Théorie des nombres

Pierron Théo

ENS Ker Lann

Table des matières

Chapitre 1

Corps finis

1.1 Rappels de théorie des corps

1.1.1 Caractéristique d'un corps, sous-corps premier

Définition 1.1 Soit k un corps. L'application :

$$f : \begin{cases} \mathbb{Z} & \to & k \\ n & \mapsto & n.1_k \end{cases}$$

définit un morphisme d'anneaux. Son noyau est un idéal de $\mathbb{Z}$. Il s'écrit donc $n\mathbb{Z}$. Si $n = n_1 n_2 \neq 0$, on a $(n_1 1_k)(n_2 1_k) = 0$ donc par intégrité, $n_1 \in \mathrm{Ker}(f)$ ou $n_2 \in \mathrm{Ker}(f)$. Ainsi, $n = 0$ ou n est premier.

Si $n \neq 0$, f induit une injection de $\mathbb{Z}/n\mathbb{Z}$ dans k. Son image est le plus petit sous-corps de k et est appelé sous-corps premier de k.

Si $n = 0$, on montre que le sous-corps premier de k est $\mathbb{Q}$. En effet, k contient $\mathrm{Im}(f) = \mathbb{Z}$, donc son corps des fractions $\mathbb{Q}$. Comme $\mathbb{Q}$ ne contient pas d'autre corps, on a bien le résultat.

Remarque 1.1 *Si k est fini, $n > 0$.*

1.1.2 Extension de corps

Définition 1.2

- Soient K et L deux corps avec $K \subset L$. On dit que L est une extension de K.
- Le degré de l'extension L/K est la dimension de L considéré comme K-espace vectoriel : $[L : K] = \dim_K L$.
- On dit qu'une extension est finie ssi son degré est fini.

- Si L/K est une extension et $\alpha \in L$, le plus petit sous-corps de L contenant α et K est noté $K(\alpha)$.
  - Si α vérifie $P(\alpha) = 0$ avec $P \in K[X]$, alors $K(\alpha)$ est finie et de degré inférieur ou égal à $\deg(P)$ et $K(\alpha) = K[\alpha]$. On dit que α est algébrique sur K.
  - Sinon, α est dit transcendant sur K et $K(\alpha) = \mathrm{Frac}(K[\alpha])$. L'extension $K(\alpha)/K$ est alors infinie. Une extension de cette forme est dite monogène.

THÉORÈME 1.1 (DE L'ÉLÉMENT PRIMITIF) *Toute extension finie séparable*[1] *est monogène.*

Exemples :
- Toute extension finie de corps de caractéristique nulle est monogène.
- Toute extension finie de corps fini est monogène.

1.1.3 Corps de rupture, corps de décomposition

THÉORÈME 1.2 *Soit K un corps et $P \in K[X]$. Il existe une extension L de K telle que P ait une racine dans L (corps de rupture). Les extensions de K minimales où P a une racine sont isomorphes.*

Démonstration. On peut supposer P irréductible, c'est-à-dire $K[X]/\langle P\rangle = K[X]/(PK[X])$.

$\exists$ La classe de X est une racine de P dans $K[X]/\langle P\rangle$.

$\sim$ Si L/K est une extension et $\alpha \in L$ vérifie $P(\alpha) = 0$, $K(\alpha)$ est une extension de K où P a une racine donc si L est minimal, on a $L = K(\alpha)$. Via l'application :

$$\delta_a : \begin{cases} K[X] & \to & K(\alpha) = L \\ Q(X) & \mapsto & Q(\alpha) \end{cases}$$

on a $K[X]/\langle P\rangle \simeq K(\alpha) = L$. ∎

THÉORÈME 1.3 *Soit K un corps et $P \in K[X]$. Il existe une extension L de K telle que P s'écrive comme produit de facteurs de degré 1 dans $L[X]$. Les extensions de K minimales pour cette propriété sont isomorphes entre elles.*

Définition 1.3 Un tel corps est appelé corps de décomposition pour P.

Démonstration. Il suffit d'itérer le processus de construction du corps de rupture. ∎

1. Une extension algébrique L d'un corps K est dite séparable ssi le polynôme minimal de tout élément de L n'admet que des racines simples.

 Tous droits réservés

1.2 Corps finis

1.2.1 Propriétés

Proposition 1.1 Soit K un corps fini.

- Sa caractéristique est un nombre premier p.
- Son sous-corps premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
- Comme K en est une extension, il a une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension finie (car K fini) notée d.
- On a $K \simeq (\mathbb{Z}/p\mathbb{Z})^d$ donc $\text{Card}(K) = p^d$.

1.2.2 Structure multiplicative

THÉORÈME 1.4 *Si K est un corps fini, alors $(K^*, \times)$ est un groupe cyclique.*

Démonstration. Si $x \in K^*$ d'ordre $n \geqslant 1$. Le sous-groupe engendré par x est un sous-groupe d'ordre n donc les éléments ont un ordre qui divise n.

Un élément de K^* dont l'ordre divise n est une racine de $X^n - 1$ et il y a au plus n éléments de K^* dont l'ordre divise n.

On a donc deux possibilités : soit il n'y a pas d'éléments d'ordre n dans K^*, soit, s'il y en a, il y a n éléments dont l'ordre divise n. Ils forment alors un sous-groupe cyclique de K^*, isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Il y a donc $\varphi(n)$ éléments d'ordre n.

Notons $q = \text{Card}(K)$.

$$\begin{aligned} q - 1 &= \text{Card}(K^*) \\ &= \sum_{n \mid q-1} \text{Card}\{x \in K^*, x \text{ est d'ordre } n\} \\ &\leqslant \sum_{n \mid q-1} \varphi(n) \end{aligned}$$

On a aussi :

$$\begin{aligned} q - 1 &= \text{Card}(\mathbb{Z}/(q-1)\mathbb{Z}) \\ &= \sum_{n \mid q-1} \text{Card}\{x \in \mathbb{Z}/(q-1)\mathbb{Z}, x \text{ est d'ordre } n\} \\ &= \sum_{n \mid q-1} \varphi(n) \end{aligned}$$

La première inégalité est donc une égalité et pour tout $n \mid q-1$, il y a au moins un élément d'ordre n. Donc il existe un élément d'ordre $q-1$ et K^* est cyclique.

■

 Tous droits réservés

Remarque 1.2 *On a montré que* $X^{q-1} - 1 = \prod_{x \in K^*} (X - x)$.

1.2.3 Morphisme de Frobenius - Sous-corps d'un corps fini

THÉORÈME 1.5 *L'application* $\varphi_p : x \mapsto x^p$ *est un automorphisme de corps.* ($a^p + b^p = (a+b)^p$ *car* p *divise les cœfficients binomiaux différents de* 1*).*

Soit K' un sous-corps de K. K' contient le sous-corps premier de K donc on a des extensions.

THÉORÈME 1.6 *On a* $[K : \mathbb{Z}/p\mathbb{Z}] = [K : K'] \times [K' : \mathbb{Z}/p\mathbb{Z}]$.

Démonstration. Si K est de cardinal p^d et si $d' \mid d$, montrons que K' est un sous-corps de K de cardinal $p^{d'}$.

Posons $E = \{x \in K, x^{p^{d'}} - x = 0\}$. E est le noyau de l'application $\mathbb{Z}/p\mathbb{Z}$-linéaire $\varphi_{p^{d'}} - \mathrm{Id}$ donc E est stable par $+$ et $\cdot$. De plus, $\varphi_{p^{d'}}(xy) = \varphi_{p^{d'}}(x)\varphi_{p^{d'}}(y) = xy$ donc E est stable par $\times$. C'est donc un sous-corps de K qui convient.

En effet, $X^{p^{d'}} - X \mid X^{p^d} - X = \prod_{x \in K} (X - x)$ donc $X^{p^{d'}} - X$ est scindé sur K donc $\mathrm{Card}(E) = p^{d'}$. ∎

Remarque 1.3 *Les éléments de* K' *sont les racines de* $X^{p^{d'}} - X$*. Il y a donc au plus un sous-corps de cardinal* $p^{d'}$*.*

THÉORÈME 1.7 *Pour tout* $q = p^d$*, il existe un unique corps fini de cardinal* q *noté* $\mathbb{F}_q$*.*

Démonstration.

∃ q s'écrit p^d.
$P = X^q - X \in \mathbb{Z}/p\mathbb{Z}[X]$ est sans facteur carré car $P' = -1$.
Notons K le corps de décomposition de P sur $\mathbb{Z}/p\mathbb{Z}$.
K est un corps fini (extension finie de $\mathbb{Z}/p\mathbb{Z}$) et $\mathrm{Card}(K) \geqslant q$ car K contient les q racines distinctes de P.
Posons $K' = \{x \in K, x^q = x\}$. K' est un sous-corps de K à q éléments.

! Si k est un corps fini de cardinal $q = p^d$, on a k^* cyclique donc pour tout $x \in k^*$, $x^{q-1} = 1$ donc $x^q = x$ et $0^q = 0$ donc $X^q - X$ est scindé dans k. Par unicité du corps de décomposition, k et K' sont isomorphes. ∎

Remarque 1.4 K' *est un sous-corps contenant* K *et les* q *racines de* P*. Donc c'est un corps de décomposition de* P *qui est de plus minimal donc* $K = K'$*.*

 Tous droits réservés

Remarque 1.5 L'isomorphisme n'est pas unique (sa composée avec le Frobénius en est aussi un).

1.2.4 Le polynôme $P = X^{q^n} - X \in \mathbb{F}_q[X]$

THÉORÈME 1.8 *Soient a, b, q trois entiers. r est le reste dans la division de a par b ssi $q^r - 1$ est le reste dans la division de $q^a - 1$ par $q^b - 1$.*

Démonstration. Il suffit d'écrire les nombres en base q. ∎

Proposition 1.2

- P est à racines simples.
- Soit $Q \in \mathbb{F}_q[X]$ irréductible. $Q \mid P$ ssi $\deg(Q) \mid n$ et $K = \mathbb{F}_q[X]/\langle Q \rangle$ est un corps à $q^{\deg(Q)}$ éléments.

Démonstration.

- $P' = -1$ donc P est à racines simples.
- Si $\deg(Q) \mid n$, $x^{q^{\deg(Q)}} = x$ donc $x^{q^n} = (((x^{q\deg(Q)})^{q\deg(Q)})^{\cdots})^{q\deg(Q)} = x$. Donc $x^{q^n} = x$ sur K et $Q \mid X^{q^n} - X$.
- Si $Q \mid X^{q^n} - X$, K est un corps à $q^{\deg(Q)}$ éléments.
  On a $Q(\overline{X}) = 0$ et $\overline{X}^{q^n} = \overline{X}$. Donc $\varphi_q^n(\overline{X}) = \overline{X}$ avec φ_q le Frobénius.
  φ_q est linéaire et $\overline{X}$ engendre K en tant que $\mathbb{F}_q$-algèbre.
  Donc, pour tout $x \in K$, $x^{q^n} = x$. En particulier, si x est un générateur de K^*, $q^{\deg(Q)} - 1 \mid q^n - 1$ donc $\deg(Q) \mid n$. ∎

On a donc :

$$X^{q^n} - X = \prod_{\substack{P \in \mathbb{F}_q[X] \text{ unitaire irréductible} \\ \deg(P) \mid n}} P$$

1.3 Carrés de $\mathbb{F}_q$

1.3.1 Dénombrement

$\mathbb{F}_q^*$ est isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$ donc x est un carré de $\mathbb{F}_q^*$ ssi x est un multiple de 2 dans $\mathbb{Z}/(q-1)\mathbb{Z}$.

- Si q est pair, tout élément de $\mathbb{F}_q$ est un carré. En effet, $q-1$ est impair donc premier avec 2 donc 2 est inversible.
- Si q est impair, il y a $\frac{q+1}{2}$ carrés dans $\mathbb{F}_q$. En effet, dans $\mathrm{Im}(x \to x^2)$ chaque élément non nul a deux antécédents.
  Donc $q = 1 + 2(\mathrm{Card}(\mathrm{Im}(x \to x^2)) - 1)$.
- Si $x \in \mathbb{F}_q$, $x^{\frac{q-1}{2}}$ vaut 0 si $x = 0$, 1 si x est un carré non nul et -1 sinon.

 Tous droits réservés

1.3.2 Symbole de Legendre

On se place maintenant dans $\mathbb{F}_p$ avec p premier.

Définition 1.4 On définit le symbole de Legendre de n et p (premier) et on note $\left(\frac{n}{p}\right)$ l'entier 0 si $p \mid n$, 1 si n est un carré modulo p avec $p \nmid n$ et -1 sinon (ie si n n'est pas un carré modulo p).

Remarque 1.6

- $\left(\frac{-1}{p}\right) = x^{\frac{p-1}{2}} \mod p$ *si* $p \neq 2$.
- *L'application :*
$$l : \begin{cases} \mathbb{F}_p^* & \to & \{1,-1\} \\ n & \mapsto & \left(\frac{n}{p}\right) \end{cases}$$
est un morphisme de groupes.
- *Pour déterminer les carrés, il suffit de savoir calculer* $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ *et* $\left(\frac{q}{p}\right)$ *avec* q *et* p *premiers et impairs.*

On suppose désormais p et q premiers impairs.

1.3.3 Calcul de $\left(\frac{-1}{p}\right)$

On a, d'après le paragraphe précédent, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \mod p$ donc $\left(\frac{-1}{p}\right)$ vaut donc la classe de p dans $\mathbb{Z}/4\mathbb{Z}$.

Définition 1.5 Soit $\sigma \in \mathfrak{S}_n$. On définit la signature de σ et on note $\varepsilon(\sigma)$ la quantité :

$$\begin{aligned} &(-1)^{\mathrm{Card}\{1 \leqslant i < j \leqslant n, \sigma(i) > \sigma(j)\}} \\ &= (-1)^{\mathrm{Card}(\mathrm{supp}\,\sigma)-1} (\text{si } \sigma \text{ est un cycle}) \\ &= 1 \text{ si } \sigma = \tau_1 \circ \cdots \circ \tau_{2p} \text{ et } -1 \text{ sinon} \end{aligned}$$

Théorème 1.9 *Si* $p \nmid n$, $\left(\frac{n}{p}\right) = \varepsilon(\sigma_n)$ *avec :*

$$\sigma_n : \begin{cases} \mathbb{F}_p^* & \to & \mathbb{F}_p^* \\ x & \mapsto & nx \end{cases}$$

Démonstration. On montre que si g est un générateur de $\mathbb{F}_p^*$, alors $\left(\frac{g}{p}\right) = \varepsilon(\sigma_g)$.

σ_g est circulaire donc $\varepsilon(\sigma_g) = (-1)^{p-1-1} = -1$. De plus g n'est pas un carré sinon tous les éléments de $\mathbb{F}_p^*$ en seraient, ce qui contredirait p impair. Donc $\left(\frac{g}{p}\right) = -1$. ∎

 Tous droits réservés

1.3.4 Calcul de $\left(\frac{2}{p}\right)$

On compte les inversions causées par σ_2.

On a, pour tout i, $2i = (2i \mod p)$ si $i \leqslant \frac{p-1}{2}$ et $2i = (2i - p \mod p)$ si $i > \frac{p-1}{2}$.

Pour avoir une inversion, il faut (et il suffit) d'avoir $i \leqslant \frac{p-1}{2}$, $j > \frac{p-1}{2}$ et $2i > 2j - p$ (ie $j \leqslant i + \frac{p-1}{2}$)

On a donc $\sum_{j=0}^{\frac{p-1}{2}} j = \frac{p^2-1}{8}$ inversions donc $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

1.3.5 Loi de réciprocité quadratique

Définition 1.6 On pose $\mu_p(E) = \{x \in E, x^p = 1\}$.

Définition 1.7 Soit K un corps et $P \in K[X]$ de degré d. On note $\overline{K}$ une clôture algébrique de K et $(\theta_1, \ldots, \theta_d)$ les racines de P dans $\overline{K}$.

Le discriminant de P, noté $\mathrm{disc}(P)$ est défini par

$$\mathrm{disc}(P) = \left(\prod_{i=1}^{d-1} \prod_{j=i+1}^{d} (\theta_i - \theta_j) \right)^2$$

THÉORÈME 1.10 $\mathrm{disc}(P) \in K$.

Démonstration. $\mathrm{disc}(P)$ est symétrique en les θ_i donc c'est un polynôme en les polynômes symétriques élémentaires en les θ_i, qui sont, au signe près les cœfficients de P.

Comme $P \in K[X]$, $\mathrm{disc}(P) \in K$. ∎

THÉORÈME 1.11 *Soient $(\theta_1, \ldots, \theta_p)$ les racines de $X^p - 1$ dans $\overline{\mathbb{F}_q}$. On pose $\delta = \prod_{i=1}^{d-1} \prod_{j=i+1}^{d} (\theta_i - \theta_j)$. On a :*

$$\delta^q = \delta \times \varepsilon \left(f : \begin{cases} \mu_p(\overline{\mathbb{F}_q}) & \to & \mu_p(\overline{\mathbb{F}_q}) \\ x & \mapsto & x^q \end{cases} \right)$$

Démonstration.

$$\delta^q = \left(\prod_{i=1}^{d-1} \prod_{j=i+1}^{d} (\theta_i - \theta_j) \right)^q = \prod_{i=1}^{d-1} \prod_{j=i+1}^{d} (\theta_i^q - \theta_j^q) = \prod_{i=1}^{d-1} \prod_{j=i+1}^{d} (\theta_i - \theta_j) \varepsilon(x \to x^q)$$

∎

 Tous droits réservés

THÉORÈME 1.12 $\varepsilon(x \to x^q) = 1$ *ssi* $\text{disc}(X^p - 1)$ *est un carré de* $\mathbb{F}_q$.

Démonstration.

$\Rightarrow$ $\varepsilon(x \to x^q) = 1$ donc $\delta^q = \delta$ (théorème 1.11). Donc δ est racine de $X^q - X$ dans $\overline{\mathbb{F}_q}$ donc $\delta \in \mathbb{F}_q$ et $\text{disc}(P) = \delta^2$.

$\Leftarrow$ Par contraposée, si $\varepsilon(x \to x^q) = -1$, $\delta^q = -\delta$ donc $\delta \notin \mathbb{F}_q$. ($\delta \neq 0$ car P est à racines simples)
Les racines, dans $\overline{\mathbb{F}_q}$, de $\text{disc}(P)$ étant $\pm\delta$, $\text{disc}(P)$ n'est pas un carré de $\mathbb{F}_q$. ∎

Proposition 1.3 Soit K un corps et $P \in K[X]$ unitaire de degré d. Notons $(\theta_1, \ldots, \theta_d)$ ses racines dans $\overline{K}$.

$$\text{disc}(P) = (-1)^{\frac{d(d-1)}{2}} \prod_{i=1}^{d} P'(\theta_i)$$

Démonstration. On a $P' = \sum_{i=1}^{d} \prod_{j \neq i} (X - \theta_j)$.

$P'(\theta_i) = \prod_{j \neq i} (\theta_i - \theta_j)$ donc $\prod_{i=1}^{d} P'(\theta_i) = \prod_{i=1}^{d} \prod_{j \neq i} (\theta_i - \theta_j)$.

Donc $\prod_{i=1}^{d} P'(\theta_i) = \text{disc}(P) \times (-1)^{1+2+\cdots+(d-1)} = (-1)^{\frac{d(d-1)}{2}} \text{disc}(P)$. ∎

THÉORÈME 1.13 $\text{disc}(X^p - 1) = (-1)^{\frac{p-1}{2}} p^p$

Démonstration.

$$\begin{aligned}
\text{disc}(X^p - 1) &= (-1)^{\frac{p(p-1)}{2}} \prod_{\theta \in \overline{K}, P(\theta) = 0} p\theta^{p-1} \quad \text{(Propriété 1.3)} \\
&= (-1)^{\frac{p-1}{2}} p^p \left(\prod_{\theta \in \overline{K}, P(\theta) = 0} \theta \right)^{p-1} \quad (p \text{ impair}) \\
&= (-1)^{\frac{p-1}{2}} p^p (-1)^{p(p-1)} \quad \text{(Relations cœfficients/racines)} \\
&= (-1)^{\frac{p-1}{2}} p^p \quad (\text{car } p(p-1) \equiv 0 \mod 2)
\end{aligned}$$

THÉORÈME 1.14 (LOI DE RÉCIPROCITÉ QUADRATIQUE) *Soient p et q deux entiers impairs premiers distincts. On a :*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

 Tous droits réservés

Démonstration. On a :

$$\left(\frac{q}{p}\right) = \varepsilon\left(\sigma_{q,p} : \begin{cases} \mathbb{F}_p^* & \to & \mathbb{F}_p^* \\ x & \mapsto & qx \end{cases}\right)$$

Comme $\mu_p(\overline{\mathbb{F}_q})$ est cyclique, via un isomorphisme, on a :

$$\left(\frac{q}{p}\right) = \varepsilon\left(f : \begin{cases} \mu_p(\overline{\mathbb{F}_q}) & \to & \mu_p(\overline{\mathbb{F}_q}) \\ x & \mapsto & x^q \end{cases}\right)$$

D'après le théorème 1.12, $\left(\frac{q}{p}\right) = \left(\frac{\text{disc}(X^p-1)}{q}\right)$.
D'après le théorème 1.13,

$$\left(\frac{q}{p}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}p^p}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)^p = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right)$$

(car p impair).

Or, $\left(\frac{p}{q}\right) \in \{1,-1\}$ donc $\left(\frac{p}{q}\right) = \frac{1}{\left(\frac{p}{q}\right)}$ donc on a bien $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$. ■

1.4 Symbole de Jacobi

1.4.1 Définition

Définition 1.8 Soit $m = \prod_{i=1}^{r} p_i \in 2\mathbb{Z}+1$, avec p_i premiers.

Le symbole de Jacobi de n et m, noté $\left(\frac{n}{m}\right)$ vaut $\prod_{i=1}^{r} \underbrace{\left(\frac{n}{p_i}\right)}_{\text{Legendre}}$.

Proposition 1.4

- $\left(\frac{n}{m}\right)\left(\frac{n'}{m}\right) = \left(\frac{nn'}{m}\right)$
- $\left(\frac{n}{m}\right)\left(\frac{n}{m'}\right) = \left(\frac{n}{mm'}\right)$
- $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$

Démonstration.

- Clair par définition
- On veut montrer que $\frac{m-1}{2} + \frac{m'-1}{2} \equiv \frac{mm'-1}{2} \mod 2$.
  En testant les cas, on obtient $\frac{m-1}{2} + \frac{m'-1}{2} \equiv 0 \mod 2$ si $mm' \equiv 1 \mod 4$ et 1 si $mm' \equiv -1 \mod 4$, ce qui correspond bien à $\frac{mm'-1}{2} \mod 2$.

 Tous droits réservés

- La propriété similaire concernant le symbole de Legendre assure le résultat d'après le point précédent. ■

Proposition 1.5 $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.

Démonstration. Le résultat avec le symbole de Legendre assure le résultat si on montre la multiplicativité de $(-1)^{\frac{m^2-1}{8}}$.

Or $\frac{m^2-1}{8} + \frac{m'^2-1}{8} \equiv 0 \mod 2$ si $mm' = \pm 1 \mod 8$ et 1 si $mm' = \pm 3 \mod 8$, ce qui correspond à la classe de $\frac{(mm')^2-1}{8}$ dans $\mathbb{Z}/2\mathbb{Z}$. ■

Proposition 1.6 Si m et n impairs, $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}$.

Démonstration. On montre de même la multiplicativité de $(-1)^{\frac{(m-1)(n-1)}{4}}$. Or, modulo 2, on a :

$$\begin{aligned}\frac{(m-1)(n-1)}{4} + \frac{(m'-1)(n-1)}{4} &\equiv \left(\frac{m-1}{2} + \frac{m'-1}{2}\right)\frac{n-1}{2} \\ &\equiv \frac{mm'-1}{2} \times \frac{n-1}{2}\end{aligned}$$ ■

1.4.2 Calcul effectif du symbole de Jacobi

On utilise un algorithme d'Euclide modifié pour ne garder que des impairs.
Pour calculer $\left(\frac{n}{m}\right)$:

Si n pair, on chasse les facteurs 2 $\left(\text{on calcule } \left(\frac{2}{m}\right)\right)$
On est ramené à n impair. Si $n = \pm 1 \mod m$, on sait calculer le symbole.

- Si $m \mid n$, $\left(\frac{n}{m}\right) = 0$
- Si $|n| > m$, on remplace n par le reste de la division euclidienne de n par m.
- On se ramène alors à $\left(\frac{m}{n}\right)$ à l'aide de la propriété précédente.

Exemple 1.1 $\left(\frac{90}{143}\right) = \left(\frac{2}{143}\right)\left(\frac{45}{143}\right)$. Or $143 \equiv -1 \mod 9$ donc $\left(\frac{2}{143}\right) = 1$.
Donc $\left(\frac{90}{143}\right) = \left(\frac{45}{143}\right) = \left(\frac{143}{45}\right)$ car $45 \equiv 1 \mod 4$ donc $(\frac{45-1}{2})(\frac{143-1}{2})$ est pair.
Or $\left(\frac{143}{45}\right) = \left(\frac{8}{45}\right)$ car $143 = 3 \times 45 + 8$.
De plus, $\left(\frac{8}{45}\right) = \left(\frac{2}{45}\right)^3 = \left(\frac{2}{45}\right) = -1$ car $45 \equiv -3 \mod 8$.
Donc $\left(\frac{90}{143}\right) = -1$.

 Tous droits réservés

1.4.3 Test de primalité

Étant donné un entier $N > 1$, on veut savoir si N est premier.

- Algorithme élémentaire : on essaie de diviser N par $2, 3, \ldots, E(\sqrt{n})$. (totalement inefficace)
- Utilisation du petit théorème de Fermat : Si N est premier et $a \wedge N = 1$ alors $a^{N-1} \equiv 1 \mod N$. On a alors une condition nécessaire non suffisante (nombres de Carmichael).
- Test de NON primalité (Soloway-Strassen) Il repose sur le fait que si N est premier et a premier avec N, $a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \mod N$.
  On prend N impair.
  Algorithme : On choisit au hasard $a \in [\![0, N-1]\!]$.
  Si $a \wedge N \neq 1$ alors N n'est pas premier,
  Sinon, on calcule $a^{\frac{N-1}{2}} \mod N$ et le symbole de Jacobi $\left(\frac{a}{N}\right)$.
  Si $a^{\frac{N-1}{2}} \not\equiv \left(\frac{a}{N}\right) \mod N$ alors N n'est pas premier.
  Sinon, on ne peut rien dire.

Théorème 1.15 *Si N n'est pas premier, alors au plus la moitié des entiers entre $[\![0, N-1]\!]$ ne détectent pas ce fait.*

Démonstration. On sait que $\left\{a \in (\mathbb{Z}/N\mathbb{Z})^*, a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \mod N\right\}$ est un sous-groupe de $\mathbb{Z}/N\mathbb{Z}^*$.
Il suffit donc de montrer que si N n'est pas premier, alors ce sous-groupe n'est pas $(\mathbb{Z}/N\mathbb{Z})^*$ tout entier.

- Si N est sans-facteur carré, soit p premier divisant N et a tel que $a \equiv 1 \mod \frac{N}{p}$ et $\left(\frac{a}{p}\right) = -1$.
  Alors, d'après le théorème chinois, $\left(\frac{a}{N}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{\frac{N}{p}}\right) = (-1)\left(\frac{1}{\frac{N}{p}}\right) = -1$.
  On a de plus $a^{\frac{N-1}{2}} = 1 \mod \frac{N}{p}$.
  Donc $a^{\frac{N-1}{2}} = \left(\frac{a}{N}\right) \mod N \Rightarrow a^{\frac{N-1}{2}} = \left(\frac{a}{N}\right) \mod \frac{N}{p} \Rightarrow 1 \equiv -1 \mod \frac{N}{p} \Rightarrow \frac{N}{p} \mid 2 \Rightarrow N \mid 2p$.
  On a donc une contradiction.
- Si N a un facteur carré, on a $p^2 \mid N$. Posons $a = 1 + \frac{N}{p}$.
  On a $a^p = (1 + \frac{N}{p})^p = \sum_{i=1}^{n} \binom{p}{i} \left(\frac{N}{p}\right)^i$;
  Comme p est premier, p divise les cœfficients binômiaux (sauf 1) donc $N \left| \binom{p}{i} \left(\frac{N}{p}\right)^i \right.$ pour tout i. De plus, $(\frac{N}{p})^p = \underbrace{\overbrace{\frac{N}{p}}^{=lN} \frac{N}{p}}_{=kp} (\frac{N}{p})^{p-2}$.
  Donc $N \mid (\frac{N}{p})^p$.

 Tous droits réservés

On a alors $a^p \equiv 1 \mod N$. Or p est premier et $a \not\equiv 1 \mod N$ donc a est d'ordre p dans $\mathbb{Z}/N\mathbb{Z}^*$.
$p \mid N$ donc $p \nmid N-1$ donc $a^{N-1} \not\equiv 1 \mod N$ donc $a^{\frac{N-1}{2}} \not\equiv \pm 1 \mod N$
Donc $a^{\frac{N-1}{2}} \not\equiv \left(\frac{a}{N}\right) \mod N$. ∎

- Test de Pocklington-Lehmer

  Théorème 1.16 *Soit $N \geqslant 2$ un entier. On suppose que la factorisation de $N-1$ est connue.*
  N est premier ssi pour tout p premier divisant $N-1$, il existe a_p tel que $a_p^{N-1} \equiv 1 \mod N$ et $a_p^{\frac{N-1}{p}} \wedge N = 1$.

  Démonstration.
  - Si N est premier, soit a un générateur de $\mathbb{Z}/N\mathbb{Z}^*$. a est d'ordre $N-1$ donc $a^{N-1} \equiv 1 \mod N$ et $a^{\frac{N-1}{p}} \not\equiv 1 \mod N$ car $0 < \frac{N-1}{p} < N-1$.
  - Réciproquement, si q est un diviseur premier de N et p un diviseur premier de $N-1$, on a $a^{N-1} \equiv 1 \mod q$ et $a^{\frac{N-1}{q}} \not\equiv 1 \mod q$.
    Soit e l'ordre de a dans $\mathbb{Z}/q\mathbb{Z}^*$. $e \mid N-1$ mais $e \nmid \frac{N-1}{p}$.
    Posons $N-1 = \prod_{i=1}^{s} p_i^{\alpha_i}$ et $e = \prod_{i=1}^{s} p_i^{\beta_i}$.
    On a, pour tout i, $\beta_i \leqslant \alpha_i$ mais il existe i_0 tel que $p_{i_0} = p$ et $\beta_{i_0} \leqslant \alpha_{i_0} - 1$ est faux donc $\alpha_{i_0} = \beta_{i_0}$.
    On a alors $v_p(e) = v_p(N-1)$.
    Comme e est l'ordre de a dans $\mathbb{Z}/q\mathbb{Z}^*$, $e \mid q-1$ donc $v_p(q-1) \geqslant v_p(e) = v_p(N-1)$.
    En quantifiant en p, on obtient $N-1 \mid q-1$. Or $q-1 > 0$ donc $q-1 \geqslant N-1$. Or $q \mid N$ donc $N = q$ et q est premier. ∎

1.5 Factorisation dans $\mathbb{F}_q[X]$

1.5.1 Algorithme de Berlekanp

On a $q = p^d$ avec p premier. $Q \in \mathbb{F}_q[X]$ peut être supposé sans facteur carrés (en faisant des PGCD avec Q',...).

Théorème 1.17 *Soit $Q = \prod_{i=0}^{m-1} Q_i$ avec Q_i irréductible. Soit $R \in \mathbb{F}_q[X]$.*

$R^q \equiv R \mod Q$ ssi $\forall i \in [\![0, m-1]\!], \exists s_i \in \mathbb{F}_q, R \equiv s_i \mod Q_i$

Démonstration.

 Tous droits réservés

$\Leftarrow$ Pour tout i, $R^q - R \equiv s_i^q - s_i \mod Q_i$. Or $s_i \in \mathbb{F}_q$ donc $s_i^q = s_i$ donc $R^q \equiv R \mod Q_i$.
Les Q_i étant premiers entre eux (pas de facteurs carrés), $R^q \equiv R \mod Q$.

$\Rightarrow$ Posons $K_i = \mathbb{F}_q[X]/\langle Q_i \rangle$.
Les K_i sont des corps et des extensions finies de $\mathbb{F}_q$. La classe de R dans K_i est une racine de $Y^q - Y \in K_i[Y]$.
Ces racines sont les éléments de $\mathbb{F}_q$ donc il existe $s_i \in \mathbb{F}_q$ tel que $R = s_i$ dans K_i ie $R \equiv s_i \mod Q_i$. ■

Remarque 1.7

- *$\{R \in \mathbb{F}_q[X]/\langle Q \rangle, R^q = R \mod Q\}$ est un sous-espace vectoriel de $\mathbb{F}_q[X]/\langle Q \rangle$ qui est un $\mathbb{F}_q$-espace vectoriel. Plus précisément, c'est le noyau de l'application $\mathbb{F}_q$ linéaire :*

$$f : \begin{cases} \mathbb{F}_q[X]/\langle Q \rangle & \to & \mathbb{F}_q[X]/\langle Q \rangle \\ R & \mapsto & R^q - R \end{cases}$$

  En particulier, on peut calculer une base de ce noyau (par exemple avec un pivot de Gauss).
- *Ce noyau est isomorphe (en tant que $\mathbb{F}_q$-espace vectoriel) à $\mathbb{F}_q^m$, donc ce noyau est de dimension m.*
- *Le cas où tous les s_i sont égaux correspond au cas où R est constant modulo Q ie à la droite vectorielle de $\mathbb{F}_q[X]/\langle Q \rangle$ engendrée par 1.*

Algorithme :

- Écrire la matrice de :

$$f : \begin{cases} \mathbb{F}_q[X]/\langle Q \rangle & \to & \mathbb{F}_q[X]/\langle Q \rangle \\ R & \mapsto & R^q - R \end{cases}$$

  dans $(1, X, \ldots, X^{\deg(Q)-1})$
- Calculer une base $(A_1 = 1, A_2, \ldots, A_m)$ de son noyau par pivot de Gauss.
  Si $m = 1$, alors Q est irréductible. Sinon,
  Choisir $j \in [\![2, m]\!]$
  Calculer $(A_j - s) \wedge Q$ pour tout $s \in \mathbb{F}_q$.
  D'après le théorème, l'un de ces PGCD donne un facteur non trivial de Q. ($A_j \in \mathrm{Ker}(f)$ donc pour $s = s_i$, $Q_i \mid (A_j - s) \wedge Q$)
  On peut alors recommencer avec les deux parties issues de Q.

 Tous droits réservés

 Tous droits réservés

Chapitre 2

Réseaux

2.1 Définition et théorème de Minkowski

Définition 2.1 Soit E un $\mathbb{R}$-espace vectoriel de dimension finie n muni d'une base $(e_1 \cdots, e_n)$. Un réseau de E est un sous-$\mathbb{Z}$-module de la forme $\mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$.

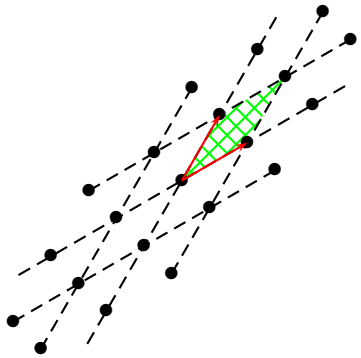

Figure 2.1 – Réseau de $\mathbb{R}^2$

Théorème 2.1 *Un sous-$\mathbb{Z}$-module qui engendre E comme $\mathbb{R}$-espace vectoriel est un réseau ssi il est discret.*

Démonstration.

$\Rightarrow$ Si Λ est un réseau de E, avec $\Lambda = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$ où $(e_1, \ldots, e_n)$ est une base de E.

$$\varphi : \begin{cases} \mathbb{R}^n & \to & E \\ (x_1, \dots, x_n) & \mapsto & \sum_{i=1}^{n} x_i e_i \end{cases}$$

est un isomorphisme d'espaces vectoriels topologiques (c'est un homéomorphisme linéaire).

$\mathbb{Z}^n$ est discret dans $\mathbb{R}^n$ donc $\Lambda = \varphi(\mathbb{Z}^n)$ est discret dans E.

$\Leftarrow$ Par récurrence sur n.

On suppose Λ discret. On prend $(g_1, \dots, g_r)$ une famille libre maximale incluse dans Λ.

On note $E_0 = \text{Vect}\{g_1, \dots, g_{r-1}\}$ et $\Lambda_0 = \Lambda \cap E_0$.

Λ_0 est un sous-$\mathbb{Z}$-module discret de E_0 (qui est de dimension inférieure à n) et Λ_0 engendre E_0.

Par hypothèse de récurrence, Λ_0 est un réseau de E_0. Donc il existe $(e_1, \dots, e_{r-1})$ base de E_0 tel que $\Lambda_0 = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_{r-1}$.

$(e_1, \dots, e_{r-1}, g_r)$ est libre et maximale car $(g_1, \dots, g_r)$ l'était.

On considère

$$D = \{\lambda_1 e_1 + \dots + \lambda_{r-1} e_{r-1} + \lambda_r g_r, (\lambda_1, \dots, \lambda_{r-1}) \in [0,1[, \lambda_r \in]0,1]\}$$

On pose $T = D \cap \Lambda$. D est borné dans E qui est de dimension finie donc il est compact.

T est donc inclus dans un compact discret donc il est fini. On prend $e_r \in T$ avec λ_r minimal.

$e_r = \sum_{i=1}^{r} \lambda_i e_i$. $(e_1, \dots, e_r)$ est donc libre maximale.

Si $x \in \Lambda$, comme Λ engendre E, toute famille libre maximale formée d'éléments de Λ est une base de E, $(e_1, \dots, e_{r-1}, g_r)$ est une base de E.

Donc $x = \sum_{i=1}^{r-1} \mu_i e_i + \mu_r e_r$.

Le soustraction d'un élément de $\mathbb{Z}e_1 + \dots + \mathbb{Z}e_r$ à x, noté y, vérifie $\mu_r \in [0, \lambda_r[$, puis $\mu_1, \dots, \mu_{r-1} \in [0,1[$.

$y \in \Lambda$ donc si $\mu_r \neq 0$, alors $y \in T$ donc on a une contradiction avec la minimalité de λ_r.

Donc $\mu_r = 0$ donc $y \in E_0 \cap \Lambda = \Lambda_0$. Or $(e_1, \dots, e_{r-1})$ est une base de Λ_0 donc $(\mu_1, \dots, \mu_{r-1}) \in \mathbb{Z}$ donc ils sont nuls et $y = 0$.

Donc $x \in \mathbb{Z}e_1 + \dots + \mathbb{Z}e_r$. Donc $\Lambda \subset \mathbb{Z}e_1 + \dots + \mathbb{Z}e_r$ donc $\Lambda = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_r$.

Par récurrence on a le résultat. ∎

Remarque 2.1 Si Λ est un réseau de E, il n'y a pas unicité de la base $(e_1, \dots, e_n)$ telle que $\Lambda = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_n$. La matrice de passage entre deux

telles bases est une matrice à cœfficients entiers, inversible et son inverse est à cœfficients entiers. En particulier, le déterminant d'une telle matrice vaut ± 1.

Définition 2.2 La dimension d'un réseau est la dimension de l'espace vectoriel qu'il engendre.

Un domaine fondamental de Λ est une partie D de E telle que $(D+x)_{x\in\Lambda}$ soit une partition de E.

Le volume de Λ est le volume du domaine fondamental

$$D = \left\{ \sum_{i=1}^{n} \lambda_i e_i, (\lambda_1, \dots, \lambda_n) \in [0,1[^n \right\}$$

C'est $|\det_{b.c.\mathbb{R}^2}(e_1, \dots, e_n)|$.

THÉORÈME 2.2 *Soit Λ un réseau de $\mathbb{R}^n$ de domaine fondamental D.*
Soit $\pi : \mathbb{R}^n \to \mathbb{R}^n/\Lambda$ et $\Phi = \pi|_D$.
Soit X une partie mesurable bornée de $\mathbb{R}^n$ et λ la mesure de Lebesgue.
Si $\lambda(\Phi^{-1}(\pi(X))) \neq \lambda(X)$, $\pi|_X$ n'est pas injective.

Démonstration. On suppose que $\pi|_X$ est injective.

On pose $U = \{v \in \Lambda, (D+v) \cap X \neq \varnothing\}$. X est borné donc U est fini.

De plus, $X = \bigcup_{v\in U} (D+v) \cap X$ car D est un domaine fondamental.

On a de plus $(D+v) \cap X = (D \cap (X-v)) + v$.

Montrons que les $D \cap (X-v)$, $v \in U$ sont deux à deux disjoints. Si $x \in D \cap (X-v_0) \cap (X-v_1)$.

$x + v_0 \in X$ et $x + v_1 \in X$ donc $\pi(x+v_0) = \pi(x+v_1) = \pi(x)$.

Par injectivité, $x + v_0 = x + v_1$ donc $v_0 = v_1$ donc $D \cap (X - v_0) = D \cap (X - v_1)$.

On a donc $\lambda(X) = \sum_{v\in U} \lambda((D+v) \cap X) = \sum_{v\in U} \lambda(D \cap (X-v))$.

De plus,

$$\begin{aligned}
\lambda(\Phi^{-1}(\pi(X))) &= \lambda\left(\Phi^{-1}\left(\pi\left(\bigcup_{v\in U}(D+v)\cap X\right)\right)\right) \\
&= \lambda\left(\Phi^{-1}\left(\bigcup_{v\in U}\pi((D+v)\cap X)\right)\right) \\
&= \sum_{v\in U}\lambda(\Phi^{-1}(\pi((D+v)\cap X)))
\end{aligned}$$

Or $\pi((D+v)\cap X) = \pi(D \cap (X-v)) = \Phi(D \cap (X-v))$.

Donc $\Phi^{-1}(\pi((D+v)\cap X)) = D \cap (X-v)$.

Donc $\lambda(\Phi^{-1}(\pi(X))) = \sum_{v\in U} \lambda(D \cap (X-v)) = \lambda(X)$. ∎

 Tous droits réservés

THÉORÈME 2.3 MINKOWSKI *Soit Λ un réseau de $\mathbb{R}^n$, D le domaine fondamental usuel.*

Soit X un convexe symétrique borné non vide de $\mathbb{R}^n$.

Si $\lambda(X) > 2^n\lambda(D)$ alors $(X \cap \Lambda) \setminus \{0\} \neq \varnothing$.

Démonstration. On applique le lemme précédent à 2Λ, $2D$ et X.

$$\lambda(\Phi^{-1}(\pi(X))) \leqslant \lambda(2D) = 2^n\lambda(D) < \lambda(X)$$

Donc $\pi|_X$ n'est pas injective donc il existe $x_0, x_1 \in X$ tel que $\pi(x_0) = \pi(x_1)$ et $x_0 \neq x_1$.

$\pi(x_0) = \pi(x_1)$ donc $x_0 - x_1 \in 2\Lambda$ donc $\frac{x_0-x_1}{2} \in \Lambda$.

Or $\frac{x_0-x_1}{2} \in X$. (X convexe et symétrique).

De plus, $\frac{x_0-x_1}{2} \neq 0$ car $x_0 \neq x_1$.

Donc $\frac{x_0-x_1}{2}$ convient. ∎

2.2 Applications

2.2.1 Théorème des deux carrés

THÉORÈME 2.4 *Soit p premier. p est somme de deux carrés ssi $p \not\equiv 3 \mod 4$.*

Démonstration.

$\Rightarrow$ Si $p = x^2 + y^2$. Les carrés dans $\mathbb{Z}/4\mathbb{Z}$ sont 0 et 1 donc $x^2 \equiv 0 \mod 4$ ou $x^2 \equiv 1 \mod 4$ et de même pour y^2.

Donc $x^2 + y^2 \equiv 0, 1, 2 \mod 4 \not\equiv 3 \mod 4$.

$\Leftarrow$ Si $p \not\equiv 3 \mod 4$.

Si $p = 2$, $p = 1^2 + 1^2$. Si $p \neq 2$, $p \equiv 1 \mod 4$.

Comme $p \equiv 1 \mod 4$, on a $\left(\frac{-1}{p}\right) = 1$ donc il existe $\alpha \in \mathbb{Z}$, $\alpha^2 \equiv -1 \mod p$.

On pose $\Lambda = \{(x, y) \in \mathbb{Z}^2, y \equiv \alpha x \mod p\}$.

$(1, \alpha)$, $(0, 1)$ est une base de $\mathbb{Z}^2$ donc $(x, y) \in \Lambda$ ssi il existe $a \in \mathbb{Z}$, $y = ap + \alpha x$ ssi $(x, y) \in \mathbb{Z}(1, \alpha) + p\mathbb{Z}(0, 1)$.

Les diviseurs élémentaires sont donc 1 et p.

Le volume de Λ est $\begin{vmatrix} 1 & 0 \\ \alpha & p \end{vmatrix} = p$.

On applique le théorème de Minkowski avec $X = B(0, r)$: si $\pi r^2 > 4p$, $X \cap \Lambda$ contient un élément non nul.

Si $(x, y) \in X \cap \Lambda$ est non nul, $y \equiv \alpha x \mod p$ et $x^2 + y^2 \leqslant r^2$.

Donc $y^2 \equiv -x^2 \mod p$ donc $x^2 + y^2 \equiv 0 \mod p$.

 Tous droits réservés

Si $r^2 < 2p$, $p = x^2 + y^2$. On cherche donc r tel que $\pi r^2 > 4p$ et $r^2 < 2p$, ce qui est possible car $2 < \pi$. ■

2.2.2 Théorème des quatre carrés

THÉORÈME 2.5 *Tout entier naturel est somme de quatre carrés.*

Démonstration.

- On a $0 = 0^2+0^2+0^2+0^2$, $1 = 0^2+0^2+0^2+1^2$ et $2 = 0^2+0^2+1^2+1^2$.
- Si a et b sont somme de 4 carrés, $a = x_0^2+x_1^2+x_2^2+x_3^2$ et $b = y_0^2+y_1^2+y_2^2+y_3^2$.
  a est le carré du module du quaternion $x_0 + ix_1 + jx_2 + kx_3$. b est celui de $y_0 + iy_1 + jy_2 + ky_3$.
  Le produit de ces quaternions est $z_0+iz_1+jz_2+kz_3$ qui a pour module au carré ab (en effet $|xy| = |x||y|$ pour tout $x, y \in \mathbb{H}$).
  Il suffit donc de montrer le résultat pour les nombres premiers impairs (fait pour 2).
- Soit p premier impair.

  Lemme 2.5.1
  Il existe (α, β) tel que $\alpha^2 + \beta^2 + 1 \equiv 0 \mod p$.

  Démonstration. Il y a $\frac{p+1}{2}$ carrés dans $\mathbb{F}_p$. Donc α^2+1 prend $\frac{p+1}{2}$ valeurs dans $\mathbb{F}_|$ et $-\beta^2$ aussi.
  Or $\frac{p+1}{2} + \frac{p+1}{2} = p + 1 > p$ donc il existe α, β tel que $\alpha^2 + 1 \equiv -\beta^2 \mod p$. ■

  On considère le réseau $\Lambda = \{(x, y, z, t) \in \mathbb{Z}^4, z \equiv \alpha x+\beta y \mod p \text{ et } t = \alpha y - \beta x \mod p\}$.
  Le volume de Λ est p^2 car $((1, 0, \alpha, -\beta), (0, 1, \beta, \alpha), pe_3, pe_4)$ est une base et le déterminant associé vaut p^2.
  On utilise le théorème de Minkowski avec pour convexe la boule de rayon r centrée en 0. Le volume de vette boule est $\frac{\pi^2}{2}r^4$.
  Si $\frac{\pi^2}{2}r^4 > 2^4p^2$, alors il existe $(x, y, z, t) \in \Lambda \setminus \{0\}$ avec $x^2+y^2+z^2+t^2 \leqslant r^2$.
  Si $(x, y, z, t) \in \Lambda$, $x^2+y^2+z^2+t^2 \equiv x^2+y^2+(\alpha x+\beta y)^2+(\alpha y-\beta x)^2 \equiv x^2(1+\alpha^2+\beta^2)+y^2(1+\alpha^2+\beta^2) \equiv 0 \mod p$.
  Comme $\pi^2 > 8$, $\frac{32}{\pi^2} < 4$ donc il existe r tel que $\frac{32p^2}{\pi^2} < r^4 < 4p^2$.
  Pour ce r, on a $\frac{\pi^2}{2}r^4 > 16p^2$ et $r^2 < 2p$.
  Donc Minkowski s'applique et $0 < x^2 + y^2 + z^2 + t^2 < r^2 < 2p$ et $p \mid (x^2 + y^2 + z^2 + t^2)$ donc $x^2 + y^2 + z^2 + t^2 = p$. ■

 Tous droits réservés

 Tous droits réservés

Chapitre 3

Anneaux des entiers d'un corps de nombres

3.1 Rappels

Définition 3.1 Un corps de nombres est une extension de $\mathbb{Q}$ (ie un $\mathbb{Q}(\alpha)$ avec α algébrique).

Définition 3.2 Si A est un anneau intègre, si $p \in A$, et $p \notin A^\times \cup \{0\}$, on dit que p est premier ssi $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$.

Proposition 3.1 p premier ssi $\langle p \rangle$ est premier ssi $A/\langle p \rangle$ est intègre.

Définition 3.3 p est irréductible ssi $p = ab \Rightarrow a \in A^\times$ ou $b \in A^\times$.

Proposition 3.2 Si p premier, p irréductible.

Démonstration. Si p est premier et $p = ab$, $p \mid ab$ donc $p \mid a$ ou $p \mid b$.

Si $p \mid a$, $a = p\alpha$ donc $p = ab = p\alpha b$ donc $\alpha b = 1$ (A intègre) donc $b \in A^\times$. ∎

Définition 3.4 Si A est un anneau intègre, on dit que A est factoriel ssi tout élément de $A \setminus \{0\}$ s'écrit $up_1 \cdots p_n$ avec $u \in A^\times$, $(p_1, \ldots, p_n)$ irréductibles et cette décomposition est unique à permutation des p_i est multiplication par $v \in A^\times$ près.

Définition 3.5 Un anneau A est dit nœthérien ssi tout idéal de A est engendré par un nombre fini d'éléments (de type fini) ssi toute suite croissante d'idéaux stationne.

Remarque 3.1 Si A est intègre nœthérien, l'existence de la décomposition est vérifiée.

Exemple 3.1

- $\mathbb{Z}$ est factoriel.
- $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel : $6 = 2 \times 3 = (1 - i\sqrt{5})(1 + i\sqrt{5})$ et 2, 3, $1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont irréductibles.

Remarque 3.2 La condition d'unicité est équivalente à (p premier ssi p irréductible) et à (a | bc et (d | a et d | b ⇒ d inversible) ⇒ a | c).

Définition 3.6 Si A est un anneau intègre, et si tout idéal de A est principal (ie monogène), on dit que A est principal.

Proposition 3.3 Les anneaux principaux sont factoriels (et clairement nœthériens).

Définition 3.7 Si A est intègre, et s'il existe une application ν [1] : $A \setminus \{0\} \to \mathbb{N}$ tel que pour tout $a, b \in A \setminus \{0\}$, il existe $q, r \in A$ tel que $a = bq + r$ avec $\nu(r) < \nu(b)$, A est dit euclidien.

Proposition 3.4 Les anneaux euclidiens sont principaux donc factoriels.

Définition 3.8 Si L/K est une extension de corps et si $x \in L$, on dit que x est algébrique sur K si x est racine d'un polynôme à cœfficients dans K.

3.2 Entiers algébriques

Définition 3.9 Un nombre algébrique est un élément d'un sur-corps de $\mathbb{Q}$ qui est algébrique sur $\mathbb{Q}$.

Définition 3.10 Un corps de nombres est une extension finie de $\mathbb{Q}$.

Remarque 3.3 D'après le théorème de l'élément primitif, tout les corps de nombres sont de la forme $\mathbb{Q}[\theta]$ pour un θ algébrique.

Proposition 3.5 Si K est un corps de nombres avec $K = \mathbb{Q}[\theta]$ et $n = [K : \mathbb{Q}]$ alors n est le degré du polynôme minimal de θ sur $\mathbb{Q}$ et il y a n morphismes de corps distincts de $K \to \mathbb{C}$ ou dans une clôture algébrique de K. Ces morphismes sont les :

$$\pi_i : \begin{cases} \mathbb{Q}[\theta] & \to & \mathbb{C} \\ P(\theta) & \mapsto & P(\theta_i) \end{cases}$$

avec $\theta_1, \ldots, \theta_n$ sont mes racines de μ_θ sur $\mathbb{Q}$.

Exemple 3.2 $\mathbb{Q}[\sqrt{2}]$ est un corps de nombres de degré 2 et les morphismes sont :

$$f_1 : \begin{cases} \mathbb{Q}[\sqrt{2}] & \to & \mathbb{C} \\ a + b\sqrt{2} & \mapsto & a + b\sqrt{2} \end{cases} \qquad f_2 : \begin{cases} \mathbb{Q}[\sqrt{2}] & \to & \mathbb{C} \\ a + b\sqrt{2} & \mapsto & a - b\sqrt{2} \end{cases}$$

1. appellée stathme

 Tous droits réservés

Définition 3.11 Si L/K est une extension de K, et si $(\alpha_1, \ldots, \alpha_n)$ une base de L comme K espace vectoriel, on appelle discriminant de la base $(\alpha_1, \ldots, \alpha_n)$ le nombre $\det(M)^2$ où M est la matrice $(\sigma_i(\alpha_j))_{i,j}$ où les σ_i sont les morphismes de corps K-linéaires de L dans $\overline{K}$.

Remarque 3.4 *Si $L = K[\theta]$ alors $(1, \theta, \ldots, \theta^{n-1})$ est une base de L comme K espace vectoriel et le discriminant de cette base est $\operatorname{disc}(\mu_\theta)$. C'est un élément de K car c'est un polynôme symétrique en les $\sigma_i(\theta)$, donc un polynôme en les cœfficients de K donc dans K.*

Définition 3.12 Soit θ un nombre algébrique. On dit que θ est un entier algébrique si θ est racine d'un polynôme unitaire à cœfficients entiers.

Exemple 3.3

- Tout élément de $\mathbb{Z}$ est un entier algébrique.
- $\sqrt{k}$ avec $k \in \mathbb{N}$ est un entier algébrique.
- $\frac{1+\sqrt{5}}{2}$ est un entier algébrique.
- $\frac{1}{2}$ n'est pas algébrique : si $\dfrac{1}{2^n} + \displaystyle\sum_{i=0}^{n-1} \frac{a_i}{2^i} = 0$, $1 + \displaystyle\sum_{i=0}^{n-1} a_i 2^{n-i} = 0$ et le terme de gauche est impair.

Lemme 3.0.2
Soit θ un nombre algébrique. θ est algébrique ssi $\mathbb{Z}[\theta]$ est un $\mathbb{Z}$-module de type fini.

Remarque 3.5 *Si θ était transcendant sur $\mathbb{Q}$, $\mathbb{Z}[\theta]$ ne serait pas de type fini.*

Démonstration.

$\Rightarrow$ Si θ est algébrique, il existe $P \in \mathbb{Z}[X]$ unitaire annulateur de θ.
Si $x \in \mathbb{Z}[\theta]$, il existe $Q \in \mathbb{Z}[X]$ tel que $x = Q(\theta)$. Notons R le reste dans la division euclidienne[2] de Q par P.
$x = Q(\theta) = R(\theta)$ et $\deg(R) < \deg(P)$ donc x est une combinaison linéaire à cœfficients entiers de $(1, \theta, \ldots, \theta^{\deg(P)-1})$.
Donc le $\mathbb{Z}$-module $\mathbb{Z}[\theta]$ est engendré par $(1, \theta, \ldots, \theta^{\deg(P)-1})$.

$\Leftarrow$ On suppose que $\mathbb{Z}[\theta] = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r$.
$\theta e_i \in \mathbb{Z}[\theta]$ donc il existe des $(b_{i,j}) \in \mathbb{Z}$ tels que $\theta e_i = \displaystyle\sum_{j=1}^{n} b_{i,j} e_j$.
Notons $M = (b_{i,j})_{i,j}$. ${}^t(e_1, \ldots, e_r) \in \operatorname{Ker}(M - \theta I_r) \setminus \{0\}$ donc $\det(M - \theta I_r) = 0$.
Le polynôme $D = \det(XI_r - M)$ appartient à $\mathbb{Z}[X]$, son cœfficient dominant vaut 1 et $D(\theta) = 0$.
Donc θ est algébrique. ∎

2. bien dans $\mathbb{Z}[X]$: cf après

 Tous droits réservés

Lemme 3.0.3
Pour tout $(P,Q) \in \mathbb{Z}[X]^2$, il existe $R \in \mathbb{Z}[X]$ tel que $Q \equiv R \mod P$ et $\deg(R) < \deg(P)$.

Démonstration. Par récurrence sur $\deg(Q)$. Supposons la propriété vraie au rang $n-1$.

Si $\deg(Q) < \deg(P)$, c'est évident.

Sinon, soit $Q_1 \in \mathbb{Z}[X]$ de degré n. $Q_1 = \sum_{i=0}^{n} a_i X^i$ et $P = \sum_{i=0}^{r-1} b_i X^i + X^r$.

$$\begin{aligned} Q_1 &= \sum_{i=0}^{n-1} a_i X^i + a_n X^{n-r} P - \sum_{i=0}^{r-1} a_n b_i X^{m-n+i} \\ &\equiv \sum_{i=0}^{n-1} a_i X^i - \sum_{i=0}^{r-1} a_n b_i X^{m-n+i} \mod P \end{aligned}$$

Par hypothèse de récurrence, il existe $R \in \mathbb{Z}[X]$ tel que $\deg(R) < r$ et :

$$R \equiv \sum_{i=0}^{n-1} a_i X^i - \sum_{i=0}^{r-1} a_n b_i X^{m-n+i} \equiv Q \mod P$$

Le principe de récurence assure le résultat. ∎

THÉORÈME 3.1 *L'ensemble des entiers algébriques est un anneau.*

Démonstration. On va montrer que c'est un sous anneau de $\mathbb{C}$.

Soient θ_1, θ_2 deux entiers algébriques. $\mathbb{Z}[\theta_1]$ et $\mathbb{Z}[\theta_2]$ sont des $\mathbb{Z}$ modules de type fini engendrées par $(e_1, \dots, e_r)$ et $(f_1, \dots, f_s)$ respectivement.

$\mathbb{Z}[\theta_1, \theta_2]$ est de type fini car engendré par $(e_i f_j)$.

$\mathbb{Z}[\theta_1 + \theta_2]$ et $\mathbb{Z}[\theta_1 \theta_2]$ sont des sous-modules de $\mathbb{Z}[\theta_1, \theta_2]$ qui est un module de type fini donc c'est un quotient d'un $\mathbb{Z}$-module libre Λ de type fini. Notons π la surjection canonique.

$\pi^{-1}(\mathbb{Z}[\theta_1 + \theta_2])$ est un module libre de type fini donc $\mathbb{Z}[\theta_1 + \theta_2]$ est de type fini. De même, $\mathbb{Z}[\theta_1 \theta_2]$ est de type fini.

Donc $\theta_1 + \theta_2$ et $\theta_1 \theta_2$ sont des entiers algébriques. ∎

Proposition 3.6 Les racines d'un polynôme à cœfficients entiers algébriques sont des entiers algébriques.

Démonstration. Soit $P = X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathbb{Z}[X]$. Soit θ une racine de P.

$\mathbb{Z}[a_0, \dots, a_{n-1}, \theta] = \mathbb{Z}[a_0, \dots, a_{n-1}][\theta]$ est de type fini sur $\mathbb{Z}[a_0, \dots, a_{n-1}]$ (par division euclidienne par P).

 Tous droits réservés

De plus, $\mathbb{Z}[a_0, \ldots, a_{n-1}]$ est de type fini sur $\mathbb{Z}$ car $\mathbb{Z}[a_0], \ldots, \mathbb{Z}[a_{n-1}]$ en sont.

Donc $\mathbb{Z}[a_0, \ldots, a_{n-1}, \theta]$ est de type fini sur $\mathbb{Z}$.

$\mathbb{Z}[\theta]$ est un sous module de type fini de $\mathbb{Z}[a_0, \ldots, a_{n-1}, \theta]$ donc de $\mathbb{Z}$.

Donc θ est un entier algébrique. ■

Proposition 3.7 Les entiers algébriques de $\mathbb{Q}$ sont les entiers relatifs.

Démonstration. On a déjà vu une inclusion.

Soit $r \in \mathbb{R}$. $r = \frac{x}{y}$ avec $x \wedge y = 1$.

Soit $P = X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathbb{Z}[X]$ tel que $P(\frac{x}{y}) = 0$.

On a $0 = \frac{x^n}{y^n} + \sum_{i=0}^{n-1} a_i \frac{x^i}{y^i}$.

Donc $0 = x^n + \sum_{i=0}^{n-1} a_i x^i y^{n-i} \equiv x^n \mod y$.

Donc $y \mid x^n$ or $x \wedge y = 1$ donc $y \mid 1$ donc $\frac{x}{y} \in \mathbb{Z}$. ■

Définition 3.13 Si K est un corps de nombres, l'anneau des entiers de K, noté $\mathcal{O}_K$ est l'ensemble $\{x \in K, x \text{ entier algébrique}\}$. C'est un sous-anneau de K.

Remarque 3.6 $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Proposition 3.8 Tout nombre algébrique est quotient d'un entier algébrique par un entier naturel non nul.

Démonstration. Si θ est algébrique, il existe $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ tel que $P(\theta) = 0$.

$a_n\theta$ est racine de $Q = X^n + a_{n-1}X^{n-1} + a_n a_{n-2} X^{n-2} + \cdots + a_n^{n-1} a_0$. En effet, $Q(\theta) = a_n^{n-1} P(\theta) = 0$.

Donc $a_n\theta$ est un entier algébrique. ■

Définition 3.14 Si $P \in \mathbb{Z}[X]$. On appelle contenu de P le pgcd de ses cœfficients.

On peut étendre la notion de contenu à $\mathbb{Q}[X]$ en posant $C(\frac{P}{\lambda}) = \frac{C(P)}{|\lambda|}$.

Proposition 3.9 Pour tout $(P, Q) \in \mathbb{Q}[X]^2$, $C(PQ) = C(P)C(Q)$.

Proposition 3.10 Soit θ un nombre algébrique. θ est un entier algébrique ssi $\mu_\theta \in \mathbb{Z}[X]$.

Démonstration.

$\Leftarrow$ Clair

 Tous droits réservés

$\Rightarrow$ Si θ est un entier algébrique, il existe $Q \in \mathbb{Z}[X]$ unitaire tel que $Q(\theta) = 0$.
$P = \mu_\theta \mid Q$ donc $Q = PS$ avec Q et P unitaires.
$C(Q) = C(P)C(S)$ donc $\frac{Q}{C(Q)} = \frac{P}{C(P)}\frac{S}{C(S)}$ et ces trois polynômes sont à cœfficients entiers.
$Q \in \mathbb{Z}[X]$ est unitaire donc $C(Q) = 1$ et $\frac{Q}{C(Q)} = Q$ est donc unitaire.
Le cœfficient dominant de $\frac{P}{C(P)}\frac{S}{C(S)}$ est le produit des cœfficients dominants p et s de $\frac{P}{C(P)}\frac{S}{C(S)}$.
Donc $ps = 1$ et $p, s \in \mathbb{Z}^2$ donc $p = s = 1$ ou $p = s = -1$. Or P est unitaire donc $p = \frac{1}{C(P)}$. Donc $C(P) = 1$ et $P = \frac{P}{C(P)} \in \mathbb{Z}[X]$. ■

 Tous droits réservés

Chapitre 4

Anneau des entiers des corps quadratiques

4.1 Détermination

Définition 4.1 On appelle corps quadratique toute extension de degré 2 de $\mathbb{Q}$.

Proposition 4.1 Ce sont les $\mathbb{Q}[\sqrt{k}]$ avec $k \in \mathbb{Z}$ non carré. On peut même supposer k sans facteur carré.

Si $k > 0$, on parle de corps quadratique réel, et si $k < 0$, on parle de corps quadratique imaginaire.

Démonstration. La première inclusion est claire.

De plus, $\mathbb{Q}[X]/(aX^2 + bX + c) = \mathbb{Q}(\frac{-b+\sqrt{b^2-4ac}}{2a}) = \mathbb{Q}[\sqrt{b^2 - 4ac}]$. ■

On cherche l'anneau des entiers de $\mathbb{Q}[\sqrt{d}]$.
$a + b\sqrt{d}$ a-t-il un polynôme minimal à cœfficients entiers ?
Si $b = 0$, $X - a$ convient.
Sinon, $a + b\sqrt{d} \notin \mathbb{Q}$ et $X^2 - 2aX + a^2 - db^2$ annule $a + b\sqrt{d}$.
Donc $a + b\sqrt{d} \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ ssi $2a \in \mathbb{Z}$ et $a^2 - db^2 \in \mathbb{Z}$.
On a doit donc avoir $a \in \mathbb{Z}$ ou $a - \frac{1}{2} \in \mathbb{Z}$.

- Si $a \in \mathbb{Z}$,
  Pour tout p premier, $v_p(db^2) \geqslant 0$ et $v_p(d) \in \{0, 1\}$ donc $v_p(b^2) \geqslant -1$ donc $2v_p(b) \geqslant -1$ donc $v_p(b) =\geqslant 0$.
  Donc $b \in \mathbb{Z}$.
- Si $a - \frac{1}{2} \in \mathbb{Z}$, $a^2 = (a - \frac{1}{2})^2 + (a - \frac{1}{2}) + \frac{1}{4}$.
  Donc $a^2 - \frac{1}{4} \in \mathbb{Z}$ donc $4a^2 \equiv 1 \mod 4$.
  $a^2 - db^2 \in \mathbb{Z}$ donc $0 \equiv 4a^2 - 4db^2 \equiv 1 - 4db^2 \mod 4$ donc $4db^2 \equiv 1 \mod 4$ et $4db^2 \in \mathbb{Z}$.

$4db^2 = d(2b)^2 \in \mathbb{Z}$ et le raisonnement précédent assure $2b \in \mathbb{Z}$.
Si $2b \in 2\mathbb{Z}$, alors $(2b)^2 d \equiv 0 \mod 4$. Or $(2b)^2 d \equiv 1 \mod 4$ donc on a une contradiction.
Donc $2b$ est impair et $b - \frac{1}{2} \in \mathbb{Z}$.
On a donc $4b^2 \equiv 1 \mod 4$ donc, comme $4db^2 \equiv 1 \mod 4$, $d \equiv 1 \mod 4$.

Réciproquement, $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ car $\sqrt{d}$ est un entier algébrique.

Si $d \equiv 1 \mod 4$, et si $u, v \in \mathbb{Z}^2$, $u + v\frac{1+\sqrt{d}}{2}$ est un entier algébrique car $\frac{1+\sqrt{d}}{2}$ est racine de $X^2 - X + \frac{1-d}{4} \in \mathbb{Z}[X]$.

Conclusion :
- Si $d \equiv 2, 3 \mod 4$, $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \mathbb{Z}[\sqrt{d}]$.
- Si $d \equiv 1 \mod 4$, $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \{a + b\sqrt{d}, (a,b) \in \mathbb{Z}^2$ ou $(a,b) \in (\frac{1}{2} + \mathbb{Z})^2\} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$

Exemple 4.1
- $\mathcal{O}_{\mathbb{Q}[\sqrt{-1}]} = \mathbb{Z}[\sqrt{-1}]$ (anneau des entiers de Gauss)
- $\mathcal{O}_{\mathbb{Q}[\sqrt{-5}]} = \mathbb{Z}[\sqrt{-5}]$
- $\mathcal{O}_{\mathbb{Q}[\sqrt{5}]} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$
- $\mathcal{O}_{\mathbb{Q}[\sqrt{-7}]} = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$
- $\mathcal{O}_{\mathbb{Q}[\sqrt{6}]} = \mathbb{Z}[\sqrt{6}]$

4.2 Unités de $\mathcal{O}_{\mathbb{Q}[\sqrt{N}]}$

Si $a + b\sqrt{N} \in \mathcal{O}^\times_{\mathbb{Q}[\sqrt{N}]}$, alors il existe $a' + b'\sqrt{N} \in \mathcal{O}_{\mathbb{Q}[\sqrt{N}]}$ tel que $(a + b\sqrt{N})(a' + b'\sqrt{N}) = 1$.

En prenant la norme, on obtient $(a^2 - Nb^2)(a'^2 - Nb'^2) = 1$ donc $a^2 - Nb^2 \in \mathbb{Z}^\times = \{-1, 1\}$.
- Si $N > 0$, $a^2 - Nb^2 \in \{\pm 1\}$ et on étudiera ça plus tard.
- Si $N < 0$, $a^2 - Nb^2 \geqslant 0$ donc $a^2 - Nb^2 = 1$.
  Donc $a^2 = 1 + Nb^2 \leqslant 1$ et de même $b^2 \leqslant -\frac{1}{N}$.
  - ▶ Si $N = -1$, $a \in \{-1, 0, 1\}$ et $b \in \{1, -1\}$ donc on a $\mathcal{O}^\times_{\mathbb{Q}[\sqrt{N}]} = \{\pm 1, \pm\sqrt{-1}\}$.
  - ▶ Si $N \equiv 2, 3 \mod 4$ et $N \neq -1$, alors $a, b \in \mathbb{Z}^2$ donc $a \in \{-1, 0, 1\}$ et $b = 0$ donc $\mathcal{O}^\times_{\mathbb{Q}[\sqrt{N}]} = \{1, -1\}$.
  - ▶ Si $N \equiv 1 \mod 4$, on a aussi $a^2 \leqslant 1$ et $b^2 \leqslant -\frac{1}{N}$ et $(a, b) \in \mathbb{Z}$ ou $(a, b) \in \frac{1}{2} + \mathbb{Z}$.

 Tous droits réservés

– Si $N \leqslant -5$ alors $b^2 \leqslant \frac{1}{5} < \frac{1}{4}$ donc $b^2 = 0$ et $b = 0$. Et $a^2 = 1$ donc $a = \pm 1$.
Donc $\mathcal{O}^\times_{\mathbb{Q}[\sqrt{N}]} = \{-1, 1\}$.
– Si $N = -3$ alors $b^2 \leqslant \frac{1}{3}$ donc $b \in \{-\frac{1}{2}, 0, \frac{1}{2}\}$.
Or $a^2 + 3b^2 = 1$ donc si $b = 0$, $a = \pm 1$, si $b = \pm\frac{1}{2}$, $a^2 = \frac{1}{4}$ donc $a = \pm\frac{1}{2}$.
Donc $\mathcal{O}^\times_{\mathbb{Q}[\sqrt{N}]} \subset \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\}$.
Or il sont inversibles donc $\mathcal{O}^\times_{\mathbb{Q}[\sqrt{N}]} = \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\}$.

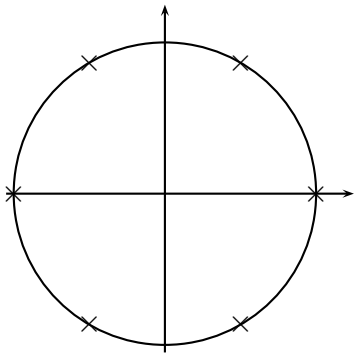

FIGURE 4.1 – Unités de $\mathbb{Q}[\sqrt{-3}]$

4.3 Factorialité, euclidianité de $\mathcal{O}_{\mathbb{Q}[\sqrt{N}]}$

S'il est euclidien, il est principal donc factoriel.

Proposition 4.2 (Admise) Si $N > 0$, $\mathcal{O}_{\mathbb{Q}[\sqrt{N}]}$ est euclidien pour le stathme défini par la norme $a + b\sqrt{N} \mapsto a^2 + Nb^2$ ssi

$$N \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 55, 73\}$$

Proposition 4.3 Si $N < 0$ alors $\mathcal{O}_{\mathbb{Q}[\sqrt{N}]}$ est euclidien ssi

$$N \in \{-1, -2, -3, -7, -11\}$$

Démonstration.

- Si $N \equiv 2, 3 \mod 4$, $\mathcal{O}_{\mathbb{Q}[\sqrt{N}]} = \mathbb{Z}[\sqrt{N}]$. Est-il euclidien ?
On considère $(a, b) \in \mathbb{Z}[\sqrt{N}]$ avec $b \neq 0$.
On cherche $q, r \in \mathbb{Z}[\sqrt{N}]$ tel que $a = bq + r$ et $\|r\| < \|b\|$.
On fixe un plongement de $\mathbb{Q}[\sqrt{N}]$ dans $\mathbb{C}$ et on identifie $\mathbb{Q}[\sqrt{N}]$ à l'image de ce prolongement.

 Tous droits réservés

Il existe $q \in \mathbb{Z}[\sqrt{N}]$ tel que $a = bq + r$ avec $\|r\| \leqslant \|b\|$ ssi il existe $q \in \mathbb{Z}[\sqrt{N}]$ tel que $|\frac{a}{b} - q|^2 < 1$.
On cherche la plus grande distance possible d'un point de $\mathbb{C}$ au réseau $\mathbb{Z}[\sqrt{N}]$. Par translation, on est ramené au cas d'un rectangle de côtés de longueur 1 et $\sqrt{-N}$.
La plus grande distance est donc $\frac{\sqrt{1-N}}{2}$.
Icelle est plus petite que 1 ssi $N > -3$.
Donc $\mathbb{Z}[\sqrt{N}]$ est donc euclidien pour la norme si $N \in \{-1, -2\}$.

- Si $N \equiv 1 \mod 4$, on peut procéder de la même façon avec le réseau $\mathbb{Z}[\frac{1+\sqrt{N}}{2}] = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{N}}{2}$.
  On est donc ramené au parallélogramme engendré par les vecteurs d'affixe 1 et $\frac{1+i\sqrt{-N}}{2}$.
  C'est un losange donc on est ramené au cas du triangle de sommets 0, $\frac{1}{2}$ et $\frac{1+i\sqrt{N}}{2}$.
  Cette distance est $\sqrt{\frac{2-N}{16} - \frac{1}{16N}}$.
  Elle est strictement inférieure à 1 ssi $N \geqslant -13$ donc $-N \in \{3, 7, 11\}$.
- Il reste à montrer qu'aucun autre N rend $\mathcal{O}_{\mathbb{Q}[\sqrt{N}]}$ euclidien pour n'importe quel stathme.
  - ▶ Si $N = -5$, $6 = 2 \times 3 = (1 + \sqrt{5})(1 - \sqrt{-5})$ et $2, 3, 1 \pm \sqrt{5}$ sont irréductibles.
  - ▶ Si $N = -6$, $6 = 2 \times 3 = \sqrt{-6}\sqrt{6}$ qui sont irréductibles.
  - ▶ Si $N = -10$, $14 = 2 \times 7 = (2 + \sqrt{10})(2 - \sqrt{10})$ qui sont irréductibles.
  - ▶ Sinon,

    Lemme 4.0.1
    Si A est un anneau euclidien, il existe x non inversible et non nul tel que la projection de $A \to A/\langle x \rangle$ induise une surjection de $A^\times \cup \{0\}$ sur $A/\langle x \rangle$.

    Démonstration. Soit ν le stathme et x non inversible et non nul tel que $\nu(x)$ soit minimal.
    Si $a \in A$, par division par x, il existe $q, r \in A$ tel que $a = qx + r$ et ($r = 0$ ou $\nu(r) < \nu(x)$).
    Si $r = 0$, $a \equiv 0 \mod x$. Sinon, comme $r \in A^* \cup \{0\}$, r est inversible a est congru à un inversible modulo x.
    D'où la surjection annoncée. ■

    Si $N < -3$ alors $\mathcal{O}^\times_{\mathbb{Q}[\sqrt{N}]} = \{\pm 1\}$ donc $\mathrm{Card}(A^* \cup \{0\}) = 3$ si $A = \mathcal{O}_{\mathbb{Q}[\sqrt{N}]}$.
    Si A est euclidien, alors il existe $x \in A \backslash (A^* \cup \{0\})$ tel que la projection $A \to A/\langle x \rangle$ soit surjective.
    On a donc $\mathrm{Card}(A/\langle x \rangle) \leqslant 3$. Or A est un réseau de $\mathbb{C}$ et $\langle x \rangle$ est un

 Tous droits réservés

sous-réseau de $\mathbb{C}$.
D'où $\text{Card}(A/\langle x\rangle) = \frac{\text{Vol}(\langle x\rangle)}{\text{Vol}(A)} = \det(y \mapsto xy) = \|x\|$.
Donc $a^2 - Nb^2 = \|x\| \leqslant 3$ et $(a,b) \in \mathbb{Z}$ ou $(a,b) \in \frac{1}{2} + \mathbb{Z}$.
Si $N < -12$, $b^2 = 0$ et $a^2 \leqslant 3$ donc $b = 0$ et $a^2 \leqslant -3$. $b \notin \frac{1}{2} + \mathbb{Z}$ donc a non plus et $a \in \mathbb{Z}$ donc $a \in \{0, 1, -1\}$.
Donc $x \in A^\times \cup \{0\}$ ce qui est une contradiction. ■

Application : Résoudre $y^2 + 4 = z^3$.

On se place dans l'anneau $\mathbb{Z}[i]$ qui est euclidien donc principal donc factoriel.

L'équation s'écrit $(y + 2i)(y - 2i) = z^3$. Si $y + 2i$ et $y - 2i$ sont premiers entre eux, ce sont des cubes. [1]

- Si y est impair, $(2 + iy)(2 - iy) = z^3$.
  - ▶ Si $a+ib$ est un diviseur commun de $2+iy$ et de $2-iy$, on a $a+ib \mid 4$ et $a + ib \mid 2iy$. En passant à la norme, $a^2 + b^2 \mid 16$ et $a^2 + b^2 \mid 4y^2$.
    Donc, comme y et 2 sont premiers entre eux, $a^2 + b^2$ (qui est une puissance de 2 car divise 16) vaut donc 1, 2 ou 4.
    On a $a+ib \mid 2+iy$ donc $a^2+b^2 \mid 4+y^2$ qui est impair donc $a^2+b^2 = 1$ donc $a + ib$ est inversible.
    Donc $2 + iy$ et $2 - iy$ sont premiers entre eux donc sont des cubes.
  - ▶ On est donc ramenés à résoudre $2 + iy = (c + id)^3$.
    On a $2 = c^3 - 3cd = c(c^2 - 3d)$ et $y = 3c^2d - d^3$
    Donc $c \mid 2$ donc $c = \pm 1$ ou $c = \pm 2$. D'où $3d^2 = c^2 - \frac{2}{c}$.
    Or pour $c = -2$ et $c = 1$, on obtient $3d^2 \not\equiv 0 \mod 3$ donc $c = 2$ ou $c = -1$. Dans ces cas, $d = \pm 1$.
  - ▶ Supposons $c = -1$. $2 + iy = (c + id)^3 = (-1 \pm i)^3 = 2 \pm 2i$ donc $y = \pm 2$ or y est supposé impair.
  - ▶ Supposons $c = 2$, on a alors $y = \pm 11$ et $y^2 + 4 = 125 = 5^3$ donc $(11, 5)$ est solution.
- ▶ Si $y = 2Y$, $(2Y)^2 + 4 = z^3$ donc $2 \mid z$ donc $z = 2Z$ et l'équation devient $Y^2 + 1 = 2Z^3$. (On peut constater que Y doit être impair)
  On a donc $(Y + i)(Y - i) = 2Z^3$. Soit $a + ib$ un diviseur commun à $Y + i$ et $Y - i$.
  On a $a + ib \mid Y + i$ donc $a^2 + b^2 \mid Y^2 + 1$.
  Or Y est impair donc $Y^2 \equiv 1 \mod 4$ donc $Y^2 + 1 \equiv 2 \mod 4$ et 4 ne divise pas $Y^2 + 1$ donc $a^2 + b^2 \neq 4$.
  Cependant, $a + ib \mid 2i$ donc $a^2 + b^2 \mid 4$ et $a^2 + b^2$ est une puissance de 2 donc vaut ± 1 ou ± 2.

1. En effet, ce sont des cubes multipliés par une unité et toutes les unités de $\mathbb{Z}[i]$ sont des cubes.

 Tous droits réservés

- ▶ Calculons $(Y+i) \wedge (Y-i)$.
  $a+ib \mid 2i$ et $2i = (1+i)^2$ avec $(1+i)$ de norme 2 qui est premier donc irréductible.
  Donc $a+ib = u$ ou $a+ib = u(1+i)$ avec u inversible. Or $1+i \mid Y+i$ car $Y+i = (1+i)(\frac{Y+1}{2} + \frac{1-Y}{2}i)$ et de même $1+i \mid Y-i$ donc $(Y+i) \wedge (Y-i) = 1+i$ (à unité près).
- ▶ On peut donc écrire $1+iY = u(1+i)^{\alpha_0} p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ et $1-iY = v(1+i)^{\beta_0} q_1^{\beta_1} \cdots q_s^{\beta_s}$.
  En remplaçant dans l'équation, on a $(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s)$ sont multiples de 3.
  De plus, $2Z^3 = (-i)(1+i)^2 Z^3$ donc $\alpha_0 + \beta_0 = v_{1+i}((1+iY)(1-iY)) = 2 + 3v_{1+i}(Z) \equiv 2 \mod 3$.
  Or $1-iY = \overline{u}(1-i)^{\alpha_0} \overline{p_1}^{\alpha_1} \cdots \overline{p_r}^{\alpha_r} = \overline{u'}(1+i)^{\alpha_0} \overline{p_1}^{\alpha_1} \cdots \overline{p_r}^{\alpha_r}$ donc $\beta_0 \geqslant \alpha_0$.
  De même, $\beta_0 \leqslant \alpha_0$ donc $\beta_0 = \alpha_0 = \min(\alpha_0, \beta_0) = 1$.
- ▶ On a donc $1+iY = (1+i)(c+id)^3$ donc $1 = (c+d)(c^2 - 4cd + d^2)$ donc $c+d = \pm 1$ et $c^2 - 4cd + d^2 = c+d$.
  Donc $c = \pm 1$ et $d = 0$ ou $c = 0$ et $d = \pm 1$. On obtient donc les solutions $y = \pm 2$ et $z = 2$.

Finalement, en testant les solutions potentielles, on trouve que les solutions de $y^2 + 4 = z^3$ sont $(\pm 11, 5)$ et $(\pm 2, 2)$.

Remarque 4.1

- *On peut donc redémontrer le théorème des deux carrés par un raisonnement sur la factorisation de l'entier p dans $\mathbb{Z}[i]$.*
  On a $\mathbb{Z}[i]/\langle p \rangle \simeq \mathbb{Z}[X]/\langle p, X^2+1 \rangle \simeq \mathbb{F}_p[X]/\langle X^2+1 \rangle$ donc le premier est intègre ssi le dernier l'est ssi X^2+1 est irréductible dans $\mathbb{F}_p[X]$.
- *Un entier $n > 0$ est somme de deux entiers ssi ($\forall p \mid n$ premier, $p \equiv 1 \mod 4$ ou $p \equiv 2 \mod 4$ ou $v_p(n)$ est pair).*
  Si $n = a^2 + b^2$, on a $n = N(a+ib)$ et on factorise $a+ib$ dans $\mathbb{Z}[i]$.

 Tous droits réservés

Chapitre 5

Bases d'entiers

5.1 Description de $\mathcal{O}_K$

THÉORÈME 5.1 *Si K est un corps de nombres, $\mathcal{O}_K$ est un $\mathbb{Z}$-module libre de rang $[K : \mathbb{Q}]$.*

Démonstration. On prend $(\omega_1, \ldots, \omega_n)$ une base du $\mathbb{Q}$-espace vectoriel K formée d'éléments de $\mathcal{O}_K$ telle que son discriminant soit minimal en valeur absolue (c'est possible car celui-ci est non nul).

Montrons que $(\omega_1, \ldots, \omega_n)$ est une $\mathbb{Z}$-base du $\mathbb{Z}$-module $\mathcal{O}_K$. Supposons qu'il existe $\omega \in \mathcal{O}_K \setminus \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$.

$(\omega_1, \ldots, \omega_n)$ est une $\mathbb{Q}$-base de K donc $\omega = \sum_{i=1}^{n} \lambda_i \omega_i$ avec un $\lambda_i \notin \mathbb{Z}$.

Quitte à soustraire de ω un élément de $\mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$, on peut supposer $0 \leqslant \lambda_i < 1$.

Quitte à permuter les ω_i, on peut supposer $\lambda_1 \notin \mathbb{Z}$ ie $0 < \lambda_1 < 1$.

La famille $(\omega, \omega_2, \ldots, \omega_n)$ est une $\mathbb{Q}$-base de K formée d'éléments de $\mathcal{O}_K$.

La matrice de passage est :

$$\begin{pmatrix} \lambda_1 & 0 & \cdots & \cdots & 0 \\ \vdots & 1 & \ddots & \ddots & \vdots \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 & 0 \\ \lambda_n & 0 & \cdots & 0 & 1 \end{pmatrix}$$

Le discriminant de $(\omega, \omega_2, \ldots, \omega_n)$ est :

$$\begin{vmatrix} \sigma_1(\omega) & \sigma_1(\omega_2) & \cdots & \sigma_1(\omega_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\omega) & \sigma_n(\omega_2) & \cdots & \sigma_n(\omega_n) \end{vmatrix} = \lambda_1^2 \operatorname{disc}(\omega_1, \ldots, \omega_n)$$

On a donc $|\operatorname{disc}(\omega, \omega_2, \dots, \omega_n)| < |\operatorname{disc}(\omega_1, \dots, \omega_n)|$, ce qui contredit la minimalité de $|\operatorname{disc}(\omega_1, \dots, \omega_n)|$.

Donc $\mathcal{O}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$. ∎

5.2 Calcul d'une base de $\mathcal{O}_K$

Proposition 5.1 Si $(\omega_1, \dots, \omega_n)$ est une $\mathbb{Q}$-base de K formée d'éléments de $\mathcal{O}_K$ mais qui n'est pas une $\mathbb{Z}$-base de $\mathcal{O}_K$, alors il existe p premier tel que :

- $p^2 \mid \operatorname{disc}(\omega_1, \dots, \omega_n)$.
- $\exists \lambda_1, \dots, \lambda_n \in [\![0, p-1]\!]^n$, $\frac{1}{p}\sum_{i=1}^{n} \lambda_i \omega_i \in \mathcal{O}_K \setminus \{0\}$.

Démonstration. $\mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_d$ est un sous-$\mathbb{Z}$-module du $\mathbb{Z}$-module de type fini $\mathcal{O}_K$ donc il existe k, $(e_1, \dots, e_n)$ une $\mathbb{Z}$-base de $\mathcal{O}_K$ et $(d_1, \dots, d_n) \in \mathbb{Z}$ tel que $d_1 \mid \cdots \mid d_n$ et $(d_1 e_1, \dots, d_k e_k)$ soit une base de $\mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$ et $d_{k+1}, \dots, d_n = 0$.

Le $\mathbb{Q}$-espace vectoriel engendré par $\mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$ est de dimension n (c'est K) et $(d_1 e_1, \dots, d_k e_k)$ en est une base donc $k = n$.

$$\operatorname{Card}(\mathcal{O}_K/(\mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n)) = \operatorname{Card}(\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_1\mathbb{Z}) = \left|\prod_{i=1}^{n} d_i\right| = r$$

De plus $\operatorname{disc}(\omega_1, \dots, \omega_n) = \operatorname{disc}(d_1 e_1, \dots, d_n e_n)$ car la matrice de passage est de déterminant ± 1.

Donc $\operatorname{disc}(\omega_1, \dots, \omega_n) = r^2 \operatorname{disc}(e_1, \dots, e_n) \in \mathbb{Z}$ donc $\operatorname{Card}(\mathcal{O}_K/(\mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n))^2 \mid \operatorname{disc}(\omega_1, \dots, \omega_n)$.

On prend p premier qui divise $\operatorname{Card}(\mathcal{O}_K/(\mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n))$.

Soit $x \in \mathcal{O}_K$ d'ordre p dans $\mathcal{O}_K/(\mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n)$.

$px \in \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$ donc $x = \frac{1}{p}\sum_{i=1}^{n} \lambda_i \omega_i$ avec $(\lambda_1, \dots, \lambda_n) \in \mathbb{Z}^n$.

Quitte à enlever de x un élément de $\mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$, on peut supposer $0 \leqslant \frac{\lambda_i}{p} < 1$ ie $0 \leqslant \lambda_i < p$. ∎

Corollaire 5.1 *Si $(\omega_1, \dots, \omega_n)$ est une $\mathbb{Q}$-base de K formée d'éléments de $\mathcal{O}_K$ et si $\operatorname{disc}(\omega_1, \dots, \omega_n)$ est sans facteurs carrés, $\omega_1, \dots, \omega_n$ est une $\mathbb{Z}$-base de $\mathcal{O}_K$.*

Démonstration. Il n'y a pas de p premier tel que $p^2 \mid \operatorname{disc}(\omega_1, \dots, \omega_n)$. ∎

 Tous droits réservés

Exemple : Calcul de $\mathcal{O}_{\mathbb{Q}[\sqrt[3]{5}]}$.
$(1, \sqrt[3]{5}, \sqrt[3]{25})$ est une base de $\mathbb{Q}[\sqrt[3]{5}]$. On a :

$$\operatorname{disc}(1, \sqrt[3]{5}, \sqrt[3]{25}) = \begin{vmatrix} \operatorname{tr}(1) & \operatorname{tr}(\sqrt[3]{5}) & \operatorname{tr}(\sqrt[3]{25}) \\ \operatorname{tr}(\sqrt[3]{5}) & \operatorname{tr}(\sqrt[3]{25}) & \operatorname{tr}(5) \\ \operatorname{tr}(\sqrt[3]{25}) & \operatorname{tr}(5) & \operatorname{tr}(5\sqrt[3]{5}) \end{vmatrix} = \begin{vmatrix} 3 & 0 & 0 \\ 0 & 0 & 15 \\ 0 & 15 & 0 \end{vmatrix} = -3^3 \times 5^2$$

car $\operatorname{tr}(1) = 3$, $\operatorname{tr}(\sqrt[3]{5}) = 0$ (car de polynôme caractéristique X^3-5), $\operatorname{tr}(\sqrt[3]{25}) = 0$ (polynôme caractéristique $X^3 - 25$), $\operatorname{tr}(5) = 5\operatorname{tr}(1) = 15$ et $\operatorname{tr}(5\sqrt[3]{5}) = 5\operatorname{tr}(\sqrt[3]{5}) = 0$.

Dans la proposition, on a donc $p = 3$ ou $p = 5$.

- Si $p = 3$, on aurait un entier de la forme $x = \frac{\lambda_1+\lambda_2\sqrt[3]{5}+\lambda_3\sqrt[3]{25}}{3}$ avec $\lambda_i \in \{-1, 0, 1\}$ non tous nuls.
  - ▶ $\operatorname{tr}(x^2) = \frac{\lambda_1^2+10\lambda_2\lambda_3}{3} \in \mathbb{Z}$ donc $\lambda_1^2 + \lambda_2\lambda_3 \equiv 0 \mod 3$.
    En calculant $\operatorname{tr}(x^2\sqrt[3]{5})$ et $\operatorname{tr}(x^2\sqrt[3]{25})$, on trouve $-\lambda_2^2 + \lambda_1\lambda_3 \equiv 0 \mod 3$ et $\lambda_3^2 + \lambda_1\lambda_2 \equiv 0 \mod 3$.
  - ▶ Si $\lambda_1 \equiv 0 \mod 3$, alors $\lambda_2^2 \equiv 0 \mod 3$ donc $\lambda_2 \equiv 0 \mod 3$ et donc $\lambda_3 \equiv 0 \mod 3$ donc, comme $\lambda_i \in \{\pm 1, 0\}$, $\lambda_1 = \lambda_2 = \lambda_3 = 0$.
  - ▶ Si $\lambda_1 \equiv 1 \mod 3$, on a $\lambda_2 \equiv -1 \mod 3$ et $\lambda_3 \equiv 1 \mod 3$ donc $(\lambda_1, \lambda_2, \lambda_3) = (1, -1, 1)$.
  - ▶ Si $\lambda_1 \equiv -1 \mod 3$, on a $\lambda_2 \equiv 1 \mod 3$ et $\lambda_3 \equiv -1 \mod 3$ donc $(\lambda_1, \lambda_2, \lambda_3) = (-1, 1, -1)$.
  - ▶ On doit donc rechercher si $\frac{1-\sqrt[3]{5}+\sqrt[3]{25}}{3} \in \mathbb{Z}$ (l'autre cas revient à chercher si son opposé est entier).
    Si c'était un entier, son carré (valant $-1 + \frac{\sqrt[3]{5}+\sqrt[3]{25}}{3}$) le resterait donc $\frac{\sqrt[3]{5}+\sqrt[3]{25}}{3}$ aussi.
    Or la norme de ce nombre vaut $\frac{1}{3^3}N(\sqrt[3]{5})N(1+\sqrt[3]{5})$.
    Le polynôme caractéristique de $\sqrt[3]{5}$ est X^3-5 et celui de $\sqrt[3]{5}+1$ est $(X-1)^3-5 = X^3-3X^2+3X-6$.
    Donc cette norme vaut $\frac{10}{9} \notin \mathbb{Z}$. D'où la contradiction.
- Si $p = 5$, $x = \frac{\lambda_1+\lambda_2\sqrt[3]{5}+\lambda_3\sqrt[3]{25}}{5} \in \mathbb{Z}$ avec $\lambda_i \in [\![0, 4]\!]$.
  $\operatorname{tr}(x) = \frac{3\lambda_1}{5}$ donc $\lambda_1 = 0$.
  Donc $N(x) = \frac{5\lambda_2^3+25\lambda_3^3}{5^3} = \frac{\lambda_2^3+5\lambda_3^3}{5^2} \in \mathbb{Z}$.
  - ▶ Si $5 \mid \lambda_2$ alors $25 \mid 5\lambda_3^3$ donc $\lambda_2 = \lambda_3 = 0$.
  - ▶ Sinon, $\lambda_2 \in (\mathbb{Z}/25\mathbb{Z})^\times$ donc -5 est un carré dans $\mathbb{Z}/25\mathbb{Z}$, ce qui est faux.

Donc $(1, \sqrt[3]{5}, \sqrt[3]{25})$ est une base de $\mathcal{O}_{\mathbb{Q}[\sqrt[3]{5}]}$. Donc $\mathcal{O}_{\mathbb{Q}[\sqrt[3]{5}]} = \mathbb{Z}[\sqrt[3]{5}]$.

 Tous droits réservés

 Tous droits réservés

Chapitre 6

Unités de l'anneau des entiers d'un corps quadratique réel, équation de Pell-Fermat

Définition 6.1 Une équation de Pell-Fermat est une équation du type $x^2 - dy^2 = \pm 1$ avec $d > 0$ fixé d'inconnues entières x et y.

Résoudre cette équation revient à chercher les unités de $\mathbb{Z}[\sqrt{d}]$.

6.1 $x^2 - dy^2 = 1$

Lemme 6.0.1
Soit $\alpha \in \mathbb{R} \setminus \mathbb{Q}$.

Pour tout $n \in \mathbb{N}^*$, il est p, q entiers premiers entre eux tels que $q > 0$ et $\left|\alpha - \frac{p}{q}\right| < \frac{1}{nq}$.

De plus, on peut supposer $q \leqslant n$.

Démonstration. On a $[0,1[= \bigcup_{k=0}^{n-1} \left[\frac{k}{n}, \frac{k+1}{n}\right[$.

$r\alpha - \lfloor r\alpha \rfloor \in [0,1[$ pour tout $r \in [\![0, n]\!]$.

Par principe des tiroirs, il existe $r_0, r_1 \in [\![0, n]\!]$ distincts tels que $(r_0\alpha - \lfloor r_0\alpha \rfloor, r_1\alpha - \lfloor r_1\alpha \rfloor) \in [\frac{k}{n}, \frac{k+1}{n}[$ pour un certain k.

On a donc $|(r_0 - r_1)\alpha - (\lfloor r_0\alpha \rfloor - \lfloor r_1\alpha \rfloor)| < \frac{1}{n}$.

Or $|r_0 - r_1| \geqslant 1 > 0$ donc $|\alpha - \frac{\lfloor r_0\alpha \rfloor - \lfloor r_1\alpha \rfloor}{r_0 - r_1}| < \frac{1}{n|r_0 - r_1|}$.

On pose $p' = (\lfloor r_0\alpha \rfloor - \lfloor r_1\alpha \rfloor) \operatorname{Sgn}(r_0 - r_1)$ et $q' = |r_0 - r_1| \leqslant n$ et $p = \frac{p'}{p' \wedge q'}$, $q = \frac{q'}{p' \wedge q'}$ conviennent. ∎

Théorème 6.1 Dirichlet *Soit $\alpha \in \mathbb{R} \setminus \mathbb{Q}$.*

Il existe une infinité de couples $(p,q) \in \mathbb{N}$ *premiers entre eux avec* $q > 0$ *tels que* $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$.

Démonstration. D'après le lemme précédent, il existe p_0, q_0 tels que $|\alpha - \frac{p_0}{q_0}| < \frac{1}{n_0 q_0} \leqslant \frac{1}{q_0^2}$.

$\alpha \notin \mathbb{Q}$ donc $|\alpha - \frac{p_0}{q_0}| > 0$ donc il existe $n_1 \in \mathbb{N}^*$ tel que $|\alpha - \frac{p_0}{q_0}| > \frac{1}{n_1}$.

Par le lemme, on a p_1 et q_1 tels que $|\alpha - \frac{p_1}{q_1}| < \frac{1}{n_1 q_1} \leqslant \frac{1}{q_1^2}$.

On a :

$$\frac{1}{n_0 q_0} > \left|\alpha - \frac{p_0}{q_0}\right| > \frac{1}{n_1} \geqslant \frac{1}{n_1 q_1} > \left|\alpha - \frac{p_1}{q_1}\right| > \frac{1}{n_2} \geqslant \cdots$$

$(n_i)_i$ est strictement croissante donc $\lim\limits_{i\to+\infty} n_i = +\infty$ donc $\lim\limits_{i\to+\infty} \alpha - \frac{p_i}{q_i} = 0$.

Donc $\{q_i, i \in \mathbb{N}\}$ n'est pas majoré donc, quitte à extraire une sous-suite, $(q_i)_i$ est strictement croissante. ∎

Remarque 6.1 *Les* $\frac{p_i}{q_i}$ *sont deux à deux distincts.*

Proposition 6.1 Soit $d \in \mathbb{N}^*$ sans facteur carré.

L'équation $x^2 - dy^2 = 1$ admet une solution avec $y \neq 0$.

Démonstration.

- Il existe une infinité de $\frac{p}{q} \in \mathbb{Q}$ tel que $|\sqrt{d} - \frac{p}{q}| < \frac{1}{q^2}$.
  Pour ces p, q, on a donc $|p - q\sqrt{d}| < \frac{1}{q}$ donc :

$$|p^2 - dq^2| < \frac{|p + q\sqrt{d}|}{q} < \frac{|p - q\sqrt{d}| + 2q\sqrt{d}}{q} < \frac{1}{q^2} + 2\sqrt{d} < 1 + 2\sqrt{d}$$

- Il existe donc $c \in \mathbb{Z}$ tel que $|c| < 1 + 2\sqrt{d}$ et qu'il y ait une infinité de $\frac{p}{q} \in \mathbb{Q}$ vérifiant $|\sqrt{d} - \frac{p}{q}| < \frac{1}{q^2}$ et $p^2 - dq^2 = c$.
  d n'est pas un carré donc $c \neq 0$.
- $\mathbb{Z}/|c|\mathbb{Z}$ est fini donc il existe donc $\overline{p}$, $\overline{q}$ tels qu'il y ait une infinité de $\frac{a}{b} \in \mathbb{Q}$ tels que $|\sqrt{d} - \frac{a}{b}| < \frac{1}{b^2}$, $a^2 - db^2 = c$, et $a \in \overline{p}$, $b \in \overline{q}$.
  On prend $\frac{p_0}{q_0}$ et $\frac{p_1}{q_1}$ comme ceci.
  On a $(p_0 + q_0\sqrt{d})(p_1 - q_1\sqrt{d}) = (p_0p_1 - dq_0q_1) + (p_1q_0 - p_0q_1)\sqrt{d}$.
  Or $\overline{p_0p_1 - dq_0q_1} = \overline{p^2} - d\overline{q}^2 = \overline{c} = 0$ et $\overline{p_1q_0 - p_0q_1} = \overline{pq} - \overline{pq} = 0$.
- Posons $u = \underbrace{\frac{(p_0p_1 - dq_0q_1)}{c}}_{u_1} + \underbrace{\frac{(p_1q_0 - p_0q_1)\sqrt{d}}{c}}_{u_2} \in \mathbb{Z}[\sqrt{d}]$.
  On a de plus $\|u\| = \frac{\left\|p_0 + q_0\sqrt{d}\right\| \times \left\|p_1 - q_1\sqrt{d}\right\|}{\|c\|} = 1$.
  On a donc $u_0^2 - du_1^2 = 1$ et $u_1 \neq 0$ car sinon $p_0q_1 = p_1q_0$ et $\frac{p_1}{q_1} = \frac{p_0}{q_0}$. ∎

 Tous droits réservés

Corollaire 6.1 *Soit $d \in \mathbb{N}^*$ sans facteur carré.*
L'équation $x^2 - dy^2 = 1$ admet une solution dans $\mathbb{N} \times \mathbb{N}^*$.

Théorème 6.2 *$G = (\{x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}], x^2 - dy^2 = 1\}, \times)$ est un groupe isomorphe à $(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$.*

Démonstration.

- Les éléments de G sont les éléments de norme 1 de $\mathbb{Z}[\sqrt{d}]^\times$ donc c'est le noyau de $\|\cdot\| : \mathbb{Z}[\sqrt{d}]^\times \to \{\pm 1\}$.
  Donc G est un groupe.
- Montrons que $G \cap \mathbb{R}_+^* \simeq \mathbb{Z}$.
  - ▶ On a $1 \in G \cap [1, +\infty[$ donc $G \cap [1, +\infty[\neq \varnothing$.
    Si $x+y\sqrt{d} \in G \cap [1, +\infty[$, $x^2 - dy^2 = 1$ donc $x - y\sqrt{d} = \frac{1}{x+y\sqrt{d}} \in]0, 1]$.
    Donc
    $$\begin{cases} x &= \frac{(x+y\sqrt{d})+(x-y\sqrt{d})}{2} \in]\frac{1}{2}, +\infty[\\ y &= \frac{(x+y\sqrt{d})-(x-y\sqrt{d})}{2\sqrt{d}} \in [0, +\infty[\end{cases}$$
    Donc $x \in \mathbb{N}^*$ et $y \in \mathbb{N}$.
  - ▶ De plus, si $x + y\sqrt{d} \leqslant M$ alors $x - y\sqrt{d} \in [\frac{1}{M}, 1]$ donc $x \in [\frac{1}{2} + \frac{1}{2M}, \frac{M+1}{2}] \cap \mathbb{Z}$ et $y \in [0, \frac{1}{2\sqrt{d}}(M - \frac{1}{M})] \cap \mathbb{Z}$.
    Donc $G \cap [1, M]$ est fini pour tout $M \geqslant 1$.
  - ▶ $G \cap]1, +\infty[$ admet un plus petit élément $x_0 + y_0\sqrt{d} > 1$ (non vide par le corollaire).
    Soit $x + y\sqrt{d} \in G \cap [1, +\infty[$, il existe n maximum tel que $(x_0 + y_0\sqrt{d})^n \leqslant x + y\sqrt{d}$.
    $u = \frac{x+y\sqrt{d}}{(x_0+y_0\sqrt{d})^n} \in G \cap [1, +\infty[$. Or, par minimalité de n, $u < x_0 + y_0\sqrt{d}$.
    Par minimalité de $x_0 + y_0\sqrt{d}$, $u = 1$.
  - ▶ Si $x + y\sqrt{d} \in G \cap]0, 1]$, alors $\frac{1}{x+y\sqrt{d}} = x - y\sqrt{d} \in G \cap [1, +\infty[$ donc il existe $n \in \mathbb{N}$, $x + y\sqrt{d} = (x_0 + y_0\sqrt{d})^{-n}$.
    On a donc un isomorphisme entre $\mathbb{Z}$ et $G \cap \mathbb{R}_+^*$ $(n \mapsto (x_0 + y_0\sqrt{d})^n)$.
- G est isomorphe à $\{\pm 1\} \times (G \cap \mathbb{R}_+^*)$ par $x \mapsto (\mathrm{Sgn}(x), |x|)$ et $\{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$ et $G \cap \mathbb{R}_+^* \simeq \mathbb{Z}$. ∎

En fait, on peut considérer l'isomorphisme

$$\varphi : \begin{cases} \mathbb{Z}/n\mathbb{Z} \times 2\mathbb{Z} & \to & G = \{z \in \mathbb{Z}[\sqrt{d}]^\times, N(z) = 1\} \\ (s, n) & \mapsto & (-1)^s g^n \end{cases}$$

avec $g = \min G \cap]1, +\infty[$.

L'équation $x^2 - dy^2 = N(z) = 1$ a pour solution les couples (x, y) tels que $x + y\sqrt{d} = \pm g^n$.

On peut aussi prendre pour g l'élément $g_0 = \min(\mathbb{Z}[\sqrt{d}]^\times \cap]1, +\infty[)$.

 Tous droits réservés

On a deux cas :
- Si $N(g_0) = 1$, pour tout $z \in \mathbb{Z}[\sqrt{d}]^\times$, $N(z) = 1$. Donc $x^2 - dy^2 = -1$ n'a pas de solutions.
- Si $N(g_0) = -1$, alors G est un sous-groupe d'indice 2 de $\mathbb{Z}[\sqrt{d}]$ correspondant à $\mathbb{Z}/2\mathbb{Z} \times 2\mathbb{Z}$ (ie $g = g_0^2$). $x^2 - dy^2 = -1$ a alors une infinité de solutions.

Dans le cas où on doit considérer $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]^\times$ ($d \equiv 1 \mod 4$), on a l'isomorphisme

$$\varphi : \begin{cases} \mathbb{Z}/n\mathbb{Z} \times 2\mathbb{Z} & \to & G = \{z \in \mathbb{Z}[\sqrt{d}]^\times, N(z) = 1\} \\ (s, n) & \mapsto & (-1)^s g_1^n \end{cases}$$

avec $g_1 = \min(\mathbb{Z}[\frac{1+\sqrt{d}}{2}]^* \cap]1, +\infty[)$, on appelle g_1 unité fondamentale.

Le but est de calculer une unité fondamentale pour pouvoir résoudre $x^2 - dy^2 = \pm 4$.

6.2 Fractions continues

6.2.1 Définition et premières propriétés

Définition 6.2 Une fraction continue est un objet de la forme :

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

avec $a_i > 0$ sauf éventuellement a_0.

Proposition 6.2 Posons $p_{-1} = 1$, $p_0 = a_0$ et $p_n = a_n p_{n-1} + p_{n-2}$. De même, $q_{-1} = 0$, $q_0 = 1$ et $q_n = a_n q_{n-1} + q_{n-2}$.

On a $\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \prod_{i=0}^{n} \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix}$.

On a alors :

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}} = \frac{p_n}{q_n}$$

 Tous droits réservés

Démonstration. Par récurrence sur n :

$a_0 = \frac{p_0}{q_0}$ donc H_0 est vraie. De même, H_1 est vraie.

Si H_n et H_{n-1} sont vraies, on remplace a_n par $a_n + \frac{1}{a_{n+1}}$.

p_n est remplacé par $p'_n = (a_n + \frac{1}{a_{n+1}})p_{n-1} + p_{n-2}$ et q_n par $q'_n = (a_n + \frac{1}{a_{n+1}})q_{n-1} + q_{n-2}$.

Donc :

$$\begin{aligned} a_0 + \cfrac{1}{\ddots + \frac{1}{a_{n+1}}} &= \frac{p'_n}{q'_n} \\ &= \frac{(a_n a_{n+1} + 1)p_{n-1} + a_{n+1}p_{n-2}}{(a_n a_{n+1} + 1)q_{n-1} + a_{n+1}q_{n-2}} \\ &= \frac{(a_n a_{n+1} + 1)p_{n-1} + a_{n+1}(p_n - a_n p_{n-1})}{(a_n a_{n+1} + 1)q_{n-1} + a_{n+1}(q_n - a_n q_{n-1})} \\ &= \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}} \\ &= \frac{p_{n+1}}{q_{n+1}} \end{aligned}$$

Donc H_{n+1} est vraie. ■

Proposition 6.3

- $(p_n)_n$ et $(q_n)_n$ sont croissantes car $a_i > 0$.
- $p_{n+1}q_n - p_n q_{n+1} = (-1)^n$.

Démonstration.

$$\begin{aligned} p_{n+1}q_n - p_n q_{n+1} &= \begin{vmatrix} p_{n+1} & p_n \\ q_{n+1} & q_n \end{vmatrix} \\ &= \prod_{i=0}^{n+1} \begin{vmatrix} a_i & 1 \\ 1 & 0 \end{vmatrix} \\ &= (-1)^n \end{aligned}$$

COROLLAIRE 6.2 *Pour tout n, p_n et q_n sont premiers entre eux.*

Proposition 6.4 $r_n = \frac{p_n}{q_n}$ est croissant en a_i si $i \equiv 0 \mod 2$ et décroissant sinon.

Démonstration. Décroissance de la fonction inverse. ■

Proposition 6.5 $(r_{2n})_n$ est strictement croissante et $(r_{2n+1})_n$ est strictement décroissante.

Proposition 6.6 $r_{n+1} - r_n = \frac{(-1)^n}{q_n q_{n+1}}$.

 Tous droits réservés

Démonstration.

$$\begin{aligned} r_{n+1} - r_n &= \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \\ &= \frac{p_{n+1}q_n - p_n q_{n+1}}{q_n q_{n+1}} \\ &= \frac{(-1)^n}{q_n q_{n+1}} \end{aligned}$$

■

Proposition 6.7 $(r_n)_n$ converge dans $\mathbb{R}$.

Démonstration. Si les a_i sont entiers alors les q_i aussi. Or (q_n) est croissante (strictement) donc sa limite est $+\infty$ et $\lim\limits_{n\to+\infty} |r_{n+1} - r_n| = 0$.

Donc $(r_{2n})_n$ et $(r_{2n+1})_n$ sont adjacentes donc r converge. ■

Réciproquement, si $x \in \mathbb{R}$, on lui associe un développement en fraction continue donné par : $x_0 = x$ et $x_{n+1} = \frac{1}{x_n - \lfloor x_n \rfloor}$ si $x_p \notin \mathbb{Z}$.

- Si la suite s'arrête, (ie il existe n tel que $x_n \in \mathbb{Z}$) alors $x \in \mathbb{Q}$.
- Sinon, on a $\lfloor x_n \rfloor \leqslant x_n < \lfloor x_n \rfloor + 1 < \infty$.
  Donc $r_{2n} < x < r_{2n+1}$ et x est bien égal au développement en fraction continue associé aux cœfficients x_i.

Remarque 6.2 *Si $x = \frac{p}{q} \in \mathbb{Q}$, on retrouve l'algorithme d'Euclide appliqué à (p, q).*

En particulier, comme tout algortihme qui se respecte, icelui termine donc le développement en fraction continue de $\frac{p}{q}$ est fini.

On a donc $x \in \mathbb{Q}$ ssi son développement en fraction continue est fini.

Proposition 6.8 x est un irrationnel quadratique ssi son développement en fraction continue est périodique à partir d'un certain rang.

Exemple 6.1 $x = \sqrt{2}$, $x_0 = \sqrt{2}$, $a_0 = \lfloor \sqrt{2} \rfloor = 1$.
$x_1 = \frac{1}{\sqrt{2}-1} = 1 + \sqrt{2}$ et $a_1 = 2$.
$x_2 = \frac{1}{\sqrt{2}+1-2} = \frac{1}{\sqrt{5}-1} = \sqrt{2} + 1$ donc $a_2 = 2$.
On a ainsi $a_i = 2$ pour $i \geqslant 1$.
Donc :

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}$$

Démonstration.

 Tous droits réservés

$\Leftarrow$ • Si le développement est périodique alors :

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n + \frac{1}{x}}}}$$

Donc $x = \frac{xp_n + p_{n-1}}{xq_n + q_{n-1}}$ donc $x^2 q_n + x q_{n-1} - x p_n - p_{n-1} = 0$.
$x \notin \mathbb{Q}$ car son développement en fraction continue est infini. Il est aussi quadratique.

- Si le développement en fraction continue de x est périodique à partir d'un certain rang i, alors on se ramène au cas précédent en posant y le réel donc le développement en fraction continue est $(a_n)_{n \geqslant i}$. y est donc un irrationnel quadratique donc, comme $\mathbb{Q}[y]$ est un corps, $x \in \mathbb{Q}[y]$. Or $x \notin \mathbb{Q}$ donc c'est gagné.

$\Rightarrow$ Si $x_0 = x$ est racine de $aX^2 + bX + c$ avec $a, b, c \in \mathbb{Z}$ et $a > 0$.
On peut supposer $a \wedge b \wedge c = 1$.
$x_0 - \lfloor x_0 \rfloor$ est racine de $aX^2 + \underbrace{(b + 2a\lfloor x_0 \rfloor)}_{b'} X + a'$ où a' est tel que $\Delta = b'^2 - 4aa' = b^2 - 4ac$.
$x_1 = \frac{1}{x_0 - \lfloor x_0 \rfloor}$ est racine de $a'X^2 + b'X + a$. On va conclure grâce à la partie suivante. ■

6.2.2 Réduction des formes quadratiques

Définition 6.3 On appelle forme (a, b, c) une forme quadratique de la forme $aX^2 + bX + c$ ou $aX^2 + bXY + cY^2$.

On dit que celle-ci est réduite ssi $0 < b < \sqrt{\Delta}$ et $\sqrt{\Delta} - b < 2|a| < \sqrt{\Delta} + b$ avec $\Delta = b^2 - 4ac$.

Remarque 6.3 *On a alors* $\frac{-b - \sqrt{\Delta}}{2|a|} < -1 < 0 < \frac{-b + \sqrt{\Delta}}{2|a|} < 1$.

Proposition 6.9 Si (a, b, c) est réduite, alors $\sqrt{\Delta} - b < 2|c| < \sqrt{\Delta} + b$.

Démonstration. $c = \frac{b^2 - \Delta}{4a}$ donc $2|c| = \frac{(\sqrt{\Delta} - b)(\sqrt{\Delta} + b)}{2|a|}$ et $\sqrt{\Delta} - b < 2|a| < \sqrt{\Delta} + b$. ■

Corollaire 6.3 *Il n'y a qu'un nombre fini de formes réduites à Δ fixé.*

On peut définir une application de réduction ρ.

Pour toute forme (a, b, c) il existe $\delta \in \mathbb{Z}$ tel que $\sqrt{\Delta} - 2|c| < -b + 2c\delta < \sqrt{\Delta}$ car $2|c| \geqslant 2$.

On a alors $\rho(a, b, c) = (c, 2c\delta - b, a - b\delta + c\delta^2) = (a', b', c')$. On a bien $b'^2 - 4a'c' = \Delta$.

D'où l'algorithme :

 Tous droits réservés

Algorithme 1: Réduction de formes quadratiques

Entrées : (a, b, c) non nécessairement réduite
Sorties : (a', b', c') réduite

```
tant que |a| > |c| faire
    Itérer ρ
```

Démonstration de l'algorithme. On sort bien de la boucle car quand on itère ρ, on fait décroitre strictement $|a|$.

Ensuite, on a $|a'| \leqslant |c'|$. Par définition de ρ, $\sqrt{\Delta} - 2|a'| < b' < \sqrt{\Delta}$.

Donc $0 < \sqrt{\Delta} - b' < 2|a'|$.

On a $\Delta = b'^2 - 4a'c'$ donc $|\sqrt{\Delta} + b'| = \frac{4|a'||c'|}{\sqrt{\Delta} - b'} > 2|c'|$.

Comme $|a'| \leqslant |c'|$, on a $|\sqrt{\Delta} + b'| > 2|c'| \geqslant 2|a'| > \sqrt{\Delta} - b'$.

Donc $\sqrt{\Delta} + |b'| \geqslant |\sqrt{\Delta} + b'| > \sqrt{\Delta} - b'$.

Donc $|b'| > -b'$ donc $b' > 0$. Donc $\sqrt{\Delta} + b' > 0$.

On a bien les conditions recherchées donc (a', b', c') est réduite. ∎

Définition 6.4 Si (a_0, b_0, c_0) et (a_1, b_1, c_1) sont deux formes réduites de discriminant Δ, on dit qu'elles sont adjacentes si $a_1 = c_0$ et $b_0 + b_1 \equiv 0 \mod 2a_1$.

On dit que (a_0, b_0, c_0) est adjacente à gauche à (a_1, b_1, c_1).

Proposition 6.10 Chaque forme réduite a une unique forme adjacente à droite et une unique forme adjacente à gauche.

Démonstration. Montrons le pour l'adjacence à droite.

On a déja $a_1 = c_0$ et $c_1 = \frac{b_1^2 - \Delta}{4a_1}$ fixés donc il faut montrer qu'il n'y a qu'un seul b_1 possible.

Or $b_1 \equiv -b_0 \mod 2a_1$. De plus, $\sqrt{\Delta} - b_1 < 2|a_1|$ donc $\sqrt{\Delta} - 2|a_1| < b_1$ et $0 < b_1 < \sqrt{\Delta}$.

Donc $\sqrt{\Delta} - 2|a_1| < b_1 < \sqrt{\Delta}$ qui est un intervalle de longueur $2|a_1|$ ce qui assure l'unicité de b_1. ∎

Proposition 6.11 Par définition de ρ, si (a, b, c) est réduite, $\rho(a, b, c)$ lui est adjacente à droite.

Dans l'ensemble des formes réduites, ρ décrit des cycles qui partitionnent l'ensemble des formes réduites.

 Tous droits réservés

6.2.3 Lien avec les fractions continues

On obtient le cœfficient suivant dans le développement en fraction continue en appliquant ρ à la forme quadratique correspondante.

Par l'application $(a,b,c) \mapsto (\tau, s) = (\frac{-b+\sqrt{\Delta}}{2|a|}, \mathrm{Sgn}(a))$, en applicant ρ, on tombe sur $(\frac{1}{\tau} - \lfloor \frac{1}{\tau} \rfloor, -1)$.

Le développement en fraction continue d'un irrationnel quadratique est donc périodique à partir d'un certain rang.

La période est égale à la longueur du cycle sur les formes quadratiques réduites ou à la moitié de cette longueur.

Cas du développement en fraction continue de $\sqrt{d}$:

On part de $(-d, 0, 1)$, $\Delta = 4d$.

$\rho(-d,0,1) = (1, 2\lfloor\sqrt{d}\rfloor, \lfloor\sqrt{d}\rfloor^2 - d)$ qui est réduite.

Le développement en fraction continue de $\sqrt{d}$ est donc de la forme

$$(a_0, a_1, \ldots, a_{r+1}, a_1, \ldots, a_{r+1}, \cdots)$$

6.2.4 Algorithme de résolution de l'équation de Pell-Fermat

On développe $\sqrt{d}$ en fraction continue : $(a_0, a_1, \ldots, a_{r+1}, a_1, \ldots, a_{r+1}, \cdots)$.

$\frac{p_r}{q_r}$ est le rationnel dont le développement en fraction continue a pour cœfficients $(a_0, \ldots, a_r)$.

Si r est impair, alors (p_r, q_r) est la solution fondamentale de $x^2 - dy^2 = 1$ et $x^2 - dy^2 = -1$ n'a pas de solutions.

Sinon, r est pair et (p_r, q_r) est la solution fondamentale de $x^2 - dy^2 = \pm 1$.

Exemple : $x^2 - 7y^2 = \pm 1$.

Le développement en fraction continue de $\sqrt{7}$ est $(2, \overline{1,1,1,4})$.

On regarde :

$$2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}} = \frac{8}{3}$$

Les solutions de $x^2 - 7y^2 = 1$ sont $\pm(8 + 3\sqrt{7})^n$ et $x^2 - 7y^2 = -1$ n'a pas de solutions.

6.3 Théorème de Dirichlet

Soit K un corps de nombres. Notons s le nombre de plongements réels et t le nombre de paires de plongements non réels. Le degré de K sur $\mathbb{Q}$ est

 Tous droits réservés

$n = s + 2t$.

Notons $\mu(K)$ l'ensembles des racines de l'unité dans K.

THÉORÈME 6.3 DIRICHLET $\mathcal{O}_K^\times \simeq \mu(K) \times \mathbb{Z}^{s+t-1}$.

Démonstration.

Définition 6.5 On définit :

$$\sigma : \begin{cases} K & \to & \mathbb{R}^s \times \mathbb{C}^t \\ z & \mapsto & (\underbrace{\sigma_1(z), \dots, \sigma_s(z)}_{\text{plongements réels}}, \underbrace{\sigma_{s+1}(z), \dots, \sigma_{s+t}(z)}_{\text{plongements non réels}}) \end{cases}$$

$$l : \begin{cases} (\mathbb{R}^\times)^s \times (\mathbb{C}^\times)^t & \to & \mathbb{R}^{s+t} \\ (z_1, \dots, z_{s+t}) & \mapsto & (\ln(|z_1|), \dots, \ln(|z_s|), \ln(|z_{s+1}|^2), \dots, \ln(|z_{s+t}|^2)) \end{cases}$$

Proposition 6.12

- Si $z \in K^*$, $\sigma(z) \in (\mathbb{R}^\times)^s \times (\mathbb{C}^\times)^t$ donc $(l \circ \sigma)$ est bien définie.
- $l \circ \sigma : K^* \to \mathbb{R}^{s+t}$ est un morphisme de groupes.
- Si $z \in K^\times$, posons $l(\sigma(z)) = (l_1, \dots, l_{s+t})$.

  $\sum l_i = \ln(|N(z)|)$.

  $\sum l_i = 0 \quad \text{ssi} \quad z \in \mathcal{O}_K^\times$.

  $\forall i, l_i = 0 \quad \text{ssi} \quad z \in \mu(K)$.

Démonstration. Tous les points sont faciles sauf le dernier.

Les l_i sont nuls ssi pour tout i, $|\sigma_i(z)| = 1$ ssi pour tout plongement σ, $|\sigma(z)| = 1$.

Lemme 6.3.1
Si B est un compact de $\mathbb{R}^{s+t}$, alors $\{z \in \mathcal{O}_K^*, (l \circ \sigma)(z) \in B\}$ est fini.

Démonstration. Soit $z \in \mathcal{O}_K$. $\prod_\sigma (X - \sigma(z)) \in \mathbb{Z}[X]$ et $(\sigma_1(z), \dots, \sigma_{s+t}(z)) \in l^{-1}(B)$ qui est compact.

Donc les cœfficients de $\prod_\sigma (X - \sigma(z))$ se trouvent dans un compact qui dépend uniquement de B donc ce polynôme appartient à un ensemble fini de polynômes.

Ceux-ci ont chacun au plus n racines dans K et z en est une.

Donc l'ensemble considéré est fini. ∎

Lemme 6.3.2
$\mu(K)$ est un sous-groupe fini de $\mathcal{O}_K^\times$.

 Tous droits réservés

Démonstration. $\mu(K) = \{x \in \mathcal{O}_K^*, l(\sigma(x)) = 0\}$ et $\{0\}$ est compact. D'où le résultat. ■

Lemme 6.3.3
Soit $z \in \mathcal{O}_K$.
(Pour tout σ, $|\sigma(z)| = 1$) ssi $z \in \mu(K)$.

Démonstration.
$\Leftarrow$ Si $z \in \mu(K)$, $z^m = 1$ donc $|\sigma(z)|^n = 1$ donc $|\sigma(z)| = 1$.
$\Rightarrow$ $G = \mathrm{Ker}(l \circ \sigma)$. $\{0\}$ est compact donc G est fini.
Soit $z \in \mathcal{O}_K$ qui vérifie l'hypothèse, $z \in G$ donc $z^{|G|} = 1$ donc $z \in \mu(K)$. ■

Ce qui permet de conclure la propriété. ■

Remarque 6.4 *$\mu(K)$ est un sous-groupe de*

$$\{z \in \mathbb{C}, z^{|\mu(K)|} = 1\} \simeq \mathbb{Z}/|\mu(K)|\mathbb{Z}$$

Donc $\mu(K)$ est cyclique (car tous les sous-groupes de $\mathbb{Z}/|\mu(K)|\mathbb{Z}$ sont cycliques).
On a de plus $\mathcal{O}_K^\times/\mu(K) \simeq \mathrm{Im}(l \circ \sigma)$.

Lemme 6.3.4
$(l \circ \sigma)(\mathcal{O}_K^\times)$ est un sous-groupe discret de $\mathbb{R}^{s+t}$ contenu dans l'hyperplan $H = \{l \in \mathbb{R}^{s+t}, \sum l_i = 0\}$.

Démonstration. On sait déjà que c'est un sous-groupe.
Soit B une boule fermée de $\mathbb{R}^{s+t}$ donc compacte.
$(l \circ \sigma)^{-1}(B)$ est un compact donc fini donc $(l \circ \sigma)(\mathcal{O}_K^\times) \cap B$ est fini donc $(l \circ \sigma)(\mathcal{O}_K)$ est discret. ■

$(l \circ \sigma)(\mathcal{O}_K)$ est donc un réseau d'un sous-espace vectoriel de H donc c'est isomorphe à $\mathbb{Z}^h$.
On veut montrer que $(l \circ \sigma)(\mathcal{O}_K^\times)$ engendre H comme $\mathbb{R}$-espace vectoriel.
Il suffit de montrer que pour toute forme linéaire $f : H \to \mathbb{R}$, $f((l \circ \sigma)(\mathcal{O}_K^\times)) \neq 0$.

Lemme 6.3.5
$\sigma(\mathcal{O}_K) \subset \mathbb{R}^s \times \mathbb{C}^t$.
$\sigma(\mathcal{O}_K)$ en est un réseau de volume $2^{-t}\sqrt{|\operatorname{disc}(K)|}$.

 Tous droits réservés

Démonstration. $\mathcal{O}_K$ est un $\mathbb{Z}$-module libre de rang n dont une $\mathbb{Z}$-base est $(z_1, \dots, z_n)$.

On veut montrer que $(\sigma(z_1), \dots, \sigma(z_n))$ est une base du $\mathbb{R}$-espace vectoriel $\mathbb{R}^s \times \mathbb{C}^t$.

$$\det(\sigma(z_1), \dots, \sigma(z_n)) = \begin{vmatrix} \sigma_1(z_1) & \cdots & \sigma_1(z_n) \\ \vdots & & \vdots \\ \sigma_s(z_1) & \cdots & \sigma_s(z_n) \\ \Re(\sigma_{s+1}(z_1)) & \cdots & \Re(\sigma_{s+1}(z_n)) \\ \Im(\sigma_{s+1}(z_1)) & \cdots & \Im(\sigma_{s+1}(z_n)) \\ \vdots & & \vdots \\ \Re(\sigma_{s+t}(z_1)) & \cdots & \Re(\sigma_{s+t}(z_n)) \\ \Im(\sigma_{s+t}(z_1)) & \cdots & \Im(\sigma_{s+t}(z_n)) \end{vmatrix}$$

$$= \begin{vmatrix} \sigma_1(z_1) & \cdots & \sigma_1(z_n) \\ \vdots & & \vdots \\ \sigma_s(z_1) & \cdots & \sigma_s(z_n) \\ \frac{\sigma_{s+1}(z_1)+\overline{\sigma_{s+1}(z_1)}}{2} & \cdots & \frac{\sigma_{s+1}(z_n)+\overline{\sigma_{s+1}(z_n)}}{2} \\ \frac{\sigma_{s+1}(z_1)-\overline{\sigma_{s+1}(z_1)}}{2} & \cdots & \frac{\sigma_{s+1}(z_n)-\overline{\sigma_{s+1}(z_n)}}{2} \\ \vdots & & \vdots \\ \frac{\sigma_{s+t}(z_1)+\overline{\sigma_{s+t}(z_1)}}{2} & \cdots & \frac{\sigma_{s+t}(z_n)+\overline{\sigma_{s+t}(z_n)}}{2} \\ \frac{\sigma_{s+t}(z_1)-\overline{\sigma_{s+t}(z_1)}}{2} & \cdots & \frac{\sigma_{s+t}(z_n)-\overline{\sigma_{s+t}(z_n)}}{2} \end{vmatrix}$$

Donc $\det(\sigma(z_1), \dots, \sigma(z_n))^2 = (-1)^t 2^{-2t} \operatorname{disc}(K) = 2^{-2t} |\operatorname{disc}(K)| \neq 0$. ■

Posons

$$B_\lambda = \{(x_1, \dots, x_{s+t}) \in \mathbb{R}^s \times \mathbb{C}^t, \forall i, |x_i| \leqslant \lambda_i\}$$

pour $\lambda = (\lambda_1, \dots, \lambda_{s+t})$.

C'est un convexe symétrique borné non vide.

Son volume vaut $2^s \pi^t \lambda_1 \cdots \lambda_s \lambda_{s+1}^2 \cdots \lambda_{s+t}^2 = 2^s \pi^t \alpha$.

- Si $2^s \pi^t \alpha \geqslant 2^n 2^{-t} \sqrt{|\operatorname{disc}(K)|}$ alors il existe un $z_\lambda \in \mathcal{O}_K^*$ tel que $\sigma(z_\lambda) \in B_\lambda$.
  Dans ce cas, $1 \leqslant |N(z_\lambda)| \leqslant \alpha$.
  $1 \leqslant |N(z_\lambda)| = |\sigma_i(z_\lambda)| \prod_{\sigma \neq \sigma_i} |\sigma(z_\lambda)| \leqslant \sigma_i(z_\lambda) \frac{\alpha}{\lambda_1}$.
  Donc $|\sigma_i(z_\lambda)| \geqslant \frac{\lambda_1}{\alpha}$.
  Donc $0 \leqslant \ln \lambda_i - \ln |\sigma_i(z_\lambda)| \leqslant \ln \alpha$.

 Tous droits réservés

Or $f((l\circ\sigma)(z_\lambda)) = \sum_i f_i \ln(|\sigma_i(z_\lambda)|)$ donc

$$\left|\sum_i f_i \log(\lambda_i) - f((l\circ\sigma)(z_\lambda))\right| \leqslant \left(\sum_i |f_i|\right)\ln\alpha$$

- On prend $\alpha \geqslant (\frac{2}{\pi})^t\sqrt{|\operatorname{disc}(\alpha)|}$, $\alpha \geqslant 1$ et $\beta > \ln(\alpha)\sum_i |f_i|$.

  Pour tout $m > 0$, on a alors des $(\lambda_1(m),\dots,\lambda_{t+s}(m))$ strictement positifs tels que $\ln(\lambda_1(m)) + \cdots + \ln(\lambda_s(m)) + 2\ln(\lambda_{s+1}(m)) + \cdots + 2\ln(\lambda_{s+t}(m)) = \ln(\alpha)$.
  On a alors $2\beta m = \sum_i f_i \ln(\lambda_i(m))$.

  Remarque 6.5 *C'est possible car* $(f_1,\dots,f_{s+t})$ *et* $(\underbrace{1,\dots,1}_{s\ fois},\underbrace{2,\dots,2}_{s+t\ fois})$ *ne sont pas colinéaires car* $f \neq 0$.

  $B_{\lambda(m)}$ est un convexe symétrique borné non vide de volume $2^s\pi^t\alpha > 2^n \operatorname{Vol}(\sigma(\mathcal{O}_K))$.
  Par Minkowski, il existe $z_{\lambda(m)} \in \mathcal{O}_K \setminus \{0\}$ tel que $\sigma(z_{\lambda(m)}) \in B_{\lambda(m)}$.
  Par le premier point, $|f((l\circ\sigma)(z_{\lambda(m)})) - 2\beta m| \leqslant \ln(\alpha)\sum_{i=1}^{s+t}|f_i| < \beta$.
  Donc $(2m-1)\beta < f((l\circ\sigma)(z_{\lambda(m)})) < (2m+1)\beta$.
  Donc les $f((l\circ\sigma)(z_{\lambda(m)})) \in \mathbb{R}$ sont tous distincts.
  De plus,

$$|N(z)| = |\sigma_1(z_{\lambda(m)})|\cdots|\sigma_s(z_{\lambda(m)})||\sigma_{s+1}(z_{\lambda(m)})|^2\cdots|\sigma_{s+t}(z_{\lambda(m)})|^2 \leqslant \alpha$$

Lemme 6.3.6
Si $a \in \mathbb{Z}$, $\{x\mathcal{O}_K, x \in \mathcal{O}_K, N(x) = a\}$ est fini.

Démonstration. $a = N(x) = \prod_\sigma \sigma(x)$ donc, comme a et $\sigma_1(x)$ appartiennent à $\sigma_1(\mathcal{O}_K)$ donc $\prod_{\sigma\neq\sigma_1}\sigma(x) \in \sigma_1(\mathcal{O}_K)$.

$a \in \sigma_1(x)\sigma_1(\mathcal{O}_K)$ donc $\sigma_1(a) \in \sigma_1(x\mathcal{O}_K)$ donc $a \in x\mathcal{O}_K$.

Donc $a\mathcal{O}_K \subset x\mathcal{O}_K$ donc $x\mathcal{O}_K/a\mathcal{O}_K$ est un idéal de $\mathcal{O}_K/a\mathcal{O}_K \simeq (\mathbb{Z}/a\mathbb{Z})^n$ qui est fini.

Donc $\mathcal{O}_K/a\mathcal{O}_K$ a un nombre fini d'idéaux donc $\mathcal{O}_K$ a un nombre fini d'idéaux qui contienent $a\mathcal{O}_K$ d'où le lemme. ∎

Considérons les idéaux $z_{\lambda(m)}\mathcal{O}_K$.

$N(z_{\lambda(m)}) \in [\![-\alpha,\alpha]\!]$ donc il existe $a \in [\![-\alpha,\alpha]\!]$ tel qu'il y ait une infinité de m tels que $N(z_{\lambda(m)}) = a$.

 Tous droits réservés

$\{z_{\lambda(m)}\mathcal{O}_K, m > 0, N(z_{\lambda(m)}) = a\}$ est donc fini donc il existe $m_0, m_1 > 0$ tels que $m_0 \neq m_1$ tels que $z_{\lambda(m_0)}\mathcal{O}_K = z_{\lambda(m_1)}\mathcal{O}_K$.

Il existe donc $u \in \mathcal{O}_K^\times$ tel que $z_{\lambda(m_1)} = uz_{\lambda(m_0)}$.

$f((l \circ \sigma)(u)) = f((l \circ \sigma)(z_{\lambda(m_1)})) - f((l \circ \sigma)(z_{\lambda(m_0)})) \neq 0$ car $m_1 \neq m_0$.

On a donc trouvé $u \in \mathcal{O}_K^\times$ tel que $f((l \circ \sigma)(u)) \neq 0$. D'où le théorème. ■

 Tous droits réservés

Chapitre 7

Analyse numérique

7.1 Fonction ζ

Définition 7.1 On définit la fonction ζ de Riemann par :

$$\zeta : \begin{cases} \mathbb{C} & \to & \mathbb{C} \\ s & \mapsto & \sum_{n \geqslant 0} n^{-s} \end{cases}$$

Proposition 7.1 Il y a convergence sur $\{s, \Re(s) > 1\}$ et convergence uniforme sur $\{s, \Re(s) \geqslant A\}$ avec $A > 1$.

Proposition 7.2 $\zeta(s) = \prod_{p \in \mathscr{P}} (1 - p^{-1})^{-1}$.

Démonstration.

$$\begin{aligned} \zeta(s) &= (1 + 2^{-s} + 2^{-2s} + \cdots)(1 + 3^{-s} + \cdots) \cdots \\ &= \sum_{n=1}^{\infty} \prod_{p \in \mathscr{P}} p^{-s v_p(n)} \\ &= \prod_{p \in \mathscr{P}} \sum_{k=0}^{\infty} p^{-ks} \\ &= \prod_{p \in \mathscr{P}} (1 - p^{-1})^{-1} \end{aligned}$$

Théorème 7.1 *$\mathscr{P}$ est infini.*

Démonstration. On a $\lim_{s \to 1} \zeta(s) = +\infty$ donc $\lim_{s \to 1} \prod_{p \in \mathscr{P}} (1 - p^{-1}) = 0$.

Si $\mathscr{P}$ était fini, cette limite vaudrait $\prod_{p \in \mathscr{P}} (1 - p^{-1}) \neq 0$. Donc $\mathscr{P}$ est infini. ∎

THÉORÈME 7.2 $\displaystyle\sum_{p\in\mathscr{P}}\frac{1}{p}=+\infty$.

Démonstration. On a $\lim\limits_{s\to1}\sum\limits_{p\in\mathscr{P}}\ln(1-p^{-1})=+\infty$.

Donc $\lim\limits_{s\to1}\sum\limits_{p\in\mathscr{P}}\sum\limits_{n=1}^{+\infty}\frac{p^{-ns}}{n}=+\infty$.

Pour $n\geqslant 2$, $\sum\limits_{p\in\mathcal{P}}p^{-ns}\leqslant\sum\limits_{k=2}^{\infty}k^{-ns}\leqslant\int_1^{+\infty}t^{-ns}\,\mathrm{d}t\leqslant\frac{1}{ns+1}$.

Donc $\sum\limits_{n=2}^{\infty}\frac{1}{n}\frac{1}{ns+1}\leqslant\frac{1}{s}\sum\limits_{n=2}^{\infty}\frac{1}{n^2}$ qui est bornée.

Donc c'est le terme en $n=1$ qui diverge. Donc $\lim\limits_{s\to1}\sum\limits_{p\in\mathscr{P}}p^{-s}=+\infty$.

Donc $\displaystyle\sum_{p\in\mathscr{P}}\frac{1}{p}=+\infty$. ∎

Proposition 7.3 $\zeta(2k)=(-1)^{k+1}\frac{2^{2k-1}b_{2k}}{(2k)!}\pi^{2k}$ avec $b_{2k}\in\mathbb{Q}$ est le $2k$-ème nombre de Bernoulli : il vérifie $\displaystyle\sum_{n=0}^{\infty}\frac{b_n}{n!}t^n=\frac{t}{\mathrm{e}^t-1}$.

THÉORÈME 7.3 (APÉRY, 1978) *$\zeta(3)$ est irrationnel.*

THÉORÈME 7.4 *La fonction ζ a un prolongement méromorphe à $\mathbb{C}$ avec un unique pôle en 1, qui vérifie une équation fonctionnelle.*

7.2 Fonction Γ

Définition 7.2 On définit la fonction Γ par :

$$\Gamma:\begin{cases}\mathbb{C} & \to & \mathbb{C}\\ s & \mapsto & \int_0^{\infty}t^{s-1}\mathrm{e}^{-t}\,\mathrm{d}t\end{cases}$$

Proposition 7.4 La fonction est définie sur le demi-plan $\Re(z)>0$. Elle admet un prolongement méromorphe à $\mathbb{C}$ dont les pôles sont les éléments de $\mathbb{Z}^-$.

Proposition 7.5 $\displaystyle n^{-2s}\pi^{-s}\Gamma(s)=\int_0^{\infty}\mathrm{e}^{n^2\pi t}t^{s-1}\,\mathrm{d}t$

Démonstration. Utiliser le changement de variables $t=n^2\pi u$. ∎

Proposition 7.6 $\displaystyle\zeta(2s)\pi^{-s}\Gamma(s)=\int_0^{\infty}\frac{\theta(t)-1}{2}t^{s-1}\,\mathrm{d}t$ avec $\theta(t)=\sum\limits_{n\in\mathbb{Z}}\mathrm{e}^{-n^2\pi t}$.

 Tous droits réservés

Démonstration. Sommer la formule précédente. ■

Lemme 7.4.1
$\theta(\frac{1}{t}) = t^{\frac{1}{2}}\theta(t)$.

Démonstration. On applique la formule sommatoire de Poisson aux transformées de Fourier de $x \mapsto \mathrm{e}^{-\pi x^2 t}$ et $x \mapsto \frac{\mathrm{e}^{-\pi \frac{x^2}{t}}}{\sqrt{t}}$. ■

THÉORÈME 7.5 *ζ :*
- *est méromorphe sur $\mathbb{C}$,*
- *a un pôle en 1 et c'est le seul,*
- *s'annule sur $\mathbb{Z}^-$,*
- *$s \mapsto \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$ est symétrique par rapport à l'axe $\Re(z) = \frac{1}{2}$.*

Démonstration. On a par les résultats précédents :

$$\begin{aligned}
\zeta(2s)\pi^{-s}\Gamma(s) &= \int_0^\infty \frac{\theta(t)-1}{2} t^{s-1}\,\mathrm{d}t \\
&= \int_0^1 \frac{\theta(t)-1}{2} t^{s-1}\,\mathrm{d}t + \int_1^\infty \frac{\theta(t)-1}{2} t^{s-1}\,\mathrm{d}t \\
&= \int_1^\infty \frac{\theta(\frac{1}{t})-1}{2} t^{-s-1}\,\mathrm{d}t + \int_1^\infty \frac{\theta(t)-1}{2} t^{s-1}\,\mathrm{d}t \\
&= \int_1^\infty \frac{\theta(t)t^{-s-\frac{1}{2}} - t^{-s-1} + \theta(t)t^{s-1} - t^{s-1}}{2}\,\mathrm{d}t \\
&= \int_1^\infty \frac{(\theta(t)-1)(t^{-s-\frac{1}{2}} + t^{s-1})}{2}\,\mathrm{d}t + \frac{1}{2s-1} - \frac{1}{2s}
\end{aligned}$$

Proposition 7.7 ζ ne s'annule pas sur la droite $\Re(z) = 1$.

Remarque 7.1 C'est de là qu'on déduit le :

THÉORÈME 7.6 DES NOMBRES PREMIERS

$$\mathrm{Card}(\{p \in \mathscr{P}, p \leqslant x\}) \sim \frac{x}{\ln(x)}$$

THÉORÈME 7.7 (CONJECTURE DE RIEMANN) *Les zéros de ζ sont les entiers négatifs ou ont pour partie réelle $\frac{1}{2}$.*

7.3 Généralisation

7.3.1 Fonctions L

Définition 7.3 Soit $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ un morphisme de groupe.

 Tous droits réservés

On définit les fonctions L par :

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \in \mathscr{P}} (1 - \chi(p)p^{-s})^{-1}$$

Définition 7.4 (Fonction ζ d'un corps de nombres) Soit K un corps de nombres et N la norme associée.

On définit la fonction ζ associée à K par :

$$\zeta_K(s) = \prod_{(0) \neq \mathfrak{p} \text{ premier } \subset \mathcal{O}_K} (1 - N(p)^{-s})^{-1}$$

THÉORÈME 7.8 *Soit $m \in \mathbb{N}^*$ et $a \in \mathbb{Z}$ premier avec m.*

Il existe une infinité de nombres premiers congrus à a modulo m.

Démonstration. Soit $A \subset \mathscr{P}$.

On définit la densité de A dans $\mathscr{P}$ par :

$$\lim_{n \to +\infty} \frac{\text{Card}(A \cap [1,n])}{\text{Card}(P \cap [1,n])}$$

et la densité analytique par :

$$\lim_{s \to 1} \frac{\sum_{p \in A} p^{-s}}{\ln(\frac{1}{s-1})}$$

Si A est fini, sa densité et sa densité analytique sont nulles. On va montrer que la densité analytique de $A = \{p \in \mathscr{P}, p \equiv a \mod m\}$ est $\frac{1}{\varphi(m)} > 0$.

Soit χ un morphisme de $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ et $f_\chi = s \mapsto \sum_{\substack{p \in \mathscr{P} \\ p \nmid m}} \chi(p)p^{-s}$.

Lemme 7.8.1

Si $\chi = \text{Id}$, $f_\chi(s) \underset{s \to 1}{\sim} \ln(\frac{1}{s-1})$.

Sinon, f_χ est bornée au voisinage de 1.

Et ça permet de conclure (cf. rapport de stage). ∎

 Tous droits réservés