. Ceci induit une application

$$\begin{array}{rccc} x: & \mathrm{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) & \longrightarrow & \{1,\dots,p-1\} \cong \mathbb{F}_p^* \\ & \sigma & \longmapsto & x(\sigma) \end{array}$$

qui est un isomorphisme de groupes.
Il est bijectif car $x(\sigma)$ détermine σ et $x(\sigma)$ peut-Ítre choisi arbitrairement dans $\mathbb{F}_p^*$.

CHAPITRE 11

Théorie de Galois des corps de nombres

Rappels de théorie de Galois

Soit F un corps fini ou de caractéristique nulle. Soit K/F une extension de degré n et soit encore $\mathrm{Aut}(K)$ le groupe des automorphismes de K.

Notons alors $\mathrm{Aut}(K/F) := \{\sigma \in \mathrm{Aut}(K) \,|\, \sigma|_F = \mathrm{Id}_F\}$. C'est un groupe pour la composition des applications.
Pour tout sous-groupe H de $\mathrm{Aut}(K/F)$, on note

$$K^H = \{x \in K \,|\, \sigma(x) = x \,\forall\, \sigma \in H\}$$

l'ensemble des éléments de K qui sont fixés par H. Il s'agit d'un sous-corps de K, appelé le **sous-corps invariant** du groupe H. On a $F \subseteq K^H \subseteq K$.

Théorème 11.1 (Admis sans démonstration)**.**
Soit K/F une extension de corps de degré n. Posons $G := \mathrm{Aut}(K/F)$. Alors les assertions suivantes sont équivalentes :

(1) $K^G = F$;

(2) *pour tout $x \in K$ le polynôme minimal de x sur F à toutes ses racines dans K ;*

(3) *K est engendré sur F par les racines d'un polynôme dans $F[X]$;*

(4) $\#G = n$.

Définition 11.2.
Si K/F vérifie l'une des propriétés équivalentes (1) à (4), alors K/F est appelée une **extension galoisienne**.
Le groupe G est appelé le **groupe de galois** de l'extension.
On note $G =: \mathrm{Gal}(K/F) = \mathrm{Aut}(K/F)$.

Correspondance Galoisienne.
Soit K/F une extension galoisienne et soit $G = \mathrm{Gal}(K/F)$. Soit K' un corps intermédiaire, i.e. $F \subseteq K' \subseteq K$. Alors on associe à K' le groupe $\mathrm{Aut}(K/K') = \{\sigma \in G \,|\, \sigma|_{K'} = \mathrm{Id}_{K'}\}$. C'est un sous-groupe de G, $K' \rightsquigarrow \mathrm{Aut}(K/K') < G$.
Soit G' un sous-groupe de G. Alors on associe à G' le corps $K^{G'}$. C'est un sous-corps intermédiaire : $F \subseteq K^{G'} \subseteq K$. $G' < G \rightsquigarrow K^{G'}$.

Théorème 11.3 (de correspondance de Galois)**.**
Ces applications sont des bijections réciproques entre

$$\{\textit{sous-groupes de } G : \{1\} < G' < G\} \longleftrightarrow \{\textit{extensions intermédiaires } : F \subseteq K' \overset{G'}{\subseteq} K\}.$$

De plus K est extension galoisienne de tous ses corps intermédiaires et $\mathrm{Gal}(K/K') \cong G'$.
L'extension K'/F est galoisienne $\Leftrightarrow$ G' est sous-groupe normal de G. Dans ce cas $\mathrm{Gal}(K'/F) \cong G'/G$.

Théorie de Galois des corps de nombres

Exemples 11.4.

(1) Soit $K = \mathbb{Q}(\sqrt[3]{2})$, ce n'est pas une extension galoisienne de $\mathbb{Q}$. En effet, le polynôme minimal de $\sqrt[3]{2}$ est :
$$X^3 - 2 = (X - \sqrt[3]{2})(X - \zeta_3\sqrt[3]{2})(x - \zeta_3^2\sqrt[3]{2})$$
où ζ_3 est racine primitive de 1 dans $\mathbb{C}$. Alors $\zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2} \notin K$.

(2) **Corps quadratiques.**
$K = \mathbb{Q}(\sqrt{d})$ et $F = \mathbb{Q}$. Alors $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ est une extension galoisienne.
En effet, ce corps est engendré par les racines de $X \leq -d \in \mathbb{Q}[X]$.
$$\text{Soit } \sigma : \begin{array}{ccc} \mathbb{Q}(\sqrt{d}) & \longrightarrow & \mathbb{Q}(\sqrt{d}) \\ a + b\sqrt{d} & \longmapsto & a - b\sqrt{d} \end{array}$$
On a $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{\mathrm{Id}, \sigma\} \cong C_2$.

(3) **Corps cyclotomiques.**
$K = \mathbb{Q}(\zeta_p)$ et $F = \mathbb{Q}$. Alors $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ est une extension galoisienne.
En effet, $\mathbb{Q}(\zeta_p)$ est engendré sur $\mathbb{Q}$ par les racines de $\phi_p \in \mathbb{Q}[X]$.
On a $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{F}_p^* \cong C_{p-1}$.

(4) Soit $q = p^r$, où p premier et $r \in \mathbb{N} \setminus \{0\}$.
Soit $F = \mathbb{F}_q$ et $K = \mathbb{F}_{q^n}$, $n \in \mathbb{N} \setminus \{0\}$. Alors $\mathbb{F}_{q^n}/\mathbb{F}_q$ est une extension galoisienne.
En effet, $\mathbb{F}_{q^n}$ est engendré par les racines de $X^{q^n} - X \in \mathbb{F}_q[X]$.
$$\text{Notons } \sigma : \begin{array}{ccc} \mathbb{F}_{q^n} & \longrightarrow & \mathbb{F}_{q^n} \\ x & \longmapsto & x^q \end{array} \text{ l'automorphisme de Froebenius.}$$
Alors $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ est le groupe cyclique d'ordre n engendré par σ.
En effet, $\sigma^n = \mathrm{Id}$. ($\sigma^n(x) = x^{q^n} = x$ en vertu du théorème 2.4).
De plus $\sigma^i \neq \mathrm{Id}$ si $0 < i < n$, car le sous-corps fixe de σ^i est $\mathbb{F}_{q^i} \neq \mathbb{F}_{q^n}$.
($\sigma^i(x) = x^{q^i} = x \Leftrightarrow x^{q^i} - x = 0 \Leftrightarrow x \in \mathbb{F}_{q^i}$).

Terminologie.
Soit $F = \mathbb{Q}$, et K un corps de nombres. Supposons que $K/\mathbb{Q}$ soit une extension galoisienne. Alors on dit que K est **abélien** si son groupe de Galois est abélien.

Probléme ouvert (Problème inverse de la théorie de Galois)**.**
Soit G un groupe fini. Existe-t-il une extension galoisienne $K/\mathbb{Q}$ avec $\mathrm{Gal}(K/\mathbb{Q}) = G$ *?*

La réponse est oui si G est abélien !

Soit K un corps de nombres galoisien, $G = \mathrm{Gal}(K/\mathbb{Q})$.

Proposition 11.5.
Soit $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Alors $\sigma(\mathscr{O}_K) = \mathscr{O}_K$.

Démonstration. Soit $x \in \mathscr{O}_K$ et $f \in \mathbb{Z}[X]$ son polynôme minimal. Comme $\mathbb{Z} \subset \mathbb{Q}$ et $\sigma \in G$ alors $\sigma(x)$ est également une racine de f, i.e $\sigma(x) \in \mathscr{O}_K$. Donc $\sigma(\mathscr{O}_K) \subseteq \mathscr{O}_K$.
Mais le mÍme argument est valable pour σ^{-1} ainsi $\sigma^{-1}(\mathscr{O}_K) \subseteq \mathscr{O}_K$ et par conséquent $\sigma(\mathscr{O}_K) \supseteq \mathscr{O}_K$.
D'où $\sigma(\mathscr{O}_K) = \mathscr{O}_K$. □

Soit p un nombre premier et soit P un idéal premier de $\mathscr{O}_K$ au-dessus de p, i.e. $P \cap \mathbb{Z} = p\mathbb{Z}$. Alors, par la proposition ci-dessus, $\sigma(P)$ est aussi un idéal premier de $\mathscr{O}_K$. En fait on a :

$$\mathscr{O}_K/P \cong \mathscr{O}_K/\sigma(P)$$

En effet on a un homomorphisme surjectif $\pi \circ \sigma$

$$\mathscr{O}_K \overset{\sigma}{\leftrightarrow} \sigma(\mathscr{O}_K) = \mathscr{O}_K \overset{\pi}{\twoheadrightarrow} \mathscr{O}_K/\sigma(P)$$

dont le noyau est P. On obtient alors l'isomorphisme voulu gr,ce au premier théorème d'isomorphie.

Définition 11.6.
Soit P et P' deux idéaux premiers de $\mathscr{O}_K$. On dit que P et P' sont **conjugués** s'il existe $\sigma \in G$ tel que $\sigma(P) = P'$.

Proposition 11.7.
Tous les idéaux premiers au-dessus d'un mÍme nombre premier p sont conjugués, de mÍme degré résiduel f et de mÍme indice de ramification e.
On a $p\mathscr{O}_K = (P_1 \cdots P_r)^e$ et $n = fer$.

Idées de preuve. Le degré résiduel est le mÍme puisque $\mathscr{O}_K/P \cong \mathscr{O}_K/\sigma(P)$.
L'indice de ramification est constant puisque $p\mathscr{O}_K = P_1^{e_1} \cdots P_r^{e_r} \Rightarrow \sigma(p\mathscr{O}_K) = \sigma(P_1^{e_1} \cdots P_r^{e_r})$ alors $p\mathscr{O}_K = \sigma(P_1)^{e_1} \cdots \sigma(P_r)^{e_r}$ et par unicité $e_i = e_j \ \forall\, i, j$. □

Supposons désormais K abélien. (I.e. G abélien).

Définition 11.8.
Soit P un idéal premier de $\mathscr{O}_K$. Posons $D_P := \{\sigma \in G \mid \sigma(P) = P\}$.
On appelle D_P le **groupe de décomposition** de P.

Remarque 11.9.
On a $\sigma D_P \sigma^{-1} = D_{\sigma(P)}$ pour tout $\sigma \in G$.
Alors comme G est supposer abélien, $D_P = D_{\sigma(P)}$. Il ne dépend donc que du nombre premier p tel que $P \cap \mathbb{Z} = p\mathbb{Z}$. On note alors $D_P = D_p$.

Notons $K(P) = \mathscr{O}_K/P$. Rappelons que $K(P)/\mathbb{F}_p$ est une extension galoisienne de degré f. Nous avons vu que $\mathrm{Gal}(K(P)/\mathbb{F}_p) \cong C_f$, engendré par l'automorphisme de Froebenius ($x \mapsto x^p$). On

obtient alors un homomorphisme de groupes

$$\begin{array}{ccc} D_P & \longrightarrow & \mathrm{Gal}(K(P)/\mathbb{F}_p) \\ \sigma & \longmapsto & \overline{\sigma} \end{array}$$

Proposition 11.10.
L'homomorphisme ci-dessus est surjectif.

Définition 11.11.
Notons I_P le noyau de cet homomorphisme.
Ce sous-groupe s'appelle le **groupe d'inertie** en P.

Pour tout $\sigma \in G$ on a $\sigma I_P \sigma^{-1} = I_{\sigma(P)}$ et comme G est abélien, $I_P = I_{\sigma(P)}$. Il ne dépend donc aussi que de p est on le note aussi $I_P = I_p$.

Nous avons donc une suite exacte de groupes abéliens

$$O \longrightarrow I_p \hookrightarrow D_P \twoheadrightarrow \mathrm{Gal}(K(P)/\mathbb{F}_p) \longrightarrow O$$

Rappelons que $n = efr$, où r est le nombre d'idéaux distincts conjugués à P. Il vient

$$r = \#(G/D_p) = \frac{\#G}{\#D_p} = \frac{efr}{\#D_p} \quad \Rightarrow \quad \#D_p = ef\,.$$

Mais $\#\mathrm{Gal}(K(P)/\mathbb{F}_p) = [K(P) : \mathbb{F}_p] = f$ donc par exactitude de la suite $\#I_p = e$ (car $D_p/I_p \cong \mathrm{Gal}(K(P)/\mathbb{F}_p)$). .

Corollaire 11.12.
Le premier p est non ramifié dans $K \Leftrightarrow I_p$ est trivial.

Démonstration. En effet, p non ramifié $\Leftrightarrow e = 1 \Leftrightarrow I_p = \{\mathrm{Id}\}$. □

Reprenons la suite exacte

$$O \longrightarrow I_p \hookrightarrow D_P \twoheadrightarrow \mathrm{Gal}(K(P)/\mathbb{F}_p) \longrightarrow O$$

et supposons maintenant que p est non ramifié, donc $I_p = \{\mathrm{Id}\}$. Alors on a un isomorphisme de groupes

$$\begin{array}{rccc} \phi : & D_p & \longrightarrow & \mathrm{Gal}(K(P)/\mathbb{F}_p) \cong C_f \\ & \sigma & \longmapsto & \overline{\sigma} \end{array}$$

ainsi D_p est aussi cyclique d'ordre f.

Notons $\left(\begin{smallmatrix} K/\mathbb{Q} \\ - \\ P \end{smallmatrix}\right)$ l'image réciproque de l'automorphisme de Froebenius par cet isomorphisme : $\left(\begin{smallmatrix} K/\mathbb{Q} \\ - \\ P \end{smallmatrix}\right) := \phi^{-1}(\mathit{Froebenius})$.

L'élément $\left(\begin{smallmatrix} K/\mathbb{Q} \\ - \\ P \end{smallmatrix}\right) = \left(\begin{smallmatrix} K/\mathbb{Q} \\ - \\ p \end{smallmatrix}\right)$ est aussi appelé **automorphisme de Froebenius**.

On a $\left(\frac{K/\mathbb{Q}}{-}{p}\right)(x) = x^p \mod P \ \forall x \in \mathcal{O}_K$, i.e $\left(\frac{K/\mathbb{Q}}{-}{p}\right)(x) - x^p \in P$.

Proposition 11.13.

Soit F un sous-corps de K. Alors $\left(\frac{K/\mathbb{Q}}{-}{P}\right)|_F = \left(\frac{F/\mathbb{Q}}{-}{P}\right)$.

CHAPITRE 12

Corps cyclotomiques et réciprocité quadratique

Théorème 12.1.
Soit p, l des premiers, $2 \neq p \neq l \neq 2$.
Alors

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

Démonstration. Soit $K = \mathbb{Q}(\zeta_l)$. Nous avons vu que $K/\mathbb{Q}$ est une extension galoisienne de groupe de Galois $G = \mathrm{Gal}(K/\mathbb{Q}) \cong C_{l-1}$.

Par la correspondance de Galois on associe à H le corps $F = K^H$. Alors $\mathbb{Q} \subseteq F \subseteq K$.
De plus, $\mathrm{Gal}(K/F) \cong H = C_{\frac{l-1}{2}}$ et $\mathrm{Gal}(F/\mathbb{Q}) \cong C_2$.

Donc $[F : \mathbb{Q}] = 2$, autrement dit F est un corps quadratique. On a donc $F = \mathbb{Q}(\sqrt{d})$ pour un certain d entier sans facteur carré.

Question :quelle est la valeur de d ?

Rappelons que si $l \equiv 1 \mod 4$ alors seul l se ramifie dans $\mathbb{Q}(\sqrt{l})$. Par contre si $l \equiv 3 \mod 4$ alors 2 se ramifie aussi. Mais $-l \equiv 1 \mod 4$ et le seul premier qui se ramifie dans $\mathbb{Q}(\sqrt{-l})$ est l.
Par conséquent

$$F = \begin{cases} \mathbb{Q}(\sqrt{l}) & \text{si } l \equiv 1 \mod 4 \\ \mathbb{Q}(\sqrt{-l}) & \text{si } l \equiv 3 \mod 4. \end{cases}$$

Le premier p ne ramifie pas dans K car $p \neq l$, donc on a l'automorphisme de Froebenius $\left(\frac{K/\mathbb{Q}}{p}\right)$.

Posons $\sigma_p := \left(\frac{K/\mathbb{Q}}{p}\right) \in G$, on a $\sigma_p(x) \equiv x^p \mod P$ où P est un idéal premier au-dessus de p.
Nous avons vu que

$$\begin{array}{ccc} G & \cong & C_{l-1} \cong \mathbb{F}_l^* \\ \sigma & \longmapsto & x(\sigma) \end{array} \quad \text{où } \sigma(\zeta_l) = \zeta_l^{x(\sigma)}.$$

On a donc $\sigma_p(\zeta_l) \equiv \zeta_l^p \mod P$ et $\sigma_p(\zeta_l) = \zeta_l^{x(\sigma_p)}$.

Affirmation.
$x(\sigma_p) = p \mod l$

Démonstration. On a $\zeta_l^{x(\sigma_p)} - \zeta_l^p \in P$. D'autre part

$$\zeta_l^{x(\sigma_p)} - \zeta_l^p = \zeta_l^{x(\sigma_p)}(1 - \zeta_l^{p-x(\sigma_p)})$$

donc

$$\mathrm{N}(\zeta_l^{x(\sigma_p)} - \zeta_l^p) = \underbrace{\mathrm{N}(\zeta_l^{x(\sigma_p)})}_{1}\,\mathrm{N}(1 - \zeta_l^{p-x(\sigma_p)})$$

où $\mathrm{N}(1-\zeta_l^{p-x(\sigma_p)}) = \begin{cases} 0 & \text{si } p \equiv x(\sigma_p) \mod l \\ l & \text{sinon} \end{cases}$

Comme $\zeta_l^{x(\sigma_p)} - \zeta_l^p \in P$ et $p \neq l$, la seule possibilité est $p \equiv x(\sigma_p) \mod l$. □

Le nombre p est soit décomposé, soit inerte dans F. Rappelons que $\left(\frac{F\mathbb{Q}}{p}\right) = \sigma_p|_F$.

p est décomposé dans $F \Leftrightarrow \left(\frac{F\mathbb{Q}}{p}\right) = \mathrm{Id} \Leftrightarrow \sigma_p|_F = \mathrm{Id}\,|_F \Leftrightarrow \sigma_p \in H \Leftrightarrow \left(\frac{p}{l}\right) = 1.$

Par aiileurs, p est décomposé dans $F \Leftrightarrow \left(\frac{(-1)^{\frac{l-1}{2}}l}{p}\right) = 1$ car $F = \mathbb{Q}(\sqrt{(-1)^{\frac{l-1}{2}}l})$ (+cf. th. de classification).

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

D'où la formule.

On aussi p inerte dans $F \Leftrightarrow \left(\frac{p}{l}\right) = -1.$

Et p inerte dans $F \Leftrightarrow (-1)^{\frac{p-1}{2}\frac{l-1}{2}} \left(\frac{l}{p}\right) = -1.$

D'où la formule.

□

CHAPITRE 13

Corps cyclotomiques et premières approches du dernier théorème de Fermat

Dernier Théorème de Fermat (1637)**.**
Soit $n \in \mathbb{N}$, $n > 2$. Si $a, b, c \in \mathbb{Z}$ avec $a^n + b^n = c^n$, alors $abc = 0$.

n=4 Fermat
Fermat Il suffit de le démontrer pour $n = p$ premier impair.
n=3 Euler
n=5 Kummer
n=7 Lammé
1847 Lamé pense l'avoir démontré pour tout p. L'idée est la suivante : on travaille dans $K = \mathbb{Q}(\zeta_p)$, $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.
$c^p = a^p + b^p = (a+b)(a+\zeta_p b)\cdots(a+\zeta_p^{p-1}b)$ car $0 = \phi_p(\zeta_p) = 1 + \zeta_p + \ldots + \zeta_p^{p-1}$
L'idée est alors de montrer que $a+b, a+\zeta_p b, \ldots, a+\zeta_p^{p-1}b$ sont premiers entre eux. Lamé pensait que $\mathcal{O}_K$ a la propriété de factorisation unique, et voulait en déduire que $a+\zeta_p^i b$ est une puissance p-ième pour tout $i = \overline{0, p-1}$.
Liouville a tout suite dit qu'il y avait un problème.
En effet, $\mathcal{O}_K$ est factoriel $\Leftrightarrow h_K = 1$.
Si $p = 3, 5, 7, 11, 13, 17, 19$ alors $h_K = 1$.
Kummer montre que si $p = 23$ alors $h_K = 3$.

Kummer. Si $p \nmid h_K$ alors le théorème de Fermat est vrai.

Définition 13.1.
Si $p \nmid h_K$ alors on dit que p est un nombre premier **régulier**. (Où $K = \mathbb{Q}(\zeta_p)$).
On dit que p est **irrégulier** si $p \mid h_K$.

Remarque 13.2.
On sait qu'il existe une infinité de nombres premiers irréguliers.

Probléme ouvert.
Existe-t-il une infinité de nombres premiers réguliers ?

Soit $K^+ := \mathbb{Q}(\zeta_p + \zeta_p^{-1})$.

On peut montrer qu'il existe une flèche injective $Cl(K^+) \hookrightarrow Cl(K)$. Ainsi $Cl(K^+)$ est un sous-groupe de $Cl(K)$ et $h_{K^+} \mid h_K$.

Notons $h_K^- := \frac{h_K}{h_K^+}$.

Experimentalement h_K^- a tendance à être très grand et h_{K^+} à Ítre très petit.

Conjecture. $p \nmid h_{K^+}$.

CHAPITRE 14

Nombres congruents et courbes elliptiques

Soit $n \in \mathbb{N}$ sans facteur carré.

Problème.
Existe-t-il $x \in \mathbb{Q}$ *tel que*[1] $\begin{cases} x^2 - n \in \mathbb{Q}^2 \\ x^2 + n \in \mathbb{Q}^2. \end{cases}$

Proposition 14.1.
Le nombre naturel n, sans facteur carré, a la propriété ci-dessus si et seulement si il existe un triangle rectangle à côtés rationnels dont la surface vaut n.

Démonstration.

" $\Leftarrow$ " Supposons que l'on ait un triangle rectangle de cathètes $X, Y \in \mathbb{Q}$, d'hypothénuse $Z \in \mathbb{Q}$ et de surface n. Alors

$$\frac{1}{2}XY = n \quad \Leftrightarrow \quad 2XY = 4n\,.$$

Par conséquent, $X^2 + Y^2 = Z^2$ entraîne que

$$(X+Y)^2 = Z^2 + 4n \quad \text{et} \quad (X-Y)^2 = Z^2 - 4n$$

ainsi

$$(\frac{Z}{2})^2 + n = (\frac{X+Y}{2})^2 \in \mathbb{Q}^2 \quad \text{et} \quad (\frac{Z}{2})^2 - n = (\frac{X-Y}{2})^2 \in \mathbb{Q}^2\,.$$

Il suffit donc de poser $x := \frac{Z}{2}$.

" $\Rightarrow$ " Supposons qu'il existe $x \in \mathbb{Q}$ tel que $\begin{cases} x^2 - n \in \mathbb{Q}^2 \\ x^2 + n \in \mathbb{Q}^2\,. \end{cases}$ Autrement dit il existe $u, v \in \mathbb{Q}$ tels que $x^2 + n = u^2$ et $x^2 - n = v^2$. On peut alors poser $X := u - v \in \mathbb{Q}$, $Y := u + v$ et $Z := 2x$. Il s'agit des côtés d'un triangle rectangle d'aire n.
En effet :

$$X^2 + Y^2 = (u-v)^2 + (u+v)^2 = 2(u^2+v^2) = 2(x^2+n+x^2-n) = 4x^2 = Z^2$$

et $\frac{1}{2}XY = \frac{1}{2}(u-v)(u+v) = n\,.$
(On trouve facilement les valeurs de X, Y et Z en se basant sur la preuve de la réciproque).

□

1. Ici $\mathbb{Q}^2$ dénote l'ensemble des carrés de $\mathbb{Q}$.

Définition 14.2.
On dit qu'un nombre $n \in \mathbb{N}$, sans facteur carré, est **congruent** s'il a les propriétés équivalentes ci-dessus.

Exemples 14.3.

(1) $n = 6$ est congruent : $X = 3$, $Y = 4$ et $Z = 5$.
(2) $n = 5$ est congruent : $X = \frac{20}{3}$, $Y = \frac{3}{2}$ et $Z = \frac{41}{6}$.
En effet, $X^2 + Y^2 = \frac{400}{9} + \frac{9}{4} = (\frac{41}{6})^2$ et $\frac{1}{2}XY = \frac{1}{2}\frac{20}{3}\frac{3}{2} = \frac{20}{4} = 5$.
(3) $n = 1$ n'est pas congruent. ($\Leftrightarrow$ th. de Fermat pour l'exposant 4).

Soit $n \in \mathbb{N}$ un nombre congruent. Il existe alors $X, Y, Z \in \mathbb{Q}^*$ avec

$$(\frac{Z}{2})^2 + n = (\frac{X+Y}{2})^2 \text{ et } (\frac{Z}{2})^2 - n = (\frac{X-Y}{2})^2 .$$

En multipliant, on obtient :

$$(\frac{X^2 - Y^2}{4})^2 = (\frac{Z}{2})^4 - n^2$$

Ainsi, en posant $u := \frac{Z}{2}$ et $v := \frac{X^2-Y^2}{4}$, il vient :

$$v^2 = u^4 - n^2$$
$$\Leftrightarrow \quad (uv)^2 = u^6 - n^2u^2$$

Posons alors $x := u^2$ et $y := uv$ et on obtient l'équation

$$y^2 = x^3 - n^2x$$

que l'on notera E_n. Il s'agit d'une **courbe cubique plane**.

Définition 14.4.
Un point d'une courbe $E : \ g(y) = f(x)$ est dit **rationnel** si ces coordonnées sont rationnelles.

Nous venons de voir que si n est un nombre congruent alors E_n a un point rationnel (x, y). De plus on peut voir que le dénominateur de x est pair. (Cf. ex.2 série 14).
La réciproque est aussi vraie.

Proposition 14.5.
Si (x, y) est un point rationnel de E_n avec $x \in \mathbb{Q}^{*2}$ et de dénominateur pair, alors n est un nombre congruent.

Démonstration. Soit (x, y) un point rationnel de E_n avec $x \in \mathbb{Q}^{*2}$ et de dénominateur pair. On a $y^2 = x^3 - n^2x$ ainsi $x^2 - n^2 = \frac{y^2}{x} \in \mathbb{Q}^2$ puisque $x \in \mathbb{Q}^{*2}$. Par conséquent $x^2 - n^2 = (x-n)(x+n)$ entraîne que $(x-n)$ et $(x+n)$ sont des carrés dans $\mathbb{Q}$ puisque $x^2 - n^2 \in \mathbb{Q}^2$. En d'autres termes, n est un nombre congruent. □

Définition 14.6.
Une **courbe elliptique** est une courbe plane d'équation

$$E : \quad y^2 = f(x)$$

où $f \in \mathbb{Q}[X]$ est de degré trois sans racine multiple (sur $\mathbb{C}[X]$).

L'ensemble des points rationnels de E est $E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid y^2 = f(x)\} \cup \{0\}$.
On peut munir cet ensemble d'une loi de groupe comme suit :
[*Graphiqueaa jouter*]

L'élément neutre noté 0 est le point à l'infini.
[*Graphiqueaa jouter*]

Théorème 14.7 (Mordell-Weil)**.**
Le groupe $E(\mathbb{Q})$ est abélien de type fini :

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}$$

où $E(\mathbb{Q})_{tors}$ est un groupe fini.
Le nombre r est appelé le ***rang*** *de la courbe elliptique et un point P est dit de n-**torsion** s'il existe $n \in \mathbb{N}$ tel que $nP = 0$.*

Exemple 14.8.
Considérons E_n : $y^2 = x^3 - n^2x$.
Alors les points $P_1 = (-n, 0)$, $P_2 = (0, 0)$ et $P_3 = (n, 0)$ sont des points de 2-torsion car $2P_1 = 2P_2 = 2P_3 = 0$.
En ajoutant le point à l'infini, on obtient que $\#E_n(\mathbb{Q}) \geq 4$.

Remarque 14.9.
Le rang r est difficile à détérminer en général. Il y a des conjectures à ce sujet, dont notamment la conjecture de Birch.

Théorème 14.10.
Soit $n \in \mathbb{N}$ sans facteur carré.
Alors n est congruent si $\Leftrightarrow$ le rang de E_n est strictement positif.

Proposition 14.11.

$$\#E_n(\mathbb{Q})_{tors} = 4\,.$$

Autrement dit, les seuls points de torsion sont $0, (-n, 0), (0, 0)$ et $(n, 0)$.

Proposition 14.12.
Soit $P \in E_n(\mathbb{Q})$ tel que $2P \neq 0$.
Soit $2P = (x, y)$. Alors $x \in \mathbb{Q}^{*2}$ et son dénominateur est pair.

Preuve du théorème.

" $\Rightarrow$ " Supposons n congruent. Alors il existe $P = (x, y) \in E_n(\mathbb{Q})$ avec $x \in \mathbb{Q}^{*2}$ et son dénominateur est pair.
Alors $P \notin E_n(\mathbb{Q})_{tors}$. En effet, $E_n(\mathbb{Q})_{tors} = \{0, (-n, 0), (0, 0), (n, 0)\}$, mais la x-coordonnée de ces points n'appartient pas $\mathbb{Q}^{*2}$. Donc P est d'ordre infini. D'où le fait que le rang de E_n et plus grand ou égal à 1.

" $\Leftarrow$ " Soit P un point d'ordre infini de $E_n(\mathbb{Q})$. Soit $2P = (x, y)$. Par la proposition ci-dessus $x \in \mathbb{Q}^{*2}$ et son dénominateur est pair. Autrement dit n est un nombre congruent.

□

Index