Nils-Peter Skoruppa

Théorie de Galois et

Théorie Algébrique des Nombres

Notes d'un cours de Maitrise

U.F.R. de Mathématiques et Informatique
Université Bordeaux 1

Version: Id: mor.tex,v 1.3 2003/11/25 14:55:13 fenrir Exp

Avant-Propos

C'est une version très préliminoire du polycopié au module *Théorie de Galois et théorie algébrique des nombres* (MOR 3) que j'ai assuré au debut de l'année 2000 à Bordeaux. Il manque toujours les chapîtres sur les faits de base de la théorie de Galois. D'autre part, dans ces sections 1.2 à 1.6 qui manquent je suis suivi en gros les sections correspondantes du livre *Serge Lange, Algebra.* En outre c'est un très bon livre (et moins cher) que je recommends beaucoup.

Il manque aussi une revision profonde de l'orthographie et de l'expression — est-ce que je vois des volontaires ?

Nils-Peter Skoruppa en mars 2000

Table des matières

Chapitre 1

Théorie de Galois et applications

1.1 Extensions finies et algébriques

— à faire —

1.2 Clotûre algébrique

— à faire —

1.3 Théorème de Steinitz et de l'élément primitif

— à faire —

1.4 Extensions normales

— à faire —

1.5 Extensions galoisiennes

— à faire —

1.6 Exemples I : Corps finis

Fixons un nombre premier p. Nous utilisons $\mathbb{F}_p$ pour le corps $\mathbb{Z}/p\mathbb{Z}$, et $\overline{\mathbb{F}}_p$ pour sa clôture algébrique. Rappelons que nous avons l'automorphisme de Frobenius

$$F : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p, \quad a \mapsto a^p.$$

Soit K un corps fini de caractéristique p. On peut supposer

$$\mathbb{F}_p \subset K \subset \overline{\mathbb{F}}_p.$$

Car K est un espace vectoriel sur $\mathbb{F}_p$, on a

$$\#K = p^{[K:\mathbb{F}_p]} =: q.$$

On a en plus

$$K^* = \langle w \rangle, \quad \mathrm{ord}(w) = q - 1.$$

En particulier, pour tout $a \in K$

$$a^q = a.$$

En conséquence K est le corps de décomposition de $x^q - x$.

Théorème. *Pour tout nombre naturel n il existe un et un seul sous-corps de $\overline{\mathbb{F}}_p$ avec $q := p^n$ éléments, noté $\mathbb{F}_q$. C'est le corps de décomposition de $x^q - x \in \mathbb{F}_p[x]$ sur $\mathbb{F}_p$.*

Démonstration. Il reste a montrer l'existence. Soit $\mathbb{F}_q$ l'ensemble des racines dans $\overline{\mathbb{F}}_p$ du polynôme $f(x) := x^q - x$. Car $f' = -1$ ces racines sont 2 à 2 différentes. Donc $\#F_q = q$. Finalement, l'ensemble $\mathbb{F}_q$ est un corps, i.e. stable sous $+$ et $\cdots$. Par exemple $+$: Si $a^q = a$ et $b^q = b$, alors $(a+b)^q = F^n(a+b) = F^n(a) + F^n(b) = a^q + b^q$, où $F : x \mapsto x^p$ et l'automorphisme de Frobenius de $\overline{\mathbb{F}}_p$. □

Evidemment, nous avons

$$m|n \Longrightarrow \mathbb{F}_{p^m} \subset \mathbb{F}_{p^n},$$

et

$$\mathbb{F}_{p^m} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^{\mathrm{pgcd}(m,n)}}.$$

Théorème. *On a* $\overline{\mathbb{F}}_p = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$.

Démonstration. Soit $a \in \overline{\mathbb{F}}_p$, et $K := \mathbb{F}_p(a)$. Nous avons déjà montré que $K = \mathbb{F}_q$ pour une puissance convenable q de p. □

En tant que corps fini $\mathbb{F}_p$ et parfait. Donc toute extension algébrique de $\mathbb{F}_p$ et separable, autrement dit, $\overline{\mathbb{F}}_p$ est separable sur $\mathbb{F}_p$. En plus, $\overline{\mathbb{F}}_p$ et tout $\mathbb{F}_q$ est normal sur $\mathbb{F}_p$.

Théorème. *Pour tout $q := p^n$ le groupe*
$\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ *est cyclique d'ordre n, engendré par $F|_{\mathbb{F}_q}$.*

Démonstration. Soit $\phi := F|_{\mathbb{F}_q}$. Clairement $\phi \in G := \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. L'ordre de G est $[\mathbb{F}_q : \mathbb{F}_p] = n$. En particulier $\phi^n = 1$. Supposons $\phi^l = 1$. Pour tout $a \in \mathbb{F}_p$ donc $a^{p^l} = a$. Car $x^{p^l} - x$ n'a que p^l racines, on a donc $p^l \geq p^n$, puis $l = n$. En conlusion, $\mathrm{ord}\,\phi = n$ et le théorème suit. □

Nous allons décrire le groupe de Galois "absolu"

$$G := \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p).$$

Pour ceci nous introduisons

$$\widehat{\mathbb{Z}} := \lim_{\leftarrow} \mathbb{Z}/n\mathbb{Z}$$

(limite projéctive du système projéctif $\{\mathbb{Z}/n\mathbb{Z}\}$). Par définition c'est le sous-groupe des $\{s_n\}$ dans le produit direct

$$\prod_n \mathbb{Z}/n\mathbb{Z},$$

tels que

$$m|n \Longrightarrow s_m \equiv s_n \bmod m.$$

Pour $s := \{s_n\} \in \widehat{\mathbb{Z}}$ nous définissons

$$F^s : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$$

par

$$F^s(a) = a^{p^{s_n}} \text{ si } a \in \mathbb{F}_{p^n}.$$

D'après la définition du groupe $\widehat{Z}$ cette définition ne dépend du chois de n. En plus, F^s et un automorphisme de $\overline{\mathbb{F}}_p$ (car sa restriction sur tout $\mathbb{F}_{p^n}$ l'est), et $s \to F^s$ est un morphisme de groupe (exercice).

Théorème. *L'application $s \mapsto F^s$ définit un isomorphisme de groupe*

$$\widehat{\mathbb{Z}} \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p).$$

Démonstration. $s \mapsto F^s$ est injectif : Si $F^s = 1$, alors pour tout n, on a $a^{p^{s_n}} = a$ pour tout $a \in \mathbb{F}_{p^n}$. D'après le théorème précédent donc $s_n \equiv 0 \bmod n$.

L'application est surjectif : Soit $\psi \in G$. Alors pour tout n il exist d'après le théorème précédent un $s_n \in \mathbb{Z}/n\mathbb{Z}$ tel que $\psi(a) = a^{p^{s_n}}$ pour tout $a \in \mathbb{F}_{p^n}$. Il est facile à vérifier que $s := \{s_n\} \in \widehat{\mathbb{Z}}$ (i.e. $s_m \equiv s_n \bmod m$ si $m|n$), et que $\psi = F^s$. □

Nous remarquons que $\widehat{\mathbb{Z}}$ est un anneau (parce que les $\mathbb{Z}/n\mathbb{Z}$ le sont). De plus $\widehat{\mathbb{Z}}$ est un anneau topologique. On munit $\widehat{\mathbb{Z}}$ par la topologie de trace de la toplogie de produit sur $\prod_n \mathbb{Z}/n\mathbb{Z}$. Ici la topologie sur $\mathbb{Z}/n\mathbb{Z}$ est la toplogie discrète. En particulier, nous remarquons que $\widehat{\mathbb{Z}}$ est compact (par le lemme d'Uryson).

1.7 Exemples II : Corps cyclotomiques

Dans cette section nous fixons *un corps de base k de caractéristique 0.* Soit $\overline{k}$ une clôture algébrique $\overline{k}$. Nous regardons $\mathbb{Q}$ comme sous-corps de k.

Pour un nombre naturel $n > 0$ nous utilisons

$$\mu_n = \{\zeta \in \overline{k} : \zeta^n - 1\}.$$

C'est donc l'ensemble des racines du polynôme $x^n - 1$, qui possède n racines différentes (différentes car $\mathrm{car}(k) = 0$). Il est clair que μ_n est un sous-groupe fini de $\overline{k}^*$, en particulier μ_n est cyclique (exercice : Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.)

Les éléments de μ_n sont appelés *racines d'unité n-ième.* Les générateurs de μ_n sont dits *racines d'unité n-ième primitives.*

Rappel : Si $\overline{k} \subset \mathbb{C}$, alors

$$\mu_n = \{\mathrm{e}^{2\pi i \frac{k}{n}} : 0 \leq k < n\}.$$

Les racines d'unités n-ième pimitives sont

$$\mathrm{e}^{2\pi i \frac{k}{n}} \qquad (\mathrm{pgcd}(k, n) = 1).$$

Le corps $k(\mu_n)$ est une extension galoisienne (en tant que corps de décomposition de $x^n - 1$ sur k). Par restriction on obtient l'homomorphisme

$$\mathrm{Gal}(k(\mu_n)/k) \to \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}), \psi \mapsto \psi|_{\mathbb{Q}(\mu_n)}.$$

Ce morphisme est injectif (exercice). Donc, pour étudier l'extension $k(\mu_n)/k$ il suffit à considérer le cas $k = \mathbb{Q}$.

Nous allons déterminer le degré $[\mathbb{Q}(\mu_n) : \mathbb{Q}]$ et le groupe de Galois

$$G_n := \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}).$$

Il est clair que

$$\mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta)$$

pour n'importe quelle racine d'unité n-ième primitive ζ. Donc nous devons dans un premier temps déterminer le polynôme minimal de ζ.

Soit

$$\phi_n = \prod (x - \zeta) \in \overline{\mathbb{Q}}[x],$$

où ζ parcourt les racines n-ièmes primitives (*n-ième polynôme cyclotomique*). Le degré de ϕ_n est égal à **la fonction $\varphi(n)$ d'Euler**, i.e. au nombre de générateurs d'un groupe cyclique d'ordre n, ou bien le nombre de classes résidues primitives $x + n\mathbb{Z}$ (i.e. classes $x + n\mathbb{Z}$ avec $\mathrm{pgcd}(x, n) = 1$). On a la formule

$$\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p}).$$

Il est clair que

$$x^n - 1 = \prod_{d|n} \phi_d.$$

En fait, si $\zeta \in \mu_n$, alors ζ engendre un sous-groupe de μ_n. mais les seuls sous-groupes sont les μ_d avec $d|n$. Donc tout $\zeta \in \mu_n$ est une racine d'unité d-ième primitive pour un $d|n$.

Par inversion de Moebius nous obtenons ainsi

$$\phi_n = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

Ici $\mu(n)$ est **la fonction de Moebius**, i.e. $\mu(n) = 0$ si $p^2|n$ pour un premier p, et $\mu(n) = (-1)^r$ sinon, où r est le nombre de diviseurs premiers de n.

En conséquence nous avons donc

Théorème. *Pour tout n on a $\phi_n \in \mathbb{Q}[x]$.*

En fait, on peut même tirer de la formule ci-dessus que $\phi_n \in \mathbb{Z}[x]$.

Lemme. *Soient f et g deux polynômes normalisés avec coéfficients dans $\mathbb{Z}$, supposons que $g = f \cdot h$ pour un polynôme $h \in \mathbb{Q}[x]$. Alors $h \in \mathbb{Z}[x]$.*

Démonstration. Exercice. □

Les premiers exemples sont

$$\phi_2 = x + 1, \quad \phi_3 = x^2 + x + 1, \quad \phi_4 = x^2 + 1,$$

et pour un nombre premier p toujours

$$\phi_p = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Le théorème de cléf de cette section est

Théorème. *Le polynôme ϕ_n est irréductible dans $\mathbb{Q}[x]$.*

Démonstration. Soit ζ une racine de ϕ_n, soit $f = \mathrm{Irr}(\zeta, \mathbb{Q}, x)$. Nous montrons que ζ^p, pour tout premier $p \not| n$, est également une racine def f. Car ζ^p est aussi une racine de ϕ_n, et car toute racine de ϕ_n peut être obtenu en prenant successivement de puisances p-ième de ζ pour des premiers p convenables, nous remarquons ainsi que toute racine de ϕ_n est racine de f, i.e. que $f = \phi_n$.

Supposons $f(\zeta^p) \neq 0$ avec un premier $p \not| n$. D'abord ζ est une racine de $x^n - 1$, donc

$$x^n - 1 = f \cdot h$$

pour un polynôme $h \in \mathbb{Q}[x]$. En fait, parce que $x^n - 1$ et f sont normalisés avec coéfficients dans $\mathbb{Z}$, on a $h \in \mathbb{Z}[x]$ (voir le lemme ci-dessus). Car $f(\zeta^p) \neq 0$ nous avons $h(\zeta^p) = 0$. Donc ζ est une racine de $h(x^p)$, i.e.

$$h(x^p) = f \cdot g.$$

pour un $g \in \mathbb{Q}[x]$. Encore, car f et h sont normalisés nous avons même $g \in \mathbb{Z}[x]$.

Désignons reduction modulo p par un bar. Nous avons modulo p

$$\overline{h(x)}^p = \overline{h(x^p)} = \overline{f} \cdot \overline{g}.$$

Donc $\overline{f}$ and $\overline{h}$ ont un commun facteur irréductible dans $\mathbb{F}_p[x]$. Mais

$$\overline{x^n - 1} = \overline{f} \cdot \overline{h},$$

et par conséquence $\overline{x^n - 1}$ possède de racines multiples dans $\overline{\mathbb{F}}_p$. Mais la dérivée de $\overline{x^n - 1}$ est $\overline{nx^{n-1}} \neq 0$ (car $p \not| n$). Contradiction. □

En particulier nous observons que

$$[\mathbb{Q}(\mu_n) : \mathbb{Q}] = \varphi(n).$$

On a même :

Théorème. *Le groupe* $G_n = \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ *est isomorphe à* $(\mathbb{Z}/n\mathbb{Z})^*$.

Démonstration. Fixons une racine d'unité n-ième primitive ζ. Un $\phi \in G_n$ donne

$$\phi : \zeta \mapsto \zeta^r$$

pour un naturel r. Le nombre r est premier à n (car ζ^r est primitif en tant que racine de ϕ_n) et unique modulo n. Donc nous avons l'application

$$G_n \to (\mathbb{Z}/n\mathbb{Z})^*, \qquad \phi \mapsto r + n\mathbb{Z}.$$

Cette application est clairement injective. Car pour toute racine θ de ϕ_n nous avons un automorphisme de $\mathbb{Q}(\mu_n)$ qui donne $\zeta \mapsto \theta$ cette application est aussi surjective.

Il est facile à verifier que l'application est un morphisme de groupes. □

Nous posons maintenant

$$\widetilde{\mathbb{Q}} = \bigcup_{n=1}^{\infty} \mathbb{Q}(\mu_n)$$

(on l'appele la clôture abélien de $\mathbb{Q}$). En utilisant

$$\mathbb{Q}(\mu_n), \mathbb{Q}(\mu_m) \subset \mathbb{Q}(\mu_l) \quad (l = \mathrm{ppcm}(m, n))$$

on montre que $\widetilde{\mathbb{Q}}$ est un corps. En tant que réunion d'extension galoisiennes de $\mathbb{Q}$ le corps $\widetilde{\mathbb{Q}}$ est galois sur $\mathbb{Q}$.

Soit $G := \mathrm{Gal}(\widetilde{\mathbb{Q}}/\mathbb{Q})$ le groupe de Galois associé.

Soit

$$\mu := \bigcup_{n=1}^{\infty} \mu_n.$$

L'application

$$G \to \mathrm{Aut}(\mu), \quad \phi \mapsto \phi|_\mu$$

est bien-définie, et définit un morphisme de groupes injectif. Ce morphisme est également surjectif : Soit $\sigma \in \mathrm{Aut}(\mu)$, alors pour tout n restriction définit un élement $\sigma_n \in \mathrm{Aut}(\mu_n)$. Par le théorème précédent il existe un $\phi_n \in G_n$ avec $\phi_n|_{\mu_n} = \sigma_n$. Définir $\phi \in G$ comme ϕ_n sur $\mathbb{Q}(\mu_n)$. Il est facile à vérifier que ϕ est bien-défini et que $\phi|_\mu = \sigma$.

Donc nous avons

Théorème. *L'applicaton*

$$\mathrm{Gal}(\widetilde{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\mu)$$

définie par restriction est un isomorphisme de groupes.

Nous remarquons que

$$\mathrm{Aut}(\mu) \approx \mathrm{Aut}(\mathbb{Q}/\mathbb{Z}) \approx \widehat{\mathbb{Z}}^*$$

(exercice :le prmier isomorphisme est $\mathrm{e}^{2\pi ir} \mapsto r + \mathbb{Z}$).

1.8 Resolution explicites d'équations de degré ≥ 2

Nous supposons dans cette séction toujours que le corps de base k et de caractéristique 0. Ainsi toute extension algébrique de k est automatiquement separable.

Nous disons que $\alpha \in \overline{k}$ est résoluble par radicaux sur k si il existe une tour de la forme

$$k = L_0 \subset L_1 \subset \cdots \subset L_n \ni \alpha,$$

où pour tout j on a $L_j = L_{j-1}(\alpha_j)$ tel que $\alpha_j^{n_j} \in L_{j-1}$ pour un naturel n_j.

Une extension comme L_j est appelée extension par radical simple de L_{j-1}. Et L_n est appelé extension par radicaux de k.

Théorème. *Soit $\alpha \in \overline{k}$, soit $f \in k[x]$ le polynôme minimal de α sur k, et soit K le corps de décomposition de f. Les deux propositions suivantes sont équivalentes :*

1. *α est resoluble par radicaux sur k.*
2. *$\mathrm{Gal}(K/k)$ est soluble.*

Nous rappelons qu'un groupe fini G est soluble si il existe une suite de sous-groupes

$$1 = G_0 \subset G_1 \subset \cdots \subset G_n = G,$$

telle que G_{j-1} et un sous-groupe distingué de G_j est le quotient G_j/G_{j-1} est abélien.

Esquisse de la preuve. Nous supposons d'abord que $\mathrm{Gal}(K/k)$ est soluble.

Soit n le produit des premiers qui divisent $[K : k]$, soit

$$k' := k(\mu_n), \quad K' := K(\mu_n).$$

Evidement k' est une extension par radicaux de k (même par radical simple), et pour montrer 1. il suffit donc à montrer que K' est une extension par radicaux de k'.

Nous notons d'abord que K' est une extension galoisienne de k' et de k (si K est le corps de décomposition de $f \in k[x]$, alors K' et le corps de

décomposition de $f(x) \cdot (x^n - 1)$ sur k ainsi que sur k'). La restriction sur K définit un morphisme

$$\mathrm{Gal}(K'/k') \to \mathrm{Gal}(K/k).$$

Ce morphisme est injectif (exercice). Donc $\mathrm{Gal}(K'/k')$ est isomorphe à un sous-groupe de $\mathrm{Gal}(K/k)$, et par conséquence soluble (un sous-groupe d'un groupe soluble est soluble - exercice). En plus, ceci entraîne que pour chaque diviseur premier p de $[K' : k']$ le corps k' contient μ_p (car $[K' : k']$ divise $[K : k]$, et alors $p|n$).

Que K'/k' est résoluble par radicaux est maintenant une conséquence du lemme suivant :

Lemme. *Soit K'/k' une extension galoisienne tel que $\mathrm{Gal}(K'/k')$ est résoluble. Supposons que k' contient μ_p pour tout premier qui divise $[K' : k']$. Alors K'/k' est resoluble par radicaux.*

Démonstration. Nous faisons une récurrence sur $m := [K' : k']$. Si $m = 1$ rien est à montrer. Supposons le lemme est vrai pour tout $[K' : k'] < n$.

Soit H un sous-groupe distingué de $G := \mathrm{Gal}(K'/k')$ tel que G/H est cyclique d'ordre premier p (existence d'un tel H : exercice — ici on utilise l'hypothèse que G est soluble).

Car H est distingúe dans G le corps $L := K'^H$ est une extension galoisienne de k', et on a

$$\mathrm{Gal}(K'/L) = H, \quad \mathrm{Gal}(L/k') \cong G/H.$$

D'après l'hypothèse de récurrence K'/L est une extension par radicaux. D'après le lemme suivant L est une extension de k' par radical simple. Ceci montre le lemme. □

Lemme. *Soit L/k' une extension cyclique d'ordre q. Supposons que k' contient μ_q. Alors il existe un $R \in L$ tel que $L = k'(R)$ et $R^q \in k'$.*

Démonstration. Soit ϕ générateur de $G := \mathrm{Gal}(L/k')$, soit ζ une racine d'unité q-ième primitive. Posons pour $a \in L$

$$R := \sum_{j=0}^{q-1} \zeta^j \phi^j(a)$$

(**résolvante de Lagrange de** a).

On a

$$\phi(R) = \zeta^{-1} R.$$

Donc, si $R \neq 0$, alors le seul élément de G qui laisse stable R, et donc $k'(R)$, est l'identité. Donc

$$L = k'(R).$$

Mais $\phi(R^q) = R^q$, donc

$$R^q \in k'.$$

Il reste à montrer qu'il existe un $a \in L$ tel que $R \neq 0$.

Considérons ϕ comme endomorphisme du k'-espace vectoriel L. Les valeurs propres de ϕ sont des racines d'unité q-ième (car $\phi^q = 1$). Car $\mathrm{ord}(\phi) = q$ au moins une valeur propre de ϕ est une racine d'unité q-ième primitive, disons θ. Car $\theta \in k'$ il existe un $b \in L$, $b \neq 0$, avec

$$\phi(b) = \theta b$$

(vecteur propre dans L par rapport à la valeur propre θ). Soit l tel que $\zeta = \theta^l$. Posons $a = b^{-l}$. Alors

$$\phi(a) = \phi(b)^{-l} = \theta^{-l} b^{-l} = \zeta^{-1} a,$$

et en général

$$\phi^j(a) = \zeta^{-j} a.$$

En particulier

$$R = \sum_{j=0}^{q-1} \zeta^j \phi^j(a) = qa \neq 0.$$

□

Nous supposons maintenant 1., i.e. *que α appartient à une extension par radicaux L de k.*

Nous montrons d'abord le

Lemme. *Toute extension par radicaux L/k est contenu dans une extension par radicaux K/k tel que K/k est galoisien.*

Démonstration. Récurrence sur $n = [L : k]$. Pour $n = 1$ rien est à montrer. Supposons donc que le lemme est vrai pour toute extension L'/k par radicaux avec degré $[L' : k] < n$.

??????????????Pour L' on choisit une sous-extension de L tel que L/L' est une extension par radical simple et L'/k une extension par radicaux, et tel que $[L : L'] \geq 2$, i.e. $[L' : k] < n$. ?????????????

Donc L'/k est contenu dans une extension par radicaux galoisienne K'/k.

Soit $L = L'(a)$, $a^l \in L'$. Soit K le corps de décomposition sur K' du polynôme

$$h = \prod_{\phi \in \mathrm{Gal}(K'/k)} (x^l - \phi(a^l)) \in K'[x].$$

Alors $L \subset K$ (car $h(a) = 0$, donc $a \in K$ et $L' \subset K'$).

Evidement, par définition, K est une extension par radicaux de K', et donc aussi de k.

Finalement K est normal sur k. En fait, h est stable sous $\mathrm{Gal}(K'/k)$, donc dans $k[x]$. En plus, K' est le corps de décomposition d'un polynôme $g \in k[x]$ sur k. En conséquence, K est le corps de décomposiion de $h \cdot g$. □

Le corps K ainsi trouvé par le lemme n'est pas forçement le corps de décompostion K_0 de $f = \mathrm{Irr}(\alpha, k, x)$. Mais il suffit à montrer que $G := \mathrm{Gal}(K/k)$ est soluble. En fait, $K_0 \subset K$ et la restriction définit un morpisme surjectif

$$G \to \mathrm{Gal}(K_0/k) =: G_0.$$

Donc, si G est soluble, alors G_0 l'est aussi (exercice).

Il suffit donc à montrer

Lemme. *Soit K/k une extension galoisienne par radicaux. Alors le groupe $G = \mathrm{Gal}(K/k)$ est soluble.*

Démonstration. Nous avons une suite

$$k = L_0 \subset \cdots \subset L_m = K$$

telle que L_j/L_{j-1} est une extension par radical simple. Soit $n = [K : k]$. Posons

$$k' = k(\mu_n), \quad L'_j = L_j(\mu_n), \quad K' = K(\mu_n).$$

K est corps de décomposition d'un $g \in k[x]$, donc K' est le corps de décomposition de $g \cdot (x^n - 1)$ sur k. En particulier K'/k est galois. Il suffit à montrer que $G' := \mathrm{Gal}(K'/k)$ est soluble (car $G = \mathrm{Gal}(K/k)$ est l'image homomorphique de G').

Pour ceci nous regardons le tours

$$k =: L'_{-1} \subset k' = L'_0 \subset L'_1 \subset \cdots \subset L'_m = K'.$$

Nous savons que L'_0/k est abélien (car $L'_0 = k(\mu_n)$). En plus, $L'_j = L'_{j-1}(a)$ tel que $a^q \in L'_{j-1}$ pour un naturel $q > 0$. Car L'_{j-1} contient les racines d'unités q-ième, l'extension L'_j/L'_{j-1} est galoisienne. En fait, nous montrons dans un instant qu'elle est cyclique.

Soit $H_j = \mathrm{Gal}(K'/L'_j)$. On a

$$G' = H_{-1} \supset H_0 \supset \cdots \supset H_m = 1.$$

Car L'_j/L'_{j-1} est galoisien, le groupe H_j est distingué dans H_{j-1}, et on a que

$$H_{j-1}/H_j \approx \mathrm{Gal}(L'_j/L'_{j-1})$$

est abélien. □

Il reste à montrer le

Lemme. *Soit $L = k(a)$ tel que $a^q \in k$ pour un naturel $q > 0$, Supposons que k contient μ_q. Alors L/k est galoisien, et $\mathrm{Gal}(L/k)$ est cyclique d'ordre divisant q.*

Démonstration. L'élément a est une racine de $g = x^q - a^q \in k[x]$. Les autre racines sont ζa, où ζ parcourt μ_q. Donc L est le corps de décomposition de g sur k, en particulier galois sur k.

Pour montrer la proposition sur le groupe de Galois nous observons que tout $\phi \in G := \mathrm{Gal}(L/k)$ donne

$$\phi : a \mapsto a\zeta$$

pour un naturel $\zeta \in \mu_q$ convenable. Si $a \neq 0$ (que nous pouvons supposer) l'application ainsi obtenue

$$G \to \mu_q, \quad \phi \mapsto \zeta$$

est un morphisme injectif (exercice). □

Ceci termine la démonstration du théorème principal. □

Nous appliquons la théorie de cette section pour trouver des formules explicites pour les racines d'une équation de degré 3.

Soit $k = \mathbb{Q}(\mu_3)(p, q, r)$ le corps des fonctions rationnelles en trois inconnus p, q, r sur le corps $\mathbb{Q}(\mu_3)$. Soit

$$f = x^3 + px^2 + qx + r \in k[x],$$

et K/k le corps de décomposition de f. Notons que K est une extension galoisienne de k. Dans K nous avons donc

$$f = (x - a)(x - b)(x - c).$$

Finalement, soit $G = \mathrm{Gal}(K/k)$. Nous avons l'application injective

$$G \to \mathrm{Perm}(a, b, c) \approx S_3$$

qui associe à un automorphisme de K/k sa restriction sur les racines a, b, c.

Théorème. *On a $G \approx S_3$ (i.e. l'application ci-dessus est un isomorphisme).*

Démonstration. Soit $F = \mathbb{Q}(\mu_3)$, et soit $F[A, B, C]$ l'anneau des polynômes en trois inconnus. Alors nous avons un diagramme de morphisme d'anneaux

$$\begin{array}{ccc} F[p,q,r] & \to_\sigma & F[p',q',r'] \\ \downarrow & & \downarrow \\ F[a,b,c] & \leftarrow_\rho & F[A,B,C] \end{array}$$

Les flèches verticales sont des inclusions, ρ est l'identité sur F et donne $A \mapsto a$, $B \mapsto b$, $C \mapsto c$, et σ, étant l'dentité sur F donne

$$\begin{aligned} p \mapsto p' &:= -(A + B + C), \\ q \mapsto q' &:= AB + AC + BC, \\ r \mapsto r' &:= -ABC. \end{aligned}$$

On vérifie que $\rho \circ \sigma = \mathrm{Id}$. Donc σ est injectif. Car σ est clairement surjectif, il définit donc un isomorphisme d'anneaux. Mais alors σ peut être prolongé à un isomorphisme

$$\sigma : k = F(p, q, r) \to F(p', q', r').$$

Il est clair que $F(A, B, C)$ est le corps de décomposition de $\sigma(f)$ sur le corps $F(p', q', r')$. Car $K = F(a, b, c)$ est le corps de décomposition de f sur $k = F(p, q, r)$, l'ismorphisme σ se prolonge à un isomorphisme

$$\sigma : K = F(a, b, c) \to F(A, B, C),$$

qui donne les racines a, b, c de f sur les racines A, B, C de $\sigma(f)$. Mais alors σ induit un isomorphisme

$$\mathrm{Gal}(K/k) \approx \mathrm{Gal}(F(A, B, C)/F(p', q', r')).$$

Le groupe à droite contient S_3, car S_3 agit sur $F[A, B, C]$ en permutant A, B, C. Mais $\mathrm{Gal}(K/k)$ est isomorphe à un sous-groupe de S_3. On en déduit que, en fait, les deux groupe ci-dessus doivent être isomorphes ou égaux à S_3. □

Le groupe G est soluble :

$$1 \subset A_3 \subset S_3,$$

ou $A_3 = \langle (a, b, c) \rangle$. Nous avons ainsi le tour associé

$$\begin{array}{ccccc} K & \supset & K^{A_3} =: L & \supset & k \\ & A_3 & & S_3/A_3 & \end{array}$$

Or, L/k est une extension simple par radical : un élément de K, invariant sous A_3, est

$$\Delta := (a-b)(a-c)(b-c).$$

En fait, Δ est stable sous A_3, mais $\Delta \notin k$ (car p.e. $(ab)(\Delta) = -\Delta$), et $\Delta^2 \in k$ (car clairement invariant sous $G = S_3$). Par un petit calcul

$$\begin{aligned}\Delta^2 &= (a-b)^2(a-c)^2(b-c)^2 \\ &= -4rp^3 + q^2p^2 + 18rqp - (4q^3 + 27r^2).\end{aligned}$$

C'est ce que l'on appele le discriminant $\mathrm{disc}(f)$ de f. Notons que cette expression se simplifie considérablement si $p = a + b + c = 0$.

De même K est extension par radical simple de L :

$$R := a + \zeta_3 b + \zeta_3^2 c$$

satisfait à

$$(abc)(R) = b + \zeta_3 c + \zeta_3^2 a = \zeta_3^2 R,$$

Donc $R^3 \in L$ (car stable sous $A_3 = \langle (abc) \rangle$), mais $R \notin L$. En conséquance $K = L(R)$. Encore par un petit calcul on trouve

$$R^3 = (3\zeta_3 + \frac{3}{2})\Delta - p^3 + \frac{9}{2}pq - \frac{27}{2}r$$

Un autre générateur de K/L est

$$R' = a + \zeta_3^2 b + \zeta_3 c.$$

Ici on a (appliquer $(bc) \in S_3$ à l'identité précédente)

$$R'^3 = -(3\zeta_3 + \frac{3}{2})\Delta - p^3 + \frac{9}{2}p * q - \frac{27}{2}r.$$

On note que

$$\begin{aligned}a &= R + R' - p, \\ b &= \zeta_3^2 R + \zeta_3 R' - p, \\ c &= \zeta_3 R + \zeta_3^2 R' - p.\end{aligned}$$

Ces identité deviennent particulierement simples si on suppose $p = 0$ (que l'on peut toujours en faisant la substitution $x \mapsto x - \frac{p}{3}$ dans $x^3 + px^2 + qx + r =$

0 avant l'application des formules ci-dessus). On a ainsi le formulaire

$$\begin{aligned}
\Delta &= \sqrt{-(4q^3+27r^2)},\\
R &= \sqrt[3]{(3\zeta_3+\frac{3}{2})\Delta-\frac{27}{2}r}\\
R' &= \sqrt[3]{-(3\zeta_3+\frac{3}{2})\Delta-\frac{27}{2}r}\\
a &= \frac{1}{3}(R+R'),\ b=\frac{1}{3}(\zeta_3^2R+\zeta_3R'),\\
c &= \frac{1}{3}(\zeta_3R+\zeta_3^2R').
\end{aligned}$$

Ces sont les célèbres **formules de Cardano**.

Exemple : $x^3+x+1=0$. On a d'après le formulaire

$$\begin{aligned}
&\Delta=\sqrt{-31},\\
&R=\sqrt[3]{\frac{3\sqrt{93}}{2}-\frac{27}{2}},\quad R'=\sqrt[3]{-\frac{3\sqrt{93}}{2}-\frac{27}{2}}\\
&a=\frac{1}{3}(R+R'),\ b=\cdots,\ c=\ldots.
\end{aligned}$$

Nous discutons fianlement l'équation générale de degré n arbitraire.

Soit maintenant k un corps de caractéristique 0, soit $k_n=k(x_{n-1},\ldots,x_0)$ le corps des fonctions rationnelles en n inconnus x_j, et soit K_n le corps de décomposition du polynôme

$$f(x)=x^n+x_{n-1}x^{n-1}+\cdots+x_1x+x_0.$$

Sans démonstration nous citons

Théorème. *On a* $\mathrm{Gal}(K_n/k_n)\approx S_n$.

Théorème. *Le groupe symmétrique à n lettres S_n n'est pas soluble si $n\geq 5$.*

Ceci est une conséquence du fait que le groupe alterné A_n est simple pour $n\geq 5$, en particulier non soluble, et du fait simple qu'un sous-groupe d'un groupe soluble est également soluble. On obtient ainsi

Théorème. *(***Théorème de Abel***) L'équation générale du degré $n\geq 5$ n'est pas resoluble par radicaux (i.e. l'extension K_n/k_n n'est pas resoluble par radicaux).*

Bien-sur, il existe des équations de degré $n \geq 5$ qui ont comme groupe de Galois un sous-groupe de S_n qui est soluble (mais c'est très rare : on peut montrer (van der Waerden) que la probabilité qu'une équation de degré n a S_n comme groupe de Galois est égal à 1).

Pour degré $n = 4$ le groupe S_4 est soluble, et il existe des formules comme ceux de Cardano (trouvé par Luigi Ferrari). A propos, Geronimo Cardano a volé ses formules de Nicolo Tartaglia qui les a pris de Scipione del Ferro.

1.9 Construction à la règle et compas

Nous identifions désormais le plan euclidien avec le plan complèxe $\mathbb{C}$. Soit M *un ensemble de point de* $\mathbb{C}$ *qui contient au moins 2 points.*. Une *droite* d est *constructible depuis* M si au moins deux point de d apartiennent à M. Un *cercle* est *constructible depuis* M si son centre appartient à M, et si son rayon est égal à la distance de deux point de M. Nous disons qu'un *point* z *est constructible depuis* M, si z est un point d'intersection de deux élément de $G(M)$; nous utilisons $M^{(1)}$ pour l'ensemble des points qui sont constructibles de M.

Remarquons que $M^{(1)}$ contient M : Si $z \in M$, alors il existe un $w \neq z$ dans M, et z est l'intersection de la droite passant z et w, et du cercle autour de w de rayon zw.

Nous posons $M^{(0)} = M$ et par récurrence

$$M^{(n)} = \left(M^{(n-1)}\right)^{(1)}.$$

Donc on a

$$M^{(0)} \subset M^{(1)} \subset \cdots \subset M^{(n)} \subset \cdots.$$

Finalement nous posons

$$\Omega(M) = \bigcup_{n=0}^{\infty} M^{(n)}.$$

C'est l'ensemble de tous les points que l'on peut construire depuis M dans un nombre fini d'ètapes par règle et compas.

Notons dans un premier temps que

$$\Omega(\Omega(M)) = \Omega(M).$$

En fait, il suffit pour ceci à montrer l'identité $(\Omega(M))^{(1)} = \Omega(M)$. Soit $z \in (\Omega(M))^{(1)}$. Alors z est l'intersection de droites ou cercles qui sont constructibles de points $z_j \in \Omega(M)$ $(1 \leq j \leq n)$. Mais pour un naturel n on a $z_j \in M^{(n)}$ pour tout j. Donc $z \in M^{(n+1)}$.

Nous pouvons supposer sans restriction de généralité et *nous supposerons désormais que* 0 *et* 1 *appartient à* M (en appliquant une homothétie suivie par une rotation à M, si necessaire).

Regardons un peu la nature de $\Omega(M)$. Pour ceci nous utilisons $D(a,b)$ pour la droite contenant a et b, et $C(a;b-c)$ pour le cercle autour de a de rayon $|b-c|$, et S_1 pour le groupe des nombres complexes de modulus 1.

Ici un tableau de plusieures quantités a, b telles que $a \in \Omega(M)$ entraîne $b \in \Omega(M)$, et la raison pour cette conclusion :

a	b	raison
z	$-z$	$\in D(0,z) \cap C(0;z-0)$
z,w	$z+w$	$\in C(z;w-0) \cap C(w;z-0)$
z	$\lvert z\rvert$	$\in D(0,1) \cap C(0;z-0)$
$z \neq 0$	$z/\lvert z\rvert$	$\in D(0,z) \cap C(0;1-0)$
z	$\overline{z}$	$\in C(0;z-0) \cap C(1,z-1)$
	i	$\in D(0,a) \cap C(0,1)$ où $a \in C(1,2) \cap C(-1,2)$
$r \in \mathbb{R}_{>0}$	ri	$\in D(0,i) \cap C(0,r-0)$
$r,s \in \mathbb{R}_{>0}$	$\frac{r}{s}$	$\in D(0,1) \cap D(ri, 1+(r-s)i)$
$r,s \in \mathbb{R}_{>0}$	$r \cdot s$	$= \frac{r}{1/s}$
$z,w \in S^1$	$z \cdot w$	$\in C(0,1-0) \cap C(z,w-1)$
$r \in \mathbb{R}_{>0}, z \in S^1$	$r \cdot z$	$\in D(0,z) \cap C(0;r-0)$
$r \in \mathbb{R}_{>0}, z$	$r \cdot z$	$= (r \cdot \lvert z\rvert) \cdot (z/\lvert z\rvert)$
$z \neq 0$	$1/z$	$= \frac{1}{\lvert z\rvert} \cdot \overline{z}$
$z,w \neq 0$	$z \cdot w$	$= (\lvert z\rvert \cdot \lvert w\rvert) \cdot (\frac{z}{\lvert z\rvert}\frac{w}{\lvert w\rvert})$
$r \in \mathbb{R}_{>1}$	$i\sqrt{r}$	$\in D(0,i) \cap C(\frac{r-1}{2}; \frac{r+1}{2})$
$r \in \mathbb{R}_{>1}$	$\sqrt{r}$	$= -i \cdot i\sqrt{r}$
$r \in \mathbb{R}_{<1}$	$\sqrt{r}$	$= 1/\sqrt{1/r}$
$z \in S^1$	$\sqrt{z}$	exercice
z	$\sqrt{z}$	$= \sqrt{\lvert z\rvert} \cdot \sqrt{z/\lvert z\rvert}$

La premiere conséquence de ce tableau est

Théorème. $\Omega(M)$ *est un corps.*

Démonstration. Soient $z,w \in \Omega(M)$. Nous devons montrer que $-z$, $z+w$, $1/z$ (si $z \neq 0$) et $z \cdot w$ appartienent à $\Omega(M)$. Mais ceci est partie du tableau ci-dessus. □

Pour décider à l'aide de l'algèbre quels points sont constructibles avec règle et compas il nous faut une déscription algébrique du corps $\Omega(M)$.

Théorème. *Posons* $k = \mathbb{Q}(M, \overline{M})$, *où* $\overline{M} = \{\overline{w} : w \in M\}$. *Pour un nombre comlexe* z *les propositions suivantes sont équivalentes :*

1. $z \in \Omega(M)$
2. *Il existe une tour de corps*

$$k = L_0 \subset L_1 \subset \cdots \subset L_n, \quad z \in L_n,$$

telle que $[L_j : L_{j-1}] \leq 2$ *pour* $1 \leq j \leq n$.

3. z *appartient à une extension galoisienne finie de* k *dont le degré est une puissances de* 2.

Remarque. Soit f le polynôme minimale de z sur k et K son corps de décomposition. On vérifie facilement que 3. est équivalent à la proposition que le degré $[K : k]$ divise 2^∞.

D'après le théorème on a

$$\Omega(M) = \bigcup_K K,$$

où K parcourt les extensions galoisiennes finies de k telle que $[K : k] | 2^\infty$. En particulier, ceci montre que $\Omega(M)$ est une extension galoisienne de k.

Démonstration. Supposons 3. Nous montrons par récurrence sur n :

(A) Si K/k est galoisienne de degré 2^n, alors $K \subset \Omega(M)$.

Le cas $n = 0$ est clair car $\Omega(M)$ est un corps contenant M. Donc il contient aussi $\overline{M}$ (voir le tableau ci-dessus), et par conséquence tout k.

La proposition (A) soit vraie pour toute extension galoisienne de k de degré $\leq 2^{n-1}$. Soit K/k galoisienne de degré 2^n.

Le groupe $G := \mathrm{Gal}(K/k)$, en tant que 2-groupe, contient un sous-groupe distingué d'ordre 2, disons H (exercice). Soit $L = K^H$. Alors L/k est galoisienne de degré 2^{n-1}. Par l'hypothèse de récurrence on a $L \subset \Omega(M)$.

Car $[K : L] = 2$ il existe un $a \in L$ tel que $K = L(\sqrt{a})$ (voir la séction précédente). Mais si $a \in \Omega(M)$, alors $\sqrt{a} \in \Omega(M)$ (voir le tableau ci-dessus). Car $\Omega(M)$ est un corps, on a donc $K = L(\sqrt{a}) \subset \Omega(M)$.

Supposons maintenant 1. Nous montron dans un premier temps 2.

Supposons pour l'instant :

(B) Si $N \subset \mathbb{C}$ contient 0 et 1, et si on pose $F := \mathbb{Q}(N, \overline{N})$, alors pour tout $z, \overline{z} \in N^{(1)}$ on a $[F(z) : F] \leq 2$, et $F(z)$ est stable sous conjugaison complexe..

Ceci entraîne immédiatement 2. En fait soit $z \in \Omega(M)$. Alors il existe une suite d'ensembles

$$M = N_0 \subset N_1 \subset \cdots \subset N_n$$

telle que $N_j = N_{j-1} \cup \{z_j\}$ pour un $z_j \in (N_{j-1})^{(1)}$ et $z = z_n$.

On a

$$k = L_0 \subset L_1 \subset \cdots \subset L_n, \quad (\, L_j = \mathbb{Q}(N_j, \overline{N}_j)\,)$$

Mais $L_j = L_{j-1}(z_j, \overline{z}_j)$, et d'après (B) donc $[L_j : L_{j-1}] \leq 2$.

Nous montrons (B). Le point $z \in N^{(1)}$ est point d'interséction de deux éléments *différents* A et B de $G(N)$. Rappelons qu'une droite passant a et b est l'ensemble des nombres complexes z tels que $\mathrm{Re}(\overline{b} - \overline{a})(z - a)_{=}0$, i.e.

$$(\overline{b} - \overline{a})z + (b - a)\overline{z} = (\overline{b} - \overline{a})a + (b - a)\overline{a}.$$

Le cercle autour de a et de rayon $|d - c|$ est l'ensemble des z tels que

$$(z - a)(\overline{z} - \overline{a}) = (d - c)(\overline{d} - \overline{c}).$$

Cas 1 : A et B sont des droites. Donc z est solution de

$$(\overline{b} - \overline{a})z + (b - a)\overline{z} = (\overline{b} - \overline{a})a + (b - a)\overline{a}$$
$$(\overline{b}' - \overline{a}')z + (b' - a')\overline{z} = (\overline{b}' - \overline{a}')a + (b' - a')\overline{a}',$$

où $a, b, a', b' \in F$. Donc $z, \overline{z} \in F$ car

Cas 2 : A est une droite et B est un cercle. Ici z est solution de

$$(\overline{b} - \overline{a})z + (b - a)\overline{z} = (\overline{b} - \overline{a})a + (b - a)\overline{a}$$
$$(z - a')(\overline{z} - \overline{a}') = (d' - c')(\overline{d}' - \overline{c}')$$

avec $a, b, a', d', c' \in F$. La première équation exprime $\overline{z}$ en terme de z et élément de F (en particulier donc $\overline{z} \in F(z)$), est si nous remplaçons $\overline{z}$ dans équation 2 par cette expression, nous obtenons que z est racine d'une équation de degré 2 avec coéficients dans F. D'où $[F(z) : F] = 2$.

Cas 3 : A et B sont des cercles.

Ici z est solution de

$$(z - a)(\overline{z} - \overline{a}) = (d - c)(\overline{d} - \overline{c})$$
$$(z - a')(\overline{z} - \overline{a}') = (d' - c')(\overline{d}' - \overline{c}')$$

avec $a, d, c, a', d', c' \in F$. On soustrait l'équation 2 de l'équation 1 qui nous montre que z est solution de

$$z(\overline{a}' - \overline{a}) + \overline{z}(a' - a) = \text{truc } \in F,$$
$$(z - a')(\overline{z} - \overline{a}') = (d' - c')(\overline{d}' - \overline{c}').$$

Maintenant nous sommes dans cas 2, qui ést déja traité.

Finalement, *que 2. et 3. sont équivalentes*, nous avons déja montré dans un contexte plus général dans la section précédente : voir la démonstration que "Toute extension par radicaux est centenu dans une extension par radicaux galoisienne." En utilise que toute extension L/F de degré 2 est de la forme $L = F(b)$ avec un $b^2 \in F$ (Exercice). □

Nous étudions maintenant quelques applications concrètes à des problèmes classiques.

Théorème. (Gauss) *Le polygône régulier à n côtés peut être construit par règle et compas si et seulement si n est de la forme*

$$n = 2^t(2^{t_1} + 1)(2^{t_2} + 1) \cdots (2^{t_r} + 1)$$

où les $2^{t_j} + 1$ $(1 \leq j \leq r)$ sont des nombres premiers deux à deux différents et $t \geq 0$.

Remarque. Un nombre premier de la forme 2^t+1 est appelé **nombre premier de Fermat**. Il est facile à montrer que t doit être une puissance de 2 afin que $2^t + 1$ est premier. (Le réciproque est faux!!!!) Le premiers nombrede Fermat sont :

$$3, 5, 17, 257, 65537.$$

Les n-polygônes réguliers constructibles avec $n \leq 10000$ sont :

$$\begin{aligned}
&3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34,\\
&40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128,\\
&136, 160, 170, 192, 204, 240, 255, 256, 257, 272,\\
&320, 340, 384, 408, 480, 510, 512, 514, 544, 640,\\
&680, 768, 771, 816, 960, 1020, 1024, 1028, 1088,\\
&1280, 1285, 1360, 1536, 1542, 1632, 1920, 2040,\\
&2048, 2056, 2176, 2560, 2570, 2720, 3072, 3084,\\
&3264, 3840, 3855, 4080, 4096, 4112, 4352, 4369,\\
&5120, 5140, 5440, 6144, 6168, 6528, 7680, 7710,\\
&8160, 8192, 8224, 8704, 8738
\end{aligned}$$

Démonstration. Ici $M = \{0, 1\}$, $k = \mathbb{Q}$, et les bouts du n-polygône régulier sont les racines d'unités n-ème. Donc le n-polygône régulier est constructible si est seulement si $\varphi(n) = [\mathbb{Q}(\mu_n) : \mathbb{Q}]$ est une puissance de 2. Mais

$$\varphi(n) = 2^{t-1}\varphi(p_1^{s_1}) \cdots \varphi(p_r^{s_r})$$

si $n = 2^t p_1^{s_1} \cdots p_r^{s_r}$. Or $\varphi(p^s) = p^{s-1}(p - 1)$, et ceci, pour p impair, est une puissance de 2 si est seulement si $s = 1$ est $p - 1 = 2^t$ pour un t. D'où le théorème. □

Théorème. *(Duplication du cube ou problème de Deli) Le côte d'un cube de volume 2 (deux fois le volume du cube de côte 1) n'est pas constructible.*

Démonstration. En fait, le côte de ce cube est $\sqrt[3]{2}$. Mais $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, donc $\sqrt[3]{2}$ n'est jamais contenu dans une extension de $\mathbb{Q}$ de degré divisant 2^∞, donc $\sqrt[3]{2} \notin \Omega(\{0,1\})$. □

Théorème. *(Quadrature du cercle) Le côté d'un carré ayant même aire que le cercle de rayon 1 n'est pas constructible.*

Démonstration. Le côté en question est $\sqrt{\pi}$. Mais π est transcendant (d'après un Théorème de Lindemann), donc $\sqrt{\pi}$ l'est aussi, et $\Omega(\{0,1\}$ ne contient que de nombres algébriques. □

Théorème. *(Trissection de l'angle) Il est impossible en général de construire par règle et compas, pour un angle α donné, l'angle $\frac{1}{3}\alpha$.*

Démonstration. En fait, sinon le 9-polygône régulier était constructible (depuis le 3-polygône régulier, qui est constructible). □

Chapitre 2

Théories des nombres algébriques

Avant-propos.

Désormais nous utilisons les mots *corps de nombres* pour indiquer une extension algébrique K de degré fini sur $\mathbb{Q}$, qui est contenu dans $\mathbb{C}$. Nous utilisons $\overline{\mathbb{Q}}$ pour le corps des nombres complexes qui sont algébrique sur $\mathbb{Q}$. C'est — à lisomorphisme près — la clôture algébrique de $\mathbb{Q}$. Ainsi tout corps de nombres est un sous-corps de $\overline{\mathbb{Q}}$.

Soit K un corps de nombres. Nous utilisons $\mathbb{A} = \mathbb{A}_K$ pour l'ensemble des plongements $K \to \mathbb{C}$. Si $\rho : K \to \mathbb{C}$ est un plongement, alors soit ρ *est réel*, i.e. $\rho(K) \subset \mathbb{R}$, soit ρ *est complexe*, i.e. $\overline{\rho} \neq \rho$, où $\overline{\rho} : K \to \mathbb{C}$ est le plongement $a \mapsto \overline{\rho(a)}$, le bar désignant conjugaison complexe. Nous utilisons toujours r_1 pour le nombre de plongements réel, et r_2 pour le nombre d'ensembles $\{\rho, \overline{\rho}\}$ de plongements complexes. On a

$$r_1 + 2r_2 = [K : \mathbb{Q}].$$

Finalement, nous définissons pour $a \in K$ *la norme et la trace* de K à $\mathbb{Q}$ par les formules

$$\mathrm{N}(a) = \mathrm{N}_{\mathrm{K}/\mathbb{Q}}(a) := \prod_{\sigma} \sigma(a),$$
$$\mathrm{Tr}(a) = \mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}(a) := \sum_{\sigma} \sigma(a).$$

Ici σ parcours tous les plongements $\sigma : K \to \mathbb{C}$. Ces symboles définissent des morphismes de groupes

$$\mathrm{N} : K^* \to \mathbb{Q}^*, \quad \mathrm{Tr} : K \to \mathbb{Q}.$$

Pour vérifier que $\mathrm{N}(a)$ et $\mathrm{Tr}(a)$ sont dans $\mathbb{Q}$ on peut procéder comme ceci : Soit K_G la *clôture galoisienne de* K, i.e. l'extension galoisienne de $\mathbb{Q}$ le plus petit contenant K. (Rappel : On a toujours $K = \mathbb{Q}(\alpha)$ avec un α convenable, et K_G est le corps de décomposition du polynôme minimal de a sur $\mathbb{Q}$.)

Le groupe $\mathrm{Gal}(K_G/\mathbb{Q})$ agit sur l'ensemble des plongement $\mathbb{A}_K$: Si $\sigma : K \to \mathbb{C}$ est un plongement, et si ρ est un automorphisme de K_G, alors $\rho \circ \sigma$ est toujours un plongement de K.

Ainsi on obtient que $\mathrm{N}(a)$ et $\mathrm{Tr}(a)$ sont stable sous $\mathrm{Gal}(K_G/\mathbb{Q})$, donc dans $\mathbb{Q}$.

2.1 Nombres entiers algébriques

Un nombre algébrique, i.e. un $a \in \overline{\mathbb{Q}}$, est *entier* si a est la racine d'un polynôme normalisé avec des coéfficient dans $\mathbb{Z}$. Soit $\overline{\mathbb{Z}}$ l'ensemble des entiers algébriques. Pour un corps de nombres K nous posons

$$O_K := K \cap \overline{\mathbb{Z}}.$$

Un nombre rationnel a est entier — selon cette définition —si et seulement si $a \in \mathbb{Z}$: en fait, si $a \in \mathbb{Z}$, alors a est racine du polynôme $X - a \in \mathbb{Z}[X]$. Réciproquement, si $a = \frac{p}{q}$, disons $\mathrm{pgcd}(p, q) = 1$, et si

$$a^n + a_{n-1}a^{n-1} + \cdots + a_1 a + a_0 = 0$$

avec des $a_j \in \mathbb{Z}$, alors

$$p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n = 0,$$

et alors $q|p^n$, d'où $q = \pm 1$ et $a \in \mathbb{Z}$. Donc les entiers algébriques dans $\mathbb{Z}$ forment un anneau. C'est vrai en général.

Lemme. *Soient $a_j \in \overline{\mathbb{Q}}$ $(1 \leq j \leq n)$. Alors les a_j sont entiers si et seulement si l'anneau $\mathbb{Z}[a_1, \cdots, a_n]$ est un $\mathbb{Z}$-module du type fini.*

Regarder l'exemple $\mathbb{Z}[\frac{1}{3}]$, qui n'est pas de type fini en tant que $\mathbb{Z}$-module, car les dénominateurs des éléments de $\mathbb{Z}[\frac{1}{3}]$ ne sont pas bornés.

Démonstration. Si $A \subset B$ sont des anneaux arbitraires (mais commutatives et avec 1), et si $b \in B$, alors on appele b entier sur A si b est racine d'un polynôme normalisé dans $A[x]$.

Supposons que b est entier sur A. Alors $A[b]$ est un A-module de type fini : en fait soit $f(b) = 0$ avec un $f \in A[x]$ normalisé. Si $c \in A[b]$, disons $c = g(b)$ pour un $g \in A[x]$, il existe $q, r \in A[x]$ tel que

$$g(x) = q(x) \cdot f(x) + r(x), \deg(r) < \deg(g) =: k$$

Ceci est une conséquence immédiate de l'algorithme usuel pour faire la division euclidienne, en utilisant que le coéfficient dominant de g est 1. Mais puis $c = g(b) = r(b)$. En conséquence $A[b]$ est engendré en tant que A-module par $1, b, \ldots, b^{k-1}$.

Que $A[b_1, \cdots, b_n]$ est un A-module de type fini, si les $b_j \in B$ sont entiers sur A, est montré maintenant par récurrence sur n, en utilisant que b_j entier sur A implique que b_j est entier sur $A[b_1, \cdots, b_{j-1}]$.

Supposons réciproquement que $b_j \in B$ sont tels que $R := A[b_1, \cdots, b_n]$ est un A-module de type fini. Soit $c_1, \cdots, c_k$ un système de générateurs de R sur A. Alors, pour tout $b \in R$, il existe une matrice M sur A tel que

$$(c_1, \cdots, c_k)(bE - M) = 0,$$

où E est la matrice d'unité. Soit $(bE - M)^*$ la matrice adjointe de $bE - M$ (i.e. la matrice sur A dont les éléments sont des sous-déterminants de $bE - M$ multipliés par ± 1 et telle que $(bE - M)(bE - M)^* = \det(bE - M)\, E$). Multipliant par $(bE - M)^*$ nous obtenons

$$(c_1, \cdots, c_k) \cdot \det(bE - M) = 0,$$

et car il existe $a_j \in A$ tels que $1 = a_1 c_1 + \cdots a_k c_k$, alors $\det(bE - M) = 0$. Mais $\det(xE - M)$ est un polynôme normalisé dans $A[x]$. □

Théorème. *$\overline{\mathbb{Z}}$ est un sous-anneau de $\overline{\mathbb{Q}}$. En particulier, tout O_K est un sous-anneau de K.*

Démonstration. En fait, si a et b sont entiers, alors $\mathbb{Z}[a, b]$ est un $\mathbb{Z}$-module de type fini, donc les sous-modules $\mathbb{Z}[a + b]$ et $\mathbb{Z}[a \cdot b]$ le sont également. □

Pour déterminer un polynôme normalisé sur $\mathbb{Z}$ qui a comme racine $a+b$ ou $a \cdot b$, pour des entiers algébriques a et b, on choisit une extension galoisiennes K contenant a et b. Puis le polynôme

$$f := \prod_{\sigma \in \mathbb{A}} \prod_{\rho \in \mathbb{A}} (X - \sigma(a) - \rho(b)).$$

est stable sous $\mathrm{Gal}(K/\mathbb{Q})$, donc dans $\mathbb{Q}[X]$. En plus les coéfficients de f sont des entiers algébriques, donc on a $f \in \mathbb{Z}[X]$. Finalement f est normalisé. Evidemment $f(a + b) = 0$. La construction pour $a \cdot b$ est similaire. Ici on considère

$$g = \prod_{\sigma \in \mathbb{A}} \prod_{\rho \in \mathbb{A}} (X - \sigma(a) \cdot \rho(b)).$$

Comme déjà utilisé nous avons immédiatement de la définition que $\sigma(a)$ est entier si $a \in K$ l'est et si $\sigma : K \to \mathbb{C}$ un plongement. En conséquence

les racines du polynôme minimal f d'un entier algébrique a sont entières, et d'après le théorème précédent les coéfficients de f (en tant que fonctions symmétrique dans les $\rho(a)$) sont entiers, alors dans $\mathbb{Z}$. On peut donc dire : *Un $a \in \overline{\mathbb{Q}}$ est entier ?????????????ssi le polynôme minimal de a a des coéfficient entier.*

Un argument pareil montre aussi que

$$\mathrm{N}_{K/\mathbb{Q}}(O_K) \subset \mathbb{Z}, \quad \mathrm{Tr}_{K/\mathbb{Q}}(O_K) \subset \mathbb{Z}.$$

Comme exemples plus subtil pour des anneaux des entiers dans un corps de nombre *nous étudions le cas* $[K : \mathbb{Q}] = 2$.

Il existe un $d \in \mathbb{Q}$, tel que $K = \mathbb{Q}(\sqrt{d})$. On vérifie que $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$ si est seulement si $d = d'x^2$ pour un $x \in \mathbb{Q}$. Autrement dit, les extensions de degré 2 sont en bijections avec les élément différent de 1 du groupe

$$\mathbb{Q}^*/(\mathbb{Q}^*)^2.$$

Chaque classe contient un unique entier d qui n'est pas divisible par un carré d'un nombre premier *(on dit :"qui ne contient aucun carré")*. On pose

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

Donc $D \equiv 0, 1 \bmod 4$, i.e. D est un carré $\bmod 4$. On appele D *le discriminant de* $K = \mathbb{Q}(\sqrt{d})$.

Tout élement a de K s'écrit de manière unique

$$a = x + y\sqrt{D}$$

avec $x, y \in \mathbb{Q}$. Si $y = 0$ alors a est entier ssi $x \in \mathbb{Z}$. Sinon le polynôme minimale f de a est

$$f = X^2 - 2xX + (x^2 - y^2 D) = X^2 - \mathrm{Tr}(a)X + \mathrm{N}(a).$$

Donc a est entier ssi

$$2x \in \mathbb{Z}, \quad x^2 - y^2 D \in \mathbb{Z}.$$

Ceci entraîne par un simple calcul

Théorème. *Soit K un corps de nombre de degré 2 sur $\mathbb{Q}$, soit D son discriminant. Alors*

$$O_K = \begin{cases} \mathbb{Z}[\frac{\sqrt{D}}{2}] & \textit{pour } D \textit{ pair} \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & \textit{pour } D \textit{ impair.} \end{cases}$$

Nous avons donc par exemple

$$O_{\mathbb{Q}[i]} = \mathbb{Z}[i], \quad O_{\mathbb{Q}(\mu_3)} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$$
$$O_{\mathbb{Q}[\sqrt{5}]} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}], \quad O_{\mathbb{Q}[\sqrt{-5}]} = \mathbb{Z}[\sqrt{-5}].$$

Nous considérons les corps cyclotomiques. Clairement $O_{\mathbb{Q}(\mu_n)} \supset \mathbb{Z}[\zeta]$. On a même

Théorème. *Soit $n > 0$ un nombre naturel et ζ une racine d'unité n-ième primitive. Alors*

$$O_{\mathbb{Q}(\mu_n)} = \mathbb{Z}[\zeta].$$

Lemme. *Soit $n = l^\nu$ pour un premier l, et soit $\lambda := 1 - \zeta$. Alors, pour $O = O_{\mathbb{Q}(\mu_n)}$, on a*

$$lO = \lambda^{l^{\nu-1}(l-1)} O.$$

Démonstration. On a

$$\phi_n = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^*} (X - \zeta^a) = \frac{x^{l^\nu} - 1}{x^{l^{\nu-1}} - 1}$$
$$= (x^{l^{\nu-1}})^{l-1} + (x^{l^{\nu-1}})^{l-2} + \cdots + 1.$$

Pour $x = 1$ on en déduit

$$l = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^*} (1 - \zeta^a).$$

Mais $1 - \zeta^a = \lambda\varepsilon$, où (en supposons $a > 0$)

$$\varepsilon = \frac{1-\zeta^a}{1-\zeta} = \zeta^{a-1} + \cdots 1 \in O.$$

De même

$$\frac{1}{\varepsilon} = \frac{1-\zeta}{1-\zeta^a} = \frac{1-\zeta^{aa'}}{1-\zeta^a} = \text{polynôme en } \zeta \in O$$

(oú a' est un entier tel que $aa' \equiv 1 \bmod n$), donc $\varepsilon \in O^*$, et d'où l'identité. □

Démo. du théorème. Nous considérons ici seulement le cas que n est un nombre premier l, en laissant le cas général comme exercice (voir les exercices à la prochaine section).

Soit $a \in O := O_{\mathbb{Q}(\mu_l)}$. Ecrivons

$$a = r_{l-2}\zeta^{l-2} + \cdots + r_0$$

avec des nombres rationnels r_j. Nous devons montrer que les r_j sont entiers.

Nous avons l'identité

$$\sum_{1 \le a \le l-1} \zeta^{ak} = \begin{cases} l-1 & \text{if } l|k \\ -1 & \text{sinon.} \end{cases}$$

Par un petit calcul donc

$$lr_k = \mathrm{Tr}(a\zeta^{-k} - a\zeta).$$

Car $a\zeta^{-k} - a\zeta$ est entier, nous en déduisons $lr_k \in \mathbb{Z}$. Nous voulons montrer $lr_k \in l\mathbb{Z}$.

Or,

$$l\mathbb{Z} = \lambda O \cap \mathbb{Z}$$

avec $\lambda = 1 - \zeta$ comme dans le lemme ci-dessus : il est clair que $l\mathbb{Z} \in \lambda O$ (car l est un multiple dans O de λ^{l-1} d'après le lemme), et si λO contenait un $m \in \mathbb{Z}$ divisible par un premier $p \neq l$, alors $lO = \lambda^{l-1}O$ contenait m^{l-1}, donc $1 = \mathrm{pgcd}(l, m^{l-1}) \in lO$, donc $1/l \in O$, i.e. $1/l$ entier, une contradiction. Il suffit donc à montrer que $lr_j \in \lambda O$.

Ecrivons

$$la = c_{l-2}\lambda^{l-2} + \cdots + c_0.$$

Alors les c_j sont des entiers. Nous montrons que tous les c_j sont multipes (dans O) de λ. Ceci implique que les lr_j le sont également.

Supposons que nous avons déjà montrer que $c_j \in \lambda O$ pour $0 \le j \le k-1$. Alors, en utilisant que $l \in \lambda^{l-1}O$, nous obtenons depuis la dernière formule pour la que

$$c_k\lambda^k \equiv la \equiv 0 \bmod \lambda^{k+1}O.$$

Mais alors $c_k \in \lambda O$, et c'était à montrer. □

Nous utilisons (comme d'habitude) O_K^* pour *les unités de* O_K, i.e. pour les entiers a dans K tel que $1/a$ est également un entier.

Théorème. *Soit $a \in K$. Alors $a \in O_K^*$ si et seulement si $\mathrm{N}_{K/\mathbb{Q}}(a) = \pm 1$.*

Démonstration. Si $a \in O_K^*$, alors $\mathrm{N}(a), \mathrm{N}(1/a) = 1/\mathrm{N}(a) \in \mathbb{Z}$, donc $\mathrm{N}(a) = \{\pm 1\}$. Réciproquement, on a

$$\mathrm{N}(a)/a = \prod_{\sigma \neq \mathrm{Id}} \sigma(a)$$

où σ parcourts les plongements de K dans $\mathbb{C}$ différent de l'Id. Donc $\mathrm{N}(a)/a$ est entier. Si $\mathrm{N}(a) = \pm 1$ nous en déduisons alors que $1/a$ est entier. □

Soient $a, b \in O_K$. Nous disons que a *divise* b (avec des symbols : $a|b$) si $b = ax$ pour un $x \in O_K$, i.e. si b/a est entier. Rappelons qu'un élément a de O_K est dit *irréductible* si $a = bc$ avec $b, c \in O_K$ implique que b ou c est une unité (i.e. dans O_K^*).

Théorème. *Tout $a \in O_K$, $a \notin O_K^*$, possède une décomposition*

$$a = I_1 I_2 \cdots I_n$$

où les I_j $(1 \leq j \leq n)$ sont des éléments irréductibles dans O_K.

Démonstration. Par récurrence sur $|\mathrm{N}(a)|$: Si a n'est pas irréductible et n'est pas une unité, alors $a = a_1 a_2$ où le a_j ne sont pas d'unités. En particulier, $\mathrm{N}(a) = \mathrm{N}(a_1)\mathrm{N}(a_2)$ et $|\mathrm{N}(\mathrm{a_j})| < |\mathrm{N}(a)|$. □

La décompoistion du théorème n'est pas unique n générale. L'exemple celèbre :

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

dans $O_{\mathbb{Q}(\sqrt{-5})}$. Ici tous les nombres à droits sont irréductibles car ses normes sont 4, 9 et 6, mais il n'existe pas des éléments dans O_K avec normes 2 ou 3 (car $x^2 + 5y^2 = 2, 3$ ne possède pas de solutions $x, y \in \mathbb{Z}$).

Théorème. *Supposons que O_K un anneau principal. Alors la décomposition du théorème précédent est unique, à l'ordre des I_j et à multiplication des I_j par des unités près.*

Démonstration. Dans un anneau principal tout élément irréductible est premier (Rappel : a est premier si pour tout $b, c \in O_K$ on a

$$a|bc \Longrightarrow a|b \text{ ou } a|c.)$$

En fait : Soit a irréductible, $a|bc$. Si $a \not| b$ alors considérer le O_K-idéal $\mathfrak{a} := O_K a + O_K b$. On a $\mathfrak{a} = O_K a'$ pour un $a' \in O_K$, en particulier $a'|a$. Car a est irréductible, alors $a' = \varepsilon$ ou $a' = a\varepsilon$ pour un $\varepsilon \in O_K^*$. Le dernier est impossible car $a'|b$, mais $a \not| b$. Donc $\mathfrak{a} = O_K$, i.e. $1 = ax + by$ pour des $x, y \in O_K$. D'où $c = acx + cby$, d'où $a|c$.)

Utilisons que les I_j sont alors premiers, entraîne le théorème par une simple récurrence sur des nombres de facteurs dans la décomposition $a = \prod I_j$. □

Il y alors deux problèmes :

1. Pour quel K est O_K un anneau principal ?
2. Est-ce qu'il existe un remplacement pour la décomposition unique en facteurs premiers dans O_K dans le cas où O_K n'est pas principal ?

Nous allons répondre à la question 2. dans le prochaine séction, et à 1. plus tard.

2.2 Idéaux fractionnaires

Dans le corps de nombre $\mathbb{Q}(\sqrt{-5})$ la décomposition en nombres irréductibles n'est pas unique :

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

L'idée de **Kummer** était qu'il existe des nombres "idéaux" dans une certaine extension dans laquelle les nombres entiers de K se décomposent uniquement en nombres premiers "idéaux". Ainsi on aurait peut-être comme décomposition premiers

$$21 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$$

et l'ambiguité ci-dessus s'expliquerait par le fait

$$3 = \mathfrak{p}_1\mathfrak{p}_2, 7 = \mathfrak{p}_3\mathfrak{p}_4,$$
$$(1 + 2\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3, (1 - 2\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_4.$$

Dedekind a découvert comment on peut construire naturellement de tels nombres idéaux :

Si $\mathfrak{a}$ est un nombre idéal, alors n'importe pas comment on la réalise, en tout cas il faut avoir des relations de divisibilités $\mathfrak{a}|a$ entre ce nombre idéal et les $a \in O_K$ avec des propriétés suivantes :

$$\mathfrak{a}|a,\ \mathfrak{a}|b,\ \lambda,\ \mu \in O_K \Longrightarrow \mathfrak{a}|(\lambda a + \mu b),$$

et $\mathfrak{a}$ doit être uniquement déterminé par l'ensemble

$$\{a \in O_K : \mathfrak{a}|a\}.$$

Mais alors la chose la plus naturelle est de considérer comme nombres idéaux les sous-ensembles $\mathfrak{a}$ de O_K qui ont la propriétés

$$a \in \mathfrak{a},\ b \in \mathfrak{a},\ \lambda, \mu \in O_K \Longrightarrow \lambda a + \mu b \in \mathfrak{a},$$

i.e. les *idéaux de* O_K comme on dit dans la langue moderne. Si on écrit pour un O_K-idéal $\mathfrak{a}|a$ *pour* $a \in \mathfrak{a}$ on a exactement les deux premières propriétes en question. Cette idée de Dedekind était en fait la naissance de la théories des idéaux dans des anneaux comme on la connait aujourdhui, et les idéaux doivent leur nom aux nombres "idéaux" de Kummer.

Nous allons étudier donc les anneaux de O_K.

Théorème. *Tout O_K-sous-module de type fini $M \neq 0$ du corps de nombre K est un $\mathbb{Z}$-module libre de rang $n = [K : \mathbb{Q}]$.*

En particulier, si $n = [K : \mathbb{Q}]$, alors

$$O_K = \mathbb{Z}a_1 + \cdot + \mathbb{Z}a_n$$

avec une $\mathbb{Q}$-base $a_1, \cdots, a_n$ de K.

Démonstration. Soit $a_1, \cdots, a_n$ une base de K sur $\mathbb{Q}$. Par le lemme précédent on peut supposer que les a_j sont entiers. Nous allons monter ci-dessous qu'il existe un nombre $d \neq 0$ tel que??????????????

$$dO_K \subset \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n =: M_0 \subset O_K.$$

Car M_0 est un $\mathbb{Z}$-module de type fini libre, et car $\mathbb{Z}$ est principal, on a alors que dO_K, et donc aussi O_K, est un $\mathbb{Z}$-module de type fini libre, et on a

$$\text{rang}(O_K) = \text{rang}(dO_K) \leq \text{rang}(M_0) = n \leq \text{rang}(O_K),$$

i.e. $\text{rang}(O_K) = n$.

Soit maintenant m_j $(1 \leq j \leq r)$ un système de générateurs du O_K-module M. Choisir $a \in \mathbb{Z}$, $a \neq 0$ tel que $am_j \in O_K$ pour tout j, i.e. $aM \subset O_K$. On a ainsi

$$adM \subset aO \subset \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n = M_0.$$

Encore, car M_0 est un $\mathbb{Z}$-module de type fini libre, et $\mathbb{Z}$ est principal, on a que adM, et donc aussi M, est un $\mathbb{Z}$-module de type fini libre. En plus

$$\text{rang}(M) = \text{rang}(adM) \leq \text{rang}(M_0) = n.$$

D'autre part, $n = \text{rang}(O_K) = \text{rang}(m_1 O_K) \leq \text{rang}(M)$ (car $m_1 O \subset M$), et d'où $\text{rang}(M) = n$.

Il reste à montrer l'existence de d. Soit $a \in O_K$. Il existe des $x_j \in \mathbb{Q}$ tel que $a = \sum_j x_j a_j$. Donc les x_j sont solutions du système d'équations linéaires

$$\text{Tr}(a_i a) = \sum_j x_1 \text{Tr}(a_i a_j) x_j \quad (1 \leq i \leq n).$$

Par le lemme ci-dessus la matrice $(\text{Tr}(a_i a_j))$ de ce système est regulière, et donc on peut prendre pour d le déterminant de cette matrice. □

Lemme. *L'application $(x, y) \mapsto \text{Tr}_{K/\mathbb{Q}}(x, y)$ définit une forme bilinéaire non-dégénérée sur le $\mathbb{Q}$-espace vectoriel K.*

Démonstration. En fait, soit $K = \mathbb{Q}[a]$. Alors, a^j $(0 \leq j < n := [K : \mathbb{Q}])$ est une base de K sur $\mathbb{Q}$, et dans cette base on a

$$(\mathrm{Tr}(a^i a^j))_{0 \leq i,j < n} = M^t M,$$

(matrice de Gram) où

$$M = \begin{pmatrix} a^0 & a^1 & \cdots & a^{n-1} \\ \sigma_2(a^0) & \sigma_2(a^1) & \cdots & \sigma_2(a^{n-1}) \\ \vdots & \vdots & \cdots & \vdots \\ \sigma_n(a^0) & \sigma_n(a^1) & \cdots & \sigma_n(a^n) \end{pmatrix}.$$

Ici les σ_i parcourt les plongement de K dans $\mathbb{C}$ (et $\sigma_1 = 1$). Or, le déterminant de M et un déterminant de Vandermond : on a

$$\det(M) = \prod_{i<j} (\sigma_i(a) - \sigma_j(a)).$$

Donc $\det(M) \neq 0$, car les $\sigma_i(a)$ (en tant que racines du olynôme minimal de a sur $\mathbb{Q}$) sont 2 à 2 différents. □

Théorème. *O_K est un anneau de Dedekind, i.e. O_K est intègre, noethérien, intégralement clos, et tout idéal premier$\neq 0$ est maximal.*

Démonstration. Comme $\mathbb{Z}$-sous-module de O_K tout idéal de O_K est libre de rang fini, donc en particulier de type fini en tant que O_K-module. Un anneau intègre A est dit intégralement clos, si tout a dans son corps de fraction, qui est entier sur A, apartient déjà à A. C'est vrai pour O_K : si $a \in K$ est racine du polynôme normalisée $f \in O_K[x]$, alors a est aussi racine de $F := \prod_\sigma \sigma(f)$ où σ parcourt les plongemants de K. Mais F est normalisé avec coéfficient dans $\mathbb{Z}$, donc a est un entier algébrique, donc dans O_K.

Soit $\mathfrak{p} \neq 0$ un idéal premier de O_K. Le rang des $\mathbb{Z}$-modules O_K et $\mathfrak{p}$ est n, donc $O_K/\mathfrak{p}$ est fini. L'idéal $\mathfrak{p} \cap \mathbb{Z}$ de $\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$, disons $p\mathbb{Z}$ avec un nombre premier p (si pour $a, b \in \mathbb{Z}$ on a $ab \in \mathfrak{p} \cap \mathbb{Z}$, $b \notin \mathfrak{p} \cap \mathbb{Z}$, alors $b \in \mathfrak{p}$, donc $b \in \mathfrak{p} \cap \mathbb{Z}$). L'inclusion $\mathbb{Z} \subset O_K$ induit une injection

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \to O_K/\mathfrak{p}.$$

L'anneau entier est donc un $\mathbb{F}_p$ espace vetoriel de dimension finie, provient de $\mathbb{F}_p$ en rajoutant des élément algébriques, est donc un corps. □

Un O_K-sous-module de K de type fini est aussi appelé *idéal fractionnaire de K. L'ensemble des idéaux fractionnaire différents de 0 est noté*

$$J = J_K.$$

Nous définissons **le produit de deux O_K-idéaux fractionnaire $\mathfrak{a}$ et $\mathfrak{b}$** par

$$\mathfrak{a} \cdot \mathfrak{b} := \{\sum_j a_j b_j : a_j \in \mathfrak{a},\ b_j \in \mathfrak{b}\}.$$

On vérifie que ceci est encore un O_K-module de type fini (si a_j est b_k sont des générateurs de $\mathfrak{a}$ et $\mathfrak{b}$ sur O, alors $a_j b_k$ sont des générateurs de $\mathfrak{a} \cdot \mathfrak{b}$.). Ainsi J_K devient un semi-groupe avec élément neutre O_K. Nous montrons que J_K, muni de cette multiplication, et même un groupe. Plus précisement, nous posons pour un élément $\mathfrak{a} \in J_K$

$$\mathfrak{a}^{-1} := \{a \in K : a\mathfrak{a} \subset O_K\},$$

et nous montrerons que $\mathfrak{a}^{-1}$ est un O-module de type fini et que $\mathfrak{a} \cdot \mathfrak{a}^{-1} = O_K$.

Si $a \in K$, $a \neq 0$, alors $(a) = aO_K$ est (évidemment) un idéal fractionnaire de K. L'ensemble des *idéaux fractionnaire principaux* (i.e. les aO_K où a parcourt K^*) est noté P_K. Il est clair que c'est un sous groupe de J_K. Le groupe de quotient

$$C_K := J_K/P_K$$

est appelé *le groupe des classes de K.*

Théorème. *L'anneau O_K est principal si et seulement si C_K est trivial.*

Lemme. *Pour tout nombre algébrique il existe un nombre entier $N \neq 0$ tel que Na est entier.*

Démonstration. Soit $f \in \mathbb{Q}[x]$ un polynôme différent de 0, qui a a comme racine. On peut supposer (en multipliant f par un nombre entier convenable) que f a des coéfficient entier, disons

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \quad (a_n \neq 0).$$

Mais alors $a_n a$ est racine de

$$x^{n-1} + a_n a_{n-1} x^{n-1} + \cdots + a_n^n a_0,$$

donc entier. □

Demo. du théorème. Supposons que $C_K = 1$. Soit $\mathfrak{a}$ un idéal de O. Alors $\mathfrak{a}P_K = P_K$, i.e. $\mathfrak{a}$ est principal.

Réciproquement, soit tout idéal de O principal. Soit $\mathfrak{a}$ un idéal fractionnaire. D'aprés le lemme il existe un naturel $N > 0$ tel que $N\mathfrak{a} \subset O$ (on utilise que $\mathfrak{a}$ possède un nombre fini de générateurs sur O). Donc $N\mathfrak{a} = (a)$, d'où $\mathfrak{a} = (a/N)$. □

Le groupe C_K est donc une mésure pour le défaut de O_K d'être principal.

Nous étudions C_K pour le cas que K est un corps de nombre quadratique imaginaire, i.e. $K = \mathbb{Q}(\sqrt{D})$ où le discriminant D de K est négatif.

Une forme quadratique binaire entière est un polynôme homogéne de degré 2

$$ax^2 + bxy + cy^2 \in \mathbb{Z}[x].$$

Suivant la notation de Gauß nous la notons

$$[a, b, c].$$

Nous appelons

$$\Delta := b^2 - 4ac$$

le discriminant de $[a, b, c]$, et nous l'appelons définie positive si $\Delta < 0$ et $a > 0$. En fait, dans ce cas-là

$$ax^2 + bxy + cy^2 = a\left|x + \frac{b + \sqrt{D}}{2a}y\right|^2 > 0$$

pour tout $(x, y) \neq 0$.

L'ensemble des formes binaires quadratiques entières defini-positives à discriminant D est noté $\mathcal{Q}$.

Nous considérons l'application

$$G : \mathcal{Q} \to J_K/P_K, \quad [a, b, c] \mapsto \left(O + O\frac{b + \sqrt{D}}{2a}\right) P_K.$$

Nous laissons comme exercice (facile) à montrer

$$O + O\frac{b + \sqrt{D}}{2a} = \mathbb{Z} + \mathbb{Z}\frac{b + \sqrt{D}}{2a}.$$

Théorème. *L'application*

$$G : [a, b, c] \mapsto \left(\mathbb{Z} + \mathbb{Z}\frac{b + \sqrt{D}}{2a}\right) P_K$$

est surjective. Pour $f, g \in \mathcal{Q}$ on a $G(f) = G(g)$ ssi il existe un $A \in \mathrm{SL}(2, \mathbb{Z})$ tel que $f = g^A$.

Ici g^A dénote l'action naturelle de $\mathrm{SL}(2, \mathbb{Z})$ sur $\mathcal{Q}$ définie par

$$g^A(x, y) = g\big((x, y)A\big)$$

(où $(x, y)A$ est le produit matriciel usuel).

Démonstration. Soit $\mathfrak{a}$ un idéal fractionnaire. Alors $\mathfrak{a} = \mathbb{Z}a + \mathbb{Z}b$. On peut supposer que $a = 1$ et $\mathrm{Im}(b) > 0$ (sinon remplacer $\mathfrak{a}$ par $(\frac{1}{a})\mathfrak{a}$ et remplacer b par $-b$ si necessaire). Donc

$$\mathfrak{a} = \mathbb{Z} + \mathbb{Z}b \quad (\mathrm{Im}(b) > 0).$$

Nous montrons dans un premier temps que

$$b = \frac{\beta + \sqrt{D}}{2a} \quad (\beta, a \in \mathbb{Z}, a > 0),$$

et que $ab \in O$.

Pour ceci nous utilisons que $\mathfrak{a}$ est un O-module. En particulier $O \subset \mathfrak{a}$ (car $1 \in \mathfrak{a}$), et donc, pour tout $c \in O$ on a que

$$\begin{pmatrix} 1 & b \\ 1 & \overline{b} \end{pmatrix}^{-1} \begin{pmatrix} c \\ \overline{c} \end{pmatrix} = \frac{\begin{pmatrix} \overline{b} & -b \\ -1 & 1 \end{pmatrix}}{\overline{b} - b} \begin{pmatrix} c \\ \overline{c} \end{pmatrix} = \begin{pmatrix} \frac{\mathrm{Im}(b\overline{c})}{\mathrm{Im}(b)} \\ \frac{\mathrm{Im}(c)}{\mathrm{Im}(b)} \end{pmatrix}$$

est dans $\mathbb{Z}^2$.

En choisissant $c = \frac{D+\sqrt{D}}{2} \in O$, nous obtenons ainsi que $\sqrt{D}/\mathrm{Im(b)}$ est un entier rationnel, d'où $b = \frac{\beta+\sqrt{D}}{2a}$ avec un nombre naturel a et un nombre rationnel β. Car $\mathrm{Im}(b) > 0$ nous avons en plus $a > 0$. En plus, $\mathrm{Im}(b\overline{c})/\mathrm{Im}(b) = (D - \beta)/2$ doit être entier, donc $\beta \in \mathbb{Z}$ et $ab \in O$

Mais alors la classe $\mathfrak{a}P_K$ est l'image réciproque de la forme

$$a|x + by|^2 = ax^2 + \beta xy + \frac{\beta^2 - D}{4a} y^2.$$

(Pour vérifier que $\frac{\beta^2-D}{4a} = a|b|^2$ est entier noter $|a\mathfrak{a}/abO| = ab\overline{b}$ — exercice.)

Soient maintenant

$$f = a\left|x + \frac{b + \sqrt{D}}{2a} y\right|^2, \; g = a'\left|x + \frac{b' + \sqrt{D}}{2a'} y\right|^2$$

deux éléments de $\mathcal{Q}$ tels que $G(f) = G(g)$, i.e.

$$\mathbb{Z} + \mathbb{Z}\frac{b + \sqrt{D}}{2a} = (\mathbb{Z} + \mathbb{Z}\frac{b' + \sqrt{D}}{2a'})c$$

avec un $c \in K$ convenable. Il existe une matrice $A \in \mathrm{Gl}(2, \mathbb{Z})$ tel que

$$A\begin{pmatrix} 1 & 1 \\ \frac{b+\sqrt{D}}{2a} & \frac{b-\sqrt{D}}{2a} \end{pmatrix} = \begin{pmatrix} c & \overline{c} \\ c\,\frac{b'+\sqrt{D}}{2a'} & \overline{c},\,\frac{b'-\sqrt{D}}{2a'} \end{pmatrix}$$

En comparant les déterminant nous observons que $\det A = +1$. En plus, la dernière identité implique

$$f^A = \frac{a|c|^2}{a'} g$$

De fait que $\operatorname{pgcd}(a,b,c) = \operatorname{pgcd}(a',b',c') = 1$ (si on avait, par exemple, $n = \operatorname{pgcd}(a,b,c) > 1$, alors $n^2|D$ et D/n^2 serait un carrée mod 4, qui n'est pas possible (exercice)), on déduit facilement $a|c|^2 = a'$. □

Théorème. *Chaque classe (orbite) de $\mathcal{Q}/\mathrm{SL}(2,\mathbb{Z})$ contient une forme $[a,b,c]$ avec $|b| \le a \le c$.*

Une forme qui satisfait les inégalités du théorème est dite *réduite*.

Démonstration. Nous utilisons les formules

$$[a,b,c]^{T^x} = [a, b+2ax, c'] \qquad \left(T = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix},\ x \in \mathbb{Z}\right)$$

$$[a,b,c]^S = [c,-b,a] \qquad \left(S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right)$$

En effectuant un suites de ces opérations avec un peu de bon sens on construit, commençant avec une forme $f = [a,b,c]$ non-réduite donné, une suite de formes $[a_n,b_n,c_n]$ qui sont tous équivalentes à f et qui satisfont $|b_n| \le a_n$, $c_n < a_n$, et $a_n < a_{n-1}$. Il est clair qu'une telle suite doit être fini (car le $|a_j|$ sont des naturels) et que l'on termine avec une forme réduite. Comme exemple pour cet argument nous regardons

$$[9,7,3] \to_S [3,-7,9] \to_T [3,-1,5].$$

□

Lemme. *Le nombre de formes réduites $[a,b,c]$ (i.e. telles que $|b| \le a \le c$) à discriminant $\Delta = b^2 - 4ac < 0$ est fini.*

Démonstration. En utilisant les inégalités pour les coéfficients on obtient

$$|\Delta| = 4ac - b^2 \ge 4a^2 - a^2 = 3a^2,$$

$$a < \sqrt{\frac{|\Delta|}{3}} =: S$$

Or le nombre de couple (a,b) d'entiers avec $|b| \le a \le S$ est fini, et, pour chaque tel couple il existe au plus un naturel c tel que $c = \frac{b^2-\Delta}{4a}$. □

Ces théorèmes nous donne un moyen facile pour calculer l'ordre du groupe de classes $G = J_K/P_K$ du corps quadratique imaginaire avec discriminant K :

1. Faire une liste des couples (a, b) avec $|b| \leq a \leq (|\Delta|/3)^{\frac{1}{2}}$ (et $b \equiv D \bmod 2$).
2. Jeter les couples pour lesquels $c := (b^2 + \Delta)/4a$ n'est pas entier ou $c < a$.
3. Le nombre des couples restant est un majorant pour $|G|$.

En fait, on peut montrer facilement que deux formes réduites sont inéquivalentes à part de quelques cas "pathologiques".

Comme exemple nous prenons le cas $K = \mathbb{Q}(\sqrt{-5})$. Le discriminant du corps est $D = -20$. Le majorant pour les a est $S = \lfloor\sqrt{20/3}\rfloor = 2$. Couples possibles donc :

$$(1, 0) : c = 5, (2, -2) : c = 3,$$
$$(2, 0) : c = \frac{5}{4}, (2, +2) : c = 3.$$

Ici $[2, -2, 3]^{T^2} = [2, 2, 3]$, et $[1, 0, 5]$ n'est pas équivalent à $[2, 2, 3]$ (exercice). Résumé :

$$|J_K/P_K| = 2.$$

En fait, on a déja vu que O_K n'est pas un anneau principal, mais ce défaut, "qui est égal à 2', n'est pas trop grand".

Nous avons maintenant un moyen pour mésurer si un O_K, pour un corps de nombres quelquonque, est un anneau principal (au moins, en principe : une formule explicite pour le nombre de classes dans le cas général est toujours à trouver). Il reste le problème à trouver les nombres idéaux (et à montrer que J_K est un groupe).

Comme domaine des nombres idéaux nous pourrons choisir J_K, parce que on a le théorème important :

Théorème. *Tout idéal $\mathfrak{a}$ de $O = O_K$ qui est différent de (0) et (1) possède une décomposition unique*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

en idéaux premiers $\mathfrak{p}_i$ de O.

Lemme. *Pour tout O-idéal $\mathfrak{a} \neq (0)$ il existe des idéaux premiers $\mathfrak{p}_j$ différents de (0) tels que*

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{a}.$$

Démonstration. Soit M l'ensemble des $\mathfrak{a}$ pour lesquels il n'existe pas un tel produit d'idéaux premiers. Car O est noethérien toute tour d'idéaux strictement croissante (par rapport à l'ordre $\subset$) est finie. Donc M est inductivement ordonné. D'après le lemme de Zorn, si M n'est pas vide, alors il existe un élément maximal dans M, disons $\mathfrak{a}$. Clairement $\mathfrak{a}$ n'est pas premier. Donc il existe $a, b \notin \mathfrak{a}$ tels que $ab \in \mathfrak{a}$, i.e.

$$\mathfrak{a} \subset_{\neq} \mathfrak{a} + (a), \mathfrak{a} + (b)?????????????.$$

Car $\mathfrak{a}$ est maximal dans M les idéaux $\mathfrak{a} + (a)$ et $\mathfrak{a} + (b)$ contiennnent des produits non-nuls d'idéaux premiers. Mais alors c'est vrai pour $\mathfrak{a}$ aussi, car

$$(\mathfrak{a} + (a)) \cdot (\mathfrak{a} + (b)) \subset \mathfrak{a}$$

(exercice — on a même =)f. Contradiction. □

Lemme. *Si $\mathfrak{p} \neq (0)$ est premier, alors $\mathfrak{p}\mathfrak{p}^{-1} = O_K$.*

Démonstration. On a $O \subset \mathfrak{p}^{-1}$, donc $\mathfrak{p} \subset \mathfrak{p}\,O \subset \mathfrak{p}\mathfrak{p}^{-1}$. D'autre part $\mathfrak{p}\mathfrak{p}^{-1} \subset O$ (d'après la définition de $\mathfrak{p}^{-1}$). Car $\mathfrak{p}$ maximal, on a $\mathfrak{p}\mathfrak{p}^{-1} = 0$ (car $\mathfrak{p}\mathfrak{p}^{-1} \neq \mathfrak{p}$). □

Lemme. *Soit $\mathfrak{p} \neq O_K$ un idéal premier. Alors pour tout idéal $\mathfrak{a} \neq (0)$ on a $\mathfrak{p}^{-1}\mathfrak{a} \neq \mathfrak{a}$.*

Démonstration. Nous montrons dans un premier temps que $\mathfrak{p}^{-1} \neq O$. En fait, soit $0 \neq a \in \mathfrak{p}$. D'après le lemme avant-précédent on a $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset aO \subset \mathfrak{p}$; on peut supposer que r est minimal.

Si $\mathfrak{p} \supset \mathfrak{a}\mathfrak{b}$ pour des idéaux entiers, et si $\mathfrak{p} \not\supset \mathfrak{a}$ alors $\mathfrak{p} \supset \mathfrak{b}$ (soit $a \in \mathfrak{a} \setminus \mathfrak{p}$, alors pour tout $b \in \mathfrak{b}$ on a $ab \in \mathfrak{p}$, donc $b \in \mathfrak{p}$). Donc on a, disons, $\mathfrak{p}_1 \subset \mathfrak{p}$. En fait, on a égalité car les idéaux premiers sont maximals.

Car r est minimal $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subset aO$, et il existe un $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus aO$. En particulier $\frac{b}{a} \notin O$.

Mais alors $\mathfrak{p}b = \mathfrak{p}_1 b \subset aO$, d'où $\mathfrak{p}\frac{b}{a} \subset O$, donc $\frac{b}{a} \in \mathfrak{p}^{-1}$.

Soit maintenant $\mathfrak{a} \neq (0)$ et a_j un système fini de générateurs de $\mathfrak{a}$ sur O. Supposons $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Alors il existe pour tout $x \in \mathfrak{p}^{-1}$

$$xa_i = \sum_j \alpha_{ij} a_j, \quad \alpha_{ij} \in O.$$

Le déterminant de $(x\delta_i j - a_i j)$ est donc 0, i.e. x est une racine du polynôme normalisé

$$\det(X\delta_{ij} - a_{ij}) \in O[x],$$

donc entier, donc dans O. On a montré $\mathfrak{p}^{-1} \subset O$. Contradiction. □

Démo. du théorème. Soit M l'ensemble des idéaux de O, différent de (0) et (1), qui ne possèdent pas une DIP (décomposition en idéaux premiers). Si M n'est pas vide, alors il existe un élément maximal $\mathfrak{a}$ dans M (raisonnement comme dans la preuve du premier lemme). Car O est noethérien il existe un idéal maximal $\mathfrak{p}$ contenant $\mathfrak{a}$.

Car $O \subset \mathfrak{p}^{-1}$ nous avons $\mathfrak{a} \subset \mathfrak{a}p^{-1}$. Mais $\mathfrak{a} \neq \mathfrak{a}p^{-1}$ (d'après le lemme précédent), et $\mathfrak{a}p^{-1} \neq (1)$ (sinon $\mathfrak{a}\mathfrak{p} = \mathfrak{a}$ également d'après le deuxième lemme). Car $\mathfrak{a}$ est maximal dans M, alors $\mathfrak{a}p^{-1}$ n'appartient pas à M, et, car $\neq (1)$, possède donc une DIP. Mais alors $\mathfrak{a} = (\mathfrak{a}\mathfrak{p}^{-1})\mathfrak{p}$ possède aussi une DIP. Contradiction.

Soient

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$$

deux DIPs de $\mathfrak{a}$. Alors $\mathfrak{p}_1$ contient un des $\mathfrak{q}_j$, disons $\mathfrak{q}_1$. Mais $\mathfrak{q}_1$ est maximal, donc $\mathfrak{p}_1 = \mathfrak{q}_1$. Multipliant par $\mathfrak{p}_1^{-1}$ et utilisant $\mathfrak{p}\mathfrak{p}^{-1} = O$ nous obtenons

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

Continuons ainsi nous obtenons finalement $r = s$, et après rénumerotation $\mathfrak{p}_j = \mathfrak{q}_j$. □

Théorème. *Pour tout idéal fractionnaire $\mathfrak{a} \neq (0)$ on a $\mathfrak{a}\mathfrak{a}^{-1} = O$.*

Démonstration. C'est vrai si $\mathfrak{a}$ est un idéal premier. C'est donc également vrai si $\mathfrak{a}$ est un idéal entier : si $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ est sa DIP, alors on a $\mathfrak{a}\mathfrak{b} = O$ où $\mathfrak{b} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$. Mais $\mathfrak{a}\mathfrak{b} = O$ implique $\mathfrak{b} \subset \mathfrak{a}^{-1}$. Réciproquement, si $x \in \mathfrak{a}^{-1}$, i.e. $x\mathfrak{a} \subset O$, alors $xO = x\mathfrak{a}\mathfrak{b} \subset \mathfrak{b}$.

Si finalement $\mathfrak{a}$ est fractionnaire, alors il existe un $c \in O$, $c \neq 0$, tel que $c\mathfrak{a} \subset O$. Mais $(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1}$ et on a déjà montré $(c\mathfrak{a})^{-1}(c\mathfrak{a}) = 0$. D'où $\mathfrak{a}^{-1}\mathfrak{a} = O$ □

Tout idéal fractionnaire $\mathfrak{a}$ possède une unique DIP de la forme

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}},$$

où le produit est sur tout idéaux premier de O, où $\nu_\mathfrak{p} \in \mathbb{Z}$ et $\nu_\mathfrak{p} = 0$ pour tout $\mathfrak{p}$ sauf pour un nombre fini. En effet, écrire $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ avec des idéaux entiers et considérer la DIP de $\mathfrak{b}$ et $\mathfrak{c}$.

En particulier, si $a \in K$, $a \neq 0$, alors $\mathfrak{a} := aO_K$ possède une DIP unique. On écrit très souvent cette DIP sous la forme (un peu incorrecte)

$$a = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}}.$$

Si O_K est un anneau principal, alors cette identité prend la forme

$$a = \prod_{\pi} (\pi O)^{\nu_\pi},$$

où π parcourt les nombres premiers de O_K (modulo la relation "associée"). Cette identité est équivalent à dire que

$$a = \varepsilon \prod_{\pi} \pi^{\nu_\pi}$$

pour une unité ε convenable.

Si $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux fractionnaires de O_K, on dit qu'ils sont premiers entre eux si leurs DIP ne contiennent aucun idéal premier commun. Si $\mathfrak{a}$ et $\mathfrak{b}$ sont entiers, c'est équivalent à dire que

$$\mathfrak{a} + \mathfrak{b} = O$$

(exercice).

Nous terminons cette séction par *quelques compléments*.

Pour un idéal $\mathfrak{a}$ entier de $O = O_K$ nous posons

$$\mathrm{N}(\mathfrak{a}) := |O/\mathfrak{a}|, \quad \Delta(\mathfrak{a}) := \det\left(\mathrm{Tr}(a_i a_j)\right)_{1 \le i,j \le n},$$

c'est *la norme et le discriminant de* $\mathfrak{a}$. Ici a_i $(1 \le i, j \le n)$ parcourt une $\mathbb{Z}$-base de $\mathfrak{a}$. On note que la norme est bien-definie (i.e. $O/\mathfrak{a}$ est fini), parce que O et $\mathfrak{a}$ ont le même rang en tant que $\mathbb{Z}$-modules. On note également que le discriminant est bien-defini (i.e. ne depend pas du choix de base a_i) : en fait la matrice de passage P à un autre $\mathbb{Z}$-base b_i de $\mathfrak{a}$ est un élément de $\mathrm{GL}(n, \mathbb{Z})$, et on a

$$P^t \left(\mathrm{Tr}(a_i a_j)\right) P = \left(\mathrm{Tr}(b_i b_j)\right).$$

Soit D le discriminant du corps de nombres quadratique K comme défini dans la séction précédente, en particulier $K = \mathbb{Q}(\sqrt{D})$. On vérifie que

$$D = \Delta(O_K).$$

En fait, si par exemple D est impair, alors

$$O = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{D}}{2},$$

et

$$\mathrm{Tr}(\frac{1+\sqrt{D}}{2}) = 1, \quad \mathrm{Tr}([\frac{1+\sqrt{D}}{2}]^2) = \frac{1+D}{2},$$

$$\left(\mathrm{Tr}(a_i a_j)\right) = \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+D}{2} \end{pmatrix},$$

ce qui entraîne la formule. Le cas D pair est similaire.

Pour un corps de nombre arbitraire on appele

$$D_K := \Delta(O_K)$$

simplement *le discriminant de* K. C'est un nombre rationnel entier.

Théorème. *Pour tout idéal* $\mathfrak{a}$ *de* $O = O_K$ *on a*

$$\Delta(\mathfrak{a}) = D_K \cdot \mathrm{N}(\mathfrak{a})^2.$$

Démonstration. Il existe une base $a_1, \cdots, a_n$ de O et des nombres naturels $\varepsilon_1, \cdots, \varepsilon_n$ tels que $\varepsilon_1 a_1, \cdots, \varepsilon_n a_n$ est une base de $\mathfrak{a}$ (théorème de la base adaptée). On a $\mathrm{Tr}(\varepsilon_i a_i \varepsilon_j a_j) = \varepsilon_i \mathrm{Tr}(a_i a_j)\varepsilon_j$, et d'où

$$\Delta(\mathfrak{a}) = \det(\mathrm{Tr}(\varepsilon_i a_i \varepsilon_j a_j) = \Delta(O) \prod_{i=1}^{n} \varepsilon_i^2.$$

D'autre part $O/\mathfrak{a} \approx \prod_{j=1}^{n} \mathbb{Z}/\varepsilon_i\mathbb{Z}$ (isomorphisme de groupes abéliens), et donc $\prod_{i=1}^{n} \varepsilon_i = N(\mathfrak{a})$. □

Théorème. *Pour tout* $a \in O_K$ *on a*

$$\left|\mathrm{N}_{K/\mathbb{Q}}(a)\right| = \mathrm{N}(aO_K).$$

Démonstration. Pour des nombres $a_1, \cdots, a_n$ de K (où $n = [K : \mathbb{Q}]$) on pose

$$D(a_1, \ldots, a_n) := \det \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \sigma_2(a_1) & \sigma_2(a_2) & \cdots & \sigma_2(a_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(a_1) & \sigma_n(a_2) & \cdots & \sigma_n(a_n) \end{pmatrix},$$

où $\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_n$ sont les plongements de K. On vérifie facilement que

$$D(a_1, \ldots, a_n)^2 = \Delta(\mathfrak{a})$$

si $\mathfrak{a}$ est un idéal de O_K et $a_1, \ldots, a_n$ une $\mathbb{Z}$-base de $\mathfrak{a}$.

Soit maintenant $a_1, \ldots a_n$ une $\mathbb{Z}$-base de O_K. Alors $aa_1, \ldots aa_n$ est une base de aO_K. On a

$$D(aa_1, \ldots aa_n) = \mathrm{N}_{K/\mathbb{Q}}(a) D(a_1, \ldots, a_n).$$

Avec la formule précédente pour $\Delta(\mathfrak{a})$ on obtient donc

$$\Delta(aO_K) = \mathrm{N}_{K/\mathbb{Q}}(a)^2 \Delta(O_K).$$

La formule désiré est maintenant une conséquence du théorème précédent. □

Pour un idéal fractionnaire $\mathfrak{a}$ on définit

$$\mathrm{N}(\mathfrak{a}) := \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c})^{-1},$$

ou $\mathfrak{b}$, $\mathfrak{c}$ sont des idéaux entiers tels que $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$. On peut vérifier que ceci ne dépend du choix de $\mathfrak{b}$ et $\mathfrak{c}$, et que ceci définit un morphisme de groupes

$$\mathrm{N} : J_K \to \mathbb{Q}^*_{\geq 0} (= \mathbb{Q}_{>0}).$$

2.3 Décomposition d'idéaux premiers

Pour le suivant on fixe une extension de corps de nombres L/K, et on fixe un idéal premier $\mathfrak{p}$ de K, $\mathfrak{p} \neq (0)$. Nous posons

$$\mathfrak{p}O_L := \{\sum_i a_i b_i : a_i \in \mathfrak{p},\ b_i \in O_L\}.$$

Ceci est un idéal de O_L, et on s'intéresse pour la DIP de cet idéal :

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

Ici le $\mathfrak{p}$ à gauche est à prendre comme $\mathfrak{p}O_L$ ("abuse de langage"), les $\mathfrak{P}_i$ sont des idéaux premier de O_L, deux à deux différents, et les e_i sont donc des nombres naturels $e_i \geq 1$.

Nous introduisons une notation standarde : Si $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux fractionnaires dans, disons, O_L, alors on dit $\mathfrak{a}$ *divise* $\mathfrak{b}$ (symboliquement :$\mathfrak{a}|\mathfrak{b}$) si $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ pour un idéal *entier* $\mathfrak{c}$. On vérifie facilement que

$$\mathfrak{a}|\mathfrak{b} \Longleftrightarrow \mathfrak{a} \supset \mathfrak{b}.$$

(En effet, si $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, alors $\mathfrak{a} \supset \mathfrak{b}$, car $\mathfrak{a} \supset \mathfrak{a}\mathfrak{c}$. Réciproquement, si $\mathfrak{a} \supset \mathfrak{b}$, alors $\mathfrak{a}^{-1} \subset \mathfrak{b}^{-1}$ (clair !) et puis $\mathfrak{b}\mathfrak{a}^{-1} \subset O_L$, i.e. est un idéal entier.)

Un idéal premier $\mathfrak{P}$ de O_L appartient à la décomposition de $\mathfrak{p}O_L$ (i.e. est égal à un des $\mathfrak{P}_i$) si et seulement si $\mathfrak{P}|\mathfrak{p}$, et d'après ce que nous avons vu, c'est équivalent à dire que $\mathfrak{P} \supset \mathfrak{p}O_L$, ou bien $\mathfrak{P} \supset \mathfrak{p}$. C'est pour ceci que l'on appele les idéaux $\mathfrak{P}_i$ *les idéaux au-dessus de* $\mathfrak{p}$, et on écrit très souvent $\mathfrak{P}|\mathfrak{p}$ pour indiquer qu'un idéal premier $\mathfrak{P}$ de O_L appartient à la décomposition de $\mathfrak{p}$.

Théorème. *Soit $\mathfrak{P}$ in idéal premier de L. Alors*

$$\mathfrak{P}|\mathfrak{p} \Longleftrightarrow \mathfrak{P} \cap O_K = \mathfrak{p}.$$

Démonstration. Supposons $\mathfrak{P}|\mathfrak{p}$. Alors $\mathfrak{p}'\mathfrak{P} \cap O_K$ est un idéal de O_K, qui contient $\mathfrak{p}$. Mais $\mathfrak{p}$ est maximal (en tant que idéal premier dans un anneau de Dedekind), donc $\mathfrak{p}' = \mathfrak{p}$ ou $\mathfrak{p}' = O_K$. Mais le dernier est imposiible, car sinon $1 \in \mathfrak{p}'$, donc $1 \in \mathfrak{P}$. La direction réciproque nous avons déjà vérifié ci-dessus. □

En particulier nous en déduisons que, pour un idéal premier $idP|\mathfrak{p}$, l'application canonique $O_K \to O_L\mathfrak{P}$ induit un morphisme d'anneaux injectif

$$O_K/\mathfrak{p} \hookrightarrow O_L/\mathfrak{P}.$$

A l'aide de cette application on peut désormais considérer le corps $O_L/\mathfrak{P}$ comme extension du corps $O_K/\mathfrak{p}$. On pose

$$f_i := [O_L/\mathfrak{P} : O_K/\mathfrak{p}] = \dim_{O_K/\mathfrak{p}} O_L/\mathfrak{P},$$

et on l'appele *degré d'inertie de $\mathfrak{P}_i$ (par rapport à K).*

Le e_i est appelé *le degré de ramification de $\mathfrak{P}_i$ sur K.*

Théorème. $\sum_{i=1}^{r} e_i f_i = [L : K]$.

Démonstration. Appliquons le morphisme de groupes norme à la DIP de $\mathfrak{p}$ nous obtenons

$$\mathrm{N}(\mathfrak{p}O_L) = \mathrm{N}(\mathfrak{P}_1)^{e_1} \cdots \mathrm{N}(\mathfrak{P}_r)^{e_r}.$$

Or nous avons

$$\mathrm{N}(\mathfrak{P}_i) = |O_L/\mathfrak{P}| = |O_K/\mathfrak{p}|^{f_i} = \mathrm{N}(\mathfrak{p})^{f_i}.$$

En plus

$$\mathrm{N}(\mathfrak{p}O_L) = \mathrm{N}(\mathfrak{p})^{[L:K]}.$$

Ceci est clair si $K = \mathbb{Q}$: dans ce cas-là, $\mathfrak{p} = p\mathbb{Z}$ pour un nombre premier rationnel p, et d'après un résultat de §2 on a alors $\mathrm{N}(\mathfrak{p}) = |\mathrm{N}_{L/Q}(p)|$; mais evidemment $\mathrm{N}_{L/Q}(p) = p^{[L:\mathbb{Q}]}$. Le cas général est un exercice (ou voir [Neukirch]).

Inserons les formules trouvés pour les normes variées entraîne le théorème. □

Por décomposer $\mathfrak{p}$ explicitement dans L il faut evidemment une description explicite de O_L. Le cas le plus convenable est le cas $O_L = O_K[\theta]$ pour un θ convenable. En général un tel θ n'existe pas (mais il en existe aussi des exemples importants où on a une telle déscription comme les corps quadratique ou les corps cyclotomiques).. Néanmoins ce raisonnement peut être poursuivi avec succès après quelques modifications.

Pour ce qui suit nous choisissons un élement primitif de L/K avec polynôme minimal p :

$$L = K[\theta], \quad p(x) = \mathrm{Irr}(L, \theta) \in K[X].$$

Nous pouvons supposer que $\theta \in O_L$. Donc θ est entier sur O_K et $p(x) \in O_K[X]$. Nous avons ainsi le sosu-anneau

$$O_K[\theta] \subset O_L.$$

Finalement nous posons

$$\mathfrak{F} = \mathfrak{F}_{O_K[\theta]} := \{a \in O_L : aO_K[\theta] \subset O_L\}.$$

C'est un idéal de O_L, appelé le *conducteur de* $O_K[\theta]$. Nous laissons comme exercice à vérifier que $\mathfrak{F} \neq 0$.

Théorème. *Supposons que* $\mathfrak{p}$ *ne divise pas* $\mathfrak{F} \cap O_K$. *Alors il existe des polynômes normalisés* $p_i(X) \in O_K[X]$ *de degré* f_i $(1 \leq i \leq r)$ *tels que*

$$\overline{p}(X) = \overline{p}_1(X)^{e_1} \cdots \overline{p}_r(X)^{e_r},$$

et tels que $\overline{p}_i(X)$ *est irréductible dans* $(O_K/\mathfrak{p})[X]$. *Ici* $\overline{q}(X)$, *pour un* $q(X) \in O_K[X]$, *indique le polynôme de* $O_K/\mathfrak{p}[X]$ *obtenu de par réduction des coéfficients de* $q(X)$ *modulo* $\mathfrak{p}$.

En plus on a

$$\mathfrak{P}_i = \mathfrak{p}O_L + p_i(\theta)O_L.$$

Démonstration. Posons $\mathbb{F} := O_K/\mathfrak{p}$. Nous considérons $\mathbb{F}$ comme sous-anneau de $O_L/\mathfrak{p}O_L$. L'application

$$\alpha : \mathbb{F}[X]/(\overline{p}(X)) \to O_L/\mathfrak{p}O_L$$

induite par $f(X) \mapsto f(\overline{\theta})$ est un isomorphisme. (Ici $\overline{\theta}$ désigne la classe de θ modulo $\mathfrak{p}O_L$.)

Elle est injective : Soit $f(X) \in \mathbb{F}[X]$ tel que $f(\theta) = 0$, disons $f(X) = \overline{F}(X)$. Nous pouvons choisir $F(X)$ tel que $F(\theta) = 0$. En effet, on a $F(\theta) \in \mathfrak{p}O_L$, i.e.

$$F(\theta) = \sum p_j a_j \quad (p_j \in \mathfrak{p},\ a_j \in O_L).$$

Mais $\mathfrak{F} \cap O_K + \mathfrak{p} = O_K$ (ici on utilise l'hypothèse $\mathfrak{p} \not| \mathfrak{F} \cap O_K$), et donc $a + p = 1$ pour un $a \in \mathfrak{F} \cap O_K$, $p \in \mathfrak{p}$. Mais puis $aF(X) \equiv F(X) \bmod \mathfrak{p}$, et $aa_j = \phi_j(\theta)$ avec des $\phi_j(X) \in O_K[X]$ convenables. Par conséquence

$$G(X) := aF(X) - \sum p_j \phi_j(X)$$

satisfait à $G(X) \in O_K[X]$, à $\overline{G}(X) = f(X)$ et $G(\theta) = 0$.

En ramplaçant $F(X)$ par ce $G(X)$ si necessaire, nous avons donc que $p(X)|F(X)$, et puis $\overline{p}(X)|\overline{F}(X)$ comme nous avons du à montrer.

Elle est surjective : Soit $b \in O_L$. Avec la décomposition $1 = a+p$ ci-dessus (ici on utilise la deuxième fois l'hypothèse $\mathfrak{p} \not| \mathfrak{F} \cap O_K$) on a $b = ab + pb = \phi(\theta)+pb$ pour un $\phi(X) \in O_K[X]$, et donc $b+\mathfrak{p}O_L$ est l'image de $\overline{\phi}(X) \in \mathbb{F}[X]$.

Les idéaux premiers de $\mathbb{F}[X]/(\overline{p}(X))$ sont les $\overline{p}_j(X)\mathbb{F}[X]/(\overline{p}(X))$. Donc, si

$$\pi : O_L \to O_L/\mathfrak{p}O_L$$

est l'application canonique, alors les idéaux premiers de O_L qui contiennent $\mathfrak{p}O_L$ sont

$$\mathfrak{Q}_j := \pi^{-1}\left(\alpha\left(p_j(X)\mathbb{F}[X]/(\overline{p}(X))\right)\right).$$

Nous laissons comme exercice à vérifier que $[O_L/\mathfrak{Q}_j : \mathbb{F}] = \deg(p_j)$, que e_j est le nombre naturel le plus grand tel que $\mathfrak{Q}_j^{e_j}|\mathfrak{p}O_L$, et que

$$\mathfrak{Q}_j = \mathfrak{p}O_L + p_j(\theta)O_L.$$

Ceci implique le théorème. □

Exemple : Décomposition de nombres premiers rationnels dans les corps quadratiques

Soit maintenant $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{D})$ où $D = D_L$, et soit p un nombre premier rationnel, $\mathfrak{p} := p\mathbb{Z}$. On a $O_L = \mathbb{Z}[\theta]$ ou

$$\theta = \begin{cases} \sqrt{D}/2 & \text{si } D \text{ pair} \\ \frac{1+\sqrt{D}}{2} & \text{si } D \text{ impair} \end{cases}.$$

Soit $p(X)$ le polynôme minimal de θ, donc

$$p(X) = \begin{cases} X^2 - D/4 & \text{si } D \text{ pair} \\ X^2 - X + \frac{1-D}{4} & \text{si } D \text{ impair} \end{cases}.$$

(Nous remarquons que l'on peut éviter à distinguer les deux cas on observant que $O_L = \mathbb{Z}[\frac{D+\sqrt{D}}{2}]$.) Le conducteur $\mathfrak{F}$ de $\mathbb{Z}[\theta]$ est O_L. En conséquence le dernier théorème s'applique à tout nombre premier p.

?????????????(p et p Pour déterminer la DIP de p dans L nous devons d'abord décomposer $\overline{p}(X)$. Si D est pair on trouve comme décomposition dans $\mathbb{F}_p[X]$:

$$\overline{p}(X) = \begin{cases} (X - \overline{a})(X + \overline{a}) & \text{si } D/4 \equiv a^2 \bmod p \\ \overline{p}(X) & \text{si } \forall a : D/4 \not\equiv a^2 \bmod p \end{cases}.$$

Nous avons donc trois cas possible à considérer.

Cas : $\left(\frac{D}{p}\right) = +1$. Alors il existe un a tel que $D/4 \equiv a^2 \bmod p$, et $p \not| a$. Donc $X - \overline{a} \neq X + \overline{a}$ (car $p \neq 2|D$) et on a la DIP

$$p = \mathfrak{p}\mathfrak{p}', \quad \mathfrak{p} \neq \mathfrak{p}',$$
$$\mathfrak{p} = (p, -a + \sqrt{D}/2), \quad \mathfrak{p}' = (p, -a - \sqrt{D}/2).$$

Ici on utilise la notation $(u, v) = O_L u + O_L v$. Donc ici *p se decompose totalement.* On trouve aussi — en applicant la norme à la DIP —

$$\mathrm{N}(\mathfrak{p}) = \mathrm{N}(\mathfrak{p}') = p,$$

i.e.

$$O_L/\mathfrak{p} \cong O_L/\mathfrak{p}' \cong \mathbb{F}_p.$$

??????????????p =2 et p impair ! *Cas :* $\left(\frac{D}{p}\right) = 0$. Ici $\overline{p}(X) = X^2$, et donc *p est ramifié* :

$$p = \mathfrak{p}^2, \quad \mathfrak{p} = (p, \sqrt{D}), \quad \mathrm{N}(\mathfrak{p}) = p, \quad O_L/\mathfrak{p} \cong \mathbb{F}_p.$$

Cas : $\left(\frac{D}{p}\right) = -1$. Dans ce cas là *$p$ est inerte* :

$$pO_L = \text{ idéal premier }, \quad [O_L/pO_L : \mathbb{F}_p] = 2.$$

Le cas D impair est analogue : on trouve le même type de DIP de p selon la valeur de $\left(\frac{D}{p}\right)$.

Il est intéressant à regarder plus proche le cas d'un anneau principal comme par exemple $O_L = \mathbb{Z}[i]$ (et discriminant $D_L = -4$). Ici on a donc que $2 = (1+i)(1-i) = -i(1+i)^2$ et pour $p \neq 2$ le résultat ci-dessus se traduit comme

$$\exists \pi \in \mathbb{Z}[i] : p = \pi \cdot \overline{\pi} \Longleftrightarrow \left(\frac{-4}{p}\right) = +1.$$

(Ici $\overline{\pi}$ indique conjugaison complexe.) Si on écrit $\pi = x + iy$ avec $x, y \in \mathbb{Z}$ ce résultat devient

$$\exists x, y \in \mathbb{Z} : p = x^2 + y^2 \Longleftrightarrow p \equiv 1 \bmod 4.$$

En effet

$$17 = 1^2 + 4^2, \quad 541 = 10^2 + 21^2, \ldots$$

(541 et le 100-ième premier) mais jamais $3 = x^2 + y^2$ etc.

Compléments : Le symbol de Legendre Soit p un nombre premier impair. On pose

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{si } \exists x \in \mathbb{Z} : a \equiv x^2 \bmod p,\ p \not| a \\ 0 & \text{si } p|a \\ -1 & \text{sinon} \end{cases} .$$

L'application $a \mapsto \left(\frac{a}{p}\right)$ ne dépend que de a modulo p. Donc elle factorise à une application

$$\mathbb{F}_p^* \to \{\pm 1\}.$$

Il est facile à montrer que cette application est donné par

$$w^n \mapsto (-1)^n,$$

où w est un générateur du groupe cyclique $\mathbb{F}_p^*$. En effet, si $\overline{a} := a + p\mathbb{Z} = w^n$, alors $\overline{a} = (w^m)^2$ pour un m si et seulement si n est pair. En particulier nous remarquons que $\left(\frac{\cdot}{p}\right)$ factorise à un morphisme de groupe, et donc

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

pour tous entiers a, b (même ceux qui sont multiples de p).

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

Démonstration. Ecrivons $\overline{a} = w^n$. Alors

$$\overline{a}^{\frac{p-1}{2}} = (w^{\frac{p-1}{2}})^n = (-1)^n = \left(\frac{a}{p}\right),$$

où nous avons utilisé $w^{\frac{p-1}{2}} = -1$ (en tant que racine de $X^{p-1} - 1 = 0$). □

Corollaire. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Démonstration. La première formule est une conséquence immédiate du théorème précédent.

Pour la deuxième on fait un calcul dans $\mathbb{Z}[i]/2\mathbb{Z}[i]$:

$$\begin{aligned} 1 + i^p &\equiv_p (1+i)^p = (1+i)(1+i)^{p-1} \\ &= (1+i)(2i)^{\frac{p-1}{2}} \equiv_p (1+i)\left(\frac{2}{p}\right) i^{\frac{p-1}{2}}, \end{aligned}$$

où pour la dernière égalité nous avons utilisé le théorème. Mais ceci implique la formule désiré (distinguer les cas selon $p \bmod 8$). □

Théorème. *(Loi de réciprocité) Soient p et l deux nombres premiers impairs différents. Alors*

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

Démonstration. Posons

$$\tau := \sum_{a\in\mathbb{F}_l^*} \left(\frac{a}{l}\right)\zeta^a.$$

Ici ζ indique une racine d'unité primitive l-ième (p.e. $\zeta = \exp(2\pi i/l)$). Nous montrons dans un instant que

$$\tau^2 = (-1)^{\frac{l-1}{2}} l.$$

(En fait, $\tau = \sqrt{(-1)^{\frac{l-1}{2}} l}$ où la racine à prendre est celui dont la partie réelle ou partie imaginaire est positive — mais la preuve de cette formule exacte est *beaucoup* plus compliquée que montrer la formule pour τ^2).

Nous faisons maintenant un calcul dans $\mathbb{Z}[\zeta]/p\mathbb{Z}[\zeta]$ (le comparer au calcul pour la formule pour $\left(\frac{2}{p}\right)$!) :

$$\tau^p \equiv_p \sum_{a\in\mathbb{F}_p^*} \left(\frac{a}{l}\right)^p \zeta^{ap} = \left(\frac{p}{l}\right)\sum_{b\in\mathbb{F}_p^*}\left(\frac{b}{l}\right)\zeta^b = \left(\frac{p}{l}\right)\tau,$$

où on montre l'égalité des deux sommes par la substitution $b \leftrightarrow ap$. D'autre part,

$$\tau^p = \tau\,\tau^{p-1} = \tau\,[(-1)^{\frac{l-1}{2}} l]^{\frac{p-1}{2}} \equiv_p \tau\,(-1)^{\frac{l-1}{2}\cdot\frac{p-1}{2}}\left(\frac{l}{p}\right),$$

la dernière congruence d'après le théorème précédent. En comparant les deux expressions pour τ^p on decouvre la loi de réciprocité. □

Lemme. $\tau^2 = (-1)^{\frac{l-1}{2}} l$.

Démonstration.

$$\tau^2 = \sum_{a,b}\left(\frac{ab}{l}\right)\zeta^{a+b} = \sum_{a,c}\left(\frac{c}{l}\right)\zeta^{a+ca} \quad (b \leftrightarrow ca)$$

$$= \left(\frac{-1}{l}\right)(l-1) + \sum_{c\neq -1}\left(\frac{c}{l}\right)\sum_a \zeta^{a(1+c)} = \left(\frac{-1}{l}\right) l,$$

où, pour la dernière identité, nous avons utilisé

$$\sum_c \left(\frac{c}{l}\right) = \sum_a \zeta^{an} = 0 \quad (n \in \mathbb{F}_p^*).$$

□

Exemple : Décomposition de nombres premiers rationnels dans les corps cyclotomiques Nous fixons un nombre naturel $n \geq 1$ et posons $L := \mathbb{Q}(\mu_n)$. Nous rappelons que le degré de $\phi_n(X)$, le n-ième polynôme cyclotomique, i.e. le polynôme minimal d'une racine d'unité n-ième primitive ζ, est $\varphi(n)$. En plus nous avons vu que $O_L = \mathbb{Z}[\zeta]$. Le conducteur de $\mathbb{Z}[\zeta]$ est O_L, et donc le théorème principal sur la DIP des idéaux premiers d'un sous-corps peut être appliquer à tout nombre premier rationnel p sans aucune restriction. Soit p^ν la puissance précise de p qui divise n.

Théorème. *Soit f l'ordre de p modulo n/p^ν. Alors la décomposition en polynômes irréductible de $\overline{\phi}_n(X)$ dans $\mathbb{F}_p[X]$ est de la forme*

$$\overline{\phi}_n(X) = (p_1 \cdots p_r)^{\varphi(p^\nu)} .$$

Ici les p_i sont deux à deux différents, leur degré est f, et on a $\varphi(n) = rf\varphi(p^\nu)$.

Démonstration. Nous fixons pour la démonstration un idéal premier $\mathfrak{p}|p$ de $O = O_L$, et nous posons $\mathbb{F} := O/\mathfrak{p}$.

Nous supposons dans un premier temps que $p \not| n$. Dans ce cas $nX^{n-1} \neq 0$ dans $\mathbb{F}_p[x]$, i.e.

$$X^n - 1 = \prod_{\eta \in \mu_n} (X - \overline{\eta})$$

ne possède pas de racines multiples dans $\overline{\mathbb{F}}_p$. Ici $\overline{\eta} = \eta + \mathfrak{p}$ indique réduction modulo $\mathfrak{p}$. En conséquence l'application canonique $O \to \mathbb{F}$ induit un morphisme de groupes injectif

$$\mu_n \to \mathbb{F}^*.$$

En plus, car $\overline{\phi}_n(X)$ également ne possède pas de racines multiples (en tan que diviseur de $X^n - 1$), et donc n'est pas divisible par un carré d'un polynôme irréductibe.

Soit $p(X)$ un des facteurs iréductibles de $\overline{\phi}_n(X)$. Il reste à montrer que son degré, disons f, est égal à f.

Pour ceci soit $\overline{\eta}$ une racine de $p(X)$, où $\phi_n(\eta) = 0$. Car η est primitive, et car $\mu_n \to \mathbb{F}^*$ est injectif, l'ordre de $\overline{\eta}$ reste n. Donc $n||\mathbb{F}_p[\overline{\eta}]^*| = p^{f'} - 1$. D'autre part, le corps $\mathbb{F}_{p^f}$ est le corps de décomposition de $X^{p^f-1} - 1$, et contient donc l'image injective de μ_n, et donc $\mathbb{F}_{p^f} \supset \mathbb{F}$, i.e. $f' \leq f$. Car f est l'entier naturel le plus petit tel que $n|p^f - 1$ nous concluons $f' = f$.

Si $\nu > 0$, i.e. si $p|n$, alors écrivons $n = mp^\nu$. Alors nous avons $\mu_n = \mu_m \mu_{p^\nu}$, et

$$X^{p^\nu} - 1 = (X - 1)^{p^\nu}$$

dans $\mathbb{F}$, i.e. $\mu_{p^\nu} \to \{1\}$ sous l'homomorphsime $\mu_n \to \mathbb{F}^*$. Mais alors, si η et θ parcourent repsectivement les racines primitives n-ièmes et p^ν-ièmes, on a

$$\begin{aligned}\overline{\phi}_n(X) &= \prod_{\eta,\theta}(X - \overline{\eta}\overline{\theta}) \\ &= \prod_{\eta,\theta}(X - \overline{\eta}) = \prod_{\eta}(X - \overline{\eta})^{\varphi(p^\nu)} \\ &= \overline{\phi}_m(X)^{\varphi(p^\nu)}\end{aligned}$$

Mais $p \not| m$ et nous avons déjà déterminé la décomposition de $\overline{\phi}_m(X)$ dans ce cas. □

La DIP de p (avec les notation du théorème) dans $\mathbb{Q}(\mu_n)$ et ainsi de la forme

$$p = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^{\varphi(p^\nu)},\ \mathrm{N}(\mathfrak{P}_i) = p^f,\ \varphi(n) = rf\varphi(p^\nu).$$

En particulier, $p \neq 2$ *se décompose totalement* (i.e. $\varphi(p^\nu) = 0$, $f = 1$, et donc $r = [\mathbb{Q}(\mu_n) : \mathbb{Q}]$), si et seulement si $p \equiv 1 \bmod n$.

Nous terminons cette paragraphe par une autre preuve (en effet, par la bonne !) de la loi de réciprocité.

Deuxième preuve de la loi de réciprocité. Soient $p \neq l$ des nombres premiers rationnels impairs. Le corps $L := \mathbb{Q}(\mu_l)$ contient le corps $K := \mathbb{Q}(\sqrt{l'})$, où $l' = (-1)^{\frac{l-1}{2}} l$. En effet, nous avons vu que

$$\sqrt{l'} = \pm \sum_{a \in \mathbb{F}_l^*} \left(\frac{a}{l}\right) \exp(2\pi i a/l).$$

Soit $\sigma_p \in \mathrm{Gal}(L/\mathbb{Q})$ l'automorphisme définit par $\zeta \mapsto \zeta^p$ sur μ_l, soit $\mathfrak{p}|p$ un idéal premier de K.

Alors on a

$$\begin{aligned}p \in \mathbb{F}_l^{*2} &\iff L^{\langle\sigma_p\rangle} \supset \mathbb{Q}(\sqrt{l'}) \\ &\iff \mathrm{N}(\mathfrak{p}) = p \\ &\iff l' \in \mathbb{F}_p^{*2}.\end{aligned}$$

La première équivalence est par théorie de Galois de L, la troisième est la loi de DIP pour p dans le corps quadratique K (ou bien, car $O_K/\mathfrak{p} = \mathbb{F}_p[\sqrt{l'} \bmod \mathfrak{p}]$).

Pour la deuxième posons $Z := L^{\langle\sigma_p\rangle}$, et soit $\mathfrak{P}_Z$ un idéal premier de Z qui divise p. On remarque que O_Z est stable sous σ_p. On en déduit facilement que $O_Z/\mathfrak{P}_Z$ est stable sous $a \mapsto a^p$, et que donc $O_Z/\mathfrak{P}_Z \cong \mathbb{F}_p$,i.e. $\mathrm{N}(\mathfrak{P}_Z) = 1$.

Par conséquence, si $Z \supset K$, alors on a $O_K/\mathfrak{p} \hookrightarrow O_Z/\mathfrak{P}_Z$ (en choisissant $\mathfrak{p} = \mathfrak{P}_Z \cap O_K$) et puis $\mathrm{N}(\mathfrak{p}) = 1$. Réciproquement, si $\mathrm{N}(\mathfrak{p}) = 1$, i.e. $O_K/\mathfrak{p} \cong \mathbb{F}_p$, alors σ_p induit l'identité sur $O_K/\mathfrak{p}$, en particulier (car $O_K/\mathfrak{p} = \mathbb{F}_p[\sqrt{l'} \bmod \mathfrak{p}]$), $\sqrt{l'} \bmod \mathfrak{p}$, et donc $\sqrt{l'}$ et puis K, est stable sous σ_p.

Or l'équivalence

$$p \in \mathbb{F}_l^{*2} \Longleftrightarrow l' \in \mathbb{F}_p^{*2}$$

peut être écrite sous la forme

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

□

Le cas d'une extension galoisienne L/K

Nous supposons maintenant que L/K est galois, soit G le groupe de Galois associé. On fixe un idéal premier $\mathfrak{p}$ de K. Le groupe G agit sur l'ensemble des idéaux $\mathfrak{P}$ de L au-dessus de $\mathfrak{p}$. En effet, si $\mathfrak{P}|\mathfrak{p}$, alors pour tout $\sigma \in G$ on a aussi $\sigma\mathfrak{P}|\mathfrak{p}$ (car $\mathfrak{p} \subset K$ et K est stable par G). En plus, σ induit par passage au quotient un isomorphisme

$$O_L/\mathfrak{P} \to O_L/\sigma\mathfrak{P}.$$

Donc $O_L/\sigma\mathfrak{P}$ est un corps, et $\sigma\mathfrak{P}$ un idéal premier.

Nous remarquons que cet isomorphisme montre aussi les degrés d'inertie de $\mathfrak{P}$ et $\sigma\mathfrak{P}$ sont les mêmes.

Théorème. *Le groupe $G = \mathrm{Gal}(L/K)$ agit transitivement sur l'ensemble des idéaux premiers divisant $\mathfrak{p}$.*

Démonstration. Soient $\mathfrak{P}', \mathfrak{P}|\mathfrak{p}$. Supposons que $\mathfrak{P}' \neq \sigma\mathfrak{P}$ pour tout $\sigma \in G$. Alors, d'après le théorème chinois il existe un $x \in O_L$ tel que

$$x \in \mathfrak{P}', \quad \forall \sigma \in G : x \equiv 1 \bmod \sigma\mathfrak{P}.$$

Mais puis $y := \prod_{\sigma\in G} \sigma(x) \in \mathfrak{P}'$, et d'autre part, car $\sigma(x) \equiv 1 \bmod \mathfrak{P}$ pour tout σ, on a $y \equiv 1 \bmod \mathfrak{P}$. Mais $y \in K$, et donc $y \in \mathfrak{p} = O_K \cap \mathfrak{P}'$ et $y \equiv 1 \bmod \mathfrak{p} (= O_K \cap \mathfrak{P})$. Contradiction. □

Comme corollaire nous obtenons

Théorème. *Soit $\mathfrak{P}|\mathfrak{p}$, et soit*

$$G_{\mathfrak{P}} := \{\sigma \in G : \sigma\mathfrak{P} = \mathfrak{P}\}$$

(groupe de décomposition de $\mathfrak{P}$ sur K). Alors on a

$$\mathfrak{p} = \left(\prod_{\sigma \in G/G_{\mathfrak{P}}} \sigma\mathfrak{P} \right)^e$$

pour un entier $e \geq 1$. On a

$$|G_{\mathfrak{P}}| = e \cdot [O_L/\mathfrak{P} : O_K/\mathfrak{p}].$$

Démonstration. La seule chose qui reste à montrer est la formule pour le degré de ramification. D'après la formule fondamentale on a

$$[L : K] = [G : G_{\mathfrak{P}}]\, e \cdot [O_L/\mathfrak{P} : O_K/\mathfrak{p}].$$

Or $[L : K] = |G|$, ce qui entraîne la formule désirée. □

Le groupe $G_{\mathfrak{P}}$ agit sur $O_L/\mathfrak{P}$ et induit ainsi un homorphisme

$$G_{\mathfrak{P}} \to \mathrm{Gal}\big((O_L/\mathfrak{P})/(O_K/\mathfrak{p})\big).$$

Théorème. *L'homorphisme ci-dessus est surjectif.*

Démonstration. Soit $\mathbb{F} := O_K/\mathfrak{p}$, soit $\theta \in O_L$ tel que $O_L/\mathfrak{P} = \mathbb{F}[\overline{\theta}]$, où la barre indique réduction modulo $\mathfrak{P}$. Soit $f(X) \in O_K[x]$ le polynôme minimal de θ sur K, et soit $g(X) \in O_K[x]$ tel que $\overline{g}(X)$ est le polynôme minimal de $\overline{\theta}$ sur $\mathbb{F}$. Car $f(\theta) = 0$ on a $\overline{g}(X) | \overline{f}(X)$.

Soit maintenant s un $\mathbb{F}$-automorpisme de $O_L/\mathfrak{P}$. Alors $s(\overline{\theta})$ est une racine de $\overline{g}(X)$, donc également une racine de $\overline{f}(X)$, et donc $s(\overline{\theta}) = \overline{\eta}$ pour une racine η de $f(X)$. Soit $\sigma \in G$ tel que $\sigma(\theta) = \eta$. Si $\sigma \in G_{\mathfrak{P}}$, alors l'automorphisme de $O_L/\mathfrak{P}$ définit par σ est égal à s, et la surjéctivité serait montré.

Or on peut supposer en effet que $G = G_{\mathfrak{P}}$, on remplaçant K par le corps fixe de $G_{\mathfrak{P}}$, *le corps de décomposition de $\mathfrak{P}$ sur K* : Nous avons les tours

$$\begin{array}{ccc} L & & \mathfrak{P} \\ | & & | \\ Z := L^{G_{\mathfrak{P}}} & & \mathfrak{P}_Z := O_Z \cap \mathfrak{P} \\ | & & | \\ K & & \mathfrak{p} \end{array}$$

On a $\mathrm{Gal}(L/Z_{\mathfrak{P}}) = G_{\mathfrak{P}}$. En particulier

$$\mathfrak{P}_Z = \mathfrak{P}^{e''},\ |G_{\mathfrak{P}}| = e''[O_L/\mathfrak{P} : O_Z/\mathfrak{P}_Z].$$

Or il est clair que $e'' \leq e$ (si $\mathfrak{p} = \mathfrak{P}_Z^{e'} \cdots$, alors $\mathfrak{p} = \mathfrak{P}^{e'e''} \cdots$), et $[O_L/\mathfrak{P} : O_Z/\mathfrak{P}_Z] \leq [O_L/\mathfrak{P} : O_K/\mathfrak{p}]$.

De

$$|G_{\mathfrak{P}}| = e[O_L/\mathfrak{P} : O_K/\mathfrak{p}]$$

nous déduisons $e'' = e$ et $[O_Z/\mathfrak{P}_Z : O_K/\mathfrak{p}] = 1$, i.e. $O_Z/\mathfrak{P}_Z \cong O_K/\mathfrak{p}$.

En remplaçant K par Z dans l'argument du debut nous pouvons ainsi supposer $G_{\mathfrak{P}} = G$. □

La fonction ζ de Dedekind

Pour un corps de nombres L la fonction ζ de Dedekind est définie par les formules

$$\zeta_L(s) = \prod_p \frac{1}{L_p(p^{-s})},\ L_p(p^{-s}) = \prod_{\mathfrak{P}|p}(1 - \mathrm{N}(\mathfrak{P})^{-s}).$$

Ici p parcourt les nombres premiers rationnels, et $\mathfrak{P}$ les idéaux premiers de L au-dessus de $\mathfrak{p}$. Nous observons que $L_p(p^{-s})$ est un polynôme en p^{-s}. Pour $L = \mathbb{Q}$ nous retrouvons la célèbre fonction $\zeta(s)$ de Riemann :

$$\zeta_{\mathbb{Q}}(s) = \zeta(s) = \prod_p \frac{1}{1 - p^{-s}} = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Théorème. *Le produit converge absolument pour* $\mathrm{Re}(s) > 1$, *et on a la formule*

$$\zeta_L(s) = \sum_{\mathfrak{a}} \frac{1}{\mathrm{N}(\mathfrak{a})^s},$$

où $\mathfrak{a}$ *parcourt les idéaux (entiers) non-nuls de* L.

Démonstration. Soit $\mathfrak{P}_l$ $(l = 1, 2, \dots)$ une énumération des idéaux premiers de L. A questions de convergence près l'étape essentiel pour la formule est :

$$\zeta_L(s) = \prod_{\mathfrak{P}} \frac{1}{1 - \mathrm{N}(\mathfrak{P})^{-s}} = \prod_{\mathfrak{P}} \sum_{n_{\mathfrak{P}}=0}^{\infty} \frac{1}{\mathrm{N}(\mathfrak{P})^{n_{\mathfrak{P}} s}}$$

$$= \prod_l \sum_{n_l=0}^{\infty} \frac{1}{\mathrm{N}(\mathfrak{P}_l)^{n_l s}}$$

$$= \sum_{n_1,n_2,\cdots=0}^{\infty} \frac{1}{[\mathrm{N}(\mathfrak{P}_1)^{n_1}\mathrm{N}(\mathfrak{P}_2)^{n_2} \cdots]^s}$$

$$\sum_{n_1,n_2,\cdots=0}^{\infty} \frac{1}{[\mathrm{N}(\mathfrak{P}_1^{n_1}\mathfrak{P}_2^{n_2} \cdots)]^s} = \sum_{\mathfrak{a}} \frac{1}{\mathrm{N}(\mathfrak{a})^s},$$

où, pour la dernière identité, nous avons utilisé la DIP unique des idéaux de L. Nous laissons les details et les questions de convergence comme exercice. □

Pour étudier ζ_L dans le cas des corps quadratique et cyclotomiques nous avons besoin des caractères de Dirichlet et leurs fonctions ζ associées.

Une application $\chi : \mathbb{Z} \to \mathbb{C}^*$ est appelé *caractère de Dirichlet modulo m* si il existe un morphisme de groupe

$$\widetilde{\chi} : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$$

tel que $\chi(a) = \widetilde{\chi}(a \bmod m)$ si $\text{pgcd}(a, m) = 1$, et si $\chi(a) = 0$ sinon. On appele χ *primitif* si il n'existe pas un caractère de Dirichlet ψ modulo t avec un $t|m$, $t < m$, tel que $\chi(a) = \psi(a)$ pour tout $\text{pgcd}(a, m) = 1$.

Pour un caractère de Dirichlet on pose

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Nous laissons comme exercice à vérifier que cette série converge absolument pour $\text{Re}(s) > 1$.

?????????????caractere de DIRI

Théorème. *Soit $L = \mathbb{Q}(\sqrt{D})$, où D est le discriminant de L. Alors*

$$\zeta_L(s) = \zeta(s)L(\left(\frac{D}{\cdot}\right), s).$$

Démonstration. En effet, la loi de décomposition dans L pour un nombres premier rationnel p se traduit comme

$$L_p(X) = \begin{cases} (1-X)^2 & \text{si } \left(\frac{D}{p}\right) = +1 \\ (1-X^2) & \text{si } \left(\frac{D}{p}\right) = -1 \\ (1-X) & \text{si } \left(\frac{D}{p}\right) = 0 \end{cases}$$
$$= (1-X)(1-\left(\frac{D}{p}\right)X).$$

D'où le théorème. □

Théorème. *Pour tout nombre naturel $n \geq 1$ on a*

$$\zeta_{\mathbb{Q}(\mu_n)} = \prod_{\chi} L(\chi, s).$$

Ici χ parcourt $\bigcup_{t|n} C(t)$, où $C(t)$ est l'ensemble des caractères de Dririchlet primitif modulo t.

Démonstration. Si $p^\nu \| n$, et si f est l'ordre de p modulo $m := n/p^\nu$, alors la loi de décomposition pour p dans $\mathbb{Q}(\mu_n)$ donne

$$L_p(X) = (1 - X^f)^{\frac{\varphi(m)}{f}} = \prod_{\eta \in \mu_f} (1 - X\eta)^{\frac{\varphi(m)}{f}}.$$

Mais, si A est le groupe des caractères de Dirichlet modulo m, alos

$$A \to \mu_f,\ \chi \mapsto \chi(p)$$

est un morphisme de groupes surjectif (exercice), $|A| = \varphi(m)$, et donc

$$\prod_{\eta \in \mu_f} (1 - X\eta) = \prod_{\chi \in A} (1 - \chi(p)X)$$

Le théorème et maintenant évident. □

2.4 Géométrie des nombres

2.4.1 Théorème de Minkowski

Soit V un $\mathbb{R}$-espace vectoriel de dimensions n. Un *réseaux L dans V* est un $\mathbb{Z}$-sous-module de V de la forme

$$L = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n$$

où $a_1, \ldots, a_n$ est une base du $\mathbb{R}$-espace vectoriel V. Un domaine fondamental pour L est une ensemble de la forme

$$F := \{\sum_{j=0}^{n} t_j a_j : 0 \leq t_1, \ldots, t_n < 1\}$$

avec des a_j comme ci-dessus. Evidemment V est la réunion disjointe des $g + F$, où g parcourt L.

Soit vol une mésure de Haar sur V, i.e. une mésure tel que $\mathrm{vol}(a + X) = \mathrm{vol}(X)$ pour tout $a \in V$ et tout sous-ensemble X (mésurable).

Ici nous utilisons que V est naturellement muni de la structure d'un espace vectoriel localment compact : via un isomorphisme avec $\mathbb{R}^n$ on peut copier la topologie de $\mathbb{R}^n$, et la topologie résultant sur V ne dépend pas du choix d'isomorphisme (exercice).

Nous posons $\mathrm{vol}(L) := \mathrm{vol}(F)$. Nous laissons comme exercice à vérifier que $\mathrm{vol}(L)$ ne dépend pas du choix de base de L.

Théorème. *(Minkowski) Soit X un sous-ensemble convexe est symmétrique de V, et soit L un réseau dans V. Supposons que*

$$\mathrm{vol}(X) > 2^n \mathrm{vol}(L).$$

Alors $X \cap L$ contient au moins un point $g \neq 0$.

(Un sous-ensemble X de V est appelé convexe, si pour tout poit $x, y \in X$ tout le segment $tx+(1-t)y$ $(0 \leq t \leq 1)$ est contenu dans X. Et X est appelé symmétrique si X est stable sous $x \mapsto -x$.)

Démonstration. Il suffit à montrer qu'il existe des $g_1 \neq g_2$ dans L tel que $(g_1 + \frac{1}{2}X) \cap (g_2 + \frac{1}{2}X) \neq 0$. Car, si x est dans cette intersection, disons $x = g_1 + \frac{1}{2}x_1 = g_2 + \frac{1}{2}x_2$, alors $g_1 - g_2 = \frac{1}{2}x_2 - \frac{1}{2}x_1$ est le milieu du segment de x_1 à $-x_2$, et donc un point de X.

Supposons que les ensembles $g + \frac{1}{2}X$ $(g \in L)$ sont deux à deux disjoints. Par conséquence on a, avec F comme domaine fondamentale de L, et par un petit calcul

$$\begin{aligned}
\mathrm{vol}(F) &\geq \mathrm{vol}\left(F \cap \bigcup_{g \in L} (g + \frac{1}{2}X)\right) \\
&= \sum_{g \in L} \mathrm{vol}\left(F \cap (g + \frac{1}{2}X)\right) \\
&= \sum_{g \in L} \mathrm{vol}\left((-g + F) \cap \frac{1}{2}X\right) \\
&= \mathrm{vol}\left((\bigcup_{g \in L} (-g + F) \cap \frac{1}{2}X\right) \\
&= \mathrm{vol}\left(\frac{1}{2}X\right) = 2^{-n}\mathrm{vol}(X).
\end{aligned}$$

Une contradiction à l'hypothèse. □

2.4.2 Finitude du groupe de classe

Nous fixons un corps de nombre K. Nous rappelons que $\mathbb{A} = \mathbb{A}_K$ désigne l'ensemble des plongements $\tau : K \to \mathbb{C}$, que r_1 et r_2 sont le nombre de plongements réels et le nombre des plongements complexes repectivement, et que finalement $D = D_K$ est le discriminant de K.

Théorème. *Soit $\mathfrak{a} \neq 0$ un idéal entier de K. Soient $c_\tau > 0$ $(\tau \in \mathbb{A})$ des nombres réels avec $c_\tau = c_{\overline{\tau}}$ et*

$$\left(\frac{\pi}{2}\right)^{-r_2} \sqrt{|D|}\, \mathrm{N}(\mathfrak{a}) < \prod_{\tau \in \mathbb{A}} c_\tau.$$

Alors il existe un $a \in \mathfrak{a}$, $a \neq 0$ *tel que*

$$\forall \tau \in \mathbb{A} : |\tau a| < c_\tau.$$

Démonstration. Soit $V := \mathbb{R} \otimes_{\mathbb{Q}} K$. C'est un $\mathbb{R}$-espace vectoriel de dimension $n := [K : \mathbb{Q}]$. Si $\mathfrak{a}$ est un idéal de K avec $\mathbb{Z}$-base $a_1, \ldots, a_n$, alors $1 \otimes a_1, \ldots, 1 \otimes a_n$ est une $\mathbb{R}$-base de V. Donc l'application

$$j : K \to V, \quad a \mapsto 1 \otimes a$$

donne des idéaux de K sur des réseaux de V.

Nous observons que

$$D(1 \otimes a_1, \ldots, 1 \otimes a_n) := \det \left(\tau_i a_j\right)_{1 \leq i,j \leq n},$$

où τ_i parcourt $\mathbb{A}_K$ et $a_1, \ldots, a_n \in K$, peut être prolongé (multi-)linéairement à une application multilinéaire et alterné $V^n \to \mathbb{C}$. (En effet, l'image et soit dans $\mathbb{R}$, sit dans $i\mathbb{R}$ — exercice). Nous pouvons donc choisir une mésure de Haar vol sur V de façon que l'on a

$$\mathrm{vol}\left(\{\sum_{j=0}^{n} t_j\, v_j : 0 \leq t_1, \ldots, t_n \leq 1\}\right) = |D(v_1, \ldots, v_n)|$$

pour tout $v_1, \ldots, v_n \in V$ (exercice).

En particulier, pour un idéal $\mathfrak{a}$ dans K avec domaine fondamental F, nous obtenons

$$\mathrm{vol}(F) = \sqrt{|D_K|}\, \mathrm{N}(\mathfrak{a})$$

(voir fin de la séction avant-dernière pour la preuve que $D(1 \otimes a_1, \ldots, 1 \otimes a_n)^2 = D_K\, \mathrm{N}(\mathfrak{a})^2$ si a_j parcourt une $\mathbb{Z}$-base de $\mathfrak{a}$).

Pour $\tau \in \mathbb{A}$ soit $\lambda_\tau : V \to \mathbb{C}$ l'application $\mathbb{R}$-linéaire telle que $\lambda_\tau(x \otimes a) = x\, \tau a$. Posons

$$X := \{x \in V : \forall \tau \in \mathbb{A} : |\lambda_\tau x| < c_\tau\}.$$

Nous laissons comme exercice à montrer que

$$\mathrm{vol}(X) = 2^{r_1 + r_2} \pi^{r_2} \prod_{\tau \in \mathbb{A}} c_\tau.$$

Nous pouvons alors appliquer le théorème de Minkowski pour conclure notre théorème. □

Corollaire. *Dans tout idéal entier* $\mathfrak{a}$ *de* K *il existe un* $a \neq 0$ *tel que*

$$|\mathrm{N}_{K/\mathbb{Q}}(a)| \leq \left(\frac{\pi}{2}\right)^{-r_2} \sqrt{|D_K|}\, \mathrm{N}(\mathfrak{a}).$$

Démonstration. Soit $c_\tau > 0$ des nombres réels tel que $c_\tau = c_{\overline{\tau}}$ et

$$\left(\frac{\pi}{2}\right)^{-r_2} \sqrt{|D_K|}\, \mathrm{N}(\mathfrak{a}) = \prod c_\tau.$$

D'après le théorème il existe pour tout $\varepsilon > 0$ un $0 \neq a \in \mathfrak{a}$ tel que

$$\forall \tau \in \mathbb{A} : |\tau a| < c_\tau + \varepsilon.$$

Mais l'ensemble des $a \in \mathfrak{a}$ avec $|\tau a| \leq C$, pour une constante C, est fini (soit par un argument topolgique en utilisant que $\mathfrak{a}$ en tant que réseau est un sous-groupe discret de V, soit on déduisant que, pour toute constante C, l'ensemble des polynômes minimals des $a \in O$ avec $|\tau a| \leq C$ pour tout τ est fini). Donc il existe un $0 \neq a \in \mathfrak{a}$ avec $|\tau a| \leq c_\tau$ pour tout τ, et d'où le corollaire. □

Théorème. *Le groupe de classe J_K/P_K est fini.*

Démonstration. Pour toute constante C le nombre d'idéaux entiers $\mathfrak{a}$ de K tels que $\mathrm{N}(\mathfrak{a}) \leq C$ est fini (exercice). Il suffit donc à montrer qu'il existe une constante C tel que toute classe $[\mathfrak{a}]$ contient un idéal entier $\mathfrak{a}_1$ tel que $\mathrm{N}(\mathfrak{a}_1) \leq C$.

Posons

$$C := \left(\frac{\pi}{2}\right)^{-r_2} \sqrt{|D_K|}.$$

Choisissons un $c \in O_K$, $c \neq 0$ tel que $\mathfrak{b} := c\mathfrak{a}^{-1}$ est entier. D'après le lemme il existe un $0 \neq a \in \mathfrak{b}$ avec

$$\mathrm{N}_{K/\mathbb{Q}}(a) \leq C \cdot \mathrm{N}(\mathfrak{b}),$$

et donc

$$\mathrm{N}(a\mathfrak{b}^{-1}) \leq C.$$

Mais $a\mathfrak{b}^{-1}$ et entier et dans $[\mathfrak{a}]$, □

2.4.3 Le Théorème de Dirichlet

Toujours K est un corps de nombre, et nous gardons les notations de la séction précédente, en particulier r_1 et r_2 pour le nombre de plongements réels respectivement couple de plongements complexes de K dans $\mathbb{C}$. Nous utilisons $O^* = O_K^*$ pour le groupe (multiplicatif) des unités de O_K, et $W = W_K$ pour le sous-groupe des racines d'unités de O^*. Il est clair que W_K est fini (car sinon K contiendrait des corps $\mathbb{Q}(\mu_l)$ de degré arbitrairement large).

Théorème. *(Théorème de Dirichlet) Le groupe O_K^*/W_K est un groupe abélien libre de rang $r_1 + r_2 - 1$.*

Démonstration. Soit $A \subset \mathbb{A}_K$ un ensemble qui contient les plongements réels et, pour chaque couple de plongements complexes, un de ces deux plongements. Nous étudions le morphisme de groupes

$$\mathrm{Log} := l \circ \iota : (\mathbb{R} \otimes_{\mathbb{Q}} K)^* \to \mathbb{R}^A,$$

où ι est la restriction sur $(\mathbb{R}\otimes_{\mathbb{Q}}K)^*$ de l'application linéaire $\mathbb{R}\otimes_{\mathbb{Q}}K \to \mathbb{R}^A$ telle que $x\otimes a \mapsto (x\,\tau a)_\tau$, et où $l : \mathbb{R}^{*A} \to \mathbb{R}^A$, $(x_\tau) \mapsto (\log|x_\tau|)$. Ici $(\mathbb{R}\otimes_{\mathbb{Q}}K)^*$ est le groupe (multiplicatif) des éléments inversible de $\mathbb{R}\otimes_{\mathbb{Q}} K$. Ce groupe contient K^* et O^* (via le plongement canonique $K \ni a \mapsto 1\otimes a$). On vérifie facilement que Log est en effet un morphisme de groupe, et que $\mathrm{Log}(a) = (\log|\tau a|)_\tau$.

En particulier, car, pour tout $\varepsilon \in O^*$, nous avons $|\mathrm{N}_{K/\mathbb{Q}}(\varepsilon)| = 1$, i.e. $\log|\mathrm{N}_{K/\mathbb{Q}}(\varepsilon)| = 0$, nous observons que

$$L := \mathrm{Log}(O^*) \subset H := \{(x_\tau)_\tau : \sum_\tau e_\tau x_\tau = 0\}.$$

Ici $e_\tau = 1$ si τ est réel, et $e_\tau = 2$ sinon. La dimension de $\mathbb{R}^A$ est $\#A = r_1 + r_2$, et H, en tant que hyperplan de $\mathbb{R}^A$, est donc de dimension $r := r_1 + r_2 - 1$.

Nous avons la suite exacte

$$1 \to W \to O^* \to L \to 1.$$

En effet, si, pour un $\varepsilon \in O^*$, nous avons $\mathrm{Log}(\varepsilon) = 0$, alors $|\tau\varepsilon| = 1$, et donc aussi $|\tau\varepsilon^n| = 1$, pour tout $\tau \in \mathbb{A}_K$ et tout $n \geq 0$, alors on en déduit facilement que l'ensemble des polynômes minimales des ε^n est fini (les coéfficients du polynôme minmal de ε^n sont des fonctions symmétriques élémentaires en les $\tau\varepsilon^n$). Par conséquence, l'ensemble des ε^n est fini, donc $\varepsilon^m = \varepsilon^n$, i.e. $\varepsilon^{m-n} = 1$, pour des $m > n$ convenable, donc $\varepsilon \in W$. Que réciproquement $\mathrm{Log}(W) = \{0\}$ et évident.

Notre but est à montrer que L est un réseau dans H. Ceci implique evidemment le théorème, car $O^*/W \cong L$ d'après la suite exacte ci-dessus.

D'abord nous montrons que L est un groupe abélien libre de rang $s \leq r := r_1 + r_2 - 1$.

Pour ceci nous remarquons que O^* est un sous-groupe discret de $(\mathbb{R}\otimes_{\mathbb{Q}}K)^*$ (i.e. chaque point ε de O^* possède un voisinage ouvert qui ne contient aucun point de O^* différent de ε), car O en tant que réseaux est discret (exercice). Mais alors L (comme image continu de O^*) est discret aussi. Soit $\mathbb{R}L$ le sous-espace de H engendré par L, soit $h_1, \ldots, h_s \in L$ une base de $\mathbb{R}L$, soit $L_0 := \mathbb{Z}h_1 + \cdots + \mathbb{Z}h_s$. Nous montrons que L/L_0 est fini, ce qui implique que

L est également libre de rang s. En fait, toute classe de L/L_0 possède un représentant dans F_0, un domaine fondamental fixé de L_0 dans $\mathbb{R}L$. Si $F_0 \cap L$ était infini, alors il existait une suite convergente (a_n),

$a_n \in F_0 \cap L$ dont les membres sont deux à deux différents (car F_0 est contenu dans un ensemble compact). Mais alors $L \ni a_n - a_{n+1} \to 0$, et donc L ne serait pas discret — contradiction.

L'étape essentielle de la preuve est à montrer que le rang de L est égal à r, la dimension de H. Nous suivons ici les arguments plus ou moins original de Dirichlet.

Il suffit à montrer que pour tout $0 \neq \lambda \in H^{-1}$ (l'espace dual de H) il existe un $\varepsilon \in O^*$ avec $\lambda(\mathrm{Log}(\varepsilon)) \neq 0$.

Pour la preuve nous prolongons λ à une forme linéaire, aussi notée λ, sur tout $\mathbb{R}^A$. Nous allons construire une suite de nombres $0 \neq a_n \in O$, tel que

$$|\mathrm{N}(a_n O))| \leq C$$

(où $C = \left(\frac{\pi}{2}\right)^{-r_2} \sqrt{|D|}$), et tel que

$$\lambda(\mathrm{Log}(a_1)) < \lambda(\mathrm{Log}(a_2)) < \lambda(\mathrm{Log}(a_3)) < \dots .$$

Car l'ensemble d'idéaux aO avec $\mathrm{N}(aO) \leq C$ est fini, il existe $h > k$ tel que $a_h = \varepsilon a_k$ pour un $\varepsilon \in O^*$, et par conséquence

$$\lambda(\mathrm{Log}((\varepsilon)) = \lambda(\mathrm{Log}((a_h)) - \lambda(\mathrm{Log}((a_k)) > 0.$$

Pour la construction des a_n nous remarquons dans un premier temps ce qui suit : Poser

$$\mu(\kappa) := \sum_{\tau \in A} e_\tau \kappa_\tau$$

pour $\kappa = (\kappa_\tau)_\tau \in \mathbb{R}^A$. Si $\kappa \in \mathbb{R}^A$ tel que $\mu(\kappa) = \log C$, alors il existe un $0 \neq a \in O$ tel que

$$\log |\tau a| < \kappa_\tau$$

pour tout $\tau \in A$ (voir le premier théorème de la section précédente). Il existe alors une constante M qui ne dépend ni du choix des κ_τ ni du choix de ce a telle que

$$|\lambda(\mathrm{Log}(1 \otimes a)) - \lambda(\kappa)| < M.$$

En effet, soient c_τ des nombres réels tels que $\lambda((x_\tau)) = \sum_\tau c_\tau x_\tau$, alors on a

$$\begin{aligned}
&|\lambda(\mathrm{Log}(1\otimes a))-\lambda(\kappa)|\\
&=|\sum_{\tau} c_\tau(\log|\tau a|-\kappa_\tau)|\\
&\leq \sum_{\tau}|c_\tau|\,|\log|\tau a|-\kappa_\tau|
\end{aligned}$$

Car $\mathrm{N}_{K/\mathbb{Q}}(a)\geq 1$, i.e. $\mu(\mathrm{Log}(1\otimes a))\geq 0$, on a

$$\begin{aligned}
e_\tau\log|\tau a| &\geq -\sum_{\tau'\neq\tau} e_{\tau'}\log|\tau' a|\\
&\geq -\sum_{\tau'\neq\tau} e_{\tau'}\kappa_{\tau'} = e_\tau\kappa_\tau-\log C.
\end{aligned}$$

En résumant on a donc

$$|\lambda(\mathrm{Log}(1\otimes a))-\lambda(\kappa)|\leq \log C\sum_{\tau}|c_\tau| =: M$$

Nous choisissons maintenant pour tout entier naturel n un $\kappa_n\in\mathbb{R}^A$ avec

$$\mu(\kappa_n)=\log C,\quad \lambda(\kappa_n)=2nM$$

L'existence d'un tel κ est justifié par le fait que $H=\mathrm{Ker}(\mu)$ et que $\lambda\neq 0$ sur H, i.e. λ et μ sont linéairement indépendants. Puis nous choissons un $0\neq a_n\in O$ tel que

$$|\lambda(\mathrm{Log}(1\otimes a_n))-\lambda(\kappa_n)|<M.$$

Nous avons donc

$$(2n-1)M<\lambda(\mathrm{Log}(1\otimes a_n))<(2n+1)M,$$

et ceci implique les inégalités désirées pour la suite des a_n. □

Chapitre 3

Exercices

EXERCICES à THEORIE DES NOMBRES 2000 — Feuille 1

Exercice 1. *Soit L l'ensemble des nombres complexes qui sont algébriques sur $\mathbb{Q}$. Montrer par calcul direct, que L est un corps. Montrer aussi que L est algébriquement clos (et donc une clôture algébrique de $\mathbb{Q}$).*

Exercice 2. *Soit $K := \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$. Montrer que $[K : \mathbb{Q}] = 6$. Calculer le polynôme minimale de $\alpha := \sqrt{3} + \sqrt[3]{2}$. En déduire que $K = \mathbb{Q}(\alpha)$.*

Exercice 3. *Déterminer le groupe d'automorphismes du corps $\mathbb{Q}(X)$.*

Exercice 4. *Montrer : Le corps $\mathbb{Q}$ et les corps $\mathbb{F}_p$ ne possèdent d'autres automorphismes que l'identité.*

Exercice 5. *Soit $K = \mathbb{F}_p(X, Y)$ le corps des fonctions rationelles en deux variables avec coéfficients dans $\mathbb{F}_p$, soit $k = \mathbb{F}_p(X^p, Y^p)$. Montrer que K/k est une extension fini (de degré p^2). Montrer que K n'est pas une extension simple de k.*

EXERCICES à THEORIE DES NOMBRES 2000 — Feuille 2

Exercice 6. *Soit K le corps de décomposition de $x^3 - 2$ sur $\mathbb{Q}$. Déterminer $[K : \mathbb{Q}]$, $\mathrm{Gal}(K/\mathbb{Q})$ et faire une liste de tous les corps intermédiaires $\mathbb{Q} \subset L \subset K$ et des groupes $\mathrm{Gal}(K/L)$ associés.*

Exercice 7. *Soit $\mathbb{F}_4 = \{0, 1, w, w^2\}$. Calculer $w + w^2$. De même soit $\mathbb{F}_8 = \{0, 1, w, w^2, w^3, w^4, w^5, w^6\}$. Calculer $w^3 + w^4$.*

Exercice 8. *Combien de polynômes irréductibles de degré 17 existe-il dans $\mathbb{F}_2[x]$? (Indication :$\mathbb{F}_{2^{17}} = \mathbb{F}_2[a]$ pour tout $a \in \mathbb{F}_{2^{17}}$, $a \neq 0, 1$, car $2^{17} - 1 = 131071$ est un nombre premier.)*

Exercice 9. *Soient $k \subset k'$ des corps, soit $f \in k[x]$, et soient K et K' les corps de décomposition de f sur k et k' respectivement. Montrer que l'application*

$$\mathrm{res} : \mathrm{Gal}(K'/k') \to \mathrm{Gal}(K/k),$$

définie par restriction sur K des k'-automophismes de K', est un morphisme de groupes injectif

Exercice 10. *Montrer : Soit K/k une extension qui est une réunion d'extensions galoisiennes de k. Alors K/k est galoisien.*

Exercice 11. *Déterminer les sous-groupes ouverts U de $\widehat{\mathbb{Z}}$ et les corps fixes associés $\overline{F}_p^U$. (Ici on identifie $\widehat{\mathbb{Z}} \approx \mathrm{Gal}(\overline{F}_p/\mathbb{F}_p)$ via l'application $s \mapsto F^s$ du cours.)*

Exercice 12. *Montrer que $\mathrm{Aut}(\mathbb{Q}/\mathbb{Z}) = \widehat{\mathbb{Z}}^*$.*

EXERCICES à THEORIE DES NOMBRES 2000 — Feuille 3

Exercice 13. *Soit G un groupe fini soluble. (1) Montrer que tout sous-groupe de G et toute image de G sous un homomorphisme est soluble. (2) Montrer qu'il existe une suite de sous-groupes $1 = H_0 \subset H_1 \subset \cdots \subset H_n = G$ telle que H_{j-1} est distingué dans H_j et telle que H_j/H_{j-1} est cyclique d'ordre premier.*

Exercice 14. *Déterminer des polynômes dans $\mathbb{Q}[x]$ d'ordre 3, 4 et 5 tels que les corps de décomposition ont degré 3, 4 et 5 respectivement.*

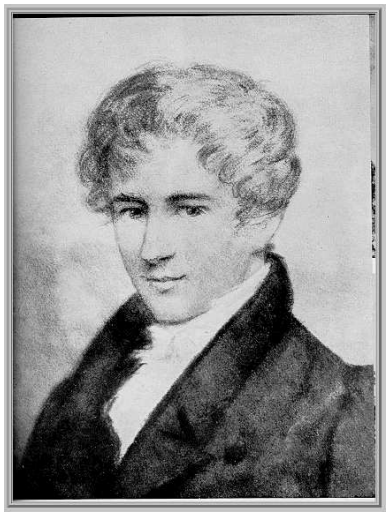
Exercice 15. *Montrer que le groupe de Galois du corps de décomposition de $f = x^5 - 2x^4 + 2$ sur $\mathbb{Q}$ est isomorphe au groupe symmétrique S_5.*

Exercice 16. *Résoudre par radicaux l'équation $x^3 + 3x^2 + x + 1 = 0$.*

Exercice 17. *Pour quelles $\alpha \in [0, 2\pi[$ est-ce que l'on peut faire une trisection de l'angle α à règle et compas ?*

Exercice 18. *Tout 2-groupe contient un sous-groupe distingué d'ordre 2.*

Indication à 3. Par l'action sur les racines de f on peut identifier G avec un sous-groupe de S_5. Or G contient une transposition — parce que : combien de racines complexes f possède-t-il ? En plus, G agit transitivement sur les racines — pourquoi ? Puis prouver ou admettre le fait : Le seul sous-groupe de S_5 qui agit transitivement sur les 5 chiffres et contient une transposition est tout S_5. Ou bien, trouver un raisonnement totalement différent !
Indication à 6. Laisser agir le 2-groupe G sur G par conjugaison, regarder la formule d'orbite associée — qu'est-ce quelle implique pour l'ordre du centre ?

Evariste Galois (1811–1832), Niels Henrik Abel (1802–1829)

EXERCICES à THEORIE DES NOMBRES 2000 — Feuille 4

Exercice 19. *Pour quelles* $\alpha \in [0, 2\pi[$ *est-ce que l'on peut faire une trisection de l'angle* α *à règle et compas ? Autrement dit, pour quelle* α *est-ce que le nombre complexe* $\exp(\pi i \frac{\alpha}{3})$ *appartient à* $\Omega(\{0, 1, \exp(\pi i \alpha)\})$ *?*

Exercice 20. *Montrer :* $a \in O_K$ *est une unité ssi le coéfficient constant du polynôme minimal* f *de* a *sur* $\mathbb{Z}$ *est égal à* ± 1*. (Indication : Exprimer le polynôme minimal de* $1/a$ *en terme de* f*.)*

Exercice 21. *Montrer que* $O_{\mathbb{Q}(\sqrt{D})}$ *est un anneau euclidien (et donc principal) pour* $D = -3, -4, -7, -11$*. Décomposer* $p = 541$ *en nombres premiers dans* $\mathbb{Z}[i]$*. (Indication : Montrer que pour tous* $a, b \in O_K$*,* $b \neq 0$*, il existe* $c, r \in O_K$ *tels que* $a = bc + r$ *et* $\mathrm{N}(r) < \mathrm{N}(b)$*.)*

Exercice 22. *Déterminer les unites de* O_K *pour les corps quadratiques imaginaires* K *(i.e. pour les corps* K *de degré 2 sur* $\mathbb{Q}$ *et à discriminant négatif).*

Exercice 23. *Déterminer une* $\mathbb{Z}$*-base de* O_K *pour* $K = \mathbb{Q}(\sqrt[3]{2})$*.*

Le monument à l'honneur de Carl-Friedrich Gauß (1777 – 1855) et Heinrich Weber (1842 – 1913).

EXERCICES à THEORIE DES NOMBRES 2000 — Feuille 5

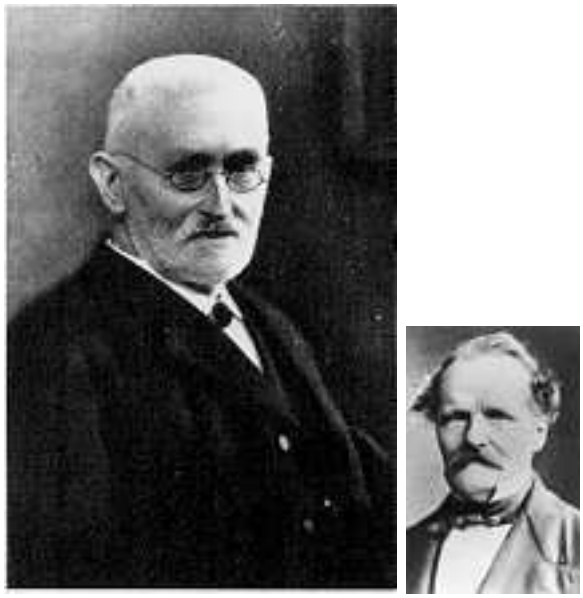
Exercice 24. *Déterminer le nombre des classes de* $\mathbb{Q}(\sqrt{D})$ *pour les discriminants* $D = -15, -19, -23$.

Exercice 25. *Soit* $\mathfrak{p} := 2O + O(1+\sqrt{-5})$ *et* $\mathfrak{q} := 3O + O(1+\sqrt{-5})$ *dans* $O = O_{\mathbb{Q}(\sqrt{-5})}$. *Montrer que* $2O = \mathfrak{p}\cdot\overline{\mathfrak{p}}$ *et* $3O = \mathfrak{q}\cdot\overline{\mathfrak{q}}$. *En déduire que* $\mathfrak{p}$ *et* $\mathfrak{q}$ *sont premiers. Décomposez* $(1+\sqrt{-5})O$ *en idéaux premiers.*

Exercice 26. *Montrer que* $O = O_{\mathbb{Q}(\sqrt{2})}$ *possède un nombre infini d'unités.*

Exercice 27. *Montrer que* 1, θ *et* $\frac{1}{2}(\theta+\theta^2)$ *est une base du* $\mathbb{Z}$*-module* $O_{\mathbb{Q}(\theta)}$ *où* $\theta^3 - \theta - 4 = 0$.

Exercice 28. *Soit* $O = O_K$ *pour un corps de nombre* K *arbitraire. Montrer que* $O/\mathfrak{a}$ *est un anneau principal pour tout idéal* $\mathfrak{a} \neq 0$. *(Tout idéal de* $O/\mathfrak{a}$ *est de la forme* $\mathfrak{b}/\mathfrak{a}$ *où* $\mathfrak{b}$ *est un* O*-idéal divisant* $\mathfrak{a}$. *Considérer dans un premier temps le cas que* $\mathfrak{a}$ *est une puissance d'un idéal premier* $\mathfrak{p}$, *prendre un* $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, *montrer que* $\mathfrak{p}^\nu = O\pi^\nu + \mathfrak{a}$.*) En déduire que tout idéal de* O *est engendré par deux éléments, i.e. qu'il est de la forme* $Oa + Ob$ *avec des* $a, b \in O$ *appropriés.*



Les pères des idéaux
Richard Dedekind
(1831–1916) et
Ernst Eduard Kummer
(1810–1893)

EXERCICES à THEORIE DES NOMBRES 2000 — Feuille 6

Exercice 29. *Soit $\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$ un idéal fractionnaire du corps des nombres K ($\mathfrak{p}_j$ idéal premiers, $n_j \in \mathbb{Z}$). Montrer que*

$$\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{p}_1)^{n_1} \cdots \mathrm{N}(\mathfrak{p}_r)^{n_r}.$$

(Indication : Appliquer le théorème chinois et regarder les applications canoniques $O/\mathfrak{p}^{n+1} \to O/\mathfrak{p}^n$.)

Leopold Kronecker (1823–1891)

Exercice 30. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux entiers de $O = O_K$. Montrer que leurs DIP ne contiennet aucun idéal premier commun si et seulement si on a $\mathfrak{a} + \mathfrak{b} = O$.*

Exercice 31. *Déterminer l'image de l'homomorphisme*

$$\mathrm{N} : J_{\mathbb{Q}(i)} \to \mathbb{Q}^*_{\geq 0}.$$

Exercice 32. *Calculer le discriminant de $\mathbb{Q}(e^{\frac{2\pi i}{7}})$.*

Exercice 33. *Calculer le discriminant de $\mathbb{Q}(\theta)$ où $\theta^3 - \theta + 1 = 0$.*

EXERCICES à THEORIE DES NOMBRES 2000 — Feuille 7

Exercice 34. *Déterminer les idéaux premiers $\mathfrak{P}_j$ de $\mathbb{Q}(\mu_5)$ tels que*

$$31 = \mathfrak{P}_1 \cdots \mathfrak{P}_r.$$

Exercice 35. *Calculer le symbole de Legendre $\left(\frac{7919}{7927}\right)$.*

Exercice 36. *Soit $K = \mathbb{Q}(\theta)$ où*

$$\theta^3 - \theta + 1 = 0.$$

Quelles sont les types de DIP dans K possibles pour un nombre premier rationnel p. Pour chaque type donner un premier p comme exemple et décomposer explicitement dans K. (Comparer Ex. 5 sur feuille 6.)

Exercice 37. *Soit D le discriminant d'un corps quadratique. Montrer qu'il existe un caractère de Dirichlet χ modulo $|D|$ tel que $\chi(p) = \left(\frac{D}{p}\right)$ pour tout nombre premier impair p.*

Exercice 38. *Montrer que, pour tout entier rationnel $n \geq 1$, le nombre de couples $(x, y) \in \mathbb{Z}^2$ tel que $n = x^2+xy+y^2$ est égal à $6 \sum_{d|n} \left(\frac{d}{3}\right)$. (Indication : Réduire à une question sur la DIP de n dans l'anneau principal $O_{\mathbb{Q}(\sqrt{-3})}$.)*

EXERCICES à THEORIE DES NOMBRES 2000 — Feuille 8

Exercice 39. *Montrer que l'inégalité* $\mathrm{vol}(X) > 2^n \mathrm{vol}(L)$ *du théorème de Minkowski est la meilleure possible. (Construire pour un* L *donné un ensemble convexe et symétrique* X *tel que* $\mathrm{vol}(X) = 2^n \mathrm{vol}(L)$ *et qui ne contient que le point 0 de* L*.)*

Hermann Minkowski (1864 – 1909)

Exercice 40. *Montrer que le nombre de classes de* $\mathbb{Q}(\sqrt{5})$ *est égal à 1. (Indication : Reviser la preuve du cours du théorème "Le groupe de classe* J_K/P_K *est fini".)*

Exercice 41. *Déterminer l'unité fondamentale* $\varepsilon > 1$ *de* $\mathbb{Q}(\sqrt{5})$*. (Indication : Quel est l'unité algebrique réelle quadratique la plus petite qui est* > 1 *?)*

Exercice 42. *Construire quelques unités qui ne sont pas des racines d'unités dans le corps cyclotomique* $K := \mathbb{Q}(\mu_n)$ *(*$n \neq 1, 2, 3, 4, 6$*). Quel est le rang de* O_K^* *?*

Exercice 43. *Soient* a, b *des nombres naturels qui ne sont pas des carrés dans* $\mathbb{Q}$*. Montrer qu'une unité fondamentale de* $\mathbb{Q}(\sqrt{a})$ *est aussi une unité fondamentale du corps* $\mathbb{Q}(\sqrt{a}, \sqrt{-b})$*.*

Exercice 44. *Calculer le volume de*

$$X = \{x \in V : \forall \tau \in \mathbb{A} : |\lambda_\tau x| < c_\tau\}.$$

(Les notations sont comme dans la démonstration du premier théorème de la section "Finitude du groupe de classe".)

Chapitre 4

La CC

CC au MOR_3 — Maitrise de Mathématiques Pures
Université de Bordeaux I
Durée : 3 heures
Les documents ne sont pas autorisés

Soit $F := \mathbb{Q}(\zeta)$ où ζ est la racine d'unité 3ième $\zeta = \exp(2\pi i/3)$.

Partie I : *Soit $a \in F$ tel que $\mathrm{N}_{F/\mathbb{Q}}(a) \in \mathbb{Q}^{*3}$, mais $a \notin F^{*3}$, et soit $K = \mathbb{Q}(r)$ où r est une racine du polynôme*

$$f := x^3 - 3mx - \mathrm{Tr}_{F/\mathbb{Q}}(a) \in \mathbb{Q}[x], \qquad m = \sqrt[3]{\mathrm{N}_{F/\mathbb{Q}}(a)},\ m > o$$

(1) Montrer : si u est un nombre tel que $u^3 = a$, alors $u\overline{u} = m$ et $f(u+\overline{u}) = 0$.

(2) Montrer que $u + \overline{u} \notin \mathbb{Q}$ (Indication : Montrer $[F(u) : F] = 3$, puis noter que si $u + \overline{u} \in \mathbb{Q}$, alors $[\mathbb{Q}(u) : \mathbb{Q}] \leq 2$.)

(3) Déduire de (1) et (2) que f est irréductible sur $\mathbb{Q}$. (Indication : Quelles sont les 3 racines a, b, c potentielles pour f ? Montrer $(x-a)(x-b)(x-c) = f$.)

(4) Montrer que $a \notin \mathbb{Q}$. En déduire qu'il existe des nombres rationnels x, y tels que $\zeta = xu^3 + y$.

(5) Montrer à l'aide de (4) : si $v^3 = u^3 = a$, alors $v + \overline{v} = h(u + \overline{u})$ pour un polynôme h dans $\mathbb{Q}[x]$.

(6) Déduire de (1) à (5) que K est une extension galoisienne de degré 3 sur $\mathbb{Q}$.

Partie II : *Soit réciproquement K une extension galoisienne de degré 3 sur $\mathbb{Q}$.*

(1) Montrer que KF est galoisienne sur $\mathbb{Q}$. (Si $K = \mathbb{Q}(\alpha)$, alors KF désigne le corps $\mathbb{Q}(\alpha, \zeta)$.)

(2) Montrer que $[KF : \mathbb{Q}] = 6$.

(3) Quels sont les groupes d'ordres 6 à isomorphismes près ? Lequel est isomorphe à $G := \mathrm{Gal}(KF/\mathbb{Q})$?

(4) Montrer (en utilisant les bons théorèmes du cours sans répétition de leurs preuves) qu'il existe un $u \in KF$ tel que $u^3 \in F$ et $KF = F(u)$.
Désormais on fixe un tel u.

(5) Si $G = \mathrm{Gal}(KF/\mathbb{Q})$, décrire $\sigma(u)$ où σ parcourt G.

(6) Montrer que $\mathrm{N}_{F/\mathbb{Q}}(a) \in \mathbb{Q}^{*3}$ où $a = u^3$ (Indication : on peut considérer $\mathrm{Tr}_{KF/\mathbb{Q}}(u\overline{u})$).

(7) Montrer que $KF = F(u)$ entraîne $K = \mathbb{Q}(u + \overline{u})$.

(8) Calculer le polynôme minimal de $u + \overline{u}$ sur $\mathbb{Q}$.

Partie III : Soient u, v des nombres complexes non-nuls tels que $u^3, v^3 \in F$. Montrer que $F(u) = F(v)$ si et seulement si $u^3F^{*3} = v^3F^{*3}$ ou $u^3F^{*3} = v^6F^{*3}$. (Si $F(u) = F(v)$ on pourrait étudier l'action de $\mathrm{Gal}(F(u)/F)$ sur u/v et u/v^2.)

Partie IV : Déduire des volets I à III que l'application

$$a \to K_a := \mathbb{Q}(r),\ r \text{ racine de } x^3 - 3\sqrt[3]{\mathrm{N}_{F/\mathbb{Q}}(a)}\, x - \mathrm{Tr}_{F/\mathbb{Q}}(a)$$

induit une bijection entre les sous-groupes d'ordre 3 de $\mathrm{N}^{-1}_{F/\mathbb{Q}}(\mathbb{Q}^{*3})/F^{*3}$ et l'ensemble des extensions galoisiennes de $\mathbb{Q}$ (et contenues dans $\mathbb{C}$) de degré 3.

Partie V : Déterminer trois $a \in F$ tels que les corps K_a sont 2 à 2 différents.

Partie VI : Cette partie est indépendante des autres parties. *D'après le cours on sait $O := O_F = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{-3}}{2}$. Un exercice sur une des feuilles, qui accompagnent le cours, a montré que O est principal ; en particulier tout élément de O possède une unique décomposition en nombre premiers (DNP).*

(1) Montrer que $\sqrt{-3}$ est un premier de O. Déterminer la DNP 3 dans O.

(2) Soit $p \neq 3$ un nombre premier rationnel. Montrer que soit p reste un nombre premier dans O, soit il existe un premier π dans O tel que $p = \pi\overline{\pi}$ est la DNP de p dans O. Dans le dernier cas montrer que π n'est pas associé à $\overline{\pi}$. (Pour l'analyse des possibles DNP de p on pourrait appliquer $\mathrm{N}_{F/\mathbb{Q}}$ à une décomposition $p = \pi_1\pi_2 \cdots \pi_r$.)

(3) Soit $a \in O$ avec une DNP de la forme $a = \pi^{t_1}\pi^{t_2} \cdots \pi^{t_r}$ ($1 \leq t_1, t_2, \ldots, t_r \leq 2$, π_h n'est pas associé à π_j pour $h \neq j$). Supposons que $N(a) \in \mathbb{Q}^{*3}$. Qu'est-ce que l'on peut conclure pour les π_h et les t_h ?

(4) Soit $p \neq 3$ un premier rationnel avec DNP $p = \pi\overline{\pi}$ dans O. Montrer que $p \equiv 1 \bmod 3$. (Ecrire $\pi = x + y\frac{1+\sqrt{-3}}{2}$ avec des entiers x, y, exprimer p en terme des x, y.)
On admet la preuve du fait qu'un premier rationnel p reste premier dans O si et seulement si $p \equiv 2 \bmod 3$.

Partie VII : Déduire des volets IV et VI que $m \mapsto \mathbb{Q}(r)$, où r est une racine de $x^3 - 3m\ x - \mathrm{Tr}_{F/\mathbb{Q}}(a)$ avec un $a \in F$ tel que $\mathrm{N}_{F/\mathbb{Q}}(a) = m^3$, définit une bijection entre l'ensemble des nombres naturels m sans facteur carré et qui contiennent seulement des premiers $p \equiv 1 \bmod 3$ et l'ensemble des extensions galoisiennes de degré 3 sur $\mathbb{Q}$ (et dans $\mathbb{C}$).

Le barême pour les 7 parties est $9+12+3+3+3+8+2 = 40$ **sur** 30**.**

Bibliographie