

Bibliography :

Borevitch Shafarevich Théorie des Nombres.

Ireland Rosen A classical introduction to modern number theory.

Pierre Samuel Théorie algébrique des nombres.

Jean-Pierre Serre Cours d'arithmétique.

Neukirch Algebraic number theory.

Washington Introduction to cyclotomic fields.

1. INTRODUCTION

1.1. Sommes de deux carrés. Pour n entier > 0 , soit à résoudre $n = x^2 + y^2$, x et y entiers dans \mathbb{Z} .

On interprète cette équation comme $n = N(x + iy)$, N étant la norme de l'anneau des entiers de Gauss $\mathbb{Z}[i]$. Ici, on a considéré $\mathbb{Z}[i]$ comme un sous anneau de \mathbb{C} et la norme est le carré de la norme de \mathbb{C} . C'est l'anneau des entiers du corps de nombres quadratique imaginaire $\mathbb{Q}(i)$. La norme est multiplicative : $N(z_1 z_2) = N(z_1)N(z_2)$. Si n_1 et n_2 sont somme de deux carrés, il en est de même de leur produit.

Théorème 1.1. *Soit $n = p$ un nombre premier impair. Alors n est somme de deux carrés si et seulement si $p \equiv 1$ modulo 4.*

Proposition 1.2. *$\mathbb{Z}[i]$ est principal.*

Prouvons la proposition. Existence d'une division euclidienne. Soient a et $b \neq 0$ dans $\mathbb{Z}[i]$. Il existe z dans $\mathbb{Z}[i]$ tel que $t := N(a/b - z) < 1$, soit $N(a - zb) < N(b)$.

L'anneau $\mathbb{Z}[i]$ est principal. Ce n'est pas toujours vrai pour $\mathbb{Z}[\sqrt{d}]$, $d < 0$ comme l'exemple $2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ le montre. En fait un théorème difficile dit que $\mathbb{Z}[\sqrt{d}]$, $d < 0$, ou plus précisément l'anneau des entiers de $\mathbb{Q}[\sqrt{d}]$, est principal pour un nombre fini de d (Stark 1967 donne la liste des d , le plus grand en valeur absolue est -163).

Les unités de $\mathbb{Z}[i]$ sont $\pm 1, \pm i$.

Faisons la liste des idéaux premiers de $O := \mathbb{Z}[i]$. Il y a (0) ! Si $\wp \neq (0)$, $\wp \cap \mathbb{Z} = p\mathbb{Z}$ pour p un nombre premier (\wp contient la norme d'un élément non nul). Donc $(p) \subset \wp$ et \wp est l'image réciproque d'un idéal premier de $O/pO = \mathbb{F}_p[X]/(X^2 + 1)$.

Pour $p = 2$, $O/2O$ a un seul idéal premier. Il est engendré par $X + 1$. L'anneau quotient n'est pas réduit. $(2) = (1 + i)^2$ n'est pas "sans carré" : (2) est ramifié.

Si $p \equiv 1 \pmod{4}$, -1 est un carré modulo p . Donc O/pO se décompose en un produit de deux corps isomorphes à \mathbb{F}_p . On a $N(\wp) = p$. Un générateur $z = x + iy$ de \wp est de norme p . L'équation $p = x^2 + y^2$ a une solution essentiellement unique. On a $pO = \wp\bar{\wp}$. On dit que (p) est décomposé.

Si $p \equiv 3 \pmod{4}$, O/pO est un corps, (p) est premier dans O . On dit que p est inerte.

On voit donc que n est somme de deux carrés si et seulement si la valuation $v_p(n)$ est paire pour $p \equiv 3 \pmod{4}$ ($n = \prod_p v_p(n)$ est la décomposition de n en facteurs premiers).

Soit χ le caractère de Dirichlet de $d \mapsto \chi(d)$, $\mathbb{Z} \rightarrow \{\pm 1\}$, qui vaut 0 si 2 divise d , 1 si $d \equiv 1 \pmod{4}$ et -1 si $d \equiv 3 \pmod{4}$. Soit a_n le nombre de solutions (x, y) avec $x > 0$ et $y \geq 0$ de l'équation $n = x^2 + y^2$. Il résulte facilement du fait que les unités de O sont $\pm 1, \pm i$ que la série de Dirichlet $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ coïncide avec la fonction $\zeta_{\mathbb{Q}[i]}$:

$$\zeta_{\mathbb{Q}[i]}(s) = \prod_{\wp} \left(1 - \frac{1}{N(\wp)^s}\right)^{-1} = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$$

\wp décrivant les idéaux premiers de O (non nuls) et \mathfrak{a} les idéaux non nuls de O . La norme $N(\mathfrak{a})$ est le cardinal de O/\mathfrak{a} , ou la norme d'un générateur de \mathfrak{a} .

C'est une conséquence de la décomposition dans O des idéaux premiers de \mathbb{Z} que :

$$\zeta_{\mathbb{Q}[i]}(s) = \zeta(s)L(s, \chi)$$

avec $\zeta(s) = \sum_n \frac{1}{n^s} = \prod_p \frac{1}{(1 - \frac{1}{p^s})}$ et $L(s, \chi) = \sum_n \frac{\chi(n)}{n^s} = \prod_p \frac{1}{(1 - \frac{\chi(p)}{p^s})}$

Il en résulte que $a_n = \sum_{d|n} \chi(d)$. On a le théorème :

Théorème 1.3. *Les fonctions ζ , $\zeta_{\mathbb{Q}[i]}$ se prolongent en des fonctions méromorphes sur \mathbb{C} avec comme seul pôle 1, et ce pôle est simple. $L(s, \chi)$ se prolonge en une fonction holomorphe sur \mathbb{C} et $L(\chi, 1) \neq 0$.*

Il résulte du fait que ζ a un pôle simple en $s = 1$ avec résidu 1 que $\sum_p \frac{1}{p^s}$ est équivalent $\ln(1/(s-1))$ lorsque s tend vers 1 par valeurs > 1 . On dit qu'un ensemble A de nombre premiers a densité un réel k si $\sum_{p \in A} \frac{1}{p^s}$ est équivalent $k \ln(1/(s-1))$ lorsque s tend vers 1 par valeurs > 1 . Il résulte du fait que $L(\chi, 1) \neq 0$ que les ensembles de nombres premiers qui congruent 1 ou 3 modulo 4 ont tous deux densité $1/2$. C'est un cas particulier du théorème de Dirichlet (1841):

Théorème 1.4. *Soit $m > 1$ et soit a un entier premier à m . L'ensemble des nombres premiers p qui congruent a modulo m a pour densité $1/\phi(m)$ (en particulier il est infini).*

Exercice 1) Euler : p premier, $x^3 + py^3 + p^2z^3 = 0$ n'a pas de solution non triviale.

2) L'équation $y^2 = x^3 + 7$ n'a pas de solution entière. x impair, $y^2 + 1 = (x+2)((x-1)^2 + 3)$, il existe p de la forme $4n+3$ divisant $(x-1)^2 + 3$, -1 est un carré modulo p , contradiction.

2. ENTIERS

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

2.1. L'anneau des entiers. Soit K un corps de nombres. On veut définir l'anneau O_K de ses entiers.

Definition 2.1. Soit A un anneau et B une A -algèbre. Soit b un élément de B . On dit que b est entier sur A s'il existe un polynôme $P \in A[X]$ unitaire tel que $P(b) = 0$.

b est entier sur A s'il est entier sur l'image A' de A dans B . On voit que l'on ne perd pas grand chose en supposant que $A \rightarrow B$ est injective, ce que l'on fait désormais.

Proposition 2.2. Les propriétés suivantes sont équivalentes.

- b est entier sur A ;
- $A[b]$ est un A -module de type fini ;
- il existe une sous A -algèbre B' de B contenant b et telle que B' soit un A -module de type fini.

1) implique 2) Si P est de degré n , $A[b]$ est engendré par $1, b, \dots, b^{n-1}$.

2) implique 3) : clair.

3) entraîne 1) Soit y_1, \dots, y_n des générateurs de B' en tant que A -module. On a $by_i = \sum_{j=1}^n a_{ij}y_j$ pour des $a_{ij} \in A$. Ceci s'écrit $\sum_{j=1}^n (\delta_{ij}b - a_{ij})y_j = 0$. Soit d le déterminant de la matrice $M = (m_{ij})$ à n lignes et n colonnes : $m_{ij} = \delta_{ij}b - a_{ij}$. M annule la matrice colonne y_j , donc aussi $MC(M) = did$. On a donc $dy_j = 0$, Comme $1 \in B'$ on a $d = 0$. Si on développe d , on voit que cela donne P .

Corollaire 2.3. Les éléments de B qui sont entiers sur A forment un sous-anneau de B qui s'appelle la clôture intégrale de A dans B .

Definition 2.4. Soit K un corps de nombres. Un élément $b \in K$ est entier si b est entier sur \mathbb{Z} .

Remarque. Si K est galoisien sur \mathbb{Q} , O_K est stable par Galois.

Definition 2.5. Soit A un anneau intègre. Soit F son corps des fractions. On dit que A est intégralement clos si A coïncide avec sa clôture intégrale dans F .

Proposition 2.6. Un anneau factoriel est intégralement clos.

Si $P(a/b) = 0$, a et b premiers entre eux, $P(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$, on a $a^n + \sum_{i=0}^{n-1} a_i a^i b^{n-i} = 0$. Par suite b divise a^n donc $b = 1$.

Si A est factoriel, $A[X]$ l'est. $k[T^2, T^3]$ n'est pas intégralement clos.

2.2. Rappels sur les extensions de corps. Soient F un corps et A une F -algèbre finie (A est un F -espace vectoriel de dimension finie).

Soit $x \in F$. On définit $f_x \in F[X]$ son polynôme caractéristique comme étant le polynôme caractéristique de la multiplication m_x par x . La trace $t(x)$ (resp. la norme $N(x)$) sont la trace et la norme de m_x .

Théorème 2.7. *Soient K un corps et A une K -algèbre. Soit L une extension de K . Alors, $\text{Hom}_{K\text{-alg}}(A, L)$ est une partie libre du L -espace vectoriel $\text{Hom}_K(A, L)$.*

Soient u_i n éléments distincts de $\text{Hom}_{K\text{-alg}}(A, L)$. Montrons par récurrence sur n qu'ils sont indépendants. Si $n = 1$ c'est clair car $u(1) = 1$. Soit $\sum_{i=1}^n \lambda_i u_i = 0$ une relation de dépendance linéaire, $\lambda_i \in L$. Pour $x \in A$, on a : $\sum_{i=1}^n \lambda_i u_i(x) u_i = 0$, donc

$$\sum_{i=1}^{n-1} \lambda_i (u_n(x) - u_i(x)) u_i = 0.$$

L'hypothèse de récurrence entraîne $\lambda_i (u_n(x) - u_i(x)) = 0$. Les u_i étant distincts, on en déduit $\lambda_i = 0$ pour $i \leq n-1$. Le cas $n = 1$ implique $\lambda_n = 0$.

Exercice. Indépendance linéaire des caractères d'un groupe abélien fini.

Il en résulte que si A est finie de dimension d sur K , $\text{Hom}_{K\text{-alg}}(A, L)$ est de cardinal $\leq d$.

Soit F' une extension finie de F de degré d et Ω une clôture algébrique de F . On a donc au plus d plongements distincts de F' dans Ω .

Definition 2.8. *On dit que F' est séparable, si le nombre des plongements est d .*

Proposition 2.9. *Si F est parfait, F' est séparable.*

Si $f \in K[X]$ est irréductible et F parfait, f' n'est pas nul, donc est premier avec f et f a d racines distinctes dans Ω .

Exercice F parfait et F'/F finie entraîne F' parfait. On pourra utiliser $x \mapsto x^p : F' \rightarrow F'$, le second F' étant muni de la structure de F -espace vectoriel $(\lambda, x) \mapsto \lambda^p x$.

Supposons F' séparable. Soient τ_1, \dots, τ_d les différents plongement de F' dans Ω . Les $\text{id} \otimes_F \tau_i$ définissent des morphismes de Ω -algèbres distincts que l'on nomme $l_i : l_i : \Omega \otimes_F F' \rightarrow \Omega$. Ils sont donc Ω -linéairement indépendants et on voit que $\Omega \otimes_F F'$ est diagonalisée :

Proposition 2.10. $\oplus l_i : \Omega \otimes_F F' \rightarrow (\Omega)^d$ est un isomorphisme de Ω -algèbres.

Soit $x \in F'$ Son image par l'isomorphisme de la proposition est $(\tau_i(x))$. On voit donc que :

$$f_x(X) = \prod_i (X - \tau_i(x)), t(x) = \sum_i \tau_i(x), N(x) = \prod_i \tau_i(x).$$

Proposition 2.11. *La forme bilinéaire $(x, y) \mapsto t(xy)$ est non dégénérée*

Cela résulte de l'indépendance linéaire des τ_i .

Definition 2.12. *Ceci permet de définir le discriminant modulo $(F^*)^2$. Si ω_i est une base de F' en tant que F -espace vectoriel, c'est*

$$\det(t(\omega_i \omega_j)) = \det(\tau_i(\omega_j))^2.$$

Exercice. Soit A une F -algèbre finie réduite. Alors A est isomorphe à un produit d'extensions finies de F .

2.3. Fermeture intégrale dans une extension séparable. Soit O intégralement clos dans son corps des fractions F . Supposons F'/F séparable de degré d . Soit O' la fermeture intégrale de O dans F' .

Proposition 2.13. *Soit $x \in F'$. Pour que $x \in O'$, il faut et il suffit que f_x ait ses coefficients dans O .*

Si le polynôme caractéristique a ses coefficients dans O , x est entier car x annule son polynôme caractéristique.

Prouvons la réciproque. Soit $x \in F'$. Soit d le degré de F'/F et τ_1, \dots, τ_d les différents plongements de F' dans sa clôture galoisienne M sur F . Le polynôme caractéristique de x est $\prod_i (X - \tau_i(x))$ (séparabilité). Comme les $\tau_i(x)$ sont entiers sur O , on voit que les coefficients du polynôme caractéristique de x sont entiers sur O et dans F . Ils sont bien dans O .

On veut maintenant étudier les anneaux d'entiers et définir une version entière du discriminant.

Rappelons qu'un A -module M est noethérien s'il vérifie les propriétés suivantes équivalentes :

- toute famille non vide de sous-modules de M possède un élément maximal ;
- toute suite croissante de sous-modules de M est stationnaire ;
- tout sous-module de M est de type fini.

Un anneau A est dit noethérien s'il l'est en tant que A -module (tout idéal est de type fini). Si A est noethérien, tout A module de type fini est noethérien et de présentation finie.

Un anneau principal est noethérien. Si A est noethérien, une A -algèbre de type fini est noethérienne.

Definition 2.14. *Soit A un anneau intègre et K son corps des fractions. Soit V un K -espace vectoriel de dimension finie d et M un sous A -module de V . On dit que M est un réseau si M est un A -module de type fini qui engendre V en tant que K -espace vectoriel.*

Exemple : (ω_i) une base de V , $L = \bigoplus_i A\omega_i$. Si $L \subset V$ est un A module libre de rang d , une base de L est une base de V .

Pour un réseau M , il existe un A -module libre $L \subset V$ de rang d et $b \in A$, $b \neq 0$, tels que $L \subset M \subset b^{-1}L$.

Si A est noethérien, et si $M_1 \subset M_2 \subset M_3$ sont trois A -modules $\subset V$, M_1 et M_3 réseaux, entraîne M_2 réseau de V .

Si A est principal, les réseaux M sont obtenus de la manière suivante : on choisit une base (ω_i) de V et $M = \bigoplus A\omega_i$ (un sous-module d'un A module libre de type fini est libre de type fini).

Revenons à $O, F, O', F', F'/F$.

Proposition 2.15. *Soit $x \in F'$ non nul. Il existe $b \in O$ tel que $bx \in O'$*

Si $x^d + \frac{a_i}{b_i}x^i = 0$ est un polynôme annulateur de x , $b = \prod b_i$ convient.

Proposition 2.16. *On suppose O noethérien. Alors O' est un réseau de F' en tant que F -espace vectoriel.*

Soit ω_i une base de F' en tant que F -espace vectoriel. Il existe $b \neq 0$ dans F tel que $b\omega_i$ soit une base de F' et $b\omega_i \in O'$. Soit L le O -module libre engendré par les $b\omega_i$. Il est clair que L , donc O' , engendre F' en tant que F -espace vectoriel. Soit L^\vee le réseau formé des $x \in F'$ tels que $t(xy) \in O$ pour tout $y \in L$. L^\vee est libre sur O de base la base duale d'une base de L . En particulier L^\vee est noethérien. $O' \subset L^\vee$ est de type fini.

On suppose de plus que O est principal. Alors, le réseau O' est un O -module libre de rang d . Soit (ω_i) une base de O' en tant que O -module.

Definition 2.17. *Le discriminant $d(F'/F)$ est le discriminant de O' muni pour la forme bilinéaire $(x, y) \mapsto t(xy)$: c'est $\det(t(\omega_i\omega_j))$. Il est bien défini modulo le carré d'une unité de O .*

Nous noterons $d(F)$ le discriminant $d(F/\mathbb{Z})$. Nous définirons le discriminant $d(F'/F)$ sans l'hypothèse O principal par localisation : $d(F'/F)$ sera un idéal non nul de O .

Soit p un nombre premier. On dit que p est ramifié dans F si p divise le discriminant $d(F)$. Le cardinal des p ramifiés est fini.

Exercice.

1) Entiers des corps quadratiques. Soit $d \in \mathbb{Z}$ sans facteur carré. L'anneau des entiers est $\mathbb{Z}[\sqrt{d}]$ si $d \equiv 2, 3 \pmod{4}$ et $\mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{d}}{2}$ si $d \equiv 1 \pmod{4}$. Le discriminant est $4d$ dans le premier cas et d dans le second.

Soit $\omega_1, \dots, \omega_d$ ($d = [F' : F]$) des éléments de O' qui sont linéairement indépendants sur F . On pose :

$$D(\omega_1, \dots, \omega_d) = \det(t(\omega_i\omega_j)).$$

Si $O = \mathbb{Z}$, $D \in \mathbb{Z}$ est bien défini et ne dépend que du réseau engendré par les ω_i : on le note $D(L)$.

On suppose $O = \mathbb{Z}$. Soient $M_1 \subset M_2$ deux réseaux de F' . M_2/M_1 est fini : on le note $[M_2 : M_1]$.

Proposition 2.18. *On a $D(M_1) = [M_2 : M_1]^2 D(M_2)$.*

Corollaire 2.19. *Soit M un réseau $\subset O'$. Si p ne divise pas $D(M)$, p est non ramifié dans F .*

Proposition 2.20. *Soit $x \in O$ tel que $F = \mathbb{Q}(x)$. Soit M_x le réseau engendré par $1, x, \dots, x^{d-1}$. On a $D(M_x) = N(f'_x(x))$.*

Si x_i sont les différents conjugués de x , $D(M_x) = \prod_{i,j,i \neq j} (x_i - x_j) = \prod_i f'_x(x_i) = N(f'_x(x))$.

Exercices. 1) Soit $\mathbb{Q}(\mu_{p^a})$ le corps cyclotomique. et $M = \mathbb{Z}[\epsilon]$ pour ϵ une racine primitive p^a -ième de l'unité. On a $D(M) = \pm p^s$ avec $s = p^{a-1}(ap - a - 1)$.

2) (difficile) a) Soient $K \subset L \subset M$ trois corps de nombres. Prouver la formule $d(M/K) = N_{L/K}(d(M/L)) \times d(L/K)^{[M:L]}$.

3. ANNEAUX DE DEDEKIND.

Definition 3.1. *Un anneau A est un anneau de Dedekind s'il est noethérien, intègre, intégralement clos, et si tout idéal premier non nul de A est maximal.*

Exemple : un anneau principal. Anneau des fonctions régulières sur une courbe algébrique affine lisse.

Proposition 3.2. *Soient O, F, F' et O' comme dans le numéro précédent (donc F'/F séparable). Supposons que O est un anneau de Dedekind. Alors O' est un anneau de Dedekind.*

En particulier les anneaux d'entiers de corps de nombres sont des anneaux de Dedekind.

O' est noethérien (A noethérien entraîne B A -algèbre de type finie noethérienne). Reste à prouver que tout idéal premier non nul \wp de O' est maximal. $\wp \cap O$ est un idéal premier non nul de O (si $x \in \wp$, $N(x) \in \wp \cap O$). $\wp \cap O$ est un idéal maximal de O et $O/\wp \cap O$ est un corps. O'/\wp est une $O/\wp \cap O$ -algèbre finie intègre, c'est un corps.

Proposition 3.3. *Soit A un anneau de Dedekind et $S \subset A$ une partie multiplicative. Alors $S^{-1}A$ est un anneau de Dedekind.*

Comme A est intègre, noethérien, idem de $S^{-1}A$. On voit facilement que $S^{-1}A$ est intégralement clos. Les idéaux premiers non nuls de $S^{-1}A$ correspondent à ceux de A qui ne rencontrent pas S .

Théorème 3.4. *Soit A un anneau de Dedekind. Tout idéal I distinct de A et (0) admet une factorisation : $I = \prod \wp_i$ en un produit fini d'idéaux premiers non nuls. Cette décomposition est unique à l'ordre des facteurs près.*

Preuve

Lemme 3.5. *Soit I un idéal non nul de A . Il existe des idéaux premiers non nuls \wp_1, \dots, \wp_r de A tels que $\prod \wp_i \subset I$.*

Supposons qu'il existe I ne vérifiant pas la condition du lemme. Soit I un idéal non nul maximal parmi ceux qui ne vérifient pas la propriété du lemme. I n'est pas un idéal premier. Il existe donc b_1 et b_2 avec $b_1 b_2 \in I$, b_1 et b_2 pas dans I . Soient $I_1 = I + (b_1)$ et $I_2 = I + (b_2)$. Par maximalité de I , I_1 et I_2 contiennent des produits d'idéaux premiers non nul. Il en est de même de $I_1 I_2 \subset I$. Contradiction.

Remarque. Nous n'avons utilisé comme seule hypothèse sur A que A est noethérien.

Lemme 3.6. *Soit I un idéal non nul de A et \wp un idéal premier non nul. Alors $\wp^{-1}I \neq I$.*

Prouvons tout d'abord le lemme lorsque $I = A$. Soit $a \in \wp$, $a \neq 0$. Soit r minimal tel qu'il existe \wp_1, \dots, \wp_r avec $\wp_1 \dots \wp_r \subset (a) \subset \wp$. L'un des \wp_i , disons \wp_1 , est inclus dans \wp . On a $\wp = \wp_1$ (car \wp_1 est maximal).

Si $r = 1$, $\wp = (a)$ et $a^{-1} \in \wp^{-1}$ et comme a n'est pas une unité, $\wp^{-1} \neq A$.

Supposons $r \geq 2$. Par minimalité de r , il existe $b \in \wp_2 \dots \wp_r$ avec $b \notin (a)$. Donc $a^{-1}b \notin A$. Mais $a^{-1}b \in \wp^{-1}$ car $b\wp \subset (a)$, donc $\wp^{-1} \neq A$.

Soit $I \neq (0)$ un idéal et supposons $I\wp^{-1} = I$. Soient $\alpha_1, \dots, \alpha_i$ des générateurs de I . Soit $x \in \wp^{-1}$. Il existe des $a_{ij} \in A$ tels que :

$$x\alpha_i = \sum_j a_{ij}\alpha_j.$$

Le déterminant de la matrice $(x\delta_{ij} - a_{ij})$ est nul. Il en résulte que x est entier sur A et $\wp^{-1} = A$. Contradiction.

Remarque Il en résulte que $\wp\wp^{-1} = A$. En effet $\wp \subset \wp\wp^{-1} \subset A$ et $\wp^{-1}\wp \neq \wp$.

Existence de la décomposition en produit d'idéaux premiers.

Soit I maximal $\neq A$ n'admettant pas de décomposition. Il existe \wp tel que $I \subset \wp$ puisque les idéaux maximaux sont les \wp . On a $I \subset I\wp^{-1} \subset \wp\wp^{-1} = A$. Par maximalité de I , $I\wp^{-1}$ est produit de premiers. Contradiction.

Unicité.

Elle résulte de ce que $I_1I_2 \subset \wp$ entraîne $I_1 \subset \wp$ ou $I_2 \subset \wp$ et de ce que les \wp sont maximaux.

Definition 3.7. *Soit $x \in K^*$. Si $(x) = \prod \wp_i^{a_i}$, les \wp_i distincts, on pose $v_{\wp_i}(x) = a_i \in \mathbb{Z}$. Pour $x \in A$, on a $v_{\wp_i}(x) \geq a_i$ si et seulement si $x \in \wp_i^{a_i}$.*

Definition 3.8. *Soit K le corps des fractions de A . Un idéal fractionnaire est un A -module de type fini dans K non réduit à (0) .*

Un idéal fractionnaire est donc un réseau de K . Ils forment un monoïde unitaire. Pour I idéal fractionnaire, I^{-1} est un idéal fractionnaire ($d \in I$, $d \neq 0$ implique $I^{-1} \subset d^{-1}A$). Tout idéal premier est inversible ($\wp\wp^{-1} = A$), donc tout idéal (théorème), puis tout idéal fractionnaire (I fractionnaire implique qu'il existe $d \neq 0$ avec $dI \subset A$). Les idéaux fractionnaires forment un groupe abélien. Il est libre de base formé des \wp . L'inverse de I est I^{-1} .

Appelons le $J(K)$. Soit $P(K)$ le sous-groupe formé des idéaux fractionnaires principaux (libres de rang 1). Le quotient $\text{Cl}(A)$ est le groupe des classes. Il est trivial si et seulement si A est principal. Nous verrons que si K est un corps de nombres, il est fini.

Proposition 3.9. *Pour un anneau A et deux idéaux I_1 et I_2 tels que $I_1 + I_2 = A$, on a $I_1I_2 = I_1 \cap I_2$, $I_1^{a_1} + I_2^{a_2} = A$ pour a_1 et a_2 entiers > 0 , et la flèche $A/I_1I_2 \rightarrow A/I_1 \oplus A/I_2$ est un isomorphisme.*

En effet, il existe $e_1 \in I_2$ et $e_2 \in I_1$ avec $1 = e_1 + e_2$. Si $x \in I_1 \cap I_2$, on a $x = xe_1 + xe_2 \in I_1I_2$.

Elever $1 = e_1 + e_2$ à la puissance $a_1 + a_2$.

La surjectivité de la flèche : prendre $x = x_1e_2 + x_2e_1$. qui s'envoie sur (x_1, x_2) .

Il en résulte que si I_i est une famille finie d'idéaux tels que $I_i + I_j = A$, on a $A/I = \bigoplus A/(I_i)^{a_i}$, $I = \prod I_i^{a_i} = \bigcap I_i^{a_i}$. Si A est de Dedekind, on peut l'appliquer avec $I_i = \wp_i$, les \wp_i étant distincts.

Proposition 3.10. *Soit A un anneau de Dedekind qui n'a qu'un nombre fini d'idéaux premiers. Alors A est principal.*

Applique le lemme chinois avec $x_1 \in \wp_1, x_1 \notin \wp_1^2$, et $x_i \in A, x_i \notin \wp_i$.

Il en résulte que si A est de Dedekind, A_\wp est principal. Ceci permet de définir le discriminant relatif.

Exercice Prouver que pour A Dedekind, tout module de torsion de type fini T est de longueur finie. Définir pour T un idéal généralisant le cardinal de T lorsque $A = \mathbb{Z}$.

Prouver que tout idéal de A est engendré par au plus deux générateurs.

3.1. Anneaux de valuation discrète.

Definition 3.11. *Un anneau de valuation discrète est un anneau principal qui possède un idéal premier non nul et un seul.*

Si A est de Dedekind et \wp est un idéal premier non nul, A_\wp est un anneau de valuation discrète.

Un générateur de l'idéal maximal \mathfrak{m} est appelé une uniformisante. Le spectre contient deux éléments : le point générique (0) et \mathfrak{m} . $k := A/\mathfrak{m}$ est appelé le corps résiduel. Les idéaux non nuls de A sont les (π^a) pour a entier ≥ 0 . Les idéaux fractionnaires sont les (π^a) pour $a \in \mathbb{Z}$. Les k -espaces $\mathfrak{m}^a/\mathfrak{m}^{a+1}$ sont de dimension 1.

Soit F le corps des fractions de A . Tout élément x non nul de F s'écrit de façon unique $\pi^a u$, $a \in \mathbb{Z}$, u unité de A . Les unités de A sont les éléments de A qui n'appartiennent pas à \mathfrak{m} .

On pose $v(x) = a$. La fonction $v : K^* \rightarrow \mathbb{Z}$ vérifie

- v est un homomorphisme de groupes surjectif ;
- $v(x + y) \geq \inf(v(x), v(y))$.

On pose $v(0) = \infty$.

Réciproquement, si K est un corps, et v une fonction comme ci-dessus, l'ensemble des $x \in F$ avec $v(x) \geq 0$ est un sous-anneau de F qui est un anneau de valuation discrète

Exemples. \mathbb{Z}_p ; $K[[X]]$ pour K un corps. v est l'ordre en 0. Ils sont complets.

Si $0 < \alpha < 1$, $x \mapsto \alpha^{v(x)}$ définit une distance sur F qui vérifie $\|x + y\| \leq \max(\|x\|, \|y\|)$. Dans le cas des corps de nombres, on prend souvent $\alpha = 1/N(\wp)$. Alors $\|x\| \times |A/(x)| = 1$ pour tout $x \in A, x \neq 0$

3.2. Décomposition des idéaux premiers dans une extension de corps de nombres. Soit $F \subset F'$ une extension de corps de nombres. Soient $O \subset O'$ les anneaux d'entiers.

Soit \wp un idéal premier (non nul) de O . L'idéal $\wp O'$ admet la décomposition :

$$\wp O' = \prod_{i=1}^r (\wp'_i)^{e_i},$$

où les \wp'_i sont des idéaux premiers (non nuls) de O' .

Proposition 3.12. *Les \wp'_i sont exactement les idéaux premiers \wp' de O' qui sont tels que $\wp' \cap O = \wp$.*

En effet, $\wp' \cap O = \wp$ implique $\wp O' \subset \wp'$ et \wp' intervient dans la décomposition de $\wp O'$. Réciproquement, si \wp' intervient dans cette décomposition, $\wp O' \subset \wp'$, on a $\wp \subset \wp' \cap O$ et $\wp = \wp' \cap O$ car \wp est maximal.

Les \wp' sont appelés les idéaux premiers au dessus de \wp .

Soit \wp' au dessus de \wp . Par la proposition précédente, l'homomorphisme $k_\wp \rightarrow k_{\wp'}$ des corps résiduels est injectif. Comme O' est finie sur O , l'extension résiduelle est finie, on note f_i son degré.

Théorème 3.13. *On a $[F' : F] = \dim_{k_\wp}(O'/\wp O') = \sum_{i=1}^r e_i f_i$.*

$O'/\wp O'$ est un O/\wp -espace vectoriel de dimension finie. Prouvons que sa dimension est $n := [F' : F]$. C'est clair si O est principal. On s'y ramène en localisant avec le lemme suivant. :

Lemme 3.14. *Soient A un anneau de Dedekind et M un A -module de type fini et de torsion. Alors, M admet une décomposition $M = \sum_i (\sum_j (A/\wp_i^{a_i,j}))$. On a : $M_{\wp_i} = \sum_j (A/\wp_i^{a_i,j})$.*

Pour la deuxième égalité de la proposition, utiliser que \wp'^a/\wp'^{a+1} est un $k_{\wp'}$ -espace vectoriel de dimension 1 car $O'_{\wp'}$ est principal.

On dit que \wp est ramifié dans F' si l'un des e_i est > 1 .

Proposition 3.15. *Pour que \wp soit ramifié, il faut et il suffit que \wp divise le discriminant $d(F'/F)$.*

On localise en \wp . Pour que tous les e_i soient 1 il faut et il suffit que $O'/\wp O'$ soit réduit.

Si c'est réduit, c'est un produit d'extensions finies de k_\wp , et le discriminant de la k_\wp -algèbre $O'/\wp O'$ est non nul. Il en résulte que $d(F'/F)$ est une unité.

Si ce n'est pas réduit, le discriminant de k_\wp -algèbre $O'/\wp O'$ est nul (un élément non nul et nilpotent est dans le radical de la forme quadratique). Il en résulte que $d(F'/F)$ n'est pas une unité.

Les \wp ramifiés sont en nombre fini.

On suppose maintenant que F'/F est galoisienne de groupe de Galois G .

Proposition 3.16. *Les premiers \wp' au dessus de \wp sont conjugués sous l'action de G .*

Soit \wp' distinct des $\sigma(\wp'_1)$, $\sigma \in G$. On sait qu'il existe $x \in \wp'$, $x \notin \sigma(\wp'_1)$ pour $\sigma \in G$. Comme $x \in \wp'$, on a : $N(x) \in \wp$. Comme $x \notin \sigma(\wp'_1)$, $\sigma^{-1}(x) \notin \wp'_1$, donc comme \wp'_1 est premier, $N(x) \notin \wp'_1$, contradiction.

Corollaire 3.17. *Sous l'hypothèse F'/F galoisienne, les entiers e_i et f_i ne dépendent pas de i ; notons les e et f . On a $n = ref$*

Soit \wp' fixé. On note $D_{\wp'}$ le sous-groupe de G qui est le stabilisateur de \wp' . C'est le sous-groupe de *décomposition*. Soit $M_{\wp'}$ la sous-extension de F' définie par $D_{\wp'}$. Soit $\wp'' = \wp' \cap M_{\wp'}$. Comme $D_{\wp'}$ fixe \wp' , \wp' est le seul idéal au dessus de \wp'' . On en déduit que si e' et f' sont les degré de inertiels et résiduels de l'extension F'/M , on a : $e'f' = n/r$. On a e' divise e , f' divise f . (formule de multiplicativité : si $F \subset F' \subset F''$: $e(\wp''/\wp) = e(\wp''/\wp')e(\wp'/\wp)$ et idem pour f). Il en suit que $e = e'$ et $f = f'$. Il en résulte que $k_{\wp} = k_{\wp''}$.

Attention : on a $D_{\sigma(\wp')} = \text{int}(\sigma)(D_{\wp})$ (et les sous-groupes de décomposition n'ont pas de raison d'être distingués).

Le groupe $D_{\wp'}$ agit sur le corps résiduel $k_{\wp'}$ en laissant fixes les éléments de k_{\wp} . Il en résulte un morphisme de $D_{\wp'}$ dans $\text{Gal}(k_{\wp'}/k_{\wp})$.

Proposition 3.18. *Ce morphisme est surjectif.*

On peut supposer $F = M$.

Soit \bar{x} un élément primitif de $k_{\wp'}/k_{\wp}$ et soit x un relèvement de \bar{x} . Soient M_x et $M_{\bar{x}}$ les polynômes minimaux. On a $\bar{M}_x(\bar{x}) = 0$, donc $M_{\bar{x}}$ divise \bar{M}_x . Les polynômes M_x et $M_{\bar{x}}$ sont scindés car les extensions F'/M et $k_{\wp'}/k_{\wp}$ sont galoisiennes.

Soit $\bar{\sigma} \in \text{Gal}(k_{\wp'}/k_{\wp})$. $\bar{\sigma}(\bar{x})$ est la réduction d'une racine x' de M_x . Soit $\sigma \in G$ tel que $\sigma(x) = x'$. On voit que la réduction de σ est $\bar{\sigma}$. Cela prouve la proposition.

Definition 3.19. *Le noyau de ce morphisme est appelé le sous-groupe d'inertie : il est noté $I_{\wp'}$.*

Proposition 3.20. *Soit M' le sous-corps de F' correspondant à $I_{\wp'}$. On a $e(F'/M') = e$, $f(F'/M') = 1$; $e(M'/M) = 1$, $f(M'/M) = f$.*

Les extensions $F'/M'/M$ sont galoisiennes. On applique la proposition précédente à l'extension F'/M' ce qui entraîne que $f(F'/M') = 1$. Donc $f(M'/M) = f$. Comme $[M' : M] = f$, on en déduit $e(M'/M) = 1$ et $e(F'/M') = e$.

Supposons \wp non ramifié. Alors $D_{\wp'}$ est isomorphe au groupe de Galois de l'extension résiduelle. Celui-ci est cyclique et engendré par le Frobenius. D'où $\text{Frob}_{\wp'} \in G$, noté parfois $(\wp', F'/F)$. Si G est abélien, $\text{Frob}_{\wp'}$ ne dépend que de \wp : on le note parfois $(\frac{F'/F}{\wp})$.

Parfois implicitement, on note Frob_{\wp} défini qu'à conjugaison près. En particulier lorsque l'on considère une représentation linéaire ρ de G , la notation $\text{tr}(\rho(\text{Frob}_{\wp}))$ n'est pas ambiguë.

Théorème 3.21. *(Cebotarev). Soit C une classe de conjugaison dans G . La densité des \wp qui sont tels que $\text{Frob}(\wp) \in C$ est $|C|/|G|$.*

Exercice.

Soient $F \subset F' \subset F''$ galoisiennes. Soient \wp'' au dessus de \wp' au dessus de \wp . Prouver que les groupes de décomposition vérifient : $D(F''/F')_{\wp''} = D(F''/F)_{\wp''} \cap \text{Gal}(F''/F')$, $D(F'/F)_{\wp'}$ est l'image de $D(F''/F)_{\wp''}$ dans $\text{Gal}(F''/F)$. Idem pour les sous-groupes d'inertie. Quelles relations pour les Frobenius ?

Proposition 3.22. *Soient F un corps de nombres et O l'anneau de ses entiers. Soit \wp un idéal premier non nul de O . Notons v_{\wp} la valuation qu'il définit. Soit $P(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$ un polynôme avec $v_{\wp}(a_i) \geq 1$ et $v_{\wp}(a_0) = 1$. Soit F' le corps de rupture, $F' = F(x)$ pour x racine de P . Alors \wp n'a qu'un seul premier au dessus \wp' . On a $r = f(\wp'/\wp) = 1$ et $e(\wp'/\wp) = n$. La clôture intégrale de O_{\wp} dans F' est $\bigoplus_{i=0}^{n-1} O_{\wp} x^i$.*

Soit \wp' au dessus de \wp et $v = v_{\wp'}$ la valuation définie par \wp' qui prolonge v_{\wp} (à valeurs dans $e^{-1}\mathbb{Z}$). On a $v(x) > 0$, dans $\sum_{i=0}^{n-1} a_i x^i$, a_0 est de plus petite valuation, c'est le seul donc $v(\sum_{i=0}^{n-1} a_i x^i) = 1$, et $v(x) = 1/n$. Donc $e(\wp'/\wp) = n$, $f(\wp'/\wp) = r = 1$.

Soit $b := \sum_{i=0}^{n-1} b_i x^i$ un élément de F' ($b_i \in F$). Comme les valuations des différents termes non nuls sont distinctes, on voit que $v(b) \geq 0$ entraîne $v(b_i x^i) \geq 0$ et donc $v(b_i) \geq 0$ et donc $b_i \in O_{\wp}$.

Exercice Soit O un anneau de valuation discrète de corps des fractions F , d'idéal maximal \mathfrak{m} . Soit $\bar{f} \in k[X]$ un polynôme irréductible unitaire de degré n et soit f un relèvement unitaire de \bar{f} qui est aussi de degré n . Alors $B_f := O[X]/f(X)$ est un anneau de valuation discrète ; on a $f = n$, $r = e = 1$. L'idéal maximal est (\mathfrak{m}, f) .

Preuve. f est irréductible donc B_f est intègre, et est un réseau de $F[X]/f$. Le discriminant de B_f est 1.

Exemples

Corps quadratiques. $\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ sans facteur carré. L'anneau des entiers O est $\mathbb{Z}[\sqrt{d}]$ si $d \equiv 2, 3 \pmod{4}$, et $\mathbb{Z}[X]/(X^2 - X - \frac{d-1}{4})$ si $d \equiv 1 \pmod{4}$. Le discriminant est $4d$ dans le premier cas et d dans le second.

Si p est un nombre premier impair, le localisé $O_{(p)}$ est $\mathbb{Z}[\sqrt{d}]_{(p)}$. p est ramifié si et seulement si p divise d . Si p ne divise pas d , p est décomposé si et seulement si d est un carré modulo p (le symbole de Legendre $(\frac{d}{p}) = 1$), sinon il est inerte.

2 est ramifié si et seulement si $d \equiv 3 \pmod{4}$ ou 2 divise d . Si $d \equiv 1 \pmod{4}$, 2 est non ramifié, décomposé si $d \equiv 1 \pmod{8}$ et inerte si $d \equiv 5 \pmod{8}$.

Corps cyclotomiques. Soit N un entier > 0 . Soit $N = \prod p_i^{n_i}$ la décomposition de N en facteurs carrés. Soit $K = \mathbb{Q}(\mu_N)$. Notons $K_i = \mathbb{Q}(\mu_{p_i^{n_i}})$. Soit G le groupe de Galois. On a un morphisme injectif $\psi : G \rightarrow (\mathbb{Z}/N\mathbb{Z})^*$ donné par l'action de G sur μ_N .

Supposons d'abord $N = p^n$. Le polynôme $(1 + Y)^{p^n} - 1/(1 + Y)^{p^{n-1}} - 1$ est d'Eisenstein pour p , donc irréductible et $e = \phi(p^n)$, $f = r = 1$ proposition 3.22. ψ est bijectif, $G = I_p$ est les autres premiers ne sont pas ramifiés (calcul du discriminant).

Passons au cas général. Les K_i sont linéairement disjoints. En effet $K_i \cap \prod K_j$ est totalement ramifié en p_i (car contenue dans K_i) et non ramifiée en p_i car contenue dans $\prod K_j$. Ceci donne une démonstration de l'irréductibilité des polynômes cyclotomiques. Cela prouve que ψ est bijective. Si l est un entier premier avec N , on note $\sigma_{\bar{l}}$ l'élément de G tel que $\psi(\sigma_{\bar{l}})$ est la réduction modulo N de l .

L'anneau des entiers est $\mathbb{Z}[\epsilon]$, ϵ racine primitive N -ième de l'unité. Le prouver d'abord pour $N = p^n$ (calcul du discriminant et proposition 3.22). Pour le cas général, utiliser le lemme :

Lemme 3.23. *Soient F' et F'' linéairement disjoints sur F , et $M = F'F''$. Supposons F'/F non ramifiée en \wp . Alors l'anneau des entiers de M localisé en \wp est le localisé en \wp de $O_{F'} \otimes_{O_F} O_{F''}$.*

Preuve : si ω_i est une base de $O_{F'}$ localisé en \wp , c'est aussi une base de O_M localisé en tant que $(O_{F''})_{\wp}$ module.

Soit ℓ ne divisant pas N . On a :

$$\text{Frob}_{\ell} = \sigma_{\bar{\ell}}.$$

Ceci résulte de ce que $\sigma_{\bar{\ell}}$ vérifie $\sigma(\epsilon) = \epsilon^{\ell}$ pour toute racine N -ième de l'unité et l'anneau des entiers de $\mathbb{Q}(\mu_N)$ est $\mathbb{Z}[\epsilon]$. Pour ℓ , on a $e = 1$, f est l'ordre de $\bar{\ell}$ dans $(\mathbb{Z}/N\mathbb{Z})^*$.

Remarque. La réduction modulo \mathcal{L} (au dessus de ℓ) de μ_N est injective ($X^N - 1$ est séparable modulo ℓ). μ_p ne se réduit pas injectivement modulo \wp au dessus de p : $\epsilon \in \mu_p$ se réduit en 1 modulo \wp au dessus de p (\wp est engendré par $\epsilon - 1$).

On voit que le théorème de Cebotarev pour le corps cyclotomique $\mathbb{Q}(\mu_N)$ est équivalent au théorème de Dirichlet qui prouve qu'il y a une infinité de premiers dans une progression arithmétique $nN + a$, $a \neq 0$ et N entiers premiers entre eux.

Soit q un nombre premier impair. Soit $q^* = (-1)^{\frac{q-1}{2}}$. Le sous corps quadratique K_q de $F(\mu_q)$ est seulement ramifié en q donc est $\mathbb{Q}(\sqrt{q^*})$. On peut aussi le prouver de façon constructive. Soit τ la somme de Gauss : $\tau = \sum_{x \in F_q^*} \left(\frac{x}{q}\right) \epsilon^x$ où ϵ est une racine primitive q -ième de 1. Elle dépend du choix de ϵ : si on remplace ϵ par ϵ^a , a premier à q , on multiplie la somme de Gauss par $\left(\frac{a}{q}\right)$. Un calcul prouve : $\tau^2 = q^*$.

Soit p premier impair $\neq q$ et soit $f \in \{\pm 1\}$ le Frobenius Frob_p dans l'extension quadratique. On a $f = \left(\frac{q^*}{p}\right)$. Par ailleurs, f est l'image du Frobenius $\left(\frac{\mathbb{Q}(\mu_q)/\mathbb{Q}}{p}\right)$ dans $\{\pm 1\} = \text{Gal}(K_q/\mathbb{Q})$. C'est donc $\left(\frac{p}{q}\right)$. D'où la loi de réciprocité quadratique :

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

Remarque. On a le théorème de Kronecker-Weber. Soit F une extension finie galoisienne de \mathbb{Q} avec $\text{Gal}(F/\mathbb{Q})$ abélienne. Alors il existe N tel que $F \subset \mathbb{Q}(\mu_N)$.

Exercice Soit L un corps de nombres, extension de \mathbb{Q} avec groupe de Galois isomorphe au groupe des permutations S_3 . Soit K un sous corps de degré 3 de \mathbb{Q} . Pour p nombre premier décrire la décomposition de p dans L selon celle de p dans K .

3.3. Géométrie des nombres. Soit $F \subset \mathbb{C}$ un corps de nombres de degré n . Soient $\sigma_1, \dots, \sigma_n$ les différents plongements de F dans \mathbb{C} . Soit c la conjugaison complexe. On numérote les σ_i de sorte que $\sigma_1, \dots, \sigma_{r_1}$ soient à valeurs réelles, et σ_{r_1+j} soit conjugué de $\sigma_{r_1+j+r_2}$ pour $1 \leq j \leq r_2$, $r_1+2r_2 = n$ ($\sigma_{r_1+j+r_2} = c\sigma_{r_1+j}$).

Exercice Soient K, L comme dans l'exercice précédent. Déterminer r_1 et r_2 pour les corps K et L selon les cas.

On note $\underline{\sigma} : F \rightarrow \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2} = \mathcal{L}^{r_1, r_2}$ le morphisme de \mathbb{Q} -algèbres $x \mapsto (\sigma_i(x))$, pour $1 \leq i \leq r_1 + r_2$.

Proposition 3.24. *Soit M un réseau de F . Alors $\underline{\sigma}(M)$ est un réseau de $\mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$, de volume (par rapport à la base $(1, \dots, 1, 1, i, 1, i, \dots, 1, i)$) $2^{-r_2} |\det_{1 \leq i, j \leq n}(\sigma_i(x_j))|$, x_j base de M .*

Considérons le déterminant $n \times n$ dont les colonnes sont

$$(\sigma_1(x), \dots, \sigma_{r_1}(x), \operatorname{re}(\sigma_{r_1+1}(x)), \operatorname{im}(\sigma_{r_1+1}(x)), \dots)$$

pour $x = x_j$. Si on remplace les lignes $L := L_{r_1+k}$ et $L' := L_{r_1+r_2+k}$ par les lignes $L + iL'$, $L - iL'$ on obtient, aux signe et une puissance de i près 2^{-r_2} fois le déterminant $|\det_{1 \leq i, j \leq n}(\sigma_i(x_j))|$. Ce dernier déterminant est non nul, ce qui prouve que le premier aussi est non nul et que $\underline{\sigma}(M)$ est bien un réseau. On a aussi le volume.

Exemples. Si M est l'anneau des entiers, le volume est $2^{-r_2} |d(F)|^{1/2}$. Si M est un idéal \mathfrak{a} , c'est $2^{-r_2} |d(F)|^{1/2} N(\mathfrak{a})$. $N(\mathfrak{a})$ le cardinal de O_F/\mathfrak{a} .

Exercices.

Étendre la définition de N aux anneaux de Dedekind et aux idéaux fractionnaires par la formule $N(\mathfrak{a}) = \prod_v |k_v|^{v(\mathfrak{a})}$. Pour \mathfrak{a} un idéal, $N(\mathfrak{a}) = 1$ entraîne $\mathfrak{a} = (1)$ (attention ce n'est pas vrai en général pour les idéaux fractionnaires).

Soient c_1, \dots, c_n des réels > 0 et (a_{ij}) une matrice à coefficients réels. On suppose $c_1 \dots c_n > |\det(a_{ij})| > 0$. Prouver qu'il existe des entiers $x_i \in \mathbb{Z}$, $1 \leq i \leq n$, tels que $|\sum_{1 \leq j \leq n} a_{ij} x_j| < c_i$ pour $1 \leq i \leq n$.

Soit V un \mathbb{R} -espace vectoriel de dimension finie n . Une base de $\wedge^d V$ définit une mesure de Haar μ sur V et pour tout réseau (complet : de rang n) L de V son volume $v(L)$.

Théorème 3.25. *(Minkowski 1864-1909) Soit L un réseau de V et soit S une partie de intégrable de V telle que $\mu(S) > v(L)$. Alors, il existe deux éléments x et y distincts de S tels que $x - y \in L$.*

Soit \underline{e} une base de V de déterminant 1 et soit $P_{\underline{e}}$ le parallélotope formé des éléments de V de coordonnées $\in [0, 1[$ dans la base \underline{e} . Comme S est la

réunion disjointe des $S \cap (l + P_{\underline{e}})$, $l \in L$, on a, en utilisant l'invariance de la mesure de Haar par translation :

$$\mu(S) = \sum_{l \in L} \mu(S \cap (l + P_{\underline{e}})) = \sum_{l \in L} \mu((-l + S) \cap P_{\underline{e}}).$$

Comme $\mu(S) > v(L)$, les ensembles $(-l + S) \cap P_{\underline{e}}$ ne peuvent être disjoints et il existe l_1 et l_2 deux éléments distincts de L et deux éléments x et y de S tels que $-l_1 + x = -l_2 + y$. On a : $x - y \in L$ et $x \neq y$ car $l_1 \neq l_2$.

Corollaire 3.26. *Soit L un réseau de V et S une partie intégrable symétrique par rapport à 0 et convexe. Supposons que $\mu(S) > 2^n v(L)$ ou que $\mu(S) \geq 2^n v(L)$ et S est compacte. Alors $S \cap L$ contient un élément non nul.*

On applique le théorème à $1/2S$. Il existe deux éléments distincts x et y de $1/2S$ avec $z := x - y \in L$. On a $z \neq 0$ et $z = 1/2(2x + (-2)y) \in S$. Ceci prouve la première partie de la proposition.

Pour la seconde, appliquons la première partie à $(1 + \epsilon_n)S$, $\epsilon_n > 0$ ayant pour limite 0. On obtient $x_n \in (1 + \epsilon_n)S \cap L$, $x_n \neq 0$. On peut supposer la suite (x_n) convergente. Elle devient stationnaire pour n grand ; soit $x \neq 0$ sa limite. On a $x \neq 0$, $x \in L$ et $x \in (1 + \epsilon_n)S$ pour n grand, donc $x \in S$.

Théorème 3.27. *Soit F comme ci-dessus un corps de nombres de discriminant d et \mathfrak{a} un idéal de $O := O_F$. Alors \mathfrak{a} contient un élément non nul x avec :*

$$|N_{F/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2} N(\mathfrak{a}).$$

Soit dans $(\mathbb{R})^{r_1} \times (\mathbb{C})^{r_2}$ le convexe symétrique par rapport à l'origine

$$B_t := \{(y_i, z_j), \sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |z_j| \leq t\}.$$

Il n'est pas très difficile de prouver que (voir le livre de Samuel) :

$$\mu(B_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}.$$

On choisit t de sorte que $\mu(B_t) = 2^n v(\underline{\sigma}(\mathfrak{a}))$ où $\underline{\sigma}$ est le plongement de F dans $(\mathbb{R})^{r_1} \times (\mathbb{C})^{r_2}$. On trouve

$$t^n = (4/\pi)^{r_2} n! |d|^{1/2} N(\mathfrak{a}).$$

Il existe un élément non nul $x \in \mathfrak{a}$ tel que $\underline{\sigma}(x) \in B_t$. On a (concavité du log) :

$$|N_{F/\mathbb{Q}}(x)| \leq \left(1/n \sum_{i=1}^{r_1} |\sigma_i(x)| + 2/n \sum_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|\right)^n \leq t^n/n^n.$$

Le théorème en résulte.

Théorème 3.28. *Toute classe d'idéaux de F contient un idéal entier \mathfrak{b} tel que :*

$$N(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2}.$$

Soit \mathfrak{a}' un idéal de la classe donnée. Quitte à remplacer \mathfrak{a}' par son produit avec un idéal principal, on peut supposer que $\mathfrak{a} := \mathfrak{a}'^{-1}$ est entier. Il existe $x \in \mathfrak{a}$ avec $|N_{F/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2} N(\mathfrak{a})$. On a : $x\mathfrak{a}'$ entier, de la classe de \mathfrak{a}' , et $N_{F/\mathbb{Q}}(x\mathfrak{a}') \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2}$.

Corollaire 3.29. *Le nombre de classes de F est fini.*

Le corollaire résulte du corollaire précédent et de la finitude des idéaux entiers de norme donnée.

Corollaire 3.30. *Pour tout $n \geq 2$, on a : $|d| \geq (\pi/3)(3\pi/4)^{n-1}$.*

Comme $|N(\mathfrak{b})| \geq 1$, on a $|d|^{1/2} \geq (\pi/4)^{r_2} \frac{n!}{n^n}$. D'où : $|d| \geq a_n$ avec $a_n = (\pi/4)^n n^{2n}/(n!)^2$. On a : $a_2 = \pi^2/4$ et $a_{n+1}/a_n = (\pi/4)(1 + 1/n)^{2n} \geq 3\pi/4$. Ceci donne le corollaire.

Remarque. Odlyzko a amélioré dans les années 70 ces inégalités en utilisant les fonctions L . Par exemple : $|d| \geq (60.1)^{r_1} (22.2)^{2r_2} e^{-254}$.

Corollaire 3.31. *(Hermite-Minkowski) Si $F \neq \mathbb{Q}$, on a $|d| > 1$.*

Théorème 3.32. *Dans \mathbb{C} , il n'y a qu'un nombre fini de corps de nombres de discriminant d donné.*

Le degré est majoré, disons par n .

Supposons $r_1 \neq 0$. Soit σ_1 un plongement réel. Soit $C(d) > 0$ tel que l'ensemble des $x \in O$ tels que $|\sigma_1(x)| \leq C(d)$, $|\sigma_i(x)| \leq 1/2$ pour $i \geq 2$, contienne un élément non nul. Alors x est un élément primitif. En effet, $|N(x)| \geq 1$ implique $\sigma_1(x) \geq 1$ et donc $\sigma_1(x) \neq \sigma_i(x)$ pour $i \geq 2$. Les fonctions symétriques élémentaires de x sont bornés en fonction de n .

Si $r_1 = 0$, on fait un raisonnement similaire en prenant $C(d)$ tel que l'ensemble des $x \in O$ tel que $\text{re}(\sigma_1(x)) \leq C(d)$, $\text{re}(\sigma_2(x)) \leq 1/2$ et $|\sigma_i(x)| \leq 1/2$ pour $i \geq 2$, possède un élément non nul.

Soit E_F le groupe des unités de O_F . Il contient le sous-groupe μ_F des racines de l'unité de F . Il n'est pas difficile de prouver que μ_F est fini (voir ci-dessus ou utiliser ce que l'on sait sur les groupes de Galois des extensions cyclotomiques). Soit $r = r_1 + r_2$.

Théorème 3.33. *(Dirichlet) Le quotient E_F/μ_F est un groupe abélien libre de rang $r - 1$.*

Soit $L : E_F \rightarrow \mathbb{R}^r$ le morphisme de groupes qui envoie ϵ sur $(\ln(|\sigma_1(\epsilon)|), \dots, \ln(|\sigma_{r_1+1}(\epsilon)|^2), \dots)$. Soit $s : \mathbb{R}^r \rightarrow \mathbb{R}$ l'application linéaire somme des coordonnées.

Lemme 3.34. *$L(E_F)$ est un réseau (sous-groupe discret) de $H := \ker(s)$.*

$L(E_F)$ est tué par s car les éléments de E_F ont une norme égale à ± 1 . Notons \mathcal{L}^{r_1, r_2} la \mathbb{R} -algèbre $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ de sorte que $\underline{\sigma}$ identifie $O = O_F$ à un réseau complet de \mathcal{L}^{r_1, r_2} . Soit $l : (\mathcal{L}^{r_1, r_2})^* \rightarrow \mathbb{R}^r$ le morphisme de groupes $(x_1, \dots, x_{r_1+1}, \dots) \mapsto (\ln(|x_1|), \dots, \ln(|x_{r_1+1}|^2), \dots)$. On a donc $L = l \circ \underline{\sigma}$.

On a le sous-lemme :

Lemme 3.35. *Soit K un compact de H . Alors $l^{-1}(K)$ est compact.*

L'ensemble $l^{-1}(K)$ est un fermé de $(\mathcal{L}^{r_1, r_2})^*$. Si $l(x_1, \dots) \in K$, il existe $M > 0$ tel que $\ln(|x_i|) \leq M$. Comme $\prod_{1 \leq i \leq r_1} |x_i| \prod_{r_1+1 \leq i \leq r} |x_i|^2 = 1$, il existe $M' > 0$ avec $M' \leq |x_i|$. Cela prouve le sous-lemme.

Prouvons le lemme. Soit K un compact de H . Alors $K \cap L(E_F)$ est dans l'image par l de $l^{-1}(K) \cap \underline{\sigma}(E_F)$ qui est fini par le sous-lemme puisque $\underline{\sigma}(O)$ est discret dans \mathcal{L}^{r_1, r_2} et $l^{-1}(K)$ est compact. Donc $L(E_F)$ est un réseau de H (il pourrait être incomplet). De plus, le noyau de L est fini, donc est μ_F qui est fini.

Pour prouver que $L(E_F)$ est un réseau complet, il suffit de trouver un compact K de H tel que $H = K + L(E_F)$. Soit S le groupe des éléments de $(\mathcal{L}^{r_1, r_2})^*$ qui sont dans le noyau de $N_{\mathcal{L}} := s \circ l$. Comme $l(S) = H$, il suffit de trouver un compact Z de S tel que $Z\underline{\sigma}(E_F)$ recouvre S .

Soit $y \in S$. Le volume $v(y\underline{\sigma}(O))$ du réseau $y\underline{\sigma}(O)$ ne dépend pas du choix de y . Il existe donc un compact Z_0 de \mathcal{L}^{r_1, r_2} convexe symétrique par rapport à l'origine tel que pour tout $y \in S$, $y\underline{\sigma}(O)$ contienne un élément z_y de Z_0 non nul : $y\underline{\sigma}(z_y) = z_y$. On a que $N(x_y) = N_{\mathcal{L}}(z_y)$ est bornée indépendamment de y . Il existe alors un nombre fini de $x_i \in O_F$, non nuls, tels que les idéaux (x_y) soient égaux l'un des (x_i) : $x_y = x_i \epsilon_y$. On a $y = \underline{\sigma}(\epsilon_y^{-1}) \underline{\sigma}(x_i^{-1}) z_y$. On note $Z_1 = \cup_i \underline{\sigma}(x_i^{-1}) Z_0$. On prend $Z = Z_1 \cap S$.

Exemple. Corps quadratiques $K = \mathbb{Q}(\sqrt{d})$, d sans carré. Si $d > 0$ $r_1 = 2, r_2 = 0$. Le groupe des unités est réduit à celui des racines de l'unité : μ_4 si $d = -1$ et μ_6 si $d = -3$.

Supposons $d > 0$ et $K \subset \mathbb{R}$ avec $\sqrt{d} > 0$. Le groupe des unités > 0 est isomorphe à \mathbb{Z} donc a un unique générateur > 1 : elle est appelé unité fondamentale ϵ .

On a $\epsilon = a + b\sqrt{d}$ avec $a, b, > 0$ et a et b entiers si $d \equiv 2, 3 \pmod{4}$ et simultanément entiers ou demi-entiers, si $d \equiv 1 \pmod{4}$. Dans le premier cas, les solutions de l'équation de Pell $x^2 - dy^2 = \pm 1$, $x, y > 0$ sont données par les puissances de l'unité fondamentale : $x + y\sqrt{d} = (a + b\sqrt{d})^n$, $n \geq 1$ entier. Dans le second cas, l'indice des unités de $\mathbb{Z}[\sqrt{d}]$ dans celles de l'anneau des entiers O est 1 ou 3 ($O/2O$ est soit $\mathbb{F}_2 \oplus \mathbb{F}_2$ soit \mathbb{F}_4). Les solutions de l'équation de Pell sont données par les puissances ϵ^n (resp. ϵ^{3n}) de l'unité fondamentale.

4. FONCTIONS L .

4.1. Le théorème de la progression arithmétique.

Théorème 4.1. (*Dirichlet*) Soit a et m deux entiers ≥ 1 premiers entre eux. Alors il existe une infinité de nombres premiers p tels que $p \equiv a \pmod{m}$.

Fonction ζ de Riemann.

On a $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. La série converge uniformément et normalement dans le domaine $\operatorname{re}(s) \geq 1 + \delta$ pour $\delta > 0$. On a dans ce domaine la formule d'Euler, p d'crivant les nombres premiers :

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}.$$

Preuve. Il s'agit de prouver la convergence de la série des logarithmes. Soit E le produit : $\log(E(s)) = \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{ns}}$. La série des normes est majorée par $\sum_p \sum_{n=1}^{\infty} (\frac{1}{p^{1+\delta}})^n$, majoré par $\sum_p \frac{1}{p^{1+\delta}-1} \leq 2 \sum_p \frac{1}{p^{1+\delta}}$. Ceci donne la convergence du produit E . Soit $N > 0$. La série développée de $\zeta(s) - \prod_{p \leq N} \frac{1}{1-p^{-s}}$ ne comporte que des termes $\frac{1}{n^s}$ pour $n \geq N$, ce qui prouve $E = \zeta$.

La fonction ζ admet un prolongement méromorphe à \mathbb{C} avec comme unique pôle $s = 1$ qui est simple et a pour résidu 1. Pour le théorème il suffit de prouver que $\zeta(s) = 1/(s-1) + \phi(s)$ avec ϕ holomorphe pour $\operatorname{re}(s) > 0$. On écrit pour $\operatorname{re}(s) > 1$: $\zeta(s) = 1/(s-1) + \sum_{n=1}^{\infty} (1/n^s - \int_n^{n+1} t^{-s} dt)$. On pose $\phi_n(s) = \int_n^{n+1} (n^{-s} - t^{-s}) dt$ pour $\operatorname{re}(s) > 0$. On a les majorations $|\frac{1}{n^s} - \frac{1}{t^{-s}}| \leq \frac{|s|}{n^{\operatorname{re}(s)+1}}$, $|\phi_n(s)| \leq |s| \int_n^{n+1} t^{-\operatorname{re}(s)-1} dt$. On en déduit le prolongement analytique de $\phi = \sum \phi_n$ pour $\operatorname{re}(s) > 0$.

Fonctions L de Dirichlet.

Faisons quelques rappels sur les séries de Dirichlet.

Théorème 4.2. Soit $\sum_{n=1}^{\infty} a_n/n^s$, $a_n \in \mathbb{C}$, une série de Dirichlet.

1) Si elle converge pour $s_0 \in \mathbb{C}$, elle converge uniformément dans tout secteur angulaire $|\arg(s - s_0)| \leq \alpha < \pi/2$ du demi-plan $\operatorname{re}(s - s_0) > 0$.

2) Si les sommes $\sum_{n=m}^{m'} a_n$ sont bornés, la série converge uniformément sur tout compact contenu dans le demi-plan $\operatorname{re}(s) > 0$.

Il résulte du théorème qu'on peut définir une abscisse de convergence absolue σ_{abs} (réel ou infini) comme l'inf des réels tels que la série converge absolument. Elle converge alors absolument pour $\operatorname{re}(s) > \sigma_{\text{abs}}$. Si la série converge pour un s_0 , on note $f(s)$ la fonction holomorphe pour $\operatorname{re}(s) > \sigma_{\text{abs}}$ somme de la série de Dirichlet.

Théorème 4.3. (*Landau*). Supposons que les a_n sont réels ≥ 0 et que σ_{abs} soit fini. Alors, la fonction f n'admet pas de prolongement analytique sur aucun voisinage de σ_{abs} .

Soit χ un caractère de $(\mathbb{Z}/m\mathbb{Z})^*$. On le prolonge par 0 pour les éléments de $\mathbb{Z}/m\mathbb{Z}$ qui ne sont pas inversibles. On forme la série : $L(s, \chi) = \sum_{n=1}^{\infty} \chi(n)/n^s$. Elle est absolument convergente pour $\operatorname{re}(s) > 1$. La fonction χ est multiplicative (au sens strict) : $\chi(a_1 a_2) = \chi(a_1) \chi(a_2)$ pour a_1 et a_2 entiers. Il

en résulte le produit eulérien $L(s, \chi) = \prod_p \frac{1}{(1-\chi(p)p^{-s})}$ pour $\text{re}(s) > 1$. On a prolongement holomorphe pour $\text{re}(s) > 0$ grâce au théorème et à la propriété : l'orthogonalité des caractères entraîne que $\sum_n^{n+m-1} \chi(n) = 0$.

On note ζ_m la fonction zeta du corps cyclotomique $\mathbb{Q}(\mu_m)$: $\zeta_m(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$ \mathfrak{a} décrivant les idéaux entiers de $\mathbb{Q}(\mu_m)$ (convergence pour $\text{re}(s) > 1$). Elle admet un produit eulérien : $\zeta_m(s) = \prod_{\mathfrak{p}} \frac{1}{1-N(\mathfrak{p})^{-s}}$, \mathfrak{p} décrivant les idéaux premiers non nuls de $\mathbb{Q}(\mu_m)$.

Théorème 4.4. Soit $G(s) = \prod_{\mathfrak{p}|n} \frac{1}{(1-N(\mathfrak{p})^{-s})}$. On a : $\zeta_m(s) = G(s) \prod_{\chi} L(s, \chi)$.

Soit p un nombre premier à m quelconque. Il suffit de prouver que : $\prod_{\mathfrak{p}|p} (1-N(\mathfrak{p})^{-s}) = \prod_{\chi} (1-\chi(p)p^{-s})$. Soit $G = \mathbb{Z}/m\mathbb{Z}$, \hat{G} le groupe dual et H le sous-groupe de \hat{G} orthogonal du sous-groupe $\langle \bar{p} \rangle$ de G engendré par \bar{p} dans $G = \mathbb{Z}/m\mathbb{Z}$. On a pour la décomposition de (p) dans $\mathbb{Q}(\mu_m)$: $e = 1$, f est l'ordre de \bar{p} dans G et r est l'ordre du groupe H . On pose $X = p^{-s}$. On a $\prod_{\mathfrak{p}|p} (1-N(\mathfrak{p})^{-s}) = (1-X^f)^r$ et $\prod_{\chi} (1-\chi(p)p^{-s}) = \prod_{\chi'} (1-\chi'(p)X)^r$ χ' décrivant \hat{G}/H , qui est cyclique d'ordre f . Le théorème est alors clair.

Théorème 4.5. On a pour $\chi \neq 1$, $L(\chi, 1) \neq 0$.

D'après le théorème de Landau, il suffit de prouver que la série de Dirichlet de $\zeta_m(s)$ ne converge pas pour un s réel > 0 . On a pour $s > 0$:

$$\sum_{\mathfrak{a}} 1/N(\mathfrak{a})^s = \prod_{\mathfrak{p}} (1 + N(\mathfrak{p})^{-s} + N(\mathfrak{p})^{-2s} + \dots) \geq \zeta(s\phi(m)),$$

la dernière inégalité résultant de $N(\mathfrak{p}) \leq p^{\phi(m)}$. Le théorème en résulte.

Prouvons le théorème de la progression arithmétique. Soit a premier à m . On a :

$$\log L(\chi)(s) = \sum_p \sum_{m=1}^{\infty} \frac{\chi(p^m)}{mp^{ms}} = \sum_p \frac{\chi(p)}{p^s} + g_{\chi}(s),$$

la série $g_{\chi}(s)$ convergent pour $\sigma > 1/2$. En effet $\sum_{p,k \geq 2} 1/p^{ks} \leq \sum_p 1/p^s (p^s - 1)$. On obtient :

$$\sum_{\chi} \chi(a)^{-1} \log L(\chi, s) = \sum_{\chi} \sum_p \frac{\chi(a^{-1}p)}{p^s} + g(\chi)$$

soit avec les relations d'orthogonalité des caractères :

$$\sum_{p \equiv a(m)} \frac{\phi(m)}{p^s} + g(s).$$

On voit que $\sum_{p \equiv a(m)} \frac{1}{p^s}$ est équivalent lorsque s tend vers 1 à $1/\phi(m) \log(1/(s-1))$.

4.2. Formule analytique du nombre de classes. Soit K un corps de nombres et ζ_K sa fonction ζ de Dedekind.

Théorème 4.6. *On a :*

$$\lim_{s \rightarrow 1^+} (s-1)\zeta_K(s) = \frac{2^{r_1+r_2}\pi^{r_2}R}{m\sqrt{d(K)}}h$$

où $d(K)$ est le discriminant, m le nombre de racines de l'unité dans K , R le régulateur et h le nombre de classes.

Rappelons la définition du régulateur. Soit dans \mathbb{R}^r ($r = r_1 + r_2$) le vecteur $l_0 = 1/\sqrt{r} \times (1, \dots, 1)$. Il est orthogonal à l'hyperplan $\ker(s)$ et normé. Le volume de $L(E_K)$ est la valeur absolue du déterminant dont les lignes sont $l_0, L(\epsilon_1), \dots, L(\epsilon_{r_1+r_2-1})$. Si on ajoute à la i -ème colonne la somme des autres, nous voyons que ce volume $\sqrt{r}R$ où le régulateur est la valeur absolue de chacun des mineurs d'ordre $r-1$ de la matrice $(r-1) \times r$ de terme général $l_j(\epsilon_i)$.

On a $\zeta(s) = \sum \frac{1}{N(\mathfrak{a})^s}$. Soit C un classe. Soit \mathfrak{a}' un idéal entier dans C^{-1} . On a $\zeta(s) = \sum_C f_C(s)$ où $f_C(s) = N(\mathfrak{a}')^s \sum_{(\alpha)} \frac{1}{|N(\alpha)|^s}$, la somme étant étendue aux (α) , $\alpha \equiv 0 \pmod{\mathfrak{a}'}$ (ces conditions ne dépendant que de l'idéal (α)). On se fixe C et on considère $f_C(s)$.

Introduisons un domaine fondamental X pour l'action de E_K sur \mathcal{L}^{r_1, r_2} . Soit l^* le vecteur de \mathbb{R}^r dont les r_1 premières coordonnées sont 1 et les r_2 autres sont 2.

$$l^* = (1, \dots, 1, 2, \dots, 2) \in \mathbb{R}^r.$$

Les vecteurs $l^*, L(\epsilon_1), \dots, L(\epsilon_{r_1+r_2-1})$ forment une base de \mathbb{R}^r . On prend pour indices des coordonnées $0, 1, \dots, r-1$: pour $N_{\mathcal{L}}(x) \neq 0$, on note :

$$l(x) = \xi_0 l^* + \xi_1 l(\epsilon_1) + \dots + \xi_{r-1} l(\epsilon_{r-1}).$$

$X \subset \mathcal{L}^{r_1, r_2}$ est défini par :

- $N_{\mathcal{L}}(x) \neq 0$ (i.e. chacun des x_i est $\neq 0$) ;
- $\xi_i(x) \in [0, 1[$ pour $1 \leq i \leq r-1$;
- $0 \leq \arg(x_1) < 2\pi/m$.

Si K admet un plongement réel, la dernière condition signifie $x_1 > 0$.

C'est un cône. En effet, on a pour ξ réel : $l(\xi x) = \log(\xi)l^* + l(x)$ donc $\xi_i(x) = \xi_i(\xi x)$ pour $1 \leq i \leq r-1$, $N_{\mathcal{L}}(\xi x) = \xi^n N_{\mathcal{L}}(x)$ et $\arg(\xi x_1) = \arg(x_1)$.

Théorème 4.7. *Dans toute classe d'entiers associés (par multiplication par une unité), il existe un et un seul représentant qui est dans X .*

Soit M l'image par σ de \mathfrak{a}' . On a :

$$f_C(s) = N(\mathfrak{a}')^s \sum_{x \in M \cap X} \frac{1}{N(x)^s}.$$

On a le théorème suivant qui donne une formule pour le comportement pour s tendant vers 1 de telles sommes.

On se donne dans \mathbb{R}^n un cône ne contenant pas 0 et une fonction F sur X à valeurs réelles > 0 et un réseau M vérifiant les propriétés suivantes :

- $F(\xi x) = \xi^n F(x)$ pour $\xi \in \mathbb{R}^r$
- L'ensemble T des $x \in X$ tels que $F(x) \leq 1$ est borné et a un volume non nul v .

Posons :

$$\tilde{\zeta}(s) = \sum_{x \in X \cap M} \frac{1}{F(x)^s}.$$

Théorème 4.8. *La série ci-dessus est convergente pour $s > 1$ et :*

$$\lim_{s \rightarrow 1} (s-1)\tilde{\zeta}(s) = v/\Delta,$$

où Δ est le volume de M

Ordonnons les éléments de $M \cap X$ de sorte que $0 < F(x_1) \leq F(x_2) \leq \dots \leq F(x_k)$: c'est possible car T est borné.

Soit $r > 0$. Soit $N(r)$ est le nombre de points de M contenu dans rT i.e. le nombre de points de $M \cap X$ tels que $F(x) \leq r^n$. C'est encore le nombre d'éléments de $(1/rM) \cap T$ et on a :

$$v = v(T) = \lim_{r \rightarrow \infty} N(r)\Delta/r^n.$$

Les points x_1, \dots, x_k appartiennent à $r_k T$ ($r_k = F(x_k)^{1/n}$). Par suite, $N(r_k) \geq k$. De plus, pour tout $\epsilon > 0$, $x_k \notin (r_k - \epsilon)T$ et $N(r_k - \epsilon) < k$. On en déduit :

$$\lim_{k \rightarrow \infty} \frac{k}{F(x_k)} = v/\Delta.$$

Soit $\epsilon > 0$. Il existe k_0 tel que pour $k \geq k_0$:

$$\left(\frac{v}{\Delta} - \epsilon\right)1/k < \frac{1}{F(x_k)} < \left(\frac{v}{\Delta} + \epsilon\right)1/k.$$

d'où (pour s réel > 1) :

$$\left(\frac{v}{\Delta} - \epsilon\right)^s \sum_{k_0}^{\infty} 1/k^s < \sum_{k=k_0}^{\infty} \frac{1}{F(x_k)^s} < \left(\frac{v}{\Delta} + \epsilon\right)^s \sum_{k_0}^{\infty} 1/k^s.$$

d'où la convergence. Faisons tendre s vers 1 :

$$v/\Delta - \epsilon \leq \underline{\lim}(s-1)\tilde{\zeta}(s) \leq \overline{\lim}(s-1)\tilde{\zeta}(s) \leq v/\Delta + \epsilon.$$

Cela prouve le théorème.

Démontrons que X est bien un domaine fondamental.

Soit $y \in \mathcal{L}^{r_1, r_2^*}$. On a $l(y) = \xi_0 l^* + \xi_1 l(\epsilon_1) + \dots$. On multiplie y par une unité η de sorte que $\xi_i(x\eta) \in [0, 1[$. En multipliant par une racine m -ième de l'unité, on obtient la condition sur l'argument de ξ_1 .

On conclue avec les formules $v = 2^{r_1} \pi^{r_2} R/m$ et $\Delta = 1/2^{r_2} N(\mathfrak{a}')\sqrt{d}$.

4.3. **Calcul de $L(\chi, 1)$.** Soit m un entier ≥ 1 .

Soit $\chi : \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{C}^*$ un caractère de Dirichlet. Soit m' un diviseur de m . Soit χ' un caractère de Dirichlet modulo m' . On dit que χ' induit χ si χ et χ' coïncident pour x premier à m . On dit que χ est *primitif* s'il n'est pas induit d'un caractère de Dirichlet modulo un diviseur strict m' de m . C'est équivalent à la propriété suivante : pour tout diviseur strict m' de m , il existe z premier à m tel que $z \equiv 1 \pmod{m'}$ et $\chi(z) \neq 1$.

Le théorème 4.4 peut s'écrire (exercice) :

$$\zeta_K(s) = \prod_{d|m} \prod_{\chi} L(\chi, s),$$

où les χ décrivent les caractères primitifs modulo d .

On suppose désormais sauf indiqué que χ est primitif modulo m .

$$L(\chi, s) = \sum_{k=1}^{\infty} \chi(k) k^{-s} = \sum_x \chi(x) \sum_{n \equiv x \pmod{m}} 1/n^s,$$

x décrivant un système de représentants de $\mathbb{Z}/m\mathbb{Z}$. Posons $\zeta = \cos(2\pi/m) + i \sin(2\pi/m)$. On a : $\sum_{k=0}^{m-1} \zeta^{rk}$ est 0 sauf si $r \equiv 0 \pmod{m}$, auquel cas la somme vaut m . On en déduit que la fonction de Dirac δ_x pour x entier modulo m peut s'écrire $\delta_x(n) = 1/m \sum_k \zeta^{(x-n)k}$.

On voit :

$$L(\chi, s) = 1/m \sum_{k=0}^{m-1} \left(\sum_{(x,m)=1} \chi(x) \zeta^{xk} \right) \sum_{n=1}^{\infty} \zeta^{-nk} / n^s.$$

On note $\tau_a(\chi)$ la somme de Gauss : $\sum_{(x,m)=1} \chi(x) \zeta^{xa}$. Elle est nulle si $a \equiv 0 \pmod{m}$. On en déduit :

$$L(\chi, 1) = 1/m \sum_{k=1}^{m-1} \tau_k(\chi) \sum_{n=1}^{\infty} \zeta^{-nk} / n.$$

On a : $\sum_{n=1}^{\infty} \zeta^{-nk} / n = -\log(1 - \zeta^{-k})$, le logarithme ayant une partie imaginaire $\in]-\pi/2, \pi/2[$. Finalement :

$$L(\chi, 1) = -1/m \sum_{k=1}^{m-1} \tau_k(\chi) \log(1 - \zeta^{-k}).$$

Lemme 4.9. Soit χ un caractère de Dirichlet modulo m (pas nécessairement primitif) et a un entier premier avec m . On a : $\tau_a(\chi) = \bar{\chi}(a) \tau_1(\chi)$. Si χ est primitif et a non premier avec m , on a $\tau_a(\chi) = 0$.

Pour la première assertion : $\chi(a) \tau_a(\chi) = \sum_{k=0}^{m-1} \chi(ak) \zeta^{ak}$. Puisque a est premier à m , les ak décrivent $(\mathbb{Z}/m\mathbb{Z})^*$.

Pour la seconde : Soient $(a, m) = r$, $m = rm'$, $r > 1$. On a si $z \equiv 1 \pmod{m'}$: $\zeta^{az} = \zeta^a$. Il en résulte que, si de plus z est premier avec m :

$$\tau_a(\chi) = \sum_{x \pmod{m}} \chi(zx) \zeta^{azx} = \chi(z) \tau_a(\chi).$$

Puisque χ est primitif, il existe un tel z avec $\chi(z) \neq 1$. Cela prouve que $\tau_a(\chi) = 0$.

On pose $\tau(\chi) = \tau_1(\chi)$. On a :

$$L(\chi, 1) = -\frac{\tau(\chi)}{m} \sum_{k, (k, m)=1} \bar{\chi}(k) \log(1 - \zeta^{-k}).$$

On dit que χ est pair si $\chi(-1) = 1$ et impair si $\chi(-1) = -1$.

On a : $\log(1 - \zeta^{-k}) = \log(|1 - \zeta^{-k}|) + i\pi(1/2 - k/m)$ avec $k \in [0, m-1]$,
et

$\log(|1 - \zeta^{-k}|) = 2 \sin(\pi k/m)$. Il en résulte :

Théorème 4.10. *Si χ est pair :*

$$L(\chi, 1) = -\frac{\tau(\chi)}{m} \sum_{k, (k, m)=1} \bar{\chi}(k) \log(|1 - \zeta^k|).$$

Si χ est impair :

$$L(\chi, 1) = \frac{\pi i \tau(\chi)}{m^2} \sum_{k, 0 < k \leq m-1, (k, m)=1} \bar{\chi}(k) k,$$

4.4. Le cas d'un corps quadratique. On note $d > 0$ le discriminant (ou plutôt sa valeur absolue).

Soit χ le caractère de K . On a : $\chi(p) = 0$ si p divise d , 1 si p se décompose dans K et -1 si p est inerte dans K . Exercice : prouver que χ est un caractère primitif.

Supposons d'abord K réel (χ pair : le prouver!). La formule analytique du nombre de classes donne : $h = \frac{\sqrt{d}}{2 \log(\epsilon)} L(\chi, 1)$. On a :

Lemme 4.11. *Pour χ primitif, on a $|\tau(\chi)| = \sqrt{m}$.*

On a :

$$\tau(\chi)\tau(\bar{\chi}) = \sum_k \tau_k(\bar{\chi}) \zeta^k = \sum_{k, k'} \bar{\chi}(k') \zeta^{kk'} \zeta^k = \sum_k \bar{\chi}(k') \sum_k \zeta^{k(k'+1)} = \bar{\chi}(-1)m,$$

les sommes portant sur k et k' d'origine $\mathbb{Z}/m\mathbb{Z}$ (on a $\tau_k(\chi) = 0$ si k n'est pas premier à m puisque χ est primitif) et $\chi(k)$ est nul si k n'est pas premier avec m .

Par ailleurs $\overline{\tau(\chi)} = \chi(-1)\tau(\bar{\chi})$.

On trouve finalement :

$$h = \frac{1}{2 \log(\epsilon)} \left| \sum_{k, (k, d)=1} \chi(k) \log \sin(k\pi/d) \right|.$$

Supposons maintenant K imaginaire (et $\mu(K) = \pm 1$, $\mathbb{Q}(i)$ et $\mathbb{Q}(j)$ ayant nombre de classes 1). La formule analytique du nombre de classes donne : $h = 1/2\pi \left| \sqrt{d} L(\chi, 1) \right|$. Avec le lemme ci-dessus :

$$h = 1/d \left| \sum_{k, 0 < k \leq d-1, (k, d)=1} \chi(k) k \right|.$$

Problem 1)

The aim of this problem is to prove that the equation $x^2 + 5 = y^3$ has no solution $(x, y) \in \mathbb{Z}^2$. We call K the quadratic number field $\mathbb{Q}(\sqrt{-5})$ and we recall that the class number h_K is 2. One supposes given (x, y) satisfying the above equation.

a) Describe the ring of integers O_K of K . What are the units of K ? How a prime p decomposes in K ?

b) Prove that if \wp is a prime of the ring of integers O_K of K which divides the principal ideals $(x + \sqrt{-5})$ and $(x - \sqrt{-5})$, \wp is above 2. Prove that if \wp is above 2, then $v_\wp(x + \sqrt{-5}) = v_\wp(x - \sqrt{-5})$ and that $v_\wp(x + \sqrt{-5}) = v_\wp(x - \sqrt{-5})$ is divisible by 3.

c) Let p be a prime $p \neq 2, 5$. If p is inert in K , prove that \wp does not divide the principal ideal $(x + \sqrt{-5})$. Prove that if p decomposes in K , 3 divides $v_\wp(x + \sqrt{-5})$.

d) Conclude that the principal ideal $(x + \sqrt{-5})$ is the cube of an ideal \mathcal{B} . Prove that \mathcal{B} is principal.

e) Prove that there exists $z \in O_K$ such that $z^3 = x + \sqrt{-5}$.

f) Let $z = a + b\sqrt{-5}$, $a, b \in \mathbb{Z}$. Prove that the equation $(a + b\sqrt{-5})^3 = x + \sqrt{-5}$ has no solution. Conclude.

Problem 2)

Let $K \subset \mathbb{C}$ be a finite extension of \mathbb{Q} . For $z \in \mathbb{C}$, let $|z|$ its absolute value. Let z be a non zero element of K , which is integral (z belongs to the ring O_K of integers of K), and such that every conjugate z' of z has absolute value ≤ 1 : $|z'| \leq 1$. The purpose of the problem is to prove that z is a root of unity.

a) Prove that the norm of z is ± 1 : $N_{K/\mathbb{Q}}(z) = \pm 1$, and that every conjugate z' of z has norm 1 : $|z'| = 1$.

b) Prove that z is a unit ($z \in E_K$). What is the image of z in the logarithmic map $E_K \rightarrow \mathbb{R}^{r_1+r_2}$? Conclude.

Problem 3) (more difficult)

Let p be an odd prime. Let $\mathbb{Q} \subset \mathbb{Q}(\mu_p) \subset \mathbb{C}$ be the cyclotomic field generated by the p roots of unity. Write K for $\mathbb{Q}(\mu_p)$. Let us define K^+ as the subfield of K which is of degree $(p-1)/2$ over \mathbb{Q} (it is the subfield of elements z in K such that $c(z) = z$ where c is the element of order 2 in $\text{Gal}(K/\mathbb{Q})$). Let ϵ be a primitive p root of unity ($\epsilon^p = 1$ and $\epsilon \neq 1$).

a) Prove that c is the restriction to K of the complex conjugation.

b) Calculate r_1 and r_2 for K and K^+ .

c) Prove that the group of unity E_{K^+} is of finite index in E_K .

d) Let u be a unit of the ring of integers O_K of K ($u \in E_K$). Let $\alpha = u/\bar{u}$, where $\bar{u} = c(u)$ is the complex conjugate of u . Prove that α is a root of unity (you may use problem 2). Prove that there exists an integer $a \in \mathbb{Z}$ such that $\bar{u} = \pm \epsilon^a u$.

- e) Prove that \bar{u} is congruent to u modulo the principal ideal of O_K generated by $\epsilon - 1$. Prove that in fact $\bar{u} = \epsilon^a u$.
- f) Prove that one can write $\epsilon^a = \delta/\bar{\delta}$ for δ a root of unity in K . Prove that $u\delta$ is in E_{K^+} . What can we conclude about $[E_K : E_{K^+}]$?