NOMBRES ALGÉBRIQUES ET NOMBRES p-ADIQUES

cours préparatoire aux études doctorales
2003-04

par **Loïc Merel**

Université Pierre et Marie Curie
Université Denis Diderot

I
Les valeurs absolues des nombres rationnels

1. Valeurs absolues d'un corps

Soit K un corps. Une *valeur absolue* de K (au sens, par exemple, de Bourbaki, attention cette notion coïncide avec "valuation" en anglais) est une fonction non nulle $|.|$ définie sur K à valeurs dans les nombres réels positifs et vérifiant les trois conditions $((x, y) \in K^2)$:

(ι) $|x| = 0$ si et seulement si $x = 0$,
($\iota\iota$) $|xy| = |x|\,|y|$,
($\iota\iota\iota$) $|x + y| \leq |x| + |y|$.

La relation ($\iota\iota$) entraîne que $|.|$ induit un homomorphisme de groupes $K^* \longrightarrow \mathbf{R}_+^*$. La relation ($\iota\iota\iota$) s'appelle *l'inégalité triangulaire*.

Lorsque L est un sous-corps de K, une valeur absolue de K induit une valeur absolue de L. Toute valeur absolue d'un corps de caractéristique 0 prolonge donc une valeur absolue du corps des nombres rationnels $\mathbf{Q}$.

Exemples. — La *valeur absolue triviale* est la fonction caractéristique de K^*. On l'exclut parfois implicitement.

Lorsqu'on a un plongement $i : K \longrightarrow \mathbf{C}$, les fonctions $x \mapsto |i(x)|_\infty^k = |i(\bar{x})|_\infty^k$ sont des valeurs absolues de K (on a noté $|.|_\infty$ la valeur absolue habituelle de $\mathbf{C}$ et k est un nombre réel vérifiant $0 < k \leq 1$). Un tel plongement définit une place de K dans $\mathbf{C}$.

Une valeur absolue est dite *non-archimédienne* si la distance associée (qui associe à (x, y) le nombre $|x - y|$) est ultramétrique, c'est-à-dire si on a, pour tout $(x, y) \in K^2$, l'inégalité

$$|x + y| \leq \mathrm{Max}(|x|, |y|).$$

Cette distance associée définit une topologie sur K. Deux valeurs absolues sont dites *équivalentes* si elles se déduisent l'une de l'autre par élévation à la puissance d'un nombre réel > 0. Une valeur absolue est dite *archimédienne* si elle n'est pas équivalente à une valeur absolue non-archimédienne. Deux valeurs absolues équivalentes définissent des distances équivalentes (au sens usuel) donc la même topologie sur K.

Soit x un élément non nul de K. Remarquons que pour la topologie définie par une valeur absolue $|.|$, les applications $K \longrightarrow K$ qui à y associe $x + y$, xy, $1/y$ (pour $y \neq 0$) et

$-y$ respectivement sont continues. De plus l'application $K \longrightarrow \mathbf{R}$ qui à y associe $|y|$ est continue.

On établit facilement que la valeur absolue d'une racine de l'unité est égale à 1 ; Il en résulte que toute valeur absolue d'un corps fini est triviale (cela résulte de la propriété $(\iota\iota)$).

2. Valuations discrètes

Un *anneau de valuation discrète* A est par définition un anneau principal (et donc intègre) qui possède un unique idéal premier et non nul $\mathcal{M}_A$. Cet idéal est nécessairement maximal.

Lemme 1. — *1. On a* $\cap_{n\geq 0}\mathcal{M}_A^n = \{0\}$.
2. Tout idéal non nul de A *est de la forme* $\mathcal{M}_A^n$, *avec* n *entier* ≥ 0.
Démonstration. — Montrons le premier point. Soit π un générateur de $\mathcal{M}_A$. L'idéal $\cap_{n\geq 0}\pi^n A$ est premier ; en effet, pour $(x, y) \in \pi^n A \times \pi^m A$, vérifiant $xy \in \cap_{n\geq 0}\pi^n A$, on a $(x/\pi^n)(y/\pi^m) \in \cap_{n\geq 0}\pi^n A \subset \mathcal{M}_A$ et donc $x/\pi^n \in \mathcal{M}_A$ ou $y/\pi^m \in \mathcal{M}_A$, c'est-à-dire $x \in \pi^{n+1}A$ ou $y \in \pi^{m+1}A$, et donc $x \in \cap_{n\geq 0}\pi^n A$ ou $y \in \cap_{n\geq 0}\pi^n A$ par un procédé inductif. L'idéal $\cap_{n\geq 0}\pi^n A$ n'est pas égal à $\mathcal{M}_A$ (car on aurait alors $\pi A = \pi^2 A$ et donc $A = \pi A$ par intégrité de A, ce qui est absurde). Il est donc nul.

Venons-en maintenant au deuxième point. Soit I un idéal non nul de A. Il existeun plus petit entier $n \geq 0$ tel que $I \subset \mathcal{M}_A^n$. L'ensemble $\pi^{-n}I$ est alors un idéal de A non contenu dans $\mathcal{M}_A$. C'est donc A et on a $I = \pi^n A = \mathcal{M}_A^n$.

Un générateur de $\mathcal{M}_A$ comme A-module est une *uniformisante* de $\mathcal{M}_A$. Le corps $A/\mathcal{M}_A$ est le *corps résiduel* de A.

On a une suite décroissante de A-modules :

$$...\mathcal{M}_A^{n+1} \subset \mathcal{M}_A^n \subset ... \subset \mathcal{M}_A \subset A.$$

Soit $x \in A$ non nul. L'idéal de A engendré par x est égal à $\mathcal{M}_A^n$ où n est un entier ≥ 0. L'entier n est la *valuation* de x. Notons cette valuation $v(x)$.

L'application $v : A \longrightarrow \mathbf{N}$ est une *valuation* de A. Elle s'étend en une fonction surjective à valeurs dans $\mathbf{Z}$, encore notée v, sur le corps des fractions K de A, par la formule $v(\frac{x}{y}) = v(x) - v(y)$. La valuation est discrète car c'est un homomorphisme de groupes $K^* \longrightarrow \mathbf{Z}$ d'image un groupe discret.

(On pose souvent par convention $v(0) = +\infty$.)

Exemples. — Soit p un nombre premier. Notons $\mathbf{Z}_{(p)}$ l'ensemble des nombres rationnels dont le dénominateur est premier à p. C'est l'anneau obtenu en localisant $\mathbf{Z}$ relativement à l'idéal premier $p\mathbf{Z}$. Il est de valuation discrète d'idéal maximal égal à $p\mathbf{Z}_{(p)}$. On note v_p la valuation associée. Le corps résiduel est $\mathbf{F}_p$ le corps à p éléments.

L'anneau $\mathbf{Z}_p$ des entiers p-adiques est un cas éminent d'anneau de valuation discrète. On verra plus tard comment le construire à partir de $\mathbf{Z}_{(p)}$.

Soit k un corps. L'anneau $k[[T]]$ est un anneau de valuation discrète d'idéal maximal $Tk[[T]]$, de corps résiduel k et de corps des fractions $k((T))$.

PROPOSITION 1. — *Soit K un corps. Soit v un homomorphisme surjectif de groupes $K^* \longrightarrow \mathbf{Z}$. Supposons que v vérifie $v(x+y) \geq \min(v(x), v(y))$ pour tout $(x,y) \in K^{*2}$. Alors l'ensemble $A = \{x \in K^*/v(x) \geq 0\} \cup \{0\}$ est un sous-anneau de K de valuation discrète d'idéal maximal $\mathcal{M}_A = \{x \in K^*/v(x) > 0\} \cup \{0\}$.*
Démonstration. — Les ensembles A et $\mathcal{M}_A$ sont stables par l'addition interne et la multiplication par les éléments de A et contiennent 0 (De plus A contient 1). Ce sont donc un anneau et un idéal de A respectivement. Observons que les éléments inversibles de A sont ceux qui sont dans le noyau de v. Soit π un élément de A tel que $v(\pi) = 1$. Tout élément x de A est de la forme $\pi^n u$ avec n entier ≥ 0 et $v(u) = 0$. Tout idéal de A s'écrit donc sous la forme $\pi^n A$ avec $n \geq 0$. Il en résulte que A est principal et a pour unique idéal premier non nul $\pi A = \mathcal{M}_A$.

Soit a un nombre réel > 1. L'application $x \mapsto a^{-v(x)}$ est une valeur absolue de K dont la classe d'équivalence est indépendante de a.

Lorsque le corps résiduel est d'ordre fini $|k|$, on choisit comme représentant canonique $a = |k|$. Lorsque $A = \mathbf{Z}_{(p)}$, on pose $|x|_p = p^{-v_p(x)}$. C'est la valeur absolue *p-adique* du corps des nombres rationnels $\mathbf{Q}$.

3. Valeurs absolues de Q

Ce qui suit est connu comme le théorème d'Ostrowski.

THÉORÈME 1. — *Soit $|.|$ une valeur absolue non triviale de $\mathbf{Q}$. Alors $|.|$ est équivalente à $|.|_p$ pour un nombre premier p ou à $|.|_\infty$.*
Démonstration. — Supposons d'abord qu'il existe $x \in \mathbf{Z}$ tel que $|x| > 1$. Puisqu'on a $|-1| = 1$, quitte à remplacer x par $-x$ on peut supposer que x est un entier positif. Soit y un entier strictement positif. Écrivons x^n en base y :

$$x^n = \alpha_k y^k + ... + \alpha_1 y + \alpha_0.$$

Rappelons qu'on a l'inégalité $0 \leq \alpha_i < y$ $(i = 0, 1, ..., k)$. Posons

$$C_y = \mathrm{Max}(|1|, ..., |y-1|).$$

En appliquant l'inégalité triangulaire, on obtient

$$|x|^n \leq C_y(1+k)\mathrm{Max}(1, |y|^k).$$

De plus, on a

$$k \leq \log_y(x^n),$$

où $\log_y$ est le logarithme en base y. Cela donne

$$|x|^n \leq C_y(1+\log_y(x^n))\mathrm{Max}(1, |y|^{log_y(x^n)}).$$

En prenant les racines n-ièmes et en faisant tendre n vers l'infini on obtient

$$|x| \leq \mathrm{Max}(1, |y|^{\log_y(x)}),$$

et donc, puisque $|x| > 1$,

$$|x|^{\frac{1}{\log x}} \leq |y|^{\frac{1}{\log y}}.$$

Cela donne $|y| > 1$ et par échange des rôles de x et y

$$|x|^{\frac{1}{\log x}} = |y|^{\frac{1}{\log y}}.$$

Cette égalité s'étend immédiatement à l'égalité suivante pour deux nombres rationnels non nuls x et y quelconques

$$|x|^{\frac{1}{\log |x|_\infty}} = |y|^{\frac{1}{\log |y|_\infty}}.$$

Par passage aux logarithmes, cela entraîne que la valeur absolue $|.|$ est équivalente à la valeur absolue archimédienne.

Abandonnons notre hypothèse de départ. Pour tout $x \in \mathbf{Z}$ on a donc $|x| \leq 1$. On va la supposer non triviale. Cela entraîne que $|.|$ est non constante égale à 1 sur les entiers non nuls par multiplicativité de la valeur absolue et en raison du fait que tout nombre rationnel est quotient de deux nombres entiers.

Lemme 2. — *La valeur absolue* $|.|$ *est non archimédienne.*
Démonstration. — Soient x et y deux nombres rationnels. On a, utilisant le fait que le coefficient binomial $\binom{n}{k}$ est un entier et donc vérifie $|\binom{n}{k}| \leq 1$ et l'inégalité triangulaire, les inégalités

$$|x+y|^n = |(x+y)^n| \leq \sum_{k=0}^{n} \binom{n}{k} |x|^k |y|^{n-k} \leq (n+1)\mathrm{Max}(|x|^n, |y|^n).$$

Par passage à la limite sur n après avoir extrait les racines n-ièmes, on obtient l'inégalité $|x+y| \leq \mathrm{Max}(|x|, |y|)$ cherchée.

Revenons à la démonstration du théorème. L'ensemble des entiers x tels que $|x| < 1$ constitue un idéal premier non nul de $\mathbf{Z}$ (Cela résulte de l'inégalité ultramétrique établie par le lemme de façon analogue à la démonstration de la proposition 1). Il est donc de la forme $p\mathbf{Z}$ où p est un nombre premier. Soit $a \in \mathbf{Q}$. Posons $a = a_0 p^n$, avec a_0 quotient de deux nombres entiers premiers à p et $n \in \mathbf{Z}$. On a $|a| = |a_0||p|^n = |p|^{v_p(a)}$. La norme $|.|$ est donc équivalente à la valeur absolue p-adique $|.|_p$. Cela achève la démonstration du théorème d'Ostrowski.

Remarque . — On verra que le théorème d'Ostrowski détermine les valeurs absolues des extensions finies de $\mathbf{Q}$ et que dans ce cas on a plus d'une valeur absolue non-archimédienne.

La formule suivante est connue sous le nom de *formule du produit.*

Proposition 2. — *Soit x un nombre rationnel non nul. On a*

$$(\prod_{p \text{ premier}} |x|_p)|x|_\infty = 1.$$

Démonstration. — Par multiplicativité des valeurs absolues, il suffit de vérifier la formule pour les nombres premiers et pour -1. Soit q un nombre premier. Lorsque p est un nombre premier différent de q on a $|q|_p = 1$. De plus on a $|q|_q = 1/q$ et $|q|_\infty = q$.

On ne s'étendra ici sur la notion de place qui ne nous sera pas vraiment utile. Une *place* d'un corps K dans un corps L est une application $K \cup \{\infty\} \longrightarrow L \cup \{\infty\}$ qui respecte l'addition et la multiplication prolongées partiellement des corps K et L à $K \cup \{\infty\}$ et $L \cup \{\infty\}$ par $x + \infty = \infty$ (x élément du corps), $x\infty = \infty$ (x non nul) et $\infty + \infty = \infty$ (0∞ n'est pas défini). Une telle place est dite *finie* (resp. *infinie*) lorsque L est fini (resp. infini).

Pour p nombre premier, la réduction modulo p fournit un place de $\mathbf{Q}$ dans le corps $\mathbf{F}_p$ à p éléments (en convenant que la réduction modulo p d'un nombre rationnel non p-entier est ∞). Il s'agit d'une place finie. Ces places coïncident naturellement avec les valeurs absolues non-archimédiennes de $\mathbf{Q}$. La place triviale de $\mathbf{Q}$ dans $\mathbf{Q}$ peut être vue comme correspondant à la valeur absolue archimédienne. Un homomorphisme de corps $K \longrightarrow L$, qui est nécessairement injectif, fournit par un prolongement trivial une place de K dans L.

Signalons que toutes les places de $\mathbf{Q}$ sont obtenues en composant celle mentionnées ci-dessus avec des places déduites d'homomorphismes injectifs de corps comme ci-dessus. À un homomorphisme de corps près, les places de $\mathbf{Q}$ correspondent donc aux valeurs absolues de $\mathbf{Q}$ à équivalence près. Cette remarque trouve son intérêt dans le fait que la notion de place est plus intrinsèque que la notion de valeur absolue : elle ne fait pas appel au corps des nombres réels.

Exercice . — Soit k un corps. Soit P un polynôme irréductible de k. Soit $Q = P^n \frac{u}{v} \in k(T)$, où u et v sont deux polynômes premiers entre eux et premiers à P et $n \in \mathbf{Z}$. Soit $\delta \in \mathbf{R}$, $0 < \delta < 1$. Posons

$$|Q|_P = \delta^n.$$

1. Démontrer que l'application qui à Q associe le nombre réel $|Q|_P$ est une valeur absolue de $k(T)$.

2. Démontrer que l'application qui à $Q = \frac{u}{v} \in k(T)$ associe $\delta^{\mathrm{d}^0 v - \mathrm{d}^0 u}$ est une valeur absolue de $k(T)$.

3. Démontrer que les valeurs absolues de $k(T)$ qui sont triviales sur k sont à équivalence près de l'un des deux types précédents.

4. En déduire que les valeurs absolues de $\mathbf{F}(T)$ sont de l'un des deux types ci-dessus lorsque $\mathbf{F}$ est un corps fini.

4. Commentaires sur les analogies en arithmétique

Les extensions finies des corps $\mathbf{Q}$ et $\mathbf{F}(T)$ sont respectivement les *corps de nombres* et les *corps de fonctions*. Les propriétés arithmétiques de ces corps sont très analogues, quoique généralement plus difficiles à établir pour les corps de nombres. D'un point de vue technique, l'étude des corps de fonctions revient à l'étude des courbes algébriques sur les corps finis, ce qui est du ressort de la géométrie algébrique.

Prenons note de quelques différences entre $\mathbf{Q}$ et $\mathbf{F}(T)$:

– Le corps $\mathbf{Q}$ possède une valeur absolue archimédienne contrairement à $\mathbf{F}(T)$. Dans l'esprit qui prévaut en théorie des nombres, cette valeur absolue doit être prise en compte et, éventuellement, placée à égalité avec les valeurs absolues non archimédiennes.

– Les anneaux de valuation discrète associés aux valeurs absolues de $\mathbf{F}(T)$ (resp. $\mathbf{Q}$) ont des corps résiduels qui ont tous même caractéristique (resp. ont des caractéristiques toutes différentes).

– Le corps $\mathbf{F}(T)$ possède des extensions finies obtenues en considérant les extensions de $\mathbf{F}$ (on s'accorde toutefois à penser que certaines extensions de $\mathbf{Q}$ obtenues en ajoutant des racines de l'unité seraient les analogues de ces extensions).

– On peut faire sur l'anneau $\mathbf{F}[T]$ (qui est l'anneau des entiers de $\mathbf{F}(T)$) l'opération suivante $\mathbf{F}[T] \otimes_{\mathbf{F}} \mathbf{F}[T] \simeq \mathbf{F}[T_1, T_2]$. On ne voit pas comment faire une telle opération pour le corps $\mathbf{Q}$ (*i.e.* on a $\mathbf{Z} \otimes \mathbf{Z} \simeq \mathbf{Z}$, ce qui n'est pas très intéressant).

– Le corps $\mathbf{F}(T)$ est muni d'une application $\mathbf{F}$-linéaire donnée par la dérivation. C'est parfois un outil très commode dont on aimerait bien disposer pour étudier les nombres.

II
Anneaux de Dedekind

1. Localisation et idéaux fractionnaires

Cette section est consacrée à rappeler quelques faits faciles d'algèbre commutative.

Soit A un anneau intègre. Notons K son corps des fractions.

Rappelons que A est dit *noethérien* si et seulement si toute suite croissante d'idéaux de A est stationnaire. Il est équivalent de dire que tout idéal de A est de type fini (c'est-à-dire engendré par un nombre fini d'éléments).

L'anneau A est dit *intégralement clos* si tout élément de K qui est *entier sur* A (c'est-à-dire racine d'un polynôme unitaire à coefficients dans A) est dans A. Par exemple $\mathbf{Z}$ est intégralement clos (mais pas $A = \mathbf{Z} + \mathbf{Z}[\sqrt{-3}]$, en effet $x = (1 + \sqrt{-3})/2)$ est solution de l'équation $x^2 - x + 1 = 0$ sans appartenir à A). Lorsque A est contenu dans un corps L, l'ensemble des éléments de L qui sont entiers sur A est un anneau qu'on appelle *clôture intégrale de A dans L*. Dire qu'un élément x de L est entier sur A revient à dire que $A[x]$ est un A-module de type fini.

Soit I un A-module contenu dans K. Posons

$$I^{-1} = \{x \in K / xI \subset A\}$$

et

$$R(I) = \{x \in K / xI \subset I\}.$$

On dit que I est un *idéal fractionnaire* si $I \neq 0$ et s'il existe $a \in A$ non nul tel que $aI \subset A$, cela revient à dire qu'il existe $a \in K$ tel que $aI \subset A$.

Un idéal fractionnaire I est dit *inversible* s'il vérifie $II^{-1} = A$.

Soient I_1 et I_2 deux idéaux fractionnaires de A contenus dans $a_1^{-1}A$ et $a_2^{-1}A$ respectivement avec $(a_1, a_2) \in (A - \{0\})^2$. Alors $I_1 + I_2$, $I_1 I_2$, $I_1 \cap I_2$ sont des idéaux fractionnaires car ils sont contenus dans $(a_1 a_2)^{-1}A$. De plus $I = \{x \in K / xI_2 \subset I_1\}$ est un idéal fractionnaire. (Preuve : c'est un A-module non nul ; on a $uvI \subset A$ avec $u \neq 0$ vérifiant $uI_1 \subset A$ et $v \in I_2$ non nul.) Il en résulte (par application à $I_1 = I$ et $I_2 = A$ d'une part et à $I_1 = I$ et $I_2 = I$ d'autre part) que I_1^{-1} et $R(I_1)$ sont des idéaux fractionnaires.

Lorsque A est un anneau noethérien, tout idéal fractionnaire I est de type fini. En effet on a un isomomorphisme de A-modules entre I et $aI \subset A$ qui est un idéal de A et qui est donc de type fini.

Soit $\mathcal{P}$ un idéal premier de A. Le *localisé* $A_{(\mathcal{P})}$ de A en $\mathcal{P}$ est le sous-anneau de K formé des éléments de la forme u/v (avec $(u, v) \in A \times (A - \mathcal{P})$). C'est un *anneau local*, c'est-à-dire un anneau contenant un unique idéal maximal. On a $\mathcal{P} = \mathcal{P}A_{(\mathcal{P})} \cap A$. Mentionnons la propriété importante suivante de la localisation :

Lemme 1. — *Soit I un idéal de $A_{(\mathcal{P})}$. On a*

$$I = (I \cap A)A_{(\mathcal{P})}.$$

Démonstration. — On l'inclusion $(I \cap A)A_{(\mathcal{P})} \subset I$. Réciproquement tout élément de I sécrit sous la forme u/v avec $(u, v) \in A \times (A - \mathcal{P})$. Comme v est inversible dans $A_{(\mathcal{P})}$, on a $u \in I \cap A$. On a donc $u/v \in (I \cap A)A_{(\mathcal{P})}$.

Tout idéal de $A_{(\mathcal{P})}$ est donc de la forme $IA_{(\mathcal{P})}$ où I est un idéal de A. Cela entraîne que, si A est noethérien, $A_{(\mathcal{P})}$ est noethérien.

Lemme 2. — Supposons que A soit intégralement clos. Alors $A_{(\mathcal{P})}$ est intégralement clos.
Démonstration. — Soit x un élément K qui est entier sur $A_{(\mathcal{P})}$. Il vérifie

$$x^n + \frac{a_{n-1}}{b}x^{n-1} + ... + \frac{a_0}{b} = 0,$$

avec $b \in A - \mathcal{P}$ et $a_i \in A$ ($i \in \{0, 1, ..., n-1\}$). On en déduit que bx est entier sur A. C'est donc un élément de A. Cela entraîne qu'on a $x \in A_{(\mathcal{P})}$.

2. Caractérisation des anneaux de valuation discrète

On a la caractérisation suivante des anneaux de valuation discrète.

Proposition 1. — *Soit A un anneau intègre, noethérien, intégralement clos et possédant un unique idéal premier non nul. Alors A est un anneau de valuation discrète.*
Démonstration. — Il suffit de prouver que A est principal. Notons $\mathcal{M}$ l'idéal maximal de A. Procédons en plusieurs étapes.

Lemme 3. — *Soit $x \in \mathcal{M}$. On a $A[\frac{1}{x}] = K$.*
Démonstration. — Il suffit de prouver que $A[\frac{1}{x}]$ est un corps, c'est-à-dire que tout idéal premier de $A[\frac{1}{x}]$ est nul. Soit $\mathcal{P}$ un idéal premier de $A[\frac{1}{x}]$. Il ne contient pas x qui est inversible dans $A[\frac{1}{x}]$. L'idéal $\mathcal{P} \cap A$ est un idéal premier de A distinct de $\mathcal{M}$ puisque $x \in \mathcal{M}$. On a donc $\mathcal{P} \cap A = \{0\}$. Soit y/x^n un élément de de $\mathcal{P}$, où on peut supposer que $y \in A$. On a $y \in \mathcal{P} \cap A = \{0\}$. Cela prouve que que $\mathcal{P}$ est nul.

Soit z un élément de A non nul.

Lemme 4. — *Soit $x \in \mathcal{M}$. Il existe $n \geq 0$ tel que $x^n \in zA$.*
Démonstration. — On a $1/z \in K = A[\frac{1}{x}]$. Il existe donc n tel que $x^n z \in A$.

Lemme 5. — *Il existe un entier $m \geq 0$ tel que $\mathcal{M}^m \subset zA$.*
Démonstration. — Puisque A est un anneau noethérien, $\mathcal{M}$ est un A-module de type fini. Soient $x_1, x_2, ..., x_k$ des générateurs de $\mathcal{M}$. Posons $m = kn$, avec n tel que $x_i^n \in zA$ pour tout i, c'est possible d'après le lemme 3. L'idéal $\mathcal{M}^m$ est engendré par les monômes de degré total m en les x_i. Tous les tels monômes contiennent un facteur du type x_i^n ; un tel facteur est dans zA. On en déduit que $\mathcal{M}^m \subset zA$.

Lemme 6. — *On a* $\mathcal{M}^{-1} \neq A$.
Démonstration. — Choisissons maintenant z dans $\mathcal{M}$. Choisissons m minimal parmi les entiers > 0 tels que $\mathcal{M}^m \subset zA$. Soit $y \in \mathcal{M}^{m-1} - zA$. On a $\mathcal{M}y \in zA$. Par conséquent on a $y/z \in \mathcal{M}^{-1} - A$.

Lemme 7. — *On a* $\mathcal{M}\mathcal{M}^{-1} = A$.
Démonstration. — C'est un sous A-module de A qui contient $\mathcal{M}$. Il est donc égal à A ou $\mathcal{M}$. Soit t un élément de $\mathcal{M}^{-1} - A$. L'élément t n'est pas entier sur A puisque A est intégralement clos. Pour tout $n > 0$, t^n n'est pas une combinaison linéaire à coefficients dans A des t^i, $i < n$. La suite de A-modules $A \subset A + At \subset A + At + At^2 \subset ...$ est donc strictement croissante. Cette suite n'est donc contenue dans aucun A-module de type fini, puisque A est noethérien. En particulier elle n'est pas contenue dans $\mathcal{M}^{-1}$, qui est de type fini (en effet c'est un idéal fractionnaire). Par conséquent il existe $n > 0$, que l'on peut choisir minimal, tel que $t^n \notin \mathcal{M}^{-1}$. On a donc que $t^n\mathcal{M}$ n'est pas contenu dans A et *a fortiori* pas contenu dans $\mathcal{M}\mathcal{M}^{-1}$ ni dans $t\mathcal{M}$. Par conséquent $t^{n-1}\mathcal{M}$ n'est pas contenu dans $\mathcal{M}$. L'idéal $\mathcal{M}\mathcal{M}^{-1}$ de A n'est donc pas contenu dans $\mathcal{M}$. Puisque $\mathcal{M}$ est maximal, cela entraîne que $\mathcal{M}\mathcal{M}^{-1} = A$.

Lemme 8. — *L'idéal* $\mathcal{M}$ *est principal.*

Puisqu'on a $\mathcal{M}\mathcal{M}^{-1} = A$, il existe un élément u de $A - \mathcal{M}$ qui s'exprime comme le produit d'un élément v de $\mathcal{M}$ par un élément w de $\mathcal{M}^{-1}$. Cet élément u est inversible puisque $\mathcal{M}$ est un idéal maximal. Soit $t \in \mathcal{M}$. On a $t = tvw/u = (tw/u)v$. Comme $w \in \mathcal{M}^{-1}$, tw appartient à A. On a donc $t \in vA$. Par conséquent $\mathcal{M}$ est engendré par v comme A-module. Il est donc principal.

Lemme 9. — *On a* $\cap_{n\geq 0}\mathcal{M}^k = 0$.

Démonstration. — C'est la même démonstration que la démonstration du lemme, partie 1), dans la leçon I. Comme $\mathcal{M}$ est principal, il est muni d'une uniformisante π. L'idéal $\cap_{n\geq 0}\pi^n A$ est premier ; en effet, pour $(x, y) \in \pi^n A \times \pi^m A$, vérifiant $xy \in \cap_{n\geq 0}\pi^n A$, on a $(x/\pi^n)(y/\pi^m) \in \cap_{n\geq 0}\pi^n A \subset \mathcal{M}$ et donc $x/\pi^n \in \mathcal{M}$ ou $y/\pi^m \in \mathcal{M}$, c'est-à-dire $x \in \pi^{n+1}A$ ou $y \in \pi^{m+1}A$, et donc $x \in \cap_{n\geq 0}\pi^n A$ ou $y \in \cap_{n\geq 0}\pi^n A$ par un procédé inductif. L'idéal $\cap_{n\geq 0}\pi^n A$ n'est pas égal à $\mathcal{M}$ (car on aurait alors $\pi A = \pi^2 A$ et donc $A = \pi A$ par intégrité de A, ce qui est absurde). Il est donc nul.

Lemme 10. — *L'anneau* A *est principal.*

Démonstration. — C'est la même démonstration que la démonstration du lemme, partie 2), dans la leçon I. Soit I un idéal de A. On considère le plus grand entier $n \geq 0$ tel que $I \subset \mathcal{M}^n$. On a $I = \pi^{n_I} A$.

Cela achève la preuve de la proposition 1.

Citons une autre caractérisation des anneaux de valuation discrète : Un anneau intègre, local, noethérien et dont l'idéal maximal est principal est de valuation discrète. Nous ne ferons pas usage de cette caractérisation.

Soit A un anneau noethérien et intégralement clos. Soit $\mathcal{P}$ est un idéal premier minimal et maximal de A. Alors $A_{(\mathcal{P})}$ est un anneau de valuation discrète dont l'idéal maximal

n'est autre que $\mathcal{P}A_{(\mathcal{P})}$. Notons $v_{\mathcal{P}}$ la valuation associée. Les idéaux fractionnaires de $A_{(\mathcal{P})}$ sont de la forme $\mathcal{P}^n$, $n \in \mathbf{Z}$.

3. Anneaux de Dedekind

Un *anneau de Dedekind* est un anneau A intègre et noethérien vérifiant l'une au moins des conditions suivantes.

(ι) A est intégralement clos et tout idéal premier et non nul de A est maximal.

($\iota\iota$) Pour tout idéal premier et non nul $\mathcal{P}$ de A, $A_{(\mathcal{P})}$ est un anneau de valuation discrète.

($\iota\iota\iota$) Tout idéal fractionnaire de A est inversible.

Exemples. — Comme on le verra plus tard, l'anneau des entiers d'un corps de nombres, en particulier $\mathbf{Z}$, est un anneau de Dedekind.

Soit k un corps. L'anneau $k[T]$ est un anneau de Dedekind. En revanche l'anneau $k[T_1, T_2]$ n'est pas de Dedekind puisque les idéaux engendrés par T_1 et T_2 sont non nuls, distincts et premiers.

Un anneau principal (*a fortiori* de valuation discrète) est un anneau de Dedekind.

En revanche un anneau de Dedekind n'est pas nécessairement principal ni même factoriel.

Proposition 2. — *Soit A un anneau intègre et noethérien. Les conditions (ι), ($\iota\iota$) et ($\iota\iota\iota$) sont équivalentes pour A.*

Démonstration. — (ι) entraîne ($\iota\iota$). On a vu que $A_{(\mathcal{P})}$ est noethérien et intégralement clos. Tout idéal premier de $A_{(\mathcal{P})}$ provient d'un idéal (lemme 1), nécessairement premier, de A et qui est donc maximal. C'est donc $\mathcal{P}A_{(\mathcal{P})}$. Le fait que $A_{(\mathcal{P})}$ est de valutaion discrète résulte maintenant de la proposition 1.

($\iota\iota$) entraîne ($\iota\iota\iota$). Soit I un idéal fractionnaire de A. Considérons l'idéal II^{-1}. Supposons qu'il soit strictement contenu dans A. Il existe alors un idéal premier $\mathcal{P}$ de A qui le contient. Soit $(a_1, a_2, ..., a_n)$ un système fini de générateurs de I. Soit x un élément de $A_{(\mathcal{P})}$ tel que $IA_{(\mathcal{P})} = xA_{(\mathcal{P})}$. On peut donc écrire les générateurs de I sous la forme $a_i = xu_i/v_i$, avec $u_i \in A$ et $v_i \in A - \mathcal{P}$.

Posons $v = \prod_i v_i$. C'est un élément de $A - \mathcal{P}$. Puisqu'on a $va_i/x \in A$, on a $v/x \in I^{-1}$. Par conséquent on a $v \in II^{-1}A_{(\mathcal{P})} \subset \mathcal{P}A_{(\mathcal{P})}$. Comme $\mathcal{P}A_{(\mathcal{P})} \cap A = \mathcal{P}$, on a $v \in \mathcal{P}$. Contradiction.

($\iota\iota\iota$) entraîne (ι). Vérifions que A est intégralement clos. Soit x un élément A-entier de K. L'anneau $A[x]$ est de type fini sur A et contenu dans K. C'est donc un idéal fractionnaire. On a $A[x]^2 = A[x]$ et donc

$$A[x] = A[x](A[x]A[x]^{-1}) = A[x]A[x]^{-1} = A,$$

puisque $A[x]$ est inversible.

Soit $\mathcal{P}$ un idéal premier de A. Soit $\mathcal{M}$ un idéal maximal qui contient $\mathcal{P}$. L'idéal fractionnaire $\mathcal{M}^{-1}\mathcal{P}$ est contenu dans A. On a donc $(\mathcal{M}^{-1}\mathcal{P})\mathcal{M} = \mathcal{P}$. Puisque $\mathcal{P}$ est un

idéal premier on a $\mathcal{P} = \mathcal{M}$ ou $\mathcal{P}\mathcal{M}^{-1} \subset \mathcal{P}$. Il reste à exclure ce dernier cas. Rappelons qu'on a $A \subset \mathcal{M}^{-1}$ et $A \neq \mathcal{M}^{-1}$. Le cas $\mathcal{P}\mathcal{M}^{-1} \subset \mathcal{P}$ entraîne

$$\mathcal{M}^{-1} \subset \mathcal{P}\mathcal{P}^{-1}\mathcal{M}^{-1} \subset \mathcal{P}\mathcal{P}^{-1} = A,$$

car $\mathcal{P}$ est inversible. Cela est absurde.

Soit A un anneau de Dedekind et $\mathcal{P}$ un idéal maximal de A. Soit I un idéal fractionnaire de K (ou, plus généralement, un sous-ensemble non nul et non vide de K en autorisant la valeur $-\infty$). Posons

$$v_{\mathcal{P}}(I) = \inf_{x \in I} v_p(x) \in \mathbf{Z}.$$

On vérifie que cette quantité est bien définie dans $\mathbf{Z}$.

Soit A un anneau de Dedekind. La multiplication des idéaux fractionnaires de A définit une loi de groupe, puisque tout idéal fractionnaire est inversible dans un anneau de Dedekind. On appelle le groupe ainsi formé par les idéaux fractionnaires *groupe des idéaux* de A. On le notera $\mathcal{I}(A)$.

PROPOSITION 3. — *Le groupe $\mathcal{I}(A)$ est isomorphe au groupe abélien libre engendré par les idéaux premiers non nuls.*

Soit I un idéal fractionnaire de K. Plus précisément on a

$$I = \prod_{\mathcal{P}} \mathcal{P}^{v_{\mathcal{P}}(I)}.$$

Démonstration. — Commençons par un résultat préliminaire.

Lemme 9. — *Soit I un idéal de A. C'est un produit d'idéaux premiers de A.*

Démonstration. — Soit $\mathcal{P}_1$ un idéal maximal de A contenant I. On a $I \subset I\mathcal{P}_1^{-1} \subset A$. Supposons que I ne soit pas produit d'idéaux maximaux. Une construction itérative permet de construire une suite croissante d'idéaux :

$$I \subset I\mathcal{P}_1^{-1} \subset I\mathcal{P}_1^{-1}\mathcal{P}_2^{-1} \subset ... \subset A.$$

Cette suite est finie puisque A est noethérien. Cette contradiction donne la preuve du lemme.

Revenons à la démonstration de la proposition 3.

Pour $\mathcal{P}$ idéal maximal de $\mathbf{Z}$, considérons l'application $i_{\mathcal{P}} : \mathcal{I}(A) \longrightarrow \mathcal{I}(A_{(\mathcal{P})})$ qui à I associe $IA_{(\mathcal{P})}$. C'est un homomorphisme de groupes. Soit $\mathcal{P}'$ un idéal premier de A distinct de $\mathcal{P}$. On a $i_{\mathcal{P}}(\mathcal{P}') = A_{(\mathcal{P})}$. En effet $\mathcal{P}'$ n'est contenu dans l'idéal maximal de $A_{(\mathcal{P})}$; l'idéal de $A_{(\mathcal{P})}$ engendré par $\mathcal{P}'$ est donc égal à $A_{(\mathcal{P})}$.

Démontrons que $\mathcal{I}(A)$ est engendré par les idéaux maximaux de A. Soit I un idéal fractionnaire de A. Soit $t \in A$ tel que $tI \subset A$. D'après le lemme 9, les idéaux tI et tA de A s'expriment comme produits d'idéaux maximaux. Puisque I est inversible, c'est le quotient de ces deux produits.

Démontrons que le sous-groupe de $\mathcal{I}(A)$ engendré par les idéaux premiers est librement engendré. Supposons qu'on ait $\prod_{\mathcal{P}} \mathcal{P}^{r_{\mathcal{P}}} = A$, avec $r_{\mathcal{P}} \in \mathbf{Z}$ et presque toujours nul. Soit $\mathcal{P}_0$ un idéal premier de A tel que $r_{\mathcal{P}_0}$ soit non nul. On a

$$A_{(\mathcal{P}_0)} = i_{\mathcal{P}_0}(A) = i_{\mathcal{P}_0}(\mathcal{P}_0^{r_{\mathcal{P}_0}}) = \mathcal{P}_0^{r_{\mathcal{P}_0}} A_{(\mathcal{P}_0)} \neq A_{(\mathcal{P}_0)}.$$

Soit I un idéal fractionnaire de K. Il s'exprime donc sous la forme

$$I = \prod_{\mathcal{P}} \mathcal{P}^{r_{\mathcal{P}}}.$$

On a

$$i_{\mathcal{P}}(I) = \mathcal{P}^{r_{\mathcal{P}}} A_{(\mathcal{P})} = (\mathcal{P} A_{(\mathcal{P})})^{r_{\mathcal{P}}}.$$

Par conséquent on a

$$r_{\mathcal{P}} = v_{\mathcal{P}}(I A_{(\mathcal{P})}) = v_{\mathcal{P}}(I).$$

Cela achève la démonstration de la proposition 3.

Dans un anneau de Dedekind on n'a pas nécessairement la factorisation unique des éléments de A (car un anneau de Dedekind n'est pas nécessairement factoriel). En revanche la proposition 3 nous assure qu'on a la factorisation unique des idéaux à partir des idéaux premiers.

Les *idéaux fractionnaires principaux* d'un anneau de Dedekind A sont les idéaux de la forme aI avec $a \in K$. Ils forment un sous-groupe de $\mathcal{I}(A)$. Le groupe quotient est le *groupe des classes d'idéaux* de A (ou de K). Ce n'est pas nécessairement un groupe fini. Le groupe des éléments inversibles de A est le *groupe des unités* de A (ou de K).

Corollaire 1. — *Soit A un anneau de Dedekind de corps de fractions K. Soit $x \in K$. On a $v_{\mathcal{P}}(x) = 0$ pour presque tout idéal maximal $\mathcal{P}$ de A.*

Corollaire 2. — *Soit A un anneau de valuation discrète. On a $\mathcal{I}(A) \simeq \mathbf{Z}$.*

Corollaire 3. — *Soit A un anneau de Dedekind. Les applications $i_{\mathcal{P}}$ définissent un isomorphisme de groupes entre $\mathcal{I}(A)$ et la somme directe des groupes $\mathcal{I}(A_{(\mathcal{P})})$, où $\mathcal{P}$ parcourt les idéaux premiers maximaux de A.*

Soient I_1 et I_2 des idéaux fractionnaires d'un anneau de Dedekind A. Soit $\mathcal{P}$ un idéal maximal de A. Indiquons les formules suivantes, qui se déduisent de la proposition 3

$$v_{\mathcal{P}}(I_1 I_2) = v_{\mathcal{P}}(I_1) + v_{\mathcal{P}}(I_2),$$

$$v_{\mathcal{P}}(I_1 + I_2) = \min(v_{\mathcal{P}}(I_1), v_{\mathcal{P}}(I_2)),$$

$$v_{\mathcal{P}}(I_1 \cap I_2) = \max(v_{\mathcal{P}}(I_1), v_{\mathcal{P}}(I_2)),$$

et

$$v_{\mathcal{P}}(I_1 I_2^{-1}) = v_{\mathcal{P}}(I_1) - v_{\mathcal{P}}(I_2).$$

Le résultat suivant est connu sous le nom de *lemme d'approximation* ou *théorème chinois.*

PROPOSITION 4. — *Soit A un anneau de Dedekind de corps de fractions K. Soit I un ensemble fini. Soient $(x_i)_{i\in I}$, $(n_i)_{i\in I}$ et $(\mathcal{P}_i)_{i\in I}$ des familles d'éléments de K, d'entiers et d'idéaux maximaux de A respectivement. Il existe alors $y \in K$ tel que $v_{\mathcal{P}_i}(y - x_i) \geq n_i$ pour tout $i \in I$ et $v_{\mathcal{P}}(y) \geq 0$ pour tout $\mathcal{P} \neq \mathcal{P}_i$, $i \in I$.*
Démonstration. — Dans un premier temps on suppose que les x_i appartiennent à A. On peut supposer, quitte à les remplacer par 0, que les n_i sont ≥ 0.

On peut supposer qu'un seul élément x_{i_0} parmi eux est non nul. En effet, notons y_{i_0} une solution trouvée dans une telle situation. Une solution du problème est donnée par $y = \sum_i y_i$.

On a $A = \mathcal{P}_{i_0}^{n_{i_0}} + \prod_{i\neq i_0} \mathcal{P}_i^{n_i}$. Par conséquent $x_{i_0} = y + z$, avec $y \in \mathcal{P}_{i_0}^{n_{i_0}}$ et $z \in \prod_{i\neq i_0} \mathcal{P}_i^{n_i}$. C'est bien l'élément y cherché.

Ne faisons plus de restriction sur les x_i. On se ramène au cas précédent en posant $x_i = a_i/s$ avec $a_i \in A$ et $s \in A$. On cherche y sous la forme a/s. Il reste à déterminer a par les conditions

$$v_{\mathcal{P}_i}(a - a_i) \geq n_i + v_{\mathcal{P}_i}(s)$$

et

$$v_{\mathcal{P}}(a) \geq v_{\mathcal{P}}(s),$$

pour $\mathcal{P}$ distinct des $\mathcal{P}_i$. Cela revient à un problème du type précédent en agrandissant la famille $\mathcal{P}_i$.

COROLLAIRE 1. — Un anneau de Dedekind qui n'a qu'un nombre fini d'idéaux est principal
Démonstration. — Il suffit de prouver que tout idéal premier $\mathcal{P}_0$ est principal. Appliquons le lemme d'approximation pour prouver qu'il existe $x \in A$ tel que $v_{\mathcal{P}_0}(x) = 1$ et $v_{\mathcal{P}}(x) = 0$ ($\mathcal{P}$ idéal premier de A distinct de $\mathcal{P}_0$). On a alors $\mathcal{P}_0 = xA$.

Exercice 1. — Déduire du lemme d'approximation qu'un anneau de Dedekind qui n'a qu'un nombre fini d'idéaux premiers est principal.

Exercice 2. — Soit A un anneau de Dedekind de corps de fractions K. Démontrer que l'application $K^* \longrightarrow \mathcal{I}(A)$ qui à a associe l'idéal fractionnaire aA est un homomorphisme de groupes qui a pour noyau le groupe des unités de A et pour conoyau le groupe des classes d'idéaux de A.

Cours du 9 septembre 2003

III
Première étude locale des extensions de corps

1. Quelques rappels de théorie de Galois

Soit K un corps. Soit L une extension de corps de K, ce que l'on signifie par $L|K$. On dit que cette extension est *finie* si L est un K-espace vectoriel de dimension finie ; cette dimension est alors le *degré* de l'extension on la note $[L : K]$.

Rappelons quelques notions de théorie de Galois. Un élément de L est dit *séparable sur* K s'il existe un polynôme *séparable*, c'est à dire sans racine multiple, de $K[X]$ dont il est une racine. L'extension $L|K$ est dite *séparable* si tout élément de L est séparable sur K.

Si K est un corps de caractéristique 0 toute extension de K est séparable ; cela résulte du fait que si $P \in K[X]$ possède une racine multiple x d'ordre $n \geq 2$, x est racine de $P' \neq 0$ d'ordre $n-1$. Lorsque L est un corps fini, l'extension est séparable. Cela se voit directement. L'extension $\mathbf{F}_p(T)[X]/(X^p - T)$ de $\mathbf{F}_p(T)$ n'est pas séparable, car le polynôme $X^p - T$ n'admet qu'une seule racine et il est irréductible.

L'extension $L|K$ est dite *normale* si le corps L contient aucune ou toutes les racines de tout polynôme irréductible de $K[X]$. Elle est dite *galoisienne* si elle est normale et séparable. Dans ce dernier cas, le groupe des automorphismes du corps L qui sont l'identité sur le corps K est le *groupe de Galois* de l'extension $L|K$; on le note $\mathrm{Gal}(L/K)$.

Lorsque l'extension $L|K$ est galoisienne, tout élément de L qui est invariant par $\mathrm{Gal}(L/K)$ est dans K. Si de plus l'extension $L|K$ est finie de degré $[L : K]$, le groupe $\mathrm{Gal}(L/K)$ est un groupe fini d'ordre $[L : K]$. L'extension de $\mathbf{Q}$ engendrée par une racine cubique de 2 n'est pas normale et donc pas galoisienne. Rappelons le théorème principal de la théorie de Galois pour les extensions de corps qui sont finies.

Théorème 1. — *Soit $L|K$ une extension finie et galoisienne de corps de groupe de Galois G. L'application qui à un sous-groupe H de G associe l'ensemble M des éléments de L fixés par H définit une bijection entre les sous-groupes de G et les sous-corps de L contenant K. De plus cette bijection induit une bijection entre les sous-groupes distingués de G et les sous corps M de L contenant K tels que l'extension $M|K$ soit normale.*

Supposons que l'extension $L|K$ soit finie. Soit x un élément de L. L'application $L \longrightarrow L$ qui à y associe xy est K-linéaire dont la trace (resp. le déterminant) est par définition la *trace* $\mathrm{Tr}_{L/K}(x)$ (resp. la *norme* $\mathrm{N}_{L/K}(x)$) de x. La trace est une application K linéaire et on a une relation de transitivité $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$ lorsque M est une extension finie de L.

Supposons l'extension $L|K$ est séparable. Soit $M|L$ une extension telle que $M|K$ soit galoisienne (par exemple une clôture algébrique de K contenant L). Il existe une galoisienne minimale $L'|K$ contenant L et contenue dans M qui contienne tous les conjugés de x dans M. On a alors

$$\mathrm{Tr}_{L'/K}(x) = \sum_{\sigma \in \mathrm{Gal}(L'/K)} \sigma(x)$$

et

$$\mathrm{N}_{L'/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L'/K)} \sigma(x).$$

Lorsque $L = K(x)$ la trace $\mathrm{Tr}_{L/K}(x)$ (resp. la norme $\mathrm{N}_{L/K}(x)$) est la somme (resp. le produit) des conjugués de x dans M.

L'extension L/K est séparable si et seulement si la forme K-bilinéaire symétrique $L \times L \longrightarrow K$ qui à (x, y) associe $\mathrm{Tr}_{L/K}(xy)$ est non dégénérée.

2. Extensions d'anneaux de Dedekind

Supposons désormais que L soit une extension de degré fini n de K. On suppose de plus que l'extension $L|K$ est séparable, ce qui nous suffira mais n'est pas indispensable.

Soit A un anneau intègre, noethérien et intégralement clos de corps des fractions égal à K. Notons B la *clôture intégrale* de A dans L (c'est-à-dire l'ensemble des éléments de L qui sont entiers sur A) . C'est un sous-anneau de L et on a $B \cap K = A$ puisque A est intégralement clos.

Proposition 1. — *L'anneau B est intégralement clos.*
Démonstration. — C'est un sous-anneau d'un corps et donc un anneau intègre. Soit $x \in L$ un élément entier sur B. C'est donc la racine d'un polynôme unitaire P de degré k et à coefficients dans B. Les coefficients de ce polynôme sont entiers sur A. Considérons l'application $L(X) \longrightarrow L(X)$ donnée par la multiplication par P. C'est une application $K(X)$-linéaire du $K(X)$-espace vectoriel de dimension finie $L(X)$. Son déterminant $D(X)$ appartient à $B[X] \cap K(X) = A[X]$ car P laisse stable $B[X]$. De plus $D(X)$ est un polynôme unitaire. Rappelons qu'un polynôme réciproque est obtenu en renversant l'ordre des coefficients *i.e.* le polynôme réciproque de P est $Q(X) = X^k P(1/X)$. Un polynôme est unitaire si et seulement si le polynôme réciproque prend la valeur 1 en 0. Le déterminant de la multiplication par Q dans $L(X)$ est le polynôme $E(X)$ réciproque de D par changement de variable et multilinéarité du déterminant. Par spécialisation on a $E(0) = 1$ lorsque $Q(0) = 1$ (le déterminant de l'identité vaut 1). Cela prouve que D est unitaire. On a $D(x) = 0$, par spécialisation (la déterminant de l'endomorphisme nul est nul). Par conséquent x est entier sur A.

Proposition 2. — *Le corps des fractions de B est égal à L.*
Démonstration. — Soit $x \in L$. C'est une racine d'un polynôme $a_n X^n + ... + a_1 X + a_0 \in A[X]$. En multipliant ce polynôme par a_n^{n-1}, il apparaît que $a_n x$ est entier sur A. Donc x est quotient de deux éléments de B.

Proposition 3. — *Tout sous-A-module d'un A-module de type fini est de type fini.*
Démonstration. — Cela résulte du fait que A et donc A^k sont noethérien. Si bien que tout A-module de type fini est noethérien. D'où le résultat.

Remarque . — Dans la démonstration de la proposition 3, on a seulement utilisé que A est noethérien. Un A-module dont tous les sous-modules sont de type fini est dit *noethérien* (un anneau noethérien est un module noethérien sur lui-même).

Proposition 4. — *L'anneau B est un A-module de type fini lorsque l'extension $L|K$ est séparable. Il en résulte que B est noéthérien comme A-module, et donc comme anneau.*
Démonstration. — On va démontrer que B est contenu dans un A-module de type fini ; cela suffit d'après la proposition 3.

Soit M un sous A-module de L. Notons M^* le sous-ensemble de A formé des éléments x qui vérifient $\mathrm{Tr}_{L/K}(xy) \in A$ pour tout $y \in M$. C'est un A-module qu'on appelle la *codifférente* de B sur A. La codifférente d'un module libre est libre et donc de type fini. En effet l'existence de la forme bilinéaire non dégénérée $(x, y) \longrightarrow \mathrm{Tr}_{L/K}(xy)$ (due à la séparabilité), permet de considérer la base duale.

Soit X une famille d'éléments de B qui est une base de L comme K-espace vectoriel. Notons V le A-module libre engendré par cette base.

Observons que l'image de B par l'application $\mathrm{Tr}_{L/K}$ est contenue dans A puisque les conjugés d'un élément entier sur A sont entiers sur A. On a donc

$$V \subset B \subset B^* \subset V^*.$$

Cela permet de conclure puisque V^* est de type fini.

Théorème 1. — *Si A est un anneau de Dedekind, B est un anneau de Dedekind.*
Démonstration. — Compte-tenu des propositions 1, 3 et 4, il suffit de prouver que le localisé de B en tout idéal premier et non nul est un anneau de valuation discrète. Pour cela il suffit de prouver que tout idéal premier et non nul de ce localisé est maximal (caractérisation des anneaux de valuation discrète) ou encore de prouver que tout idéal premier non nul de B est maximal.

Soit $\mathcal{P}$ un idéal premier de B non maximal. Il est contenu dans un idéal maximal $\mathcal{M}$ de B. Les ensembles $\mathcal{P} \cap A$ et $\mathcal{M} \cap A$ sont des idéaux premiers non nuls de A. Puisque tout idéal premier non nul de A est maximal, ces ensembles sont égaux. Cela contredit le lemme suivant.

Lemme 2. — *Soient A et B deux anneaux tels que $A \subset B$ et B entier sur A. Soient $\mathcal{P}$ et $\mathcal{Q}$ deux idéaux premiers de B tels que $\mathcal{P} \subset \mathcal{Q}$. Supposons qu'on ait $\mathcal{P} \cap A = \mathcal{Q} \cap A$. Alors on a $\mathcal{P} = \mathcal{Q}$.*
Démonstration. — Supposons que l'inclusion $\mathcal{P} \subset \mathcal{Q}$ soit stricte. Il existe $x \in \mathcal{Q} - \mathcal{P}$. Soit $P(X) = X^n + ... + a_1X + a_0$ un polynôme unitaire à coefficient dans A de degré minimal qui vérifie $P(x) \in \mathcal{P}$. Un tel polynôme existe puisque x est entier. Il est de degré > 1. Comme $\mathcal{P}$ est premier on a $a_0 \in \mathcal{Q} \cap A = \mathcal{P} \cap A$. Cela entraîne qu'on a $(P(x) - a_0)/x \in \mathcal{P}$ puisque $\mathcal{P}$ est premier. C'est absurde puisque P est de degré minimal. On a donc une contradiction. Cela prouve le lemme et donc le théorème.

Rappelons que l'*anneau des entiers* d'un corps de nombres L est la clôture intégrale de $\mathbf{Z}$ dans L.

COROLLAIRE 1. — *L'anneau des entiers d'un corps de nombres est un anneau de Dedekind.*
Démonstration. — Cela résulte de l'application de la proposition à $A = \mathbf{Z}$.

3. Etude locale

Supposons désormais que A soit un anneau de Dedekind. Soit $\mathcal{P}$ un idéal premier non nul de B. Posons $\mathcal{Q} = \mathcal{P} \cap A$. Dans cette situation on dit que $\mathcal{P}$ *divise* $\mathcal{Q}$ et on note $\mathcal{P}|\mathcal{Q}$. Posons

$$e_{\mathcal{P}} = v_{\mathcal{P}}(\mathcal{Q}B).$$

C'est l'*indice de ramification* de $\mathcal{P}$ dans l'extension $L|K$. On a, dans $\mathcal{I}(B)$,

$$\mathcal{Q}B = \prod_{\mathcal{P}|\mathcal{Q}} \mathcal{P}^{e_{\mathcal{P}}}.$$

Puisqu'on a $\mathcal{Q} \subset \mathcal{P}$, le corps $B/\mathcal{P}$ est une extension de $A/\mathcal{Q}$. Le degré $f_{\mathcal{P}}$ de cette extension est le *degré résiduel* de $\mathcal{P}$ dans l'extension $L|K$. Si $\mathcal{P}$ est le seul idéal premier qui divise $\mathcal{Q}$, et si le degré résiduel est égal à 1, on dit que l'extension $L|K$ est *totalement ramifiée* en $\mathcal{P}$.

Lorsque l'extension $(B/\mathcal{P})|(A/\mathcal{Q})$ est séparable, et que l'indice de ramification est égal à 1 on dit que l'extension $L|K$ est *non ramifiée* en $\mathcal{P}$.

PROPOSITION 5. — *Soit $\mathcal{Q}$ un idéal maximal de A. On a*

$$[L : K] = [B/\mathcal{Q}B : A/\mathcal{Q}] = \sum_{\mathcal{P}|\mathcal{Q}} e_{\mathcal{P}} f_{\mathcal{P}}.$$

Démonstration. — Pour démontrer la seconde égalité, considérons la suite d'idéaux de B :

$$B\mathcal{Q} = \prod_{\mathcal{P}|\mathcal{Q}} \mathcal{P}^{e_{\mathcal{P}}} \subset ... \subset \mathcal{P}_1^{e_{\mathcal{P}_1}} \mathcal{P}_2^{e_{\mathcal{P}_2}} \subset ... \subset \mathcal{P}_1^{e_{\mathcal{P}_1}} \mathcal{P}_2 \subset \mathcal{P}_1^{e_{\mathcal{P}_1}} \subset ... \subset \mathcal{P}_1^2 \subset \mathcal{P}_1 \subset B.$$

Il n'y a pas d'idéal strictement compris entre deux termes successifs, puisque deux tels termes diffèrent par multiplication par un idéal maximal. Les quotients successifs sont des espaces vectoriels de dimension 1 sur $B/\mathcal{P}_i$, et donc de dimension $f_{\mathcal{P}_i}$ sur $A/\mathcal{P}$. Un simple comptage donne la deuxième égalité.

Démontrons maintenant la première égalité. Lorsque A est principal, elle résulte du fait qu'une base du A-module B donne une base de $B/\mathcal{P}$ comme $A/\mathcal{Q}$-module, puisque qu'un A-module de type fini et sans torsion est libre sur un anneau principal.

Nous allons nous ramener au cas principal. Considérons l'anneau de valuation discrète (donc principal) $A_{(\mathcal{Q})} = A_0$. Sa clôture intégrale dans L est égale à $A_{(\mathcal{Q})}B = B_0$. On a donc

$$n = [B_0/\mathcal{Q}B_0 : A_0/\mathcal{Q}A_0].$$

La décomposition de l'idéal $\mathcal{Q}B_0$ donne

$$\mathcal{Q}B_0 = \prod_i (B_0\mathcal{P}_i)^{e_{\mathcal{P}_i}}.$$

Les $B_0\mathcal{P}_i$ sont des idéaux premiers non nuls de B_0. D'après l'égalité déjà démontrée on a

$$[B_0/\mathcal{Q}B_0 : A_0/\mathcal{Q}] = \sum_i e_{\mathcal{P}_i}[B_0/B_0\mathcal{P}_i : A_0/\mathcal{Q}].$$

Puisqu'on a $A_0/\mathcal{Q}A_0 \simeq A/\mathcal{Q}A$ et $B_0/\mathcal{P}_iB_0 \simeq B/\mathcal{P}_i$, on obtient

$$n = \sum_i e_i f_i.$$

Cela achève la démonstration.

Corollaire 1. — *L'anneau $B/\mathcal{Q}$ est isomorphe à $\prod_{\mathcal{P}} B/\mathcal{P}^{e_{\mathcal{P}}}$.*
Démonstration. — On a un homomorphisme d'anneau $B/\mathcal{Q}B \longrightarrow \prod_{\mathcal{P}} B/\mathcal{P}^{e_{\mathcal{P}}}$ déduit de l'application diagonale

$$B \longrightarrow \prod_{\mathcal{P}} B.$$

Démontrons qu'il s'agit de l'isomorphisme cherché. L'injectivité résulte de l'égalité $\mathcal{Q} = \cap_{\mathcal{P}}\mathcal{P}^{e_{\mathcal{P}}}$. La surjectivité se voit directement en utilisant le lemme d'approximation.

4. Les sous-groupes de décomposition et d'inertie

Reprenons la situation de la section précédente en supposant que l'extension $L|K$ est galoisienne.

Proposition 6. — *Soit $\mathcal{Q}$ un idéal maximal de A. Le groupe* $\mathrm{Gal}(L/K)$ *opère transitivement sur les idéaux premiers de B qui divise $\mathcal{Q}$.*
Démonstration. — Soit $\mathcal{P}$ un idéal de B qui divise $\mathcal{Q}$. L'image par un élément de $\mathrm{Gal}(L/K)$ de $\mathcal{P}$ est un sous B-module de L. Il est contenu dans B puisque le conjugué d'un élément entier est entier. C'est donc un idéal et il est premier. De plus il divise $\mathcal{Q}$.

Vérifions la transitivité de l'action de $\mathrm{Gal}(L/K)$. Soit x un élément non nul de $\mathcal{P}$. Soit $\mathcal{P}'$ un idéal premier de B divisant $\mathcal{Q}$. D'après le lemme d'approximation, on peut choisir x en dehors de tout ensemble fini d'idéaux premiers de B distincts de $\mathcal{P}$, en particulier en dehors des conjugués de $\mathcal{P}'$ distincts de $\mathcal{P}$. On a

$$\mathrm{N}_{L/K}(x) = \prod_{\sigma\in\mathrm{Gal}(L/K)} \sigma(x).$$

C'est un élément de A qui est dans $\mathcal{P}$ et donc dans $\mathcal{Q}$. Comme on a $\mathcal{Q} = \mathcal{P}\cap A = \mathcal{P}'\cap A$, $\mathrm{N}_{L/K}(x)$ est dans $\mathcal{P}'$. Comme $\mathcal{P}'$ est un idéal premier, il existe $\sigma \in \mathrm{Gal}(L/K)$ tel que $x \in \sigma(\mathcal{P}')$. L'un des conjugés de $\mathcal{P}'$ est donc égal à $\mathcal{P}$.

Corollaire 1. — *Soit $\mathcal{Q}$ un idéal premier non nul de A. Les nombres entiers $e_\mathcal{P}$ et $f_\mathcal{P}$ ne dépendent que $\mathcal{Q}$. On peut donc les noter $e_\mathcal{Q}$ et $f_\mathcal{Q}$. Notons $g_\mathcal{Q}$ le nombre d'idéaux premiers de A qui divisent $\mathcal{Q}$. On a*

$$[L : K] = g_\mathcal{Q} e_\mathcal{Q} f_\mathcal{Q}.$$

Démonstration. — Utilisation de la conjugaison qui transporte toutes les structures.

Le *sous-groupe de décomposition* $D_\mathcal{P}$ en $\mathcal{P}$ de $\mathrm{Gal}(L/K)$ est le sous-groupe des éléments σ qui vérifient $\sigma(\mathcal{P}) = \mathcal{P}$. C'est un sous-groupe d'indice $g_\mathcal{Q}$. Il ne dépend à conjugaison près que de $\mathcal{Q}$.

Le *sous-groupe d'inertie* $I_\mathcal{P}$ en $\mathcal{P}$ de $\mathrm{Gal}(L/K)$ est le sous-groupe des éléments σ qui vérifient $(\sigma(x) - x) \in \mathcal{P}$ pour tout $x \in B$. C'est un sous-groupe de $D_\mathcal{P}$.

5. Rappels sur les corps finis

Soit p un nombre premier. Rappelons que tout corps fini de caractéristique p possède un nombre d'élément égal à une puissance de p, puisque c'est un espace vectoriel sur le corps à p éléments.

Soit n un entier ≥ 1. Il existe un et un seul, à isomorphisme près, corps fini ayant $q = p^n$ éléments. Voici comment on le construit. Soit K un corps algébriquement clos de caractéristique p. L'application $K \longrightarrow K$ qui à x associe x^q est un automorphisme de K (elle préserve évidemment la multiplication ; le fait qu'elle préserve l'addition résulte de la formule du binôme). Les éléments invariants par cette application forment un sous-corps de K. Comme le polynôme $X^q - X$ possèdent q racines distinctes dans K (sa dérivée ne s'annule jamais), ce sous-corps possède q éléments. Inversement si k est un sous-corps de K ayant q éléments, k^* est un groupe d'ordre $q - 1$. Tout élément x de k^* vérifie donc $x^{q-1} = 1$. Tout élément de k est racine de $X^q - X$.

Le corps à q éléments est noté $\mathbf{F}_q$.

Soit m un nombre entier. Le corps $\mathbf{F}_{p^m}$ est isomorphe à un sous-corps de $\mathbf{F}_{p^n}$ si et seulement si $m|n$. En effet $\mathbf{F}_{p^m}$ est isomorphe au sous-corps de $\mathbf{F}_{p^n}$ formé par les racines du polynôme $X^{p^m} - X$.

Cela prouve que l'extension de corps $\mathbf{F}_{p^n}|\mathbf{F}_{p^m}$ est normale. Cette extension est séparable car les racines de l'unité sont séparables. Le groupe $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_{p^m})$ est cyclique et engendré par l'automorphisme de $\mathbf{F}_{p^n}$ qui à x associe x^{p^m}.

6. La substitution de Frobenius

Reprenons la situation de la section 3 en supposant désormais que K est un *corps de nombres*, c'est-à-dire une extension finie de $\mathbf{Q}$.

Dans ce cas, tout corps résiduel de A est un corps fini. Le corps fini $B/\mathcal{P}$ est une extension de $A/\mathcal{Q}$.

Proposition 7. — *L'application*

$$D_{\mathcal{P}} \longrightarrow \mathrm{Gal}((B/\mathcal{P})/(A/\mathcal{Q}))$$

est un homomorphisme surjectif de groupes. Son noyau est égal à $I_{\mathcal{P}}$.
Démonstration. — Seule la surjectivité n'est pas évidente. Pour l'établir, il suffit de prouver que $D_{\mathcal{P}}$ agit transitivement sur les éléments primitifs, puisque $\mathrm{Gal}((B/\mathcal{P})/(A/\mathcal{Q}))$ est un groupe cyclique.

Soit α un élément primitif de l'extension de corps finis $(B/\mathcal{P})/(A/\mathcal{Q})$. D'après le lemme d'approximation, on peut choisir un représentant a de α dans B tel que $a \in \sigma(\mathcal{P})$ pour tout $\sigma \notin D_{\mathcal{P}}$. Considérons le polynôme $\prod_\sigma(X - \sigma(a)) \in A[X]$, où σ parcourt $\mathrm{Gal}(L/K)$. Sa réduction modulo $\mathcal{Q}$ est le produit d'une puissance de X et d'un polynôme de $(A/\mathcal{Q})[X]$ qui annule α. Un tel polynôme annule tous les conjugués de α. Tout conjugué de α est donc de la forme $\sigma(a) + \mathcal{P}$ avec $\sigma \in D_{\mathcal{P}}$.

Proposition 8. — *Le cardinal du groupe d'inertie* $I_{\mathcal{P}}$ *est égal à* $e_{\mathcal{P}}$.
Démonstration. — Cela revient à prouver que le cardinal du groupe de décomposition est égal à $e_{\mathcal{P}} f_{\mathcal{P}}$, puisqu'on vient de voir que le quotient $D_{\mathcal{P}}/I_{\mathcal{P}}$ s'identifie au groupe de Galois de l'extension résiduelle qui a pour ordre $f_{\mathcal{P}}$. Le nombre de conjugué $g_{\mathcal{P}}$ de $\mathcal{P}$ par $\mathrm{Gal}(L/K)$ est égal à l'ordre du groupe $\mathrm{Gal}(L/K)/D_{\mathcal{P}}$. Comme l'ordre de $\mathrm{Gal}(L/K)$ est égal à $g_{\mathcal{P}} e_{\mathcal{P}} f_{\mathcal{P}}$ on obtient le résultat cherché.

Tout cela est résumé en disant que les indices successifs correspondant aux inclusions de groupes

$$1 \subset I_{\mathcal{P}} \subset D_{\mathcal{P}} \subset \mathrm{Gal}(L/K)$$

sont égaux à $e_{\mathcal{P}}$, $f_{\mathcal{P}}$ et $g_{\mathcal{P}}$ respectivement.

Corollaire 1. — *L'extension* $L|K$ *est non ramifiée en* $\mathcal{P}$ *si et seulement si le sous-groupe d'inertie en* $\mathcal{P}$ *est trivial.*

Supposons que l'extension $L|K$ soit non ramifiée en $\mathcal{P}$. La *substitution de Frobenius* $\phi_{\mathcal{P}}$ de $D_{\mathcal{P}}$ est l'élément d'ordre $f\mathcal{P}$ de $D_{\mathcal{P}}$ correspondant à l'automorphisme $x \mapsto x^q$ du corps fini $B/\mathcal{P} \simeq \mathbf{F}_q$. Il est caractérisé par la propriété :

$$\phi_{\mathcal{P}}(x) \equiv x^q \pmod{\mathcal{P}},$$

pour tout $x \in B$. On le note encore $(\mathcal{P}, L/K)$. Soit $\sigma \in \mathrm{Gal}(L/K)$. On a

$$(\sigma(\mathcal{P}), L/K) = \sigma(\mathcal{P}, L/K)\sigma^{-1}.$$

On dira qu'une extension de corps L/K est *abélienne* si elle est galoisienne et que le groupe $\mathrm{Gal}(L/K)$ est abélien. Toute extension de corps finis est abélienne.

Reprenons la situation étudiée au cours de cette section. Lorsque $\mathrm{Gal}(L/K)$ est un groupe abélien, la substitution de Frobenius en $\mathcal{P}$ ne dépend que de $\mathcal{Q}$. C'est le *symbole d'Artin* noté $(\mathcal{Q}, L/K)$. Cette définition se généralise à tout idéal fractionnaire

I de K qui est à support en dehors des idéaux premiers ramifiés de l'extension L/K par multiplicativité, *i.e.* on pose

$$(\prod_{\mathcal{P}} \mathcal{P}^{n_{\mathcal{P}}}, L/K) = \prod_{\mathcal{P}} (\mathcal{P}, L/K)^{n_{\mathcal{P}}}.$$

IV
Discriminants

1. Définition

Soient A et B des anneaux de Dedekind avec A sous-anneau de B. Supposons que B soit un A-module libre de rang n.

Soit $v = (x_1, ..., x_n) \in B^n$. On appelle *discriminant* du système $(x_1, ..., x_n)$ l'élément de A donné par la formule :

$$D(v) = D(x_1, ..., x_n) = \det(\mathrm{Tr}_{B/A}(x_i x_j)),$$

où, par abus de notation, $\mathrm{Tr}_{B/A}(x_i x_j)$ est la matrice de $M_n(A)$ qui a pour coefficient (i, j) l'élément $\mathrm{Tr}_{B/A}(x_i x_j)$ de A.

Proposition 1. — *Soit $M \in \mathrm{M}_n(A)$. On a*

$$D(vM) = \det(M)^2 D(v).$$

Démonstration. — Posons $w = (y_1, ...y_n) = vM$. En prenant le déterminant, et en posant la proposition résulte de l'égalité :

$$\mathrm{Tr}_{B/A}(y_i y_j) = {}^{\mathrm{t}}M \mathrm{Tr}_{B/A}(x_i x_j) M.$$

Corollaire 1. — *Le discriminant de n'importe quelle base de B sur A ne dépend pas de la base à multiplication par un élément inversible de A près. En particulier l'idéal principal engendré par un tel discriminant ne dépend que de A et B.*

On appelle cet idéal principal *discriminant* de B sur A. On le note $\mathcal{D}_{B/A}$.

Ne supposons plus que B est libre sur A. Notons K et L les corps de fractions de A et B. Appelons discriminant de B sur A et notons $\mathcal{D}_{B/A}$ l'idéal engendré par les discriminants des systèmes formés par les bases de L sur K qui sont dans B. Cette définition est compatible à la précédente lorsque B est libre sur A. La proposition suivante permet de déterminer localement le discriminant.

Proposition 2. — *Soit $\mathcal{Q}$ un idéal premier de A. On a*

$$\mathcal{D}_{B/A} A_{(\mathcal{Q})} = \mathcal{D}_{B_{(\mathcal{Q})}/A_{(\mathcal{Q})}}.$$

Démonstration. — Une base de L sur K qui est contenue dans B est contenue dans $B_{(\mathcal{Q})}$. On a donc une inclusion

$$\mathcal{D}_{B/A}A_{(\mathcal{Q})} \subset \mathcal{D}_{B_{(\mathcal{Q})}/A_{(\mathcal{Q})}}.$$

Démontrons l'inclusion inverse. Soit $(x_1, ..., x_n)$ une base de $B_{(\mathcal{Q})}$ comme $A_{(\mathcal{Q})}$-module (il en existe puisque $A_{(\mathcal{Q})}$ est principal et donc $B_{(\mathcal{Q})}$ est libre sur $A_{(\mathcal{Q})}$). Il existe $s \in A - \mathcal{Q}$ tel que $(sx_1, ..., sx_n) \in B^n$. Le n-uplet $(sx_1, ..., sx_n)$ est une base de L sur K qui est contenue dans B. On a

$$D(sx_1, ..., sx_n) = s^{2n}D(x_1, ..., x_n).$$

On a donc, puisque s est inversible dans $A_{(\mathcal{Q})}$,

$$\mathcal{D}_{B_{(\mathcal{Q})}/A_{(\mathcal{Q})}} \subset s^{-2n}\mathcal{D}_{B/A}A_{(\mathcal{Q})} = \mathcal{D}_{B/A}A_{(\mathcal{Q})}.$$

Corollaire 1. — *On a*

$$\mathcal{D}_{B/A} = \prod_{\mathcal{Q}} \mathcal{D}_{B_{(\mathcal{Q})}/A_{(\mathcal{Q})}},$$

où $\mathcal{Q}$ parcourt les idéaux premiers et non nuls de A.

Supposons désormais que l'extension $L|K$ soit séparable.

Proposition 3. — *L'idéal $\mathcal{D}_{B/A}$ est non nul. Plus précisément le discriminant de toute base de L sur K est non nul.*
Démonstration. — On utilise d'abord le lemme suivant.

Lemme 1. — *Soit $(x_1, ..., x_n) \in B^n$. Soit $\bar{K}$ un corps algébriquement clos qui contient K. Notons σ_1, ..., σ_n les n plongements distincts de L dans $\bar{K}$ qui sont l'identité sur K. On a*

$$D(x_1, ..., x_n) = \det(\sigma_j(x_i))^2.$$

Démonstration. — Cela résulte de la formule (en utilisant la séparabilité de l'extension $L|K$) :

$$D(x_1, ..., x_n) = \det(\mathrm{Tr}_{L/K}(x_i x_j)) = \det(\sum_k (\sigma_k(x_i)\sigma_k(x_j)))$$

$$= \det((\sigma_k(x_i))\det((\sigma_k(x_j)) = \det(\sigma_j(x_i))^2.$$

Cela achève de prouver le lemme.

Revenons à la démonstration de la proposition. Soit $(x_1, ..., x_n)$ une base de B sur A. On veut démontrer qu'on a

$$\det(\sigma_j(x_i)) \neq 0.$$

Supposons le contraire. Il existe une combinaison linéaire non triviale des σ_j qui annule tous les x_i et par conséquent tous les éléments de L puisque les x_i forment une base. Ecrivons cette combinaison linéaire à coefficients dans L sous la forme

$$\sum_{i=1}^{q} \alpha_i \sigma_i = 0,$$

avec $2 \leq q \leq n$. On peut supposer que les α_i sont tous non nuls et q est minimal. Soient x et y deux éléments de L^*. On a

$$\sum_{i=1}^{q} \alpha_i \sigma_i(x)\sigma_i(y) = \sum_{i=1}^{q} \alpha_i \sigma_i(xy) = 0.$$

En soustrayant à cette dernière identité l'égalité $\sigma_q(y) \sum_{i=1}^{q} \alpha_i \sigma_i(x) = 0$ on obtient :

$$\sum_{i=1}^{q-1} \alpha_i \sigma_i(x)(\sigma_i(y) - \sigma_q(y)) = 0.$$

Comme cela est vérifié pour tout $x \in L$, on a obtenu une nouvelle combinaison linéaire des σ_i à coefficients dans L. Elle doit être triviale puisqu'on a choisi $q \geq 2$ minimal ou on a $q = 2$. Dans chaque cas on en déduit que $\sigma_1(y) = \sigma_2(y)$ pour tout $y \in L$. Cela entraîne $\sigma_1 = \sigma_2$, ce qui est absurde puisque les σ_i sont distincts.

Cela permet de démontrer une conséquence de la séparabilité à laquelle nous avons déjà fait référence.

COROLLAIRE 1. — *Lorsque qu'une extension de corps $L|K$ est séparable, la forme bilinéaire $L \times L \longrightarrow K$ donnée par $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$est non dégénérée.*

2. Lien avec la ramification

Soient A un anneau de Dedekind de corps des fractions K. Soit $L|K$ une extension séparable finie. Notons B l'anneau des entiers de L. On pose $\mathcal{D}_{L/K} = \mathcal{D}_{B/A}$. Ce discriminant est bien défini puisque A et B sont déterminé par le fait que ce sont les anneaux des entiers de K et L.

On dit qu'un idéal premier $\mathcal{Q}$ de A *se ramifie* dans B s'il existe un idéal premier de B au dessus de $\mathcal{Q}$ qui n'est pas non ramifié.

Lorsque L est un corps de nombres, on peut considérer le cas $A = \mathbf{Z}$. Le discriminant $\mathcal{D}_L = \mathcal{D}_{L/\mathbf{Q}}$ est le *discriminant absolu* de L. Puisque c'est un idéal de $\mathbf{Z}$, on est souvent amené a considérer l'entier > 0 qui l'engendre. On note souvent cet entier $|\mathcal{D}_L|$.

Revenons-en à une situation plus générale. Le théorème suivant fait le lien entre la ramification et la notion de discriminant.

THÉORÈME 1. — *Soit A un anneau de Dedekind de corps de fractions K. Soit L/K une extension finie et séparable. Notons B la clôture intégrale de A dans L. Les idéaux premiers de A qui se ramifient dans B coïncident avec les idéaux premiers de A qui divisent $\mathcal{D}_{B/A}$. En particulier il n'y a qu'un nombre fini d'idéaux premiers de A qui sont ramifiés dans B.*

Démonstration. — Cela se vérifie localement puisque le discriminant et la ramification peuvent se déterminer en localisant les anneaux d'après la proposition 2 et le théorème de décomposition en produit d'idéaux premiers dans les anneaux de Dedekind.

Supposons donc que A soit un anneau de valuation discrète. Notons $\mathcal{Q}$ son idéal maximal. L'anneau A est principal. Cela entraîne que B est libre sur A.

Supposons qu'il existe un idéal maximal $\mathcal{P}$ de B qui soit ramifié. Il existe $x \in B - \mathcal{Q}B$ et $n > 1$ tel que $x^n \in \mathcal{Q}B$. La classe $\bar{x}$ de x dans $B/\mathcal{Q}$ est un élément non nul de $B/\mathcal{Q}$. Ce dernier est un $A/\mathcal{Q}$-espace vectoriel. On peut compléter $\bar{x}$ en une base $(\bar{x}_1 = \bar{x}, \bar{x}_2, ..., \bar{x}_n)$de $B/\mathcal{Q}$. Un représentant $(x_1 = x, x_2, ..., x_n)$ de cette base dans B^n donne une base de B comme A-module (cela se voit en identifiant B à A^n et en remarquant que la réduction modulo $\mathcal{Q}$ de $\det(x_1, ..., x_n)$ dans la base canonique de A^n est non nulle ; ce déterminant est donc inversible).

Soit $x_0 \in B$. Puisque B est un A-module libre, la trace de l'endomorphisme de $B/\mathcal{Q}$ donné par $y \mapsto x_0 y$ est l'image dans $A/\mathcal{Q}$ de la trace de l'endomorphisme de B donné par $y \mapsto x_0 y$. On a $(x_1 x_i)^n \in \mathcal{Q}$ pour tout i. L'endomorphisme de $B/\mathcal{Q}$ donné par $y \mapsto y(\bar{x}_1 x_i)$ est donc nilpotent. Sa trace est donc nulle. Le déterminant $\det(\mathrm{Tr}(x_i x_j))$ est donc dans $\mathcal{Q}$. On a donc $\mathcal{D}_{B/A} \subset \mathcal{Q}$.

Réciproquement, supposons que tout idéal premier de B divisant $\mathcal{Q}$ soit non ramifié. On a alors un isomorphisme de A-modules

$$B/\mathcal{Q} \simeq B/\mathcal{P}_1 \oplus ... \oplus B/\mathcal{P}_n,$$

où $\mathcal{P}_1$,..., $\mathcal{P}_n$ sont les idéaux premiers de B qui divisent $\mathcal{Q}$. Soient β_1, β_2,...β_n des bases des $A/\mathcal{Q}$ espaces vectoriels $B/\mathcal{P}_1$,...,$B/\mathcal{P}_n$. Elles définissent, par l'isomorphisme ci-dessus, une base β de $B/\mathcal{Q}$. Dans cette base la matrice de l'endomorphisme $B/\mathcal{Q} \longrightarrow B/\mathcal{Q}$ qui à y associe $x_0 y$ est une matrice par blocs ($x_0 \in B$). Le discriminant du système formé par la base β est donc le produit des discriminants $\mathcal{D}_i$ des systèmes formés par les β_i. Chacun de ces discriminants est non nul (cela résulte de la proposition 3, puisque les extensions de corps résiduels sont séparables). Leur produit est donc non nul.

La base β est la réduction modulo $\mathcal{Q}$ d'une base de B sur A (voir ci-dessus). La réduction modulo $\mathcal{Q}$ du discriminant du système formé par cette base est donc égal au discriminant du système formé par la base β ; Ce dernier discriminant est non nul. Le discriminant de B/A n'est donc pas contenu dans $\mathcal{Q}$. Cela achève la démonstration du théorème.

Remarque . — Pour démontrer qu'un idéal premier $\mathcal{Q}$ de A est non ramifié dans une extension $L|K$ il suffit donc de trouver un système d'éléments de B de discriminant premier à $\mathcal{Q}$. On va voir ci-dessous une méthode qui permet parfois de trouver de tels systèmes lorsque que l'extension est donnée par un polynôme explicite.

3. Exemple de calcul de discriminant

Soit K un corps et $L = K(x)$ $(x \in L)$ une extension séparable de K de degré n. Soit P le polynôme minimal de x.

PROPOSITION 4. — *Le discriminant du système* $(1, x, x^2, ..., x^{n-1})$ *est donné par la formule :*

$$D(1, x, ..., x^{n-1}) = (-1)^{n(n-1)/2} N_{L/K}(P'(x)).$$

Démonstration. — Notons x_1, x_2,..., x_n les conjugués de x. Utilisons le lemme 1. On a

$$D(1, x, ..., x^{n-1}) = (\det(x_i^j))^2,$$

où i parcourt les entiers entre 1 et n et j parcourt les entiers entre 0 et $n-1$. Ce déterminant est un déterminant de Van der Monde. Il est égal à

$$(-1)^{n(n-1)/2} \prod_{i_1 \neq i_2} (x_{i_1} - x_{i_2}).$$

En dérivant l'identité

$$P(X) = \prod_i (X - x_i),$$

on obtient la formule

$$P'(x_i) = \prod_{i' \neq i} (x_i - x_{i'}).$$

Or on a

$$N_{L/K}(P'(x_i)) = \prod_{i'} (P'(x_{i'})) = \prod_{i_1 \neq i_2} (x_{i_1} - x_{i_2}).$$

Cela nous donne la formule cherchée.

COROLLAIRE 1. — *Lorsque x est un élément de B (i.e. c'est un élément entier de L), le discriminant $\mathcal{D}_{L/K}$ contient l'idéal principal de A engendré par $N_{L/K}(P'(x))$.*
Démonstration. — Cela résulte immédiatement du fait que B contient $A[x]$ et donc le système $(1, x, x^2, ..., x^{n=1}) \in B^n$ est une base de L comme K-espace vectoriel.

4. Compléments

Reprenons la situation suivante. Soit K un corps et $L = K(x)$ $(x \in L)$ une extension séparable de K de degré n. Soit P le polynôme minimal de x. Supposons que x soit entier sur A. Notons A et B les anneaux des entiers de K et L. Supposons que ce soient des anneaux de Dedekind.

Proposition 5. — *On a*

$$D(1, x, ..., x^{n-1})B \subset A[x] \subset B.$$

Démonstration. — La deuxième inclusion est évidente. Démontrons la première.

Lemme 2. — *Soit $\mathcal{Q}$ un idéal maximal de A. On a*

$$D(1, x, ..., x^{n-1})B_{(\mathcal{Q})} \subset A_{(\mathcal{Q})}[x].$$

Démonstration. — Le $A_{(\mathcal{Q})}$-module $B_{(\mathcal{Q})}$ est libre car $A_{(\mathcal{Q})}$ est principal. Considérons-en une base $(x_1, ..., x_n)$. Ecrivons la matrice M de passage de cette base à la base de L comme K-espace vectoriel donnée par $(1, ..., x^{n-1})$. Notons $a_{i,j}$ les coefficients de M. Ce sont des éléments de A. Le déterminant d de cette matrice est non nul. Notons $b_{j,i}$ les coefficients de M^{-1}. Ce sont des éléments de $\frac{1}{d}A$. On a donc $dB_{(\mathcal{Q})} \subset A_{(\mathcal{Q})}[x]$. On en déduit

$$D(1, x, ..., x^{n-1})B_{(\mathcal{Q})} = d^2 D(x_1, ..., x_n)B_{(\mathcal{Q})} = (dB_{(\mathcal{Q})})(dD(x_1, ..., x_n)) \subset A_{(\mathcal{Q})}[x].$$

Cela prouve le lemme.

Pour déduire la proposition du lemme 2, utilisons la formule

$$M = \cap_{\mathcal{Q}} A_{(\mathcal{Q})}M,$$

qui est valide pour tout A-sous-module M contenu dans un K-espace vectoriel de dimension finie. Par application à $M = A[x]$ on obtient la proposition.

Proposition 6. — *Soient L_1 et L_2 des extensions finies et séparables de K qui sont contenues dans un corps M et qui sont linéairement disjointes (i.e. le sous-corps $L = L_1L_2$ de M engendré par L_1 et L_2 est de degré $[L_1 : K][L_2 : K]$ sur K). Notons B_1, B_2 et B les clôtures intégrales de A dans L_1, L_2 et L. On a*

$$\mathcal{D}_{L_2/K}B \subset B_1B_2.$$

Démonstration. — On le vérifie idéal maximal par idéal maximal en localisant. Supposons donc que A soit un anneau de valuation discrète.

Soit $(y_1, ..., y_n)$ une base de B_2 sur A et donc une base de L sur L_1. Notons $(y'_1, ..., y'_n)$ la base duale de L_2 sur K vis-à-vis de la forme bilinéaire $(x, y) \mapsto \mathrm{Tr}_{L_1/K}(xy)$. C'est aussi une base de L sur L_1. Soit $x \in B$. Il s'écrit $\sum_i \alpha_i y'_i$ avec $\alpha_i \in L$. On a

$$\mathrm{Tr}_{L/L_1}(xy_i) = \sum_j \alpha_j \mathrm{Tr}_{L/L_1}(y'_j y_i) = \alpha_i$$

On a donc $\alpha_i = \mathrm{Tr}_{L/L_1}(xy_i) \in B_1$.

En prenant $x = y_i$, on constate que la matrice $\mathrm{Tr}_{L_2/K}(y_i y_j)$ est la matrice de passage de $(y'_1, ..., y'_n)$ à $(y_1, ..., y_n)$. De façon analogue, $\mathrm{Tr}_{L_2/K}(y'_i y'_j)$ est la matrice de passage de $(y_1, ..., y_n)$ à $(y'_1, ..., y'_n)$. C'est pourquoi les matrices $\mathrm{Tr}_{L_2/K}(y_i y_j)$ et $\mathrm{Tr}_{L_2/K}(y'_i y'_j)$ sont inverses l'une de l'autre. Cette dernière est donc à coefficients dans $D(y_1, ..., y_n)^{-1} M_n(A)$ Par conséquent, on a $y'_1, y_2 ... y_n \in D(y_1, ..., y_n)^{-1} B_2 = \mathcal{D}^{-1}_{L_2/K} B_2$.

On a donc

$$x = \sum_i \mathrm{Tr}_{L/L_1}(x y_i) y'_i \in \sum_i B_1 y'_i \subset \mathcal{D}^{-1}_{L_2/K} B_2 B_1.$$

Cela démontre le résultat cherché.

Corollaire 1. — *Supposons de plus que les discriminants $\mathcal{D}_{L_2/K}$ et $\mathcal{D}_{L_1/K}$ soient premiers entre eux. On a*

$$B = B_1 B_2.$$

De plus on a

$$\mathcal{D}_{B/A} = \mathcal{D}^{[L_2:K]}_{B_1/A} \mathcal{D}^{[L_1:K]}_{B_2/A}.$$

Démonstration. — On a $B_1 B_2 \subset B$ par définition de B.

Démontrons l'inclusion inverse. On a, d'après la proposition 6,

$$\mathcal{D}_{L_2/K} B + \mathcal{D}_{L_1/K} B \subset B_1 B_2.$$

On conclut immédiatement puisque, par hypothèse, on a $B = \mathcal{D}_{L_2/K} B + \mathcal{D}_{L_1/K} B$.

Venons-en à la deuxième assertion. Par localisation on se ramène au cas où A est un anneau de valuation discrète. Choisissons des bases $(x_i)_{i=1,...,[L_1:K]}$ et $(y_j)_{j=1,...,[L_2:K]}$ de B_1 et B_2 sur A. Alors la famille $(x_i y_j)$ forme une base de B sur A puisqu'on a $B = B_1 B_2$. La matrice

$$\mathrm{Tr}_{L/K}(x_i x_{i'} y_j y_{j'}) = \mathrm{Tr}_{L_1/K}(x_i x_{i'}) \mathrm{Tr}_{L_2/K}(y_j y_{j'})$$

est le produit tensoriel des matrices $\mathrm{Tr}_{L_1/K}(x_i x_{i'})$ et $\mathrm{Tr}_{L_2/K}(y_j y_{j'})$. En utilisant la formule donnant le déterminant du produit tensoriel de deux matrices on obtient le résultat.

Remarque . — En pratique ce corollaire est très utile pour déterminer les anneaux des entiers des corps de nombres.

La deuxième assertion du corollaire pourrait se déduire de la formule des tours :

$$\mathcal{D}_{M/K} = \mathcal{D}^{[M:L]}_{L/K} N_{L/K}(\mathcal{D}_{M/L}),$$

où $L|K$ et $M|L$ sont des extensions finies et où $N_{L/K}$ est la norme d'un idéal de L (voir la leçon suivante).

V
La géométrie des nombres et le groupe des classes

1. Norme d'un idéal

Soit A un anneau de Dedekind. Notons K son corps des fractions. Soit L une extension séparable et finie de K. Notons B la clôture intégrale de A dans L. Soit I un idéal de B. La *norme* $\mathrm{N}_{L/K}(I)$ de I est par définition l'idéal de A engendré par les normes $\mathrm{N}_{L/K}(b)$ des éléments b de I. En d'autres termes, on a

$$\mathrm{N}_{L/K}(I) = \sum_{b\in I} A\mathrm{N}_{L/K}(b).$$

Voici quelques propriétés de la norme.

Proposition 1. — *On a les formules suivantes :*
(ι) $\mathrm{N}_{L/K}(bB) = \mathrm{N}_{L/K}(b)A$, $b \in B$.
(ιι) $\mathrm{N}_{L/K}(IB_{(\mathcal{Q})}) = \mathrm{N}_{L/K}(I)A_{(\mathcal{Q})}$, *$I$ idéal de B et $\mathcal{Q}$ idéal premier non nul de A.*
(ιιι) $\mathrm{N}_{L/K}(I_1I_2) = \mathrm{N}_{L/K}(I_1)\mathrm{N}_{L/K}(I_2)$, *$I_1$ et I_2 idéaux de B.*
(ιv) $\mathrm{N}_{L/K}(\mathcal{P}) = \mathcal{Q}^{f_{\mathcal{P}}}$, *$\mathcal{Q}$ idéal premier non nul de A, $\mathcal{P}$ idéal premier de B au dessus de $\mathcal{Q}$.*
Démonstration. — La première formule résulte de $\mathrm{N}_{L/K}(B) = A$ et de la multiplicativité de la norme.

On a l'inclusion $\mathrm{N}_{L/K}(I)A_{(\mathcal{Q})} \subset \mathrm{N}_{L/K}(IB_{(\mathcal{Q})})$. Démontrons l'inclusion inverse. Soit $x \in \mathrm{N}_{L/K}(IB_{(\mathcal{Q})})$. Il s'écrit $\sum_{b\in IB_{(\mathcal{Q})}} \lambda_b \mathrm{N}_{L/K}(b)$, cette somme étant finie avec $\lambda_b \in A$. Il suffit donc de prouver que $\mathrm{N}_{L/K}(b) \in \mathrm{N}_{L/K}(I)A_{(\mathcal{Q})}$ pour tout $b \in IB_{(\mathcal{Q})}$. Soit $s \in A - \mathcal{Q}$ tel que $sb \in IB$. On a $\mathrm{N}_{L/K}(sb) = s^{[L:K]}\mathrm{N}_{L/K}(b)$. Comme $s^{[L:K]} \in A - \mathcal{Q}$, on a $\mathrm{N}_{L/K}(b) \in \mathrm{N}_{L/K}(I)A_{(\mathcal{Q})}$. Cela démontre l'inclusion cherchée et donc $(\iota\iota)$.

Lemme 1. — *Un anneau de Dedekind ne possédant qu'un nombre fini d'idéaux premiers est principal.*
Démonstration. — Soit A un tel anneau. Notons K son corps des fractions. Soit I un idéal de A. Il s'écrit sous la forme $\prod_{\mathcal{P}} \mathcal{P}^{n_{\mathcal{P}}}$ où $\mathcal{P}$ parcourt les idéaux maximaux de A. Soit $(x_{\mathcal{P}})_{\mathcal{P}}$ une famille (finie) indexée par les idéaux maximaux de A d'éléments de A telle que $v_{\mathcal{P}}(x_{\mathcal{P}}) = n_{\mathcal{P}}$. D'après le lemme d'approximation, il existe $x \in K$ tel que $v_{\mathcal{P}}(x - x_{\mathcal{P}}) > n_{\mathcal{P}}$. On a donc $v_{\mathcal{P}}(x) = n_{\mathcal{P}}$ pour tout idéal maximal $\mathcal{P}$ de A ; Cela entraîne que x est entier. L'idéal I est donc engendré par x. Tout idéal de A est donc principal.

En vertu de $(\iota\iota)$ on peut procéder par localisation pour démontrer $(\iota\iota\iota)$. D'après le lemme 1, l'anneau $B_{(\mathcal{Q})}$ est principal puisque c'est un anneau de Dedekind qui a pour seuls idéaux maximaux les idéaux engendrés par les idéaux maximaux de B au-dessus de $\mathcal{Q}$ qui sont en nombre fini. On se ramène donc au cas où A est un anneau de valuation discrète et où B est un anneau principal. On utilise alors (ι).

On démontre d'abord (ιv) dans le cas d'une extension $L|K$ galoisienne. Soit $b \in \mathcal{P}$. On a $\mathrm{N}_{L/K}(b) \in \mathcal{P} \cap K \subset \mathcal{Q}$. On a donc $\mathrm{N}_{L/K}(\mathcal{P}) \subset \mathcal{Q}$. De plus $\mathrm{N}_{L/K}(\mathcal{P})$ n'est contenu dans aucun idéal premier non nul distinct de $\mathcal{Q}$ en raison de $(\iota\iota)$. Par localisation on se ramène au cas où A est un anneau de valuation discrète. Posons $\mathrm{N}_{L/K}(\mathcal{P}) = \mathcal{Q}^{m_{\mathcal{P}}}$ pour un certain entier $m_{\mathcal{P}}$. On a la décomposition de $\mathcal{Q}$ donnée par $\mathcal{Q} = \prod_{\mathcal{P}'|\mathcal{Q}} \mathcal{P}'^{e_{\mathcal{P}'}}$. De plus on a

$$\prod_{\mathcal{P}'|\mathcal{Q}} \mathcal{Q}^{e_{\mathcal{P}'} m_{\mathcal{P}'}} = \mathrm{N}_{L/K}(\mathcal{Q}B) = \mathcal{Q}^{[L:K]}B = \prod_{\mathcal{P}'|\mathcal{Q}} \mathcal{Q}^{e_{\mathcal{P}'} f_{\mathcal{P}'}}.$$

En comparant ces formules on obtient $m_{\mathcal{P}} = f_{\mathcal{Q}} = f_{\mathcal{P}}$.

Ne supposons plus que l'extension $L|K$ soit galoisienne pour démontrer (ιv). Soit $M|L$ une extension finie de corps telle que $M|K$ soit galoisienne. L'extension $M|L$ est alors galoisienne. Utilisons la transitivité de la norme et appliquons le résultat dans le cas galoisien. Soit $\mathcal{R}$ un idéal premier de M au dessus de $\mathcal{P}$. Pour lever toute ambiguïté, indiquons dans ce qui suit à quelle extension de corps le degré résiduel fait référence.

On a

$$\mathcal{Q}^{f_{\mathcal{R}}(M/K)} = \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(\mathcal{R})) = \mathrm{N}_{L/K}(\mathcal{P})^{f_{\mathcal{P}}(L/K)}.$$

Soient $k_2|k_1$ et $k_3|k_2$ deux extension finies de corps. Rappelons que le théorème de la *base télescopique* donne la formule suivante pour le degré de l'extension composée :

$$[k_3 : k_1] = [k_3 : k_2][k_2 : k_1].$$

On en déduit la formule suivante pour les degrés résiduels

$$f_{\mathcal{R}}(M/K) = f_{\mathcal{P}}(L/K) f_{\mathcal{R}}(M/L).$$

Cela donne le résultat cherché en combinant avec ce qui précède.

Dans le cas où $A = \mathbf{Z}$, $\mathrm{N}_{L/\mathbf{Q}}(I)$ est la *norme absolue* de I. On l'identifie à l'entier > 0 qui l'engendre comme idéal de $\mathbf{Z}$. Notons cet entier N_I.

Proposition 2. — *On a*

$$\mathrm{N}_{L/\mathbf{Q}}(I) = |B/I|\mathbf{Z}.$$

Démonstration. — Il suffit de le vérifier pour I premier car $|B/I_1I_2| = |B/I_1||B/I_2|$ lorsque I_1 et I_2 sont des idéaux premiers entre eux. On s'est donc ramené au cas où I est une puissance d'un idéal premier. Lorsque $I = \mathcal{P}$ est un idéal premier, $\mathcal{P}^k/\mathcal{P}^{k+1}$ est un espace vectoriel de dimension 1 sur $B/\mathcal{P}$. Par conséquent on a $|B/\mathcal{P}^k| = |B/\mathcal{P}|^k$. Il reste à vérifier l'égalité cherchée pour un idéal premier $\mathcal{P}$. Cela résulte de la formule

$$|B/\mathcal{P}| = p^{f_p}$$

et de la proposition 1.

Remarque . — On généralise la notion de norme aux idéaux fractionnaires par la formule (où les fractions sont calculées dans le groupe des idéaux fractionnaires)

$$\mathrm{N}_{L/K}(I_1/I_2) = \mathrm{N}_{L/K}(I_1)/\mathrm{N}_{L/K}(I_2).$$

2. La finitude du groupe des classes

Soit K une extension de degré d de $\mathbf{Q}$. Soit L une extension normale (et donc galoisienne) de $\mathbf{Q}$ qui contient K et qui est contenue dans $\mathbf{C}$.

Soient σ_1,...,σ_d des représentants de $\mathrm{Gal}(L/\mathbf{Q})/\mathrm{Gal}(L/K)$. Ce sont des plongements de K dans $\mathbf{C}$. Considérons ceux d'entre eux dont l'image est contenue dans $\mathbf{R}$ (les *places. réelles* de K). Numérotons-les σ_1, ..., σ_{r_1}. Les autres (les *places complexes non réelles* de K) sont intervertis deux-à-deux par la conjugaison complexe. Écrivons-les sous la forme σ_{r_1+1}, ...,$\sigma_{r_1+r_2}$, $\sigma_{r_1+r_2+1} = \bar{\sigma}_{r_1+1}$,..., $\sigma_d = \bar{\sigma}_{r_1+r_2}$. Les entiers r_1 et r_2 ne dépendent pas du choix de L. On a

$$d = r_1 + 2r_2.$$

Notons $\mathcal{O}_K$ l'anneau des entiers de K. Notons $\mathcal{C}\ell(K)$ le *groupe des classes* de K, c'est-à-dire le groupe obtenu en considérant le quotient du groupe des idéaux fractionnaires de K par le sous-groupe des idéaux fractionnaires principaux.

Théorème 1. — *Le groupe $\mathcal{C}\ell(K)$ est fini.*

Le théorème 1 est dû à Dirichlet. On va voir qu'il résulte du théorème de Minkowski, qui a été démontré postérieurement. Il n'est pas valide si K est remplacé par le corps des fractions d'un anneau de Dedekind quelconque.

Proposition 3. — *Soit M un nombre entier > 0. Il n'existe qu'un nombre fini d'idéaux I de $\mathcal{O}_K$ norme absolue $< M$.*

Démonstration. — Rappelons que N_I est la norme de l'idéal I. Soient I_1 et I_2 deux idéaux premiers entre eux de $\mathcal{O}_K$. On a

$$N_{I_1 I_2} = N_{I_1} N_{I_2}.$$

Soit $\mathcal{P}$ un idéal premier. Le $\mathcal{O}_K/\mathcal{P}$-espace vectoriel $\mathcal{P}^k/\mathcal{P}^{k+1}$ est de dimension 1. On a donc

$$N_{\mathcal{P}^k} = N_{\mathcal{P}}^k.$$

La fonction $I \mapsto N_I$ est donc multiplicative.

Il suffit donc de prouver qu'il n'existe qu'un nombre fini d'idéaux premiers de $\mathcal{P}$ de norme $< M$. Cela résulte du fait qu'il n'existe qu'un nombre fini de nombres premiers

$< M$ et du fait qu'il n'y a nombre fini d'idéaux premiers de $\mathcal{O}_K$ au dessus de ces nombres premiers.

Pour démontrer la finitude du groupe des classes, il suffit donc de démontrer qu'il existe un nombre M_K ne dépendant que de K tel que tout élément de $\mathcal{C}\ell(K)$ possède un représentant dans $\mathcal{O}_K$ de norme $< M_K$. ΛC'est l'objet du théorème de Minkowski.

Remarque . — Lors de la démonstration de la formule du nombre de classes, on comptera le nombre d'idéaux de $\mathcal{O}_K$ dans une classe donnée et de norme absolue bornée.

3. Le théorème de Minkowski

C'est le théorème suivant. Reprenons les notations de la section précédente. Rappelons que $\mathcal{D}_K$ est le discriminant absolu de K.

THÉORÈME 2. — *Tout élément de $\mathcal{C}\ell(K)$ possède un représentant I dans $\mathcal{O}_K$ de norme N_I vérifiant*

$$N_I \leq \frac{d\,!}{d^d}(\frac{\pi}{4})^{-r_2}|\mathcal{D}_K|^{1/2}.$$

La quantité $\frac{d\,!}{d^d}(\frac{4}{\pi})^{r_2} = M(r_1, r_2)$ est la *constante de Minkowski* du corps K. Voici les valeurs approchées de cette constantes pour $d \leq 5$: $M(1,0) = 1$, $M(0,1) = 0,63661$, $M(2,0) = 0,5$, $M(1,1) = 0,28299$, $M(3,0) = 0,22222$, $M(0,2) = 0,15198$, $M(2,1) = 0,11937$, $M(4,0) = 0,09375$, $M(1,2) = 0,06225$, $M(3,1) = 0,04889$, $M(5,0) = 0,0384$.

On démontrera le théorème 2 dans les sections suivantes. Indiquons-en quelques conséquences.

COROLLAIRE 1. — *On a l'inégalité :*

$$|\mathcal{D}_K| \geq (\frac{\pi}{4})^{2r_2}\frac{d^{2d}}{(d\,!)^2}.$$

Démonstration. — Cela résulte du théorème 3 en remarquant que la norme d'un idéal quelconque de $\mathcal{O}_K$ est ≥ 1.

COROLLAIRE 2. — *Il n'y a pas d'extension de corps de* $\mathbf{Q}$ *non ramifée autre que* $\mathbf{Q}$.
Démonstration. — Il suffit de remarquer que les quantités

$$|\mathcal{D}_K|^{1/2} \geq N_I(\frac{\pi}{4})^{r_2}\frac{d^d}{d\,!} \geq (\frac{\pi}{4})^{-d}\frac{d^d}{d\,!},$$

sont > 1 pour $d > 1$. Il existe donc un diviseur premier de $\mathcal{D}_K$. Ce nombre premier est donc ramifié dans l'extension $K/\mathbf{Q}$.

Le corollaire 2 est un résultat dû à Hermite. Le corollaire 3 ci-dessous pourrait aussi se déduire de la (difficile) loi de réciprocité d'Artin. Le corps de classe de Hilbert H_K d'un corps de nombres K est la plus grande extension abélienne $H_K|K$ partout non ramifiée et telle que toutes les places réelles de K se prolongent en des places réelles de H_K. On reviendra par la suite sur ce corps.

COROLLAIRE 3. — *Le corps de classe de Hilbert de* $\mathbf{Q}$ *est égal à* $\mathbf{Q}$.
Démonstration. — Cela résulte du corollaire 1 puisque le corps de classe de Hilbert est une extension non ramifiée.

COROLLAIRE 4. — *Le discriminant d'un corps tend vers l'infini lorsque le degré tend vers l'infini.*
Démonstration. — Il suffit de vérifier que l'expression $\mathcal{D}_K \geq (\frac{\pi}{4})^{-2r_2} \frac{d^{2d}}{(d\,!)^2}$ tend vers l'infini lorsque d tend vers l'infini.

Remarque . — La "réciproque" du corollaire 4 est fausse : Le discriminant d'un corps quadratique peut être arbitrairement grand (plus précisément, lorsque p est un nombre premier, le discriminant absolu du corps $\mathbf{Q}(\sqrt{p})$ est divisible par p). Le théorème d'Hermite est une version plus forte du corollaire 4.

On va voir que le théorème de Minkowski résulte de la proposition suivante.

PROPOSITION 4. — *Soit I un idéal non nul de $\mathcal{O}_K$. Il existe un élément a non nul de I tel que*

$$\mathrm{N}_{K/\mathbf{Q}}(a) \leq \frac{d\,!}{d^d}(\frac{4}{\pi})^{r_2} N_I |\mathcal{D}_K|^{1/2}.$$

Cette proposition sera démontrée plus loin. Voyons pourquoi elle entraîne le théorème de Minkowski.
Démonstration. — Soit I' un idéal fractionnaire de K. Soit $b \in I'$ tel que bI'^{-1} soit un idéal de $\mathcal{O}_K$. Appliquons la proposition 4 à bI'^{-1} : Il existe $a \in bI'^{-1}$ tel que

$$\mathrm{N}_{K/\mathbf{Q}}(a) \leq \frac{d\,!}{d^d}(\frac{4}{\pi})^{r_2} N_{bI'^{-1}} |\mathcal{D}_K|^{1/2} = \frac{d\,!}{d^d}(\frac{4}{\pi})^{r_2} N_{I'}^{-1} \mathrm{N}_{K/\mathbf{Q}}(b) |\mathcal{D}_K|^{1/2}.$$

Posons $I = (a/b)I'$. C'est un idéal fractionnaire de même classe que I'. Il est contenu dans $\mathcal{O}_K$ car $a \in bI'^{-1}$. On a

$$N_I = N_{I'b^{-1}} \mathrm{N}_{K/\mathbf{Q}}(a) = \mathrm{N}_{K/\mathbf{Q}}(a)/N_{I'^{-1}b} \leq \mathrm{N}_{K/\mathbf{Q}}(a),$$

puisque bI'^{-1} est un idéal de $\mathcal{O}_K$ et donc de norme absolue ≥ 1. En combinant avec l'inégalité ci-dessus, on obtient

$$N_I \leq \frac{d\,!}{d^d}(\frac{\pi}{4})^{r_2} |\mathcal{D}_K|^{1/2}.$$

On a donc prouvé que tout idéal fractionnaire de K est dans même classe qu'un idéal entier de $\mathcal{O}_K$ de norme absolue vérifiant l'inégalité demandée.

4. Ingrédients disparates

Rappelons qu'un *réseau* de $\mathbf{R}^d$ est un sous-groupe discret de $\mathbf{R}^d$ isomorphe à $\mathbf{Z}^d$. Il revient au même de dire que c'est un sous-groupe abélien engendré sur $\mathbf{Z}$ par une base sur $\mathbf{R}$ de $\mathbf{R}^d$. Rappelons que le *volume* $\mathrm{vol}(E)$ d'un ensemble mesurable E est sa mesure de Lebesgue. Le volume d'un réseau L est par abus de notation le volume de $\mathbf{R}^d/L$.

PROPOSITION 5. — *Soit L un réseau de $\mathbf{R}^d$. Soit X un sous-ensemble de $\mathbf{R}^d$ borné, convexe et symétrique par rapport à l'origine (i.e. stable par $x \mapsto -x$). Supposons de plus qu'on ait*

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

Alors l'ensemble $X \cap (L - \{0\})$ est non vide.
Démonstration. —

Le volume de L est le volume d'un parallépipède fondamental de L (rappelons qu'un *parallépipède fondamental* est un parallépipède P ouvert de $\mathbf{R}^d$ tel que deux éléments distincts de P définissent deux classes distinctes de $\mathbf{R}^d/L$ et tel que tout élément de $\mathbf{R}^d/L$ ait un représentant dans l'adhérence de P).

Lemme 2. — *Soit A un sous-ensemble borné de $\mathbf{R}^d$, tel que deux éléments distincts de A définissent deux éléments distincts de $\mathbf{R}^d/L$. Alors on a* $\mathrm{vol}(A) \leq \mathrm{vol}(L)$.
Démonstration. — Puisque A est borné il est contenu dans l' adhérence d'un nombre fini de parallépipèdes fondamentaux. Rappelons que la translation préserve le volume. Quitte à décomposer A en un nombre fini de sous-ensemble que l'on translate par des éléments de L, on peut supposer que A est contenu dans l'adhérence $\bar{P}$ d'un parallépipède fondamental. On a donc $\mathrm{vol}(A) \leq \mathrm{vol}(\bar{P}) = \mathrm{vol}(P)$. La dernière égalité provient du fait que P est ouvert.

Déduisons la proposition 5 du lemme 2. Considérons l'ensemble

$$\frac{1}{2}X = \{\frac{1}{2}x / x \in X\}.$$

Son volume est égal à $2^{-d}\mathrm{vol}(X) > \mathrm{vol}(L)$. D'après le lemme 1, il existe deux éléments distincts x et y de $\frac{1}{2}X$ qui sont congrus modulo L. On a donc $x - y \in L$. Comme $2x$ et $2y$ sont éléments de X et comme X est convexe et symétrique on a $\frac{2x-2y}{2} = x - y \in X$. On a donc un élément non nul de $X \cap L$.

Considérons l'application $v_K : K \mapsto \mathbf{R}^d \simeq \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ qui à $x \in K$ associe $(\sigma_1(x), ..., \sigma_{r_1}(x), \sigma_{r_1+1}(x), ..., \sigma_{r_1+r_2}(x))$. C'est un homomorphisme de groupes. Précisons que l'identification entre $\mathbf{C}$ et $\mathbf{R}^2$ est donnée par l'application qui à un nombre complexe associe le couple formé par sa partie réelle et sa partie imaginaire. On en déduit l'identification $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2} \simeq \mathbf{R}^d$.

Proposition 6. — *Soit I un idéal de $\mathcal{O}_K$. L'image de I par v_K est un réseau de volume $2^{-r_2}N_I|\mathcal{D}_K|^{1/2}$.*
Démonstration. — C'est essentiellement le lemme suivant.

Lemme 2. — Soit M un sous-$\mathbf{Z}$-module libre de rang d de K de base $(x_i)_{i=1,...,d}$. Alors $v_K(M)$ est un réseau de $\mathbf{R}^d$ dont le volume est donné par la formule :

$$\mathrm{vol}(v_K(M)) = 2^{-r_2}|\det(\sigma_j(x_i)|.$$

Démonstration. — L'image de $v_K(M)$ dans $\mathbf{R}^d$ est engendrée comme $\mathbf{Z}$-module par les $U_i = (\sigma_1(x_i), ..., \sigma_{r_1}(x_i), \mathrm{Re}(\sigma_{r_1+1}(x_i)), \mathrm{Im}(\sigma_{r_1+1}(x_i)), ..., \mathrm{Re}(\sigma_{r_1+r_2}(x_i)), \mathrm{Im}(\sigma_{r_1+r_2}(x_i))$. Remarquons qu'on a $|\det(U, \bar{U})| = 2|\det(\mathrm{Re}(U), \mathrm{Im}(U))|$, $U \in \mathbf{C}^2$. On en déduit $|D| = |\det(U_1, ..., U_d)| = 2^{-r_2}|\det(\sigma_j(x_i))|$. Ce dernier déterminant est non nul (voir la leçon sur les discriminants). Les $v_K(x_i)$ forment bien une base de $\mathbf{R}^d$ et on a bien un réseau de $\mathbf{R}^d$.

On a $\mathrm{vol}(v_K(M)) = |D|$ puisque les vecteurs U_i définissent un parallépipède fondamental de $v_K(M)$.

Venons-en maintenant à la démonstration de la formule du volume. Appliquons d'abord le lemme 2 à $M = \mathcal{O}_K$ qui est un $\mathbf{Z}$-module libre de rang d. On obtient

$$\mathrm{vol}(v_K(\mathcal{O}_K)) = 2^{-r_2}|\det(\sigma_j(x_i)| = 2^{-r_2}\mathcal{D}_K^{1/2},$$

où les x_i forment une base de $\mathcal{O}_K$ sur $\mathbf{Z}$. Un idéal I de $\mathcal{O}_K$ est un $\mathbf{Z}$-module libre de rang d, puisqu'il est d'indice fini N_I dans $\mathcal{O}_K$. Son volume est égal au volume de $\mathcal{O}_K$ multiplié par cet indice. Cela se voit par exemple en remarquant qu'un parallépipède fondamental de $v_K(I)$ se décompose en N_I parallépipèdes fondamentaux de $v(\mathcal{O}_K)$.

Soit t un nombre réel > 0. Posons

$$X_t = \{(x_1, ..., x_{r_1}, z_{r_1+1}, ..., z_{r_1+r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} /$$

$$|x_1| + ... + |x_{r_1}| + 2|z_{r_1+1}| + ... + 2|z_{r_1+r_2}| < t\}.$$

Proposition 7. — *Le volume de X_t est donné par la formule*

$$\mathrm{vol}(X_t) = 2^{r_1-r_2}\pi^{r_2}t^d/d\,!.$$

Démonstration. — On établit cette formule de volume par une double récurrence sur r_1 et r_2. Notons $V(r_1, r_2, t)$ le volume de X_t. On vérifie la formule pour $r_1 + r_2 = 1$. On trouve

$$V(0, 1, t) = \frac{\pi t^2}{4}$$

et

$$V(1, 0, t) = 2t$$

Cela initialise la récurrence.

Calculons $V(r_1+1, r_2, t)$ en utilisant l'hypothèse de récurrence. On a, en isolant la (r_1+1)-ième variable,

$$V(r_1+1, r_2, t) = \int_{-t}^{t} V(r_1, r_2, t-|y|)\, dy = \int_{-t}^{t} 2^{r_1-r_2}\pi^{r_2}\frac{(t-|y|)^d}{d\,!}\, dy.$$

Un calcul direct montre que le dernier membre est égal à

$$2^{r_1+1-r_2}\pi^{r_2}\frac{t^{d+1}}{(d+1)\,!}.$$

C'est le résultat désiré.

Calculons maintenant $V(r_1, r_2+1, t)$ de façon analogue. On a

$$V(r_1, r_2+1, t) = \int_{|z|\leq\frac{t}{2}, z=x+iy} V(r_1, r_2, t-2|z|)\, dx\, dy.$$

Passons en coordonnées polaires : $z = \rho e^{i\theta}$ et $dx\, dy = \rho\, d\rho\, d\theta$. On obtient

$$V(r_1, r_2+1, t) = \int_0^{\frac{t}{2}}\int_0^{2\pi} 2^{r_1}(\frac{\pi}{2})^{r_2}\frac{(t-2\rho)^d}{d\,!}\rho\, d\rho\, d\theta$$

Le calcul de $\int_0^{\frac{t}{2}}(t-2\rho)^d\rho\, d\rho$ donne $\frac{t^{d+2}}{4(d+1)(d+2)}$ (par récurrence sur d et en utilisant une intégration par parties). On obtient :

$$V(r_1, r_2+1, t) = 2^{r_1}(\frac{\pi}{2})^{r_2}\frac{2\pi}{d\,!}\frac{t^{d+2}}{4(d+1)(d+2)} = 2^{r_1}(\frac{\pi}{2})^{r_2+1}\frac{t^{d+2}}{(d+2)\,!}.$$

C'est formule cherchée.

5. Démonstration de la proposition 4

Soit I un idéal de $\mathcal{O}_K$. Soit t un nombre réel > 0. L'ensemble X_t est un sous-ensemble convexe, borné et symétrique par rapport à l'origine de $\mathbf{R}^d$. En combinant les propositions 5, 6 et 7 (appliquées à $X = X_t$ et $L = v_K(I)$), on obtient qu'il existe un élément $x_t \in X_t \cap (v_K(I) - 0)$ dès lors qu'on a l'inégalité

$$t^d > d\,!\frac{2^{d-r_1}}{\pi^{r_2}}N_I|\mathcal{D}_K|^{1/2}.$$

Ces éléments forment un ensemble fini (car $v_K(I)$ est discret et X_t est borné) et non vide A_t. La famille des A_t est décroissante quand t décroît. Par conséquent l'ensemble

$$A = \cap_{t, t^d > d\,!\frac{2^{d-r_1}}{\pi^{r_2}}N_I|\mathcal{D}_K|^{1/2}} A_t$$

est non vide. Soit $x \in A$. Posons

$$t_0 = (d!\frac{2^{d-r_1}}{\pi^{r_2}} N_I |\mathcal{D}_K|^{1/2})^{1/d}.$$

On a $A = A_{t_0}$ et donc, en raison des proposition 5, 6 et 7, il existe $x \in X_{t_0} \cap (v_K(I) - 0)$. Posons $x = v_K(a)$. Calculons la valeur absolue de la norme de a. On a

$$|\mathrm{N}_{K/\mathbf{Q}}(a)| = \prod_{i=1}^{d} |\sigma_i(a)| = \prod_{i=1}^{r_1} |\sigma_i(a)| \prod_{i=r_1+1}^{r_2} |\sigma_i(a)|^2.$$

Appliquons l'inégalité (dite de la *moyenne arithmético-géométrique*)

$$(\prod_{i=1}^{n} |x_i|)^{1/n} \leq \frac{1}{n} \sum_{i=1}^{n} |x_i|,$$

où les x_i sont des nombres réels. On obtient

$$|\mathrm{N}_{K/\mathbf{Q}}(a)| \leq \frac{t_0^d}{d^d},$$

puisque $v_K(a) \in X_{t_0}$. Remplaçons t_0 par sa valeur, on obtient :

$$\mathrm{N}_{K/\mathbf{Q}}(a) \leq \frac{d!}{d^d} (\frac{4}{\pi})^{r_2} N_I |\mathcal{D}_K|^{1/2}.$$

Cela achève de prouver la proposition 4.

VI
La géométrie des nombres et le groupe des unités

1. Le théorème des unités

Soit K un corps de nombres. Rappelons qu'on note désormais $\mathcal{O}_K$ l'anneau des entiers de K. On note d le degré de K sur $\mathbf{Q}$ et r_1 (resp. r_2) le nombre de places réelles de K (resp. de places complexes non réelles à conjugaison près). On note $\mathcal{D}_K$ le discriminant absolu de K.

Le groupe $\mathcal{O}_K^*$ des éléments inversibles de l'anneau $\mathcal{O}_K$ est le *groupe des unités* de K.

THÉORÈME 1. — *Le groupe $\mathcal{O}_K^*$ est isomorphe au produit d'un groupe cyclique par $\mathbf{Z}^{r_1+r_2-1}$.*

Le théorème 1 est le *théorème des unités* de Dirichlet. Sa démonstration repose sur la théorie de Minkowski.

Il en résulte que les seuls corps de nombres possédant un nombre fini d'unités sont le corps des nombres rationnels et les corps quadratiques imaginaires.

2. Le théorème d'Hermite

C'est le théorème suivant. Il est antérieur au théorème de Minkowski.

THÉORÈME 1. — *Il n'y a qu'un nombre fini de corps de nombres de discriminant absolu donné.*

Démonstration. — D'après le corollaire 4 du théorème V-2, il suffit de démontrer qu'il n'y a qu'un nombre fini de corps K de degré d et discriminant $\mathcal{D}_K$ donnés. On peut supposer qu'on a $d > 1$. On peut également supposer que r_1 et r_2 sont donnés.

Lemme 1. — *Soient M un nombre réel > 0 et d un entier > 0. Les entiers algébriques dont tous les conjugués sont majorés en valeur absolue par M n'engendrent qu'un nombre fini de corps de nombres de degré d.*

Démonstration. — Soit K un tel corps de nombres. Soit x un entier algébrique qui l'engendre tel que $|\sigma_i(x)| \leq M$ $(1 \leq i \leq d)$. Le polynôme minimal de x est donné par la formule

$$\prod_i (X - \sigma_i(x)) \in \mathbf{Z}[X].$$

Les coefficients de ce polynôme sont des nombres entiers bornés en termes de d et M puisque les $\sigma_i(x)$ sont bornés en fonctions de M et que ce polynôme est de degré d. Il n'y a qu'un nombre fini de possibilités pour un tel polynôme, puisqu'il n'y qu'un nombre fini de possibilités pour chacun des d coefficients, et donc un nombre fini de possibilités pour $\mathbf{Q}(x) = K$.

Pour obtenir le théorème 1 il suffit de démontrer que K est engendré par un entier algébrique dont les conjugués sont bornés par des nombres ne dépendant que de r_1, r_2 et $\mathcal{D}_K$.

Démontrons-le lorsque K possède au moins une place réelle (*i.e.* $r_1 \geq 1$). Considérons le sous-ensemble X de $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ formé par les éléments $(x_1, ..., x_{r_1}, z_{r_1+1}, ..., z_{r_1+r_2})$ tels que $|x_1| \leq 2^d(\frac{\pi}{2})^{-r_2}\mathcal{D}_K^{1/2}$, $|x_i| \leq \frac{1}{2}$ $(1 < i \leq r_1)$ et $|z_i| \leq \frac{1}{2}$ $(r_1 < i \leq r_1 + r_2)$. C'est un ensemble borné, convexe, symétrique par rapport à l'origine et de volume donné par la formule

$$\mathrm{vol}(X) = 2^{d-r_2+1}\mathcal{D}_K^{1/2} > 2^{d-r_2}|\mathcal{D}_K|^{1/2}.$$

D'après les propositions V-5 et V-7, il existe $x \in \mathcal{O}_K - \{0\}$ tel que $v_K(x) \in X$. Les conjugués de x sont majorés en valeur absolue par des quantités ne dépendant que de r_1, r_2 et $\mathcal{D}$.

Lemme 2. — *On a* $K = \mathbf{Q}(x)$.
Démonstration. — Il suffit de démontrer qu'on a $\sigma_1(x) \neq \sigma_i(x)$ pour tout $i \neq 1$. En effet le groupe $\mathrm{Gal}(L/\mathbf{Q})$ (où $L/\mathbf{Q}$ est une extension galoisienne qui contient K, voir la leçon VII) permute transitivement les conjugués de x. Le stabilisateur de x dans $\mathrm{Gal}(L/\mathbf{Q})$ est égal à $\mathrm{Gal}(L/\mathbf{Q}(x))$. Ce dernier est égal à $\mathrm{Gal}(L/K)$ si et seulement si $K = \mathbf{Q}(x)$. Si on a $K \neq \mathbf{Q}(x)$, il existe donc $\tau \in \mathrm{Gal}(L/\mathbf{Q}) - \mathrm{Gal}(L/K)$ tel que $\tau(x) = x$. On a alors $\sigma_1(\tau(x)) = \sigma_1(x)$. De plus $\sigma_1 \circ \tau$ et σ_1 définissent des plongements distincts de K dans L puisque $\tau \notin \mathrm{Gal}(L/K)$.

On a $|\sigma_i(x)| \leq \frac{1}{2}$ lorsque $i \neq 1$. Par ailleurs on a $\mathrm{N}_K(x) \in \mathbf{Z}$ puisque x est un entier algébrique. On a

$$|\mathrm{N}_K(x)| = \prod_i |\sigma_i(x)| > 1.$$

On a donc, pour $i \neq 1$,

$$|\sigma_1(x)| \geq 2^{r_1+2r_2-1} > 1 > 1/2 \geq |\sigma_i(x)|.$$

Cela entraîne la relation $\sigma_1(x) \neq \sigma_i(x)$ pour tout $i \neq 1$.

Lorsque K ne possède pas de plongement réel, on peut adapter la démonstration ci-dessus. On considère le sous-ensemble Y de $\mathbf{C}^{r_2}$ formé par les éléments $(z_1, ..., z_{r_2})$ vérifiant $|z_1 - \bar{z}_1| \leq 2^d\frac{8}{\pi}(\frac{\pi}{2})^{-r_2}|\mathcal{D}_K|^{1/2}$, $|z_1 + \bar{z}_1| \leq \frac{1}{2}$ et $|z_i| \leq \frac{1}{2}$ pour $i \neq 1$. C'est aussi un ensemble borné, convexe, symétrique par rapport à l'origine et de volume $\mathrm{vol}(Y)$ vérifiant

$$\mathrm{vol}(Y) > 2^{d-r_2}|\mathcal{D}_K|^{1/2}.$$

Il existe donc $y \in \mathcal{O}_K - \{0\}$ tel que $v_K(y) \in Y$.

Lemme 3. — *On a* $K = \mathbf{Q}(y)$.
Démonstration. — En adaptant les arguments du lemme 2 on obtient qu'on a $|\sigma_1(y)| = |\bar{\sigma}_1(y)| \geq 1$. Par conséquent on a $\sigma_1(y) \neq \sigma_i(y)$ et $\sigma_1(y) \neq \bar{\sigma}_i(y)$ pour tout $i \neq 1$. Il reste à montrer qu'on a $\sigma_1(y) \neq \bar{\sigma}_1(y)$, c'est-à-dire $\sigma_1(y)$ non réel. Cela résulte des conditions $|\sigma_1(y) + \bar{\sigma}_1(y)| \leq \frac{1}{2}$ et $|\sigma_1(y)| = |\bar{\sigma}_1(y)| \geq 1$ qui ne peuvent être satisfaites par deux nombres réels égaux.

3. Démonstration du théorème des unités

Commençons par caractériser les unités de K parmi les entiers de K.

Proposition 1. — *Soit K un corps de nombres. Les unités de K coïncident avec les entiers de K de norme* 1 *ou* -1.
Démonstration. — Soit x une unité de K. Les nombres rationnels $\mathrm{N}_{K/\mathbf{Q}}(x)$ et $\mathrm{N}_{K/\mathbf{Q}}(x^{-1})$ sont des entiers inverses l'un de l'autre. On a donc $\mathrm{N}_{K/\mathbf{Q}}(x) \in \{-1, 1\}$.

Soit $x \in \mathcal{O}_K$ de norme égale à 1 ou -1. On a $x^n + a_{n-1}x^{n-1} + ... + a_1 x + \epsilon = 0$ avec $\epsilon \in \{-1, 1\}$ et avec $a_i \in \mathbf{Z}$ ($i \in \{1, 2, ..., n-1\}$). La quantité

$$y = -\epsilon(x^{n-1} + a_{n-1}x^{n-2} + ... + a_1)$$

est un entier algébrique. On a $xy = 1$ si bien que x est une unité de K.

L'application $K^* \longrightarrow \mathbf{R}^{r_1+r_2}$ qui à x associe

$$\Lambda(x) = (\log(|\sigma_1(x)|), ..., \log(|\sigma_{r_1}(x)|), 2\log(|\sigma_{r_1+1}(x)|), ..., 2\log(|\sigma_{r_1+r_2}(x)|))$$

est un homomorphisme de groupes (relativement à la multiplication et à l'addition respectivement) qu'on appelle le *plongement logarithmique* de K^*.

Lemme 4. — *L'image réciproque dans $\mathcal{O}_K$ par Λ d'un ensemble compact est un ensemble fini (autrement dit Λ est une application propre).*
Démonstration. — Soit C un sous ensemble compact de $\mathbf{R}^{r_1+r_2}$. Il existe des nombre réels strictement positifs α et β tels que pour tout $x \in \Lambda^{-1}(C)$ on ait $\alpha < |\sigma_i(x)| < \beta$ pour toute place σ_i de K dans $\mathbf{C}$. Les fonction symétriques élémentaires de degré $\leq d$ en les $\sigma_i(x)$ sont donc bornées en valeur absolue. Le polynôme minimal de x est à coefficients dans $\mathbf{Z}$ et ces coefficients sont donnés par les fonctions symétriques élémentaires de degré $\leq d$ en les $\sigma_i(x)$. Il appartient donc à un ensemble fini ne dépendant que de α, β et d. L'entier algébrique x appartient à l'ensemble fini des racines de tels polynômes. On en déduit que l'ensemble $\Lambda^{-1}(C)$ est fini.

Donnons quelques conséquences du lemme 4.

Lemme 5. — *L'ensemble des unités contenues dans le noyau de Λ constitue un groupe cyclique.*
Démonstration. — C'est un groupe fini G d'après le lemme 4 puisque c'est l'image réciproque de $\{0\}$ qui est un ensemble fini et donc compact. Tout élément de G est donc

d'ordre fini. C'est donc une racine de l'unité. Le groupe G est donc un sous-groupe fini du groupe cyclique des racines n-ièmes de l'unité pour n approprié (par exemple l'exposant du groupe G). C'est donc un groupe cyclique.

Lemme 6. — *L'image par* Λ *de* $\mathcal{O}_K^*$ *est un sous-groupe discret de l'hyperplan* H *de* $\mathbf{R}^{r_1+r_2}$ *formé par les éléments* $(x_1, ..., x_{r_1+r_2})$ *vérifiant*

$$x_1 + ... + x_{r_1} + x_{r_1+1} + ... + x_{r_1+r_2} = 0.$$

Démonstration. — Soit $x \in \mathcal{O}_K^*$. On a $|\mathrm{N}_{K/\mathbf{Q}}(x)| = 1$ et donc $\log(|\mathrm{N}_{K/\mathbf{Q}}(x)|) = 0$. Par ailleurs on a

$$\log(|\mathrm{N}_{K/\mathbf{Q}}(x)| = \log(|\sigma_1(x)|)+...+\log(|\sigma_{r_1}(x)|)+2\log(|\sigma_{r_1+r_2}(x)|)+...+2\log(|\sigma_{r_1+r_2}(x)|).$$

On a donc $\Lambda(\mathcal{O}_K^*) \subset H$.

Le fait que $\Lambda(\mathcal{O}_K^*)$ soit un sous-groupe discret résulte directement du lemme 4.

Corollaire . — *Le groupe* $\Lambda(\mathcal{O}_K^*)$ *est engendré par au plus* $r_1 + r_2 - 1$ *éléments.*
Démonstration. — En effet un sous-groupe discret d'un espace vectoriel réel de dimension n est engendré par au plus n éléments. Par application à H, ce fait on obtient le résultat.

Pour démontrer le théorème des unités, il reste à établir le résultat suivant.

Proposition 2. — *Le groupe* $\Lambda(\mathcal{O}_K^*)$ *contient* $r_1 + r_2 - 1$ *éléments* $\mathbf{Z}$*-linéairement indépendants.*
Démonstration. — Soit f une forme linéaire non nulle sur H. Prolongeons-la en une forme linéaire sur $\mathbf{R}^{r_1+r_2}$ nulle sur $\{0\}^{r_1+r_2-1} \times \mathbf{R}$. Un tel prolongement existe et est unique. On va démontrer qu'il existe une unité x de $\mathcal{O}_K$ telle que $f(\Lambda(x)) \neq 0$, ce qui suffit à démontrer l'indépendance linéaire cherchée.

Pour cela il suffit de trouver deux entiers x_1 et x_2 tels que $f(\Lambda(x_1)) \neq f(\Lambda(x_2))$ et $x_1\mathcal{O}_K = x_2\mathcal{O}_K$. Cette existence est établie si on peut trouver une infinité d'entiers de $\mathcal{O}_K$ d'images distinctes par $f \circ \Lambda$ et de norme bornée puisqu'il n'existe qu'un nombre fini d'idéaux de $\mathcal{O}_K$ de norme bornée (proposition V-3).

Soit α un nombre réel vérifiant

$$\alpha > 2^{d-r_1}(\frac{1}{2\pi})^{r_2}|\mathcal{D}_K|^{1/2}.$$

Pour chaque entier $k \geq 0$ on va trouver un élément $x_k \in \mathcal{O}_K$ tel que $\mathrm{N}_{K/\mathbf{Q}}(x_k) \leq \alpha$ et tel que les images des x_k par $f \circ \Lambda$ soient deux à deux distinctes.

Soit β un nombre réel $> \log(\alpha)\,||f||_1$, où on a posé

$$||f||_1 = \max_{|x_1|\leq 1,...,|x_{r_1+r_2}|\leq 1}|f(x_1, ..., x_{r_1+r_2})|.$$

Soit k un entier > 0. Soit $\Lambda_k = (\log(\lambda_1), ..., \log(\lambda_{r_1+r_2})) \in \mathbf{R}^{r_1+r_2}$ vérifiant les égalités

$$f(\Lambda_k) = 2\beta k \qquad \text{et} \qquad \prod_{i=1}^{r_1}\lambda_i \prod_{i=r_1+1}^{r_1+r_2}\lambda_i^2 = \alpha.$$

Notons X_k le sous-ensemble de l'espace $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ constitué par les $(r_1 + r_2)$-uplets $(x_1, ..., x_{r_1}, z_{r_1+1}, ..., z_{r_1+r_2})$ vérifiant $|x_i| \leq \lambda_i$ et $|z_i| \leq \lambda_i$. C'est un ensemble compact, convexe, symétrique par rapport à 0 et de volume

$$\mathrm{vol}(X_k) = \prod_{i=1}^{r_1} 2|\lambda_i| \prod_{i=r_1+1}^{r_1+r_2} \pi|\lambda_i|^2 = 2^{r_1}\pi^{r_2}\alpha > 2^d 2^{-r_2}|\mathcal{D}_K|^{1/2}.$$

En comparant ce volume à celui du réseau $v_K(\mathcal{O}_K)$, on établit l'existence, grâce à la proposition V-5 (appliquée à $X = X_k$ et $L = v(\mathcal{O}_K)$), d'un élément non nul $x_k \in v_K(\mathcal{O}_K) \cap X_k$. On alors

$$1 \leq |\mathrm{N}_{K/\mathbf{Q}}(x_k)| = \prod_i |\sigma_i(x_k)| \leq \prod_{i=1}^{r_1} \lambda_i \prod_{i=r_1+1}^{r_1+r_2} \lambda_i^2 = \alpha.$$

De plus on a

$$\frac{\lambda_i}{\alpha} \leq \prod_{j=1, j\neq i}^{d} \lambda_j^{-1} \leq |\mathrm{N}_{K/\mathbf{Q}}(x_k)| \prod_{j\neq i} |\sigma_j(x_k)|^{-1} \leq |\sigma_i(x_k)| \leq \lambda_i.$$

On a donc

$$0 \leq \log(\lambda_i) - \log(|\sigma_i(x_k)|) \leq \log(\alpha).$$

Or $(\log(\lambda_i) - \log(|\sigma_i(x_k)|)$ est la i-ième coordonnée de $(\Lambda_k - L(x_k))$. On en déduit les relations

$$|f(\Lambda(x_k)) - 2\beta k| = |f(\Lambda(x_k)) - f(\Lambda_k)| = f(\Lambda(x_k) - \Lambda_k) \leq ||f||_1 \log(\alpha) < \beta,$$

car on a, pour k réel > 0,

$$\mathrm{max}_{|x_1|\leq k, ..., |x_{r_1+r_2}|\leq k} f(x_1, ..., x_{r_1+r_2}) = k||f||_1.$$

Cela entraîne

$$... < f(\Lambda(x_{k-1})) < (2k-1)\beta < f(\Lambda(x_k)) < (2k+1)\beta < f(\Lambda(x_{k+1})) < ...$$

Les $f(\Lambda(x_k))$ sont donc deux à deux distincts et les x_k sont de norme $\leq \alpha$. Cela termine la démonstration de la proposition 2.

Le théorème des unités résulte de la proposition 2, du lemme 7 et du lemme 8 puisqu'on a établi l'existence d'une suite exacte :

$$0 \longrightarrow U_K \longrightarrow \mathcal{O}_K^* \longrightarrow \Lambda(\mathcal{O}_K^*) \longrightarrow 0,$$

où U_K est le sous-groupe cyclique de $\mathcal{O}_K^*$ formé par les racines de l'unité de K, et $\Lambda(\mathcal{O}_K)$ est un groupe isomorphe à $\mathbf{Z}^{r_1+r_2-1}$.

Remarques. — On formulera un énoncé en termes d'idèles qui contient simultanément le théorème des unités et la finitude du nombre de classes.

Le lemme 6 n'est pas contenu dans le théorème des unités. C'est un énoncé dont on aura besoin lors de notre étude des idèles.

Les racines de l'unité de K sont en nombre fini d'après le lemme 5. Ce n'était pas un résultat évident *a priori*. En effet on peut trouver des anneaux de Dedekind qui possèdent une infinité de racines de l'unité. Ce nombre fini de racine de l'unité est, comme le nombre de classe, un invariant important du corps K.

Parmi les unités on a la caractérisation suivante des racines de l'unité dans K : ce sont les élément de K dont toutes les valeurs absolues (*i.e.* archimédiennes et non archimédiennes) sont égales à 1. Cela n'était pas *a priori* évident et résulte des lemme 4 et 5.

Soit $(u_1, ..., u_{r_1+r_2-1})$ un système de générateurs de $\Lambda(\mathcal{O}_K^*)$. Une image réciproque par L de cet élément est un *système fondamental d'unités* de $\mathcal{O}_K^*$. Le volume du réseau $\Lambda(\mathcal{O}_K^*)$ de H est le *régulateur* du corps K. Il interviendra, ainsi que le nombre de classes, le théorème des unités, le nombres de racines de l'unité dans la formule du nombre de classes. De façon plus précise, si on pose $u_i = (\log|(\sigma_1(u_i))|, ..., \log|(\sigma_{r_1+r_2}(u_i))|)$, le régulateur est donné par la formule

$$|\det{}_{1\leq i,j\leq r_1+r_2-1}(\log(|\sigma_j(u_i)|)|.$$

Remarque . — Le régulateur n'est pas en général un nombre algébrique puisqu'il est construit à partir de logarithmes.

4. Les S-unités

Voici une autre caractérisation des unités de K : ce sont les éléments de K^* sur lesquels toutes les valuations discrètes de K s'annulent.

Relâchons cette condition de la façon suivante. Soit S un ensemble de valeurs absolues normalisées de K contenant les valeurs absolues archimédiennes. Rappelons qu'on normalise les places réelles en considérant la valeur absolue usuelle dans $\mathbf{R}$ et qu'on normalise les places complexes en considérant le carré du module. Le groupe K_S des *S-unités* de K est l'ensemble des éléments x de K^* qui vérifient $|x|_v = 1$ pour tout $|.|_v \in S$. Il contient le groupe des unités.

Notons S_∞ l'ensemble des valeurs absolues archimédiennes de K (qui sont au nombre de r_1+r_2 car elles coïncident avec les places complexes à conjugaison près). Les valuations de K définissent des homonorphismes de groupes $K_S \longrightarrow \mathbf{Z}$. En considérant toutes les valuations associées aux valeurs absolues de $S - S_\infty$, on en déduit l'existence d'une suite exacte

$$1 \longrightarrow \mathcal{O}_K^* \longrightarrow K_S \longrightarrow \mathbf{Z}^{(S-S_\infty)} \longrightarrow 0.$$

Il en résulte, en combinant avec le théorème des unités, que K_S est isomorphe au produit d'un groupe cyclique et de $\mathbf{Z}^{|S|-1}$. Considérons l'application $\Lambda_S : K_S \longrightarrow \mathbf{R}^{(S)}$ qui à x

associe $(\log(|x|_v))_{v\in S}$. Soit T un sous-ensemble de S. Considérons la surjection canonique $\pi_T : \mathbf{R}^{(S)} \longrightarrow \mathbf{R}^{(T)}$; on a $\pi_{S_\infty} \circ \Lambda_S = \Lambda$.

L'homomorphisme Λ_S jouit de propriété analogues à celles établies pour Λ dans la section précédente.

PROPOSITION 3. — *Le noyau de Λ_S est constitué par les racines de l'unité de K. L'image de Λ_S est contenue dans l'hyperplan $\pi_{S_\infty}^{-1}(H)$ de $\mathbf{R}^{(S)}$. Le groupe $\Lambda_S(K_S)$ est un sous-groupe discret de $\mathbf{R}^{(S)}$ isomorphe à $\mathbf{Z}^{|S|-1}$.*

Démonstration. — La première assertion est une conséquence du lemme 5, puisque le noyau de Λ_S est contenu dans le noyau de Λ et puisque les valeurs absolues non archimédiennes des racines de l'unité valent toutes 1.

La deuxième assertion résulte de l'identité $\pi_{S_\infty} \circ \Lambda_S = \Lambda$.

La troisième assertion résulte du fait que $\pi_{S-S_\infty} \circ \Lambda_S(K_S)$ est un réseau de $\mathbf{R}^{(S-S_\infty)}$ (la projection sur chaque composante est isomorphe à $\mathbf{Z}$) et du lemme 6.

VII
Topologie sur les corps

1. Complétion d'un corps

Rappelons brièvement comment on construit le complété d'un corps muni d'une valeur absolue. Cette construction suit le modèle de la construction de $\mathbf{R}$ à partir de $\mathbf{Q}$.

Soit K un corps muni d'une valeur absolue $|.|$. L'application $(x, y) \mapsto |x - y|$ est une distance sur K. Considérons l'ensemble A formé par les suites de Cauchy à valeurs dans K. Rappelons qu'une suite de Cauchy $(u_n)_{n\geq 0}$ vérifie que pour tout nombre réel $\epsilon > 0$ il existe un entier $k > 0$ tel que $|u_n - u_m| < \epsilon$ pour tous $n > k$, $m > k$. En particulier une suite de Cauchy est de valeur absolue bornée.

Lemme 1. — *L'ensemble des suites de Cauchy est un sous-anneau de l'anneau des suites à valeurs dans* K.
Démonstration. — Il faut vérifier que le produit et la somme de deux suites de Cauchy est une suite de Cauchy. Soient $(u_n)_{n\geq 0}$ et $(v_n)_{n\geq 0}$ deux suites de Cauchy majorées respectivement en valeur absolue par les nombres réels positifs U et V. Vérifions que le produit de ces deux suites est une suite de Cauchy. Cela résulte de l'inégalité triangulaire et de la multiplicativité de la valeur absolue :

$$|u_n v_n - u_m v_m| = |(u_n - u_m)v_n - u_m(v_n - v_m)| \leq V|(u_n - u_m)| + U|(v_n - v_m)|.$$

Le fait que la somme de deux suites de Cauchy est de Cauchy est laissé au lecteur.

Lemme 2. — *Le sous-groupe* I *de* A *formé par les suites qui convergent vers* 0 *est un idéal de* A.
Démonstration. — C'est un sous-groupe de A. Le produit d'une suite qui converge vers 0 et d'une suite de Cauchy (donc bornée) converge vers 0.

Lemme 3. — *L'anneau* A/I *est un corps.*
Démonstration. — Il suffit de vérifier que toute suite de Cauchy qui ne converge pas vers 0 est inversible dans A/I. Soit $(u_n)_{n\geq 0}$ une telle suite. Elle est non nulle à partir d'un certain rang. Considérons la suite $(v_n)_{n\geq 0}$, définie par $v_n = u_n$ si $u_n \neq 0$ et $v_n = 1$ sinon. La suite $(u_n - v_n)_{n\geq 0}$ appartient à I. La suite v_n est minorée en valeur absolue par un nombre réel $t > 0$ en valeur absolue car c'est une suite de Cauchy qui ne converge pas vers 0. La suite v_n est inversible dans A. Son inverse est une suite de Cauchy ; cela se voit grâce à l'inégalité

$$|\frac{1}{v_n} - \frac{1}{v_m}| = |v_n - v_m||\frac{1}{v_n v_m}| \leq \frac{1}{t^2}|v_n - v_m|.$$

La suite $(u_n v_n - 1)_{n\geq 1}$ appartient à I puisqu'elle est nulle à partir d'un certain rang. La suite $(1/v_n)_{n\geq 0}$ est donc l'inverse de de la suite $(u_n)_{n\geq 0}$ dans A/I.

Le corps $\hat{K} = A/I$ est le *complété* de K pour la valeur absolue $|.|$. L'application qui à un élément x de K associe la suite constante égale à x définit un plongement (c'est-à-dire un homomorphisme de corps) $K \longrightarrow \hat{K}$. En particulier c'est une place de K dans $\hat{K}$.

Lemme 4. — *La valeur absolue* $|.|$ *se prolonge en une valeur absolue sur* $\hat{K}$. *De plus* $\hat{K}$ *est complet pour la topologie définie par cette valeur absolue.*
Démonstration. — Soit $u = (u_n)_{n\geq 0}$ une suite de Cauchy à valeurs dans K. L'application $K \longrightarrow \mathbf{R}$ qui à x associe $|x|$ est continue. La suite $(|u_n|)_{n\geq 0}$ est donc une suite de Cauchy. Puisque $\mathbf{R}$ est complet, elle converge vers une limite $l \in \mathbf{R}$. Posons $|u| = l$. Cette notation est compatible avec le plongement $K \longrightarrow \hat{K}$. On vérifie sans peine que $x \mapsto |x|$ définit bien une valeur absolue sur $\hat{K}$.

Pour voir que $\hat{K}$ est complet, considérons une suite de Cauchy $(u_k)_{k\geq 0}$ à valeurs dans $\hat{K}$. On peut représenter u_k dans A par une suite de Cauchy $(u_{k,n})_{n\geq 0}$ à valeurs dans K telle que $|u_{k,n} - u_k| < \min(\frac{1}{k}, \frac{1}{n})$ pout tout couple (n, k). La suite $(u_{n,n})_{n\geq 0}$ à valeurs dans K est une suite de Cauchy ; cela se vérifie grâce à l'inégalité

$$|u_{k,k} - u_{q,q}| \leq |u_{k,k} - u_k| + |u_k - u_q| + |u_q - u_{q,q}|,$$

et au fait que $(u_k)_{k\geq 0}$ est une suite de Cauchy. La suite $(u_{n,n})_{n\geq 0}$ converge donc dans $\hat{K}$. Sa limite est aussi la limite de $(u_k)_{k\geq 0}$ puisqu'on a $|u_{k,k} - u_k| < \frac{1}{k}$.

En utilisant la continuité de la valeur absolue, on vérifie que si la valuation $|.|$ est non archimédienne sur K, il en est de même pour le prolongement de $|.|$ à $\hat{K}$.

2. Le cas des anneaux de valuation discrète

Soit A un anneau de valuation discrète. Notons K son corps des fractions et v la valuation associée.

Soit a un nombre réel > 1. Rappelons que la valuation définit une valeur absolue sur K, dont la classe d'équivalence ne dépend pas de a, par la formule

$$|x|_a = a^{-v(x)}.$$

Lorsque $A/\mathcal{P}$ est fini on dispose d'une valeur privilégiée pour a. C'est $a = |A/\mathcal{P}|$. On dit que la valeur absolue correspondante est la *valeur absolue normalisée* de K.

Notons $\mathcal{P}$ l'idéal maximal de A. Le *complété* $\mathcal{P}$*-adique* de A est par définition l'ensemble $A_\mathcal{P}$ formé par les éléments $(a_1, ..., a_n, ...) \in A/\mathcal{P} \times A/\mathcal{P}^2 \times ... \times A/\mathcal{P}^n \times ...$, vérifiant pour tout $n \geq 1$ l'égalité $a_{n+1} + \mathcal{P}^n = a_n$. C'est la *limite projective*

$$A_\mathcal{P} = \varprojlim A/\mathcal{P}^n.$$

C'est un sous-anneau de $A/\mathcal{P} \times A/\mathcal{P}^2 \times ... \times A/\mathcal{P}^n \times ...$

Lemme 5. — *L'anneau* $A_\mathcal{P}$ *est intègre.*
Démonstration. — Soient $a = (\alpha_1 + \mathcal{P}, ..., \alpha_n + \mathcal{P}^n, ...)$ et $b = (\beta_1 + \mathcal{P}, ..., \beta_n + \mathcal{P}^n, ...)$ deux éléments de $A_\mathcal{P}$ tels que $ab = 0$. On a $\alpha_n\beta_n \in \mathcal{P}^n$ pour tout n. On a donc $\alpha_{2n} \in \mathcal{P}^n$ ou

$\beta_{2n} \in \mathcal{P}^n$, et donc $\alpha_n \in \mathcal{P}^n$ ou $\beta_n \in \mathcal{P}^n$ pour tout n. Supposons qu'il existe $n \geq 1$ tel que $\alpha_n \notin \mathcal{P}^n$. Alors pour tout $m \geq n$ on a $\alpha_m \notin \mathcal{P}^m$. On donc $\beta_m \in \mathcal{P}^m$ pour tout $m \geq 1$.

On a un homomorphisme d'anneaux $A \longrightarrow A_{\mathcal{P}}$ déduit diagonalement des homomorphismes canoniques $A \longrightarrow A/\mathcal{P}^n$: cet homomorphisme est donné par

$$a \mapsto (a + \mathcal{P}, a + \mathcal{P}^2, ..., a + \mathcal{P}^n, ...).$$

Lemme 6. — *Cet homomorphisme $A \longrightarrow A_{\mathcal{P}}$ est injectif.*
Démonstration. — Cela résulte immédaitement du fait que $\cap_{n\geq 1}\mathcal{P}^n = \{0\}$.

Le lemme 6 permet donc d'identifier A à un sous-anneau de $A_{\mathcal{P}}$. Notons $K_{\mathcal{P}}$ le corps des fractions de $A_{\mathcal{P}}$. Le corps K s'identifie donc à un sous-corps de $K_{\mathcal{P}}$. Soit $a = (\alpha_1 + \mathcal{P}, ..., \alpha_n + \mathcal{P}^n, ...)$ un élément non nul de $A_{\mathcal{P}}$. La suite d'entiers $(v(\alpha_n))_{n\geq 1}$ est stationnaire (puisque $a \neq 0$ on a $\alpha_n \notin \mathcal{P}^n$ pour n assez grand). Notons sa valeur d'adhérence $v(a)$. La fonction $a \mapsto v(a)$ coïncide avec la valuation v sur A, via le plongement $A \longrightarrow A_{\mathcal{P}}$.

Lemme 7. — *Soient a et b deux éléments non nuls de $A_{\mathcal{P}}$. On a $v(ab) = v(a) + v(b)$ et $v(a + b) \geq \min(v(a), v(b))$.*
Démonstration. — Posons $a = (\alpha_1 + \mathcal{P}, ..., \alpha_n + \mathcal{P}^n, ...)$ et $b = (\beta_1 + \mathcal{P}, ..., \beta_n + \mathcal{P}^n, ...)$. Il existe un entier $n_0 > 0$ tel que pour tout entier $n \geq n_0$ on ait $v(\alpha_n) = v(a)$ et $v(\beta_n) = v(b)$. On a donc pour tout entier $n \geq n_0$ les relations $v(\alpha_n\beta_n) = v(\alpha_n)v(\beta_n) = v(a)v(b)$ et $v(\alpha + \beta) = v(\alpha_n + \beta_n) \geq \min(v(\alpha_n, \beta_n))$. On a donc $v(ab) = v(a) + v(b)$ et $v(a + b) \geq \min(v(a), v(b))$.

La fonction v se prolonge en une fonction encore notée $v : K_{\mathcal{P}}^* \longrightarrow \mathbf{Z}$ par la formule $v(a/b) = v(a) - v(b)$ pour $(a, b) \in (A_{\mathcal{P}} - \{0\})^2$. Ce prolongement est bien défini car on a $v(ac/bc) = v(ac) - v(bc) = v(a) + v(c) - v(b) - v(c) = v(a/b)$ pour $(a, b, c) \in (A_{\mathcal{P}} - \{0\})^3$. La fonction v sur $K_{\mathcal{P}}$ coïncide avec la valuation v sur K identifié à un sous-corps de $K_{\mathcal{P}}$. Il n'y a donc pas d'ambiguïté dans la définition.

Proposition 1. — *La fonction v défini une valuation discrète sur $K_{\mathcal{P}}$. L'anneau $A_{\mathcal{P}}$ est un anneau de valuation discrète d'idéal maximal $\mathcal{P}A_{\mathcal{P}}$.*
Démonstration. — Il suffit de vérifier que $v : K_{\mathcal{P}}^* \longrightarrow \mathbf{Z}$ est un homomorphisme surjectif de groupes et qu'on a l'inégalité $v(a + b) \geq \min(v(a), v(b))$. La surjectivité résulte du fait que v est surjective sur K^*. On a, en utilisant le lemme 7 et la définition de v sur $K_{\mathcal{P}}$,

$$v((a/b)(a'/b')) = v(aa'/bb') = v(aa') - v(bb') = v(a) + v(a') - v(b) - v(b') = v(a/b) + v(a'/b').$$

Cela prouve que v est un homomorphisme de groupes.

Soient $a = (\alpha_1 + \mathcal{P}, ..., \alpha_n + \mathcal{P}^n, ...)$ et $b = (\beta_1 + \mathcal{P}, ..., \beta_n + \mathcal{P}^n, ...)$ deux éléments de $K_{\mathcal{P}} - \{0\}$. Soit $c \in (A_{\mathcal{P}} - \{0\})$ tel que ac et bc soient éléments de $A_{\mathcal{P}}$. On a, en utilisant le lemme 7,

$$v(a + b) = v(ac + bc) - v(c) \geq \min(v(ac), v(bc)) - v(c)$$
$$= \min(v(a), v(b)) + v(c) - v(c) = \min(v(a), v(b)).$$

La fonction v est bien une valuation sur $K_{\mathcal{P}}$.

L'ensemble $\{x \in K_{\mathcal{P}}/v(x) \geq 0\}$ coïncide avec $A_{\mathcal{P}}$ qui est donc un sous-anneau de valuation discrète de $K_{\mathcal{P}}$. L'idéal maximal de $A_{\mathcal{P}}$ est $\{x \in K_{\mathcal{P}}/v(x) \geq 1\}$ qui n'est autre que $\mathcal{P}A_{\mathcal{P}}$. Cela achève de démontrer la proposition.

Notons $\hat{K}$ le complété de K pour la valeur absolue $|.|$ associée à l'idéal $\mathcal{P}$. Soit $a = (\alpha_1 + \mathcal{P}, ..., \alpha_n + \mathcal{P}^n, ...) \in A_{\mathcal{P}}$. La suite $(\alpha_n)_{n\geq 1}$ est une suite de Cauchy de K (cela résulte immédiatement des propriétés de compatibilité vérifiées par les α_n). On a donc une application $A_{\mathcal{P}} \longrightarrow \hat{K}$ qui à a associe la classe de $(\alpha_n)_{n\geq 1}$. C'est un homomorphisme d'anneaux. Cet homomorphisme est injectif ; en effet son noyau est constitué par les éléments $a = (\alpha_1 + \mathcal{P}, ..., \alpha_n + \mathcal{P}^n, ...) \in A_{\mathcal{P}}$ tels que pour tout $k \geq$ on ait $\alpha_n \in \mathcal{P}^k$ pour n assez grand et donc $\alpha_n \in \mathcal{P}^k$ pour tout n. Puisque $\hat{K}$ est un corps, cela entraîne que l'homomorphisme $\phi : A_{\mathcal{P}} \longrightarrow \hat{K}$ se prolonge de façon unique en un homomorphisme de corps encore noté $\phi : K_{\mathcal{P}} \longrightarrow \hat{K}$ grâce à la formule $\phi(a/b) = \phi(a)/\phi(b)$.

Proposition 2. — *Toute suite de Cauchy (pour la valeur absolue $\mathcal{P}$-adique) à valeurs dans K converge dans $K_{\mathcal{P}}$. Les corps $\hat{K}$ et $K_{\mathcal{P}}$ sont donc isomorphes.*
Démonstration. — Soit $(u_n)_{n\geq 1}$ une suite de Cauchy de K. Supposons quelle ne converge pas vers 0. Puisque c'est une suite de Cauchy on a $u_n - u_m \in A$ pour presque n et m assez grands. Il existe donc $v_0 \in K$ tel que $u_n \in v_0 + A$ pour presque tout n. Soit $c \in A - \{0\}$ tel que $cv_0 \in A$. La suite $(cu_n)_{n\geq 1}$ est de Cauchy. Quitte à remplacer un nombre fini de termes par 0, on peut supposer qu'elle est à valeurs dans A. On s'est donc ramené au cas où la suite $(u_n)_{n\geq 1}$ est à valeurs dans A.

Soit k un entier ≥ 1. On a $u_n - u_m \in \mathcal{P}^k$ pour m et n assez grands. Il existe donc $v_k \in A$ tel que $u_n \in v_k + \mathcal{P}^k$ pour presque tout n. Posons $v = (v_1 + \mathcal{P}, ..., v_k + \mathcal{P}^k, ...)$. C'est un élément de $A_{\mathcal{P}}$. La suite $(u_n)_{n\geq 1}$ converge vers v.

Par construction un élément de $\hat{K}$ est la limite d'une suite de Cauchy à valeurs dans K. Le plongement $K_{\mathcal{P}} \longrightarrow \hat{K}$ est donc un isomorphisme.

Exemple . — Soit p un nombre premier. Lorsque $A = \mathbf{Z}_{(p)}$, l'anneau $A_{\mathcal{P}}$ est noté $\mathbf{Z}_p$. C'est *l'anneau des entiers p-adiques*. Son corps des fractions est le corps $\mathbf{Q}_p$ des *nombres p-adiques*.

Les boules ouvertes de centre de $x \in K_{\mathcal{P}}$ pour la distance définie par la valeur absolue coïncident avec les ensembles de la forme $x + \mathcal{P}^n A_{\mathcal{P}}$, avec n entier ≥ 0. Elle sont donc fermées. Tout élément d'une boule ouverte de $K_{\mathcal{P}}$ en est un centre. Le singleton $\{x\}$ est une boule fermée non ouverte de $K_{\mathcal{P}}$.

Soit π une uniformisante de $\mathcal{P}$ (c'est-à-dire un élément de A tel que $v(\pi) = 1$). C'est aussi une uniformisante de $\mathcal{P}A_{\mathcal{P}}$. Soit $(a_n)_{n\geq 0}$ une suite d'éléments de A. La suite $(a_0 + a_1\pi + a_2\pi^2 + ... + a_n\pi^n)_{n\geq 0}$ converge vers un élément noté

$$\sum_{n=0}^{\infty} a_n \pi^n \in A_{\mathcal{P}}.$$

Proposition 3. — *Soit R un système de représentants de $A/\mathcal{P}$. Tout élément non nul de $K_\mathcal{P}$ s'écrit de façon unique sous la forme*

$$\sum_{n=k}^{\infty} a_n \pi^n,$$

où les a_n sont éléments de R et $k \in \mathbf{Z}$ avec $a_k \neq 0$.

Démonstration. — Quitte à multiplier par une puissance de π il suffit de d'étudier la proposition pour les éléments de $A_\mathcal{P}$.

Soient $(a_n)_{n\geq 0}$ et $(a'_n)_{n\geq 0}$ deux suites de R telles que $\sum_{n=0}^{\infty} a_n\pi^n = \sum_{n=0}^{\infty} a'_n\pi^n$. On a donc $\sum_{n=0}^{\infty} a_n\pi^n + \mathcal{P}^k = \sum_{n=0}^{\infty} a'_n\pi^n + \mathcal{P}^k$ pour tout $k \geq 0$. Pour $k = 1$ cela donne $a_0 + \mathcal{P} = a'_0 + \mathcal{P}$ et donc $a_0 = a'_0$. On démontre par une récurrence facile $a_n = a'_n$ pour tout $n \geq 0$. Cela donne l'unicité de l'écriture.

Soit $x = (\alpha_1+\mathcal{P}, ..., \alpha_n+\mathcal{P}^n, ...) \in A_\mathcal{P}$. Construisons les a_n par récurrence. Définissons a_0 comme le représentant de $\alpha_0 + \mathcal{P}$ dans R. Définissons a_{n+1} comme le représentant de $(\alpha_{n+1} - \sum_{k=0}^{n} a_k\pi^k)/\pi^n$ dans R. On vérifie qu'on a $x = \sum_{n=0}^{\infty} a_n\pi^n$.

Cela prouve qu'un élément de $A_\mathcal{P}$ s'écrit de façon unique sous la forme $\sum_{n=0}^{\infty} a_n\pi^n$. Le résutat s'en suit facilement.

Lorsque $A = \mathbf{Z}_p$, on peut choisir pour système de représentants de $\mathbf{Z}_p/p\mathbf{Z}_p \simeq \mathbf{Z}/p\mathbf{Z}$ l'ensemble $\{0, ..., p-1\}$, ou mieux encore l'ensemble constitué de 0 et des racines $(p-1)$-ièmes de l'unité de $\mathbf{Z}_p$. L'anneau $\mathbf{Z}_p$ possède $(p-1)$ racines $(p-1)$-ièmes de l'unité puisque les groupes $(\mathbf{Z}/p^n\mathbf{Z})^* \simeq (\mathbf{Z}/p^{n-1}\mathbf{Z})\times\mathbf{Z}/(p-1)\mathbf{Z}$ possèdent tous $(p-1)$ racines $(p-1)$-ièmes de l'unité.

Proposition 4. — *Supposons que le corps résiduel $A/\mathcal{P}$ soit fini. Le corps $K_\mathcal{P}$ est localement compact pour la topologie définie par la valeur absolue $\mathcal{P}$-adique. L'anneau $A_\mathcal{P}$ est un sous-ensemble compact de $K_\mathcal{P}$.*

Démonstration. — La deuxième assertion entraîne la première puisque $A_\mathcal{P}$ est une boule ouverte. En effet, soit $x \in K_\mathcal{P}$. La boule ouverte $x + A_\mathcal{P}$ est un voisinage de x ; elle est compacte lorsque $A_\mathcal{P}$ est compact.

Démontrons que $A_\mathcal{P}$ est compact. Soit $(U_i)_{i\in I}$ un recouvrement de $A_\mathcal{P}$ par des ouverts. Supposons qu'on ne puisse pas extraire un sous-recouvrement fini du recouvrement formé par les U_i. Soit $R = \{r_1, r_2, ..., r_k\}$ un système de représentants de $A/\mathcal{P}$. Chacun des ensembles $r_j + \mathcal{P}$ est recouvert par les ouverts U_i. Il existe donc $a_0 \in R$ tel qu'on ne puisse extraire un sous-recouvrement fini de $a_0+\mathcal{P}$. Soit π une uniformisante de $A_\mathcal{P}$. Les $a_0+r_j\pi$ forment un sytème de représentants de $(a_0 + \mathcal{P})/\mathcal{P}^2$. Il existe donc $a_1 \in R$ tel qu'on ne puisse extraire un sous-recouvrement fini de $a_0 + a_1\pi + \mathcal{P}^2$. En itérant cette construction, on établit l'existence d'une suite $(a_i)_{i\geq 0}$ d'éléments de R telle que pour tout n la boule ouverte $B_n = a_0 + a_1\pi + A_2\pi^2 + ... + a_n\pi^n + \mathcal{P}^{n+1}$ n'est pas recouverte par un nombre fini de U_i. Considérons l'élément $\alpha = \sum_{n=0}^{\infty} a_n\pi^n$ de $A_\mathcal{P}$. C'est un centre de toutes les boules B_n. Il appartient à l'un des ouverts U_{i_0}. Il existe donc une boule ouverte contenant α et qui est contenue dans U_{i_0}. Il existe donc $n \geq 0$ tel que la boule B_n soit contenue dans U_{i_0}. Cela contredit notre hypothèse.

3. Extensions de corps complets

Soit A un anneau de valuation discrète de corps des fractions K complet pour la topologie définie par la valuation discrète v. Soit $L|K$ une extension finie et séparable. Notons B la clôture intégrale de A dans L. Notons $\mathcal{Q}$ l'idéal premier non nul de A.

Nous allons voir que la structure topologique de L est imposée par ces données. Cela repose de façon essentielle sur le fait que K est complet.

PROPOSITION 5. — *L'anneau B est un anneau de valuation discrète et L est complet pour la topologie définie par cette valuation.*

Démonstration. — On sait que B est un anneau de Dedekind puisque A est un anneau de Dedekind. Soit $\mathcal{P}$ un idéal premier de B. Notons w la valuation correspondante. Le couple (L, w) est un K-espace vectoriel qui est aussi un espace topologique. L'anneau de valuation discrète associé à w coïncide avec l'ensemble des éléments x de L tels que x^{-k} ne tende pas vers 0 lorsque $k \to \infty$. Il est donc déterminé par la structure d'espace topologique de L.

Rappelons qu'un *espace vectoriel topologique sur K* est un espace vectoriel E sur K, muni d'une topologie telle que l'addition $E \times E \longrightarrow E$ soit continue et telle que l'application $K \times E \longrightarrow E$ qui à (λ, e) associe λe soit continue (les produits sont munis ici de la topologie produit).

Lemme 8. — *Soit E un espace vectoriel topologique séparé de dimension finie n sur un corps complet K non discret. Soit $(e_i)_{i\in\{1,2,...,n\}}$ une base de E sur K. La bijection linéaire $K^n \longrightarrow E$ qui à $(\lambda_1, ..., \lambda_n)$ associe $\lambda_1 e_1 + ... + \lambda_n e_n$ est un isomorphisme d'espaces topologiques.*

En particulier E est isomorphe à K^n comme espace vectoriel topologique et est donc complet.

Démonstration. — Démontrons-le d'abord dans le cas où $n = 1$. L'application $\phi_1 : K \longrightarrow E$ qui à λ associe λe_1 est bijective et continue par hypothèse. Il reste à prouver que sa réciproque est continue c'est-à-dire que l'image d'un ouvert par ϕ_1 est un ouvert. Il suffit pour cela de prouver que l'image de toute boule ouverte de centre 0 est un voisinage de 0 (on utilise l'additivité de ϕ_1). Soit B la boule ouverte de centre 0 et de rayon $\alpha > 0$ de K. Soit $\lambda_0 \in K$ tel que $|\lambda_0| < \alpha$. Un tel scalaire existe car K n'est pas discret. Soit U un ouvert de E contenant 0 mais pas $\lambda_0 e_1$ (il en existe puisque E est séparé). Considérons l'application $\phi : K \times E \longrightarrow E$ qui à (λ, e) associe λe. Elle est continue par hypothèse. L'image réciproque de U par ϕ est un ouvert contenant $(0, 0)$. Elle contient donc un ouvert de la forme $B' \times W$, où B' est une boule ouverte de K de centre 0 et où W est un ouvert de E contenant 0. L'ensemble $V = \phi(B' \times W)$ est un ouvert de $E = \cup_{\lambda\in B'} \lambda W$ est une réunion d'ouverts. Il contient 0 mais pas $\lambda_0 e_1$. De plus B' et donc aussi V sont stables par multiplication par les scalaires de valeur absolue ≤ 1. Vérifions qu'on a $V \subset \phi_1(B)$ c'est-à-dire $\phi_1^{-1}(V) \subset B$, ce qui achèvera la démonstration. Soit un élément de V qui s'écrit sous la forme λe_1, avec $\lambda \in K$. Comme V est stable par multiplication par les scalaires de valeur absolue ≤ 1 et ne contient pas $\lambda_0 e_1 = (\lambda_0/\lambda)\lambda e_1$, on a $|\lambda_0/\lambda| > 1$ et donc $|\lambda| < \alpha$ si bien qu'on a $\lambda = \phi_1^{-1}(\lambda e_1) \in B$.

Démontrons maintenant le lemme par récurrence sur n. On vient de voir le cas où $n = 1$. Considérons l'hyperplan H de E engendré par les $(n-1)$ premiers vecteurs de la

base. Par hypothèse de récurrence, il est isomorphe à K^{n-1} comme espace topologique. Il est donc muni d'une distance $|.|$. Comme K est complet, on en déduit que K^{n-1} et donc H sont complets. Soit $(x_n)_{n\geq 0}$ une suite à valeurs dans H qui converge vers $x \in E$. Montrons que la suite $|x_n|$ est non bornée. Si elle l'était, quitte à extraire une sous-suite, on pourrait supposer que $|x_n|$ tend vers l'infini lorsque n tend vers l'infini. La suite de terme général

$$\frac{|x_n|^{1/2}}{(1+|x_n|)}x_n = \frac{|x_n|^{1/2}}{(1+|x_n|)}x + \frac{|x_n|^{1/2}}{(1+|x_n|)}(x_n - x)$$

convergerait alors vers 0, puisque les deux termes du membres de droite convergent vers 0. Cela contredit le fait que la suite de terme général $|x_n|$ est bornée. La suite $(x_n)_{n\geq 0}$ est donc à valeurs dans un compact de H, si bien qu'elle admet une valeur d'adhérence dans H qui ne peut être que x. On a donc $x \in H$. Cela prouve que H est fermé dans E et donc que E/H est un espace séparé. La surjection canonique $E \longrightarrow E/H$ est donc continue. Notons D la droite de E engendrée par e_n. C'est un espace séparé puisque $\{0\}$, qui est l'intersection des fermés H et D, est fermé dans E. La droite D est donc isomorphe à K comme espace topologique d'après l'étude du cas $n = 1$. Pour prouver que l'isomorphisme d'espaces vectoriels $E \simeq H \times D$ (déduit de la somme directe), est un isomorphisme d'espaces topologiques il suffit de vérifier que c'est une application continue (la continuité de l'inverse est claire). Comme H est isomorphe, en tant qu'espace vectoriel topologique, à un produit de $n-1$ espaces de dimension 1 (tous isomorphes à K, et donc séparés), l'espace E est linéairement isomorphe à un produit de n espaces séparés de dimension 1. Pour prouver que cet isomorphisme est continu il suffit de vérifier que la projection sur chacun des facteurs de dimension 1 est continue. Cela résulte de l'étude du cas $n = 1$ en tenant compte du fait que chacun de ces facteurs est séparé. Cela achève de prouver le lemme.

Revenons à la démonstration de la proposition. Le K-espace vectoriel L muni de sa topologie est un espace vectoriel topologique, puisque l'addition et la multiplication sont continues dans L. Le corps K étant complet, il n'est pas discret puisque 0 n'est pas isolé dans K. Par application du lemme 8, L muni de la topologie métrique (et donc séparée) définie par la distance associée à w est isomorphe à K^n comme espace topologique. La topologie de L ainsi considérée est donc indépendante de w.

Il n'y a donc qu'une seule valuation discrète sur L à équivalence près qui prolonge v (plus précisément dont la topologie associée prolonge la topologie associée à v) et donc un seul idéal premier de B divisant $\mathcal{Q}$.

Remarques. — L'hypothèse de complétude est nécessaire dans l'énoncé du lemme 8, comme le montre le cas où $K = \mathbf{Q}$ et où $E = \mathbf{Q} + \mathbf{Q}\sqrt{2} \subset \mathbf{R}$ (la topologie de E est induite par celle de $\mathbf{R}$). En effet, dans ce cas $\mathbf{Q}$ est partout dense dans E mais $\mathbf{Q}$ n'est pas partout dense dans $\mathbf{Q}^2$ pour la topologie produit. On n'a donc pas d'isomorphisme topologique entre E et $\mathbf{Q}^2$.

L'énoncé du lemme 8 est encore valable si $K = \mathbf{R}$ ou $\mathbf{C}$. Il en résulte qu'il n'existe qu'une seule extension à $\mathbf{C}$ d'une valeur absolue de $\mathbf{R}$.

La démonstration du lemme 8 serait légèrement plus simple si on avait tenu compte du fait que la topologie de E est donnée par une distance dans l'application qui nous intéresse

(*i.e.* $E = L$).

COROLLAIRE 1. — *On a, en notant respectivement e et f l'indice de ramification et le degré résiduel en l'idéal premier $\mathcal{P}$ de B qui divise $\mathcal{Q}$,*

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

Démonstration. — C'est un cas particulier de la formule générale pour les anneaux de Dedekind reliant degré de l'extension d'une part au degré résiduel et à l'indice de ramification d'autre part (voir la leçon sur les études locales des extensions de corps), en tenant compte du fait qu'il n'existe qu'un seul idéal premier de B qui divise $\mathcal{Q}$.

COROLLAIRE 2. — *Deux éléments de L conjugués sur K ont même valuation.*
Démonstration. — On peut supposer, quitte à agrandir L, que l'extension $L|K$ est galoisienne. Soit $\sigma \in \mathrm{Gal}(L/K)$. Notons w l'unique valuation de L qui prolonge v. On obtient une autre valuation w' de L qui prolonge v en posant $w' = w \circ \sigma$ (en effet w' vérifie les conditions additives et multiplicatives demandées au valuations). Cette dernière n'est autre que w en raison de l'unicité de la valuation de L qui prolonge v (proposition 1). Soit $x \in L$. Les conjugués de x sont de la forme $\sigma(x)$ pour $\sigma \in \mathrm{Gal}(L/K)$. Ils sont donc tous de même valuation.

COROLLAIRE 3. — *L'unique valuation w de L qui prolonge v est donnée par la formule*

$$w(x) = \frac{1}{f} v(\mathrm{N}_{L/K}(x)).$$

Démonstration. — On peut se ramener au cas où l'extension $L|K$ est galoisienne. En effet, soit une extension finie $M|L$ telle que $M|K$ soit galoisienne. La formule du corollaire 3 se déduit des formules relatives aux extensions galoisiennes $M|K$ et $M|L$.

Supposons donc que $L|K$ soit galoisienne. D'après le corollaire 2, on a, pour tout $x \in L$,

$$w(x) = \frac{1}{[L : K]} w(\mathrm{N}_{L/K}(x)) = \frac{1}{fe} w(\mathrm{N}_{L/K}(x)).$$

Soit π une uniformisante de $\mathcal{Q}$. On a $v(\pi) = 1$, $w(\pi) = e$ (puisque $(\pi)B = \mathcal{Q}B = \mathcal{P}^e$) et $v(\mathrm{N}_{L/K}(\pi)) = [L : K] = ef$. On en déduit la formule cherchée pour $x = \pi$. La formule générale s'en déduit facilement en écrivant $\mathrm{N}_{L/K}(x)$ comme une puissance de π multipliée par une unité de A.

4. Extensions de complétions d'anneaux de valuation discrète

Soit A un anneau de valuation discrète de corps des fractions K. Soit L/K une extension finie et séparable de degré n. Notons $\mathcal{Q}$ l'idéal premier non nul de A et B la

clôture intégrale de A dans L. Pour chaque idéal premier $\mathcal{P}$ de B divisant $\mathcal{Q}$ notons $K_\mathcal{Q}$ et $L_\mathcal{P}$ les complétés de K et L pour les valeurs absolues associées à $\mathcal{Q}$ et $\mathcal{P}$.

PROPOSITION 6. — *L'extension $L_\mathcal{P}/K_\mathcal{Q}$ est de degré $e_\mathcal{P} f_\mathcal{P}$. Il existe une unique valuation de $L_\mathcal{P}$ qui prolonge la valuation de $K_\mathcal{Q}$.*

On a un isomorphisme continu de $K_\mathcal{Q}$-espaces vectoriels ϕ :

$$L \otimes_K K_\mathcal{Q} \simeq \prod_{\mathcal{P}|\mathcal{Q}} L_\mathcal{P},$$

déduit des injections canoniques diagonales $L \longrightarrow \prod_\mathcal{P} L_\mathcal{P}$ et $K_\mathcal{Q} \longrightarrow \prod_{\mathcal{P}|\mathcal{Q}} L_\mathcal{P}$.
Démonstration. — Les deux premières assertions résultent directement de ce qui précède (proposition 5 et ses corollaires).

Pour prouver la dernière assertion, remarquons que l'image diagonale de L dans $\prod_\mathcal{P} L_\mathcal{P}$ est dense d'après le lemme d'approximation. Par conséquent l'image de ϕ est dense dans $\prod_\mathcal{P} L_\mathcal{P}$. Comme $L \otimes_K K_\mathcal{Q}$ est isomorphe à $K_\mathcal{Q}^{[L:K]}$ en tant que $K_\mathcal{Q}$-espace vectoriel topologique (lemme 8), c'est un espace complet. Son image par ϕ est un espace complet, donc fermé, car ϕ est une application continue. Elle est donc égale à $\prod_{\mathcal{P}|\mathcal{Q}} L_\mathcal{P}$. L'application $K_\mathcal{Q}$-linéaire ϕ est surjective car d'image dense. Elle est donc bijective puisque ses espaces de départ et d'arrivée sont tous les deux des $K_\mathcal{Q}$-espaces vectoriels de dimension $[L : K]$.

COROLLAIRE 1. — *Supposons que l'extension $L|K$ soit galoisienne. Soit $\mathcal{P}$ un idéal premier de L au dessus de $\mathcal{Q}$. Notons $D_\mathcal{P}$ le groupe de décomposition en $\mathcal{P}$ de l'extension $L|K$. Tout élément σ de $D_\mathcal{P}$ se prolonge par continuité en un élément $\hat{\sigma}$ de* $\mathrm{Gal}(L_\mathcal{P}/K_\mathcal{Q})$. *L'application $\sigma \mapsto \hat{\sigma}$ est un isomorphisme de groupes*

$$D_\mathcal{P} \simeq \mathrm{Gal}(L_\mathcal{P}/K_\mathcal{Q}).$$

Démonstration. — Un élément de $D_\mathcal{P}$ est une application continue $L \longrightarrow L$ pour la topologie $\mathcal{P}$-adique puisqu'il laisse stable $\mathcal{P}$ et donc toute boule ouverte. L'application $\sigma \mapsto \hat{\sigma}$ est un homomorphisme injectif de groupes puisque L est un sous-corps de son complété. Comme les ordres des groupes $D_\mathcal{P}$ et $\mathrm{Gal}(L_\mathcal{P}/K_\mathcal{Q})$ sont égaux, il s'agit bien d'un isomorphisme.

COROLLAIRE 2. — *Soit $x \in L$. Le polynôme caractéristique de l'endomorphisme du K-espace vectoriel L qui à y associe xy est égal au produit pour $\mathcal{P}$ idéal premier divisant $\mathcal{Q}$ des polynômes caractéristiques des endomorphismes des $K_\mathcal{Q}$-espaces vectoriels $L_\mathcal{P}$ qui à y associe xy.*

En particulier on a

$$\mathrm{Tr}_{L/K}(x) = \sum_{\mathcal{P}|\mathcal{Q}} \mathrm{Tr}_{L_\mathcal{P}/K_\mathcal{Q}}(x)$$

et

$$\mathrm{N}_{L/K}(x) = \prod_{\mathcal{P}|\mathcal{Q}} \mathrm{N}_{L_\mathcal{P}/K_\mathcal{Q}}(x).$$

Démonstration. — Cela résulte de la comparaison des polynômes caractéristiques de l'application $y \mapsto xy$ sur les $K_{\mathcal{Q}}$-espaces vectoriels figurant dans l'isomorphisme établi par la proposition 6.

PROPOSITION 7. — *L'homomorphisme canonique de $A_{\mathcal{Q}}$-modules*

$$B \otimes_A A_{\mathcal{Q}} \longrightarrow \prod_{\mathcal{P}|\mathcal{Q}} B_{\mathcal{P}}$$

est un isomorphisme de groupes.

Démonstration. — Ces groupes sont des $A_{\mathcal{Q}}$-modules libres de rang $[L : K]$. Il suffit donc de prouver la surjectivité. Il suffit de prouver cette surjectivité pour la réduction modulo $\mathcal{Q}$ (en effet toute famille d'éléments d'un $A/\mathcal{Q}$-module libre M dont la réduction modulo $\mathcal{Q}$ est une base de $M/\mathcal{Q}$ est elle-même une base de M). Cela résulte de la formule

$$B\mathcal{Q} \simeq \prod_{\mathcal{P}|\mathcal{Q}} \mathcal{P}^{e_{\mathcal{P}}}.$$

VIII
Adèles

1. Valeurs absolues normalisées

Soit K un corps de nombres. Notons $\mathcal{O}_K$ son anneau des entiers. On a vu ce que sont les valeurs absolues non archimédiennes de K.

PROPOSITION 1. — *Les valeurs absolues archimédiennes de K sont de la forme $x \mapsto |\sigma(x)|_\infty^k$, où $|.|_\infty$ est la valeur absolue usuelle de $\mathbf{C}$, où σ est un plongement de K dans $\mathbf{C}$ et où k est un nombre réel > 1.*
Démonstration. — Une valeur absolue non archimédienne v de K induit une valeur absolue non archimédienne de $\mathbf{Q}$. Elle est donc de la forme cherchée sur $\mathbf{Q}$. Le complété de K pour v est donc une extension finie de $\mathbf{R}$ qui ne peut être que $\mathbf{R}$ ou $\mathbf{C}$ (puisque $\mathbf{C}$ est de degré 2 sur $\mathbf{R}$ et que $\mathbf{C}$ est algébriquement clos). La valeur absolue v se prolonge donc en une valeur absolue de $\mathbf{C}$ qui est de la forme cherchée sur $\mathbf{R}$. Grâce au lemme VII-8, on voit qu'une valeur absolue de $\mathbf{R}$ se prolonge de manière unique à $\mathbf{C}$. Notre valeur absolue est donc de la forme cherchée sur $\mathbf{C}$. Par conséquent le plongement de K dans son complété K_v définit un plongement de K dans $\mathbf{C}$ compatible aux valeurs absolues par continuité de v.

Puisque les valeurs absolues de la proposition 1 définissent la même topologie lorsqu'on change la valeur de k, il n'est pas utile de toutes les considérer.

On les normalise en posant $k = 1$ si le plongement σ est réel et $k = 2$ sinon (on peut condenser cela en posant $k = [\sigma(K)\mathbf{R} : \mathbf{R}]$, cette formule est à comparer avec le corollaire 3 de la proposition 1). Autrement dit, pour toute valeur absolue normalisée $|.|_w$ de K au dessus d'une valeur absolue normalisée $|.|_v$ de $\mathbf{Q}$, on a

$$|x|_w = |x|_v^{[K_w:\mathbf{Q}_v]},$$

où K_w et $\mathbf{Q}$ désigne les complétés de K et $\mathbf{Q}$ pour les valeurs absolues w et v. L'ensemble S_K des places de K coïncide avec l'ensemble des valeurs absolues normalisées de K. Rappelons qu'il est constitué d'un nombre fini de places archimédiennes et d'un nombre infini de places non-archimédiennes. Notons S_∞ l'ensemble des places archimédiennes. On a $|S_\infty| = r_1 + r_2$, où r_1 désigne le nombre de plongements réels de K dans $\mathbf{C}$ et $2r_1$ désigne le nombre de plongements non réels de K dans $\mathbf{C}$.

Notons K_v le complété de K en la valeur absolue associée à la place v. Lorsque v est non-archimédienne, notons $\mathcal{O}_v$ l'anneau des entiers de K_v, $\mathcal{P}_v$ l'idéal premier non nul de

$\mathcal{O}_v$ et v valuation discrète associée. L'anneau $\prod_{v\in S} K_v$ est énorme. Cette constatation amène à considérer l'anneau des adèles ci-dessous.

2. Produit restreint d'espaces topologiques

Soit $(X_i)_{i\in I}$ une famille d'espaces topologiques. Soit $(Y_i)_{i\in I}$ une famille d'ouverts des X_i. Le *produit topologique restreint* X de la famille des $(X_i)_{i\in I}$ est l'ensemble des éléments $(x_i)_{i\in I} \in \prod_{i\in I} X_i$ tels que $x_i \in Y_i$ pour tout $i \in I$ excepté un nombre fini.

On munit X d'une topologie en considérant comme base de voisinages d'un point $(x_i)_{i\in I}$ les ensembles $\prod_{i\in I} O_i$ où O_i est un ouvert de X_i qui est contenu dans Y_i pour tout $i \in I$ excepté un nombre fini et où $x_i \in O_i$ $(i \in I)$. En particulier, pour J sous-ensemble fini de I, l'ensemble $X_J = \prod_{i\in J} X_i \times \prod_{i\in I-J} Y_i$ est un ouvert de X. On a donc

$$X = \cup_J X_J.$$

Cela permet de voir X comme une limite injective. Lorsque l'ensemble des $i \in I$ tels que $X_i \neq Y_i$ est infini, l'ensemble X n'est pas compact. Si chacun des X_i est localement compact, l'espace X est localement compact (en effet les ensembles X_J sont alors localement compacts, lorsque J est fini).

3. Adèles d'un corps de nombres

L'anneau $\mathbf{A}_K$ des *adèles* de K est par définition le sous-anneau de $\prod_{v\in S_K} K_v$ formé par les éléments de la forme $(x_v)_{v\in S_K}$ avec $x_v \in \mathcal{O}_v$ pour toute place v de K excepté un nombre fini d'entre elles. C'est donc le produit restreint relativement aux sous-groupes $\mathcal{O}_v$ des corps K_v lorsque v parcourt les places de K.

Soit x un élément de K. Considérons les plongements de K dans ses complétés. On a $x \in \mathcal{O}_v$ pour presque toute place non archimédienne v de K. On a donc une application injective

$$K \longrightarrow \mathbf{A}_K$$

qui à $x \in K$ associe l'élément qui a pour coordonnée x dans K_v pour chaque place v. Il s'agit d'un homomorphisme d'anneaux.

Ajoutons que tout complété K_v de K s'identifie à un sous-anneau de $\mathbf{A}_K$ de façon évidente. On pourrait dire que $\mathbf{A}_K$ est le plus petit anneau qui contienne tous les K_v. C'est même le plus petit anneau qui contienne K, tous les $\mathcal{O}_v$ (v valuation de $\mathcal{O}_K$) et les complétés archimédiens.

On munit donc $\mathbf{A}_K$ de la topologie de produit restreint pour laquelle $\Omega_S = \prod_{v\in S} K_v \times \prod_{v\notin S} \mathcal{O}_v$ est ouvert lorsque S est un ensemble fini de places de K contenant les places archimédiennes et pour laquelle Ω_S est muni de la topologie produit.

On a

$$\mathbf{A}_K = \cup_S \Omega_S$$

(Cela permet de voir $\mathbf{A}_K$ comme une limite injective). L'anneau $\mathbf{A}_K$ muni de la topologie de produit restreint est un anneau topologique. En effet l'addition et la multiplication sont

continues sur $\mathbf{A}$, puisqu'elles sont continues sur les ouverts Ω_S et que les Ω_S recouvrent $\mathbf{A}_K$.

PROPOSITION 2. — *Les homomorphismes injectifs de $\mathbf{Q}$-espaces vectoriels $K \longrightarrow A_K$ et $A_{\mathbf{Q}} \longrightarrow A_K$ définissent un isomorphisme continu de K-espaces vectoriels*

$$K \otimes_{\mathbf{Q}} \mathbf{A}_{\mathbf{Q}} \simeq \mathbf{A}_K,$$

où la topologie de $K \otimes_{\mathbf{Q}} \mathbf{A}_{\mathbf{Q}}$ est la topologie définie par le produit tensoriel (voir la définition ci-dessous).

Démonstration. — Pour $\mathcal{P}$ parcourant les idéaux maximaux de $\mathcal{O}_K$ au dessus du nombre premier p on a les isomorphismes (leçon VII)

$$K \otimes_{\mathbf{Q}} \mathbf{Q}_p \simeq \prod_{\mathcal{P}|p} K_{\mathcal{P}}$$

et

$$\mathcal{O}_K \otimes \mathbf{Z}_p \simeq \prod_{\mathcal{P}|p} \mathcal{O}_{\mathcal{P}}.$$

De plus on a l'isomorphisme déduit des plongements complexes de K

$$K \otimes \mathbf{R} \simeq \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}.$$

La topologie sur $K \otimes_{\mathbf{Q}} \mathbf{A}_{\mathbf{Q}}$ n'est autre que la topologie de produit restreint relativement aux

$$\Omega_P = K \otimes_{\mathbf{Q}} \mathbf{R} \times \prod_{p \in P} K \otimes_{\mathbf{Q}} \mathbf{Q}_p \times \prod_{p \notin P} \mathcal{O}_K \otimes \mathbf{Z}_p,$$

où P est un ensemble fini de nombres premiers. Cette topologie coïncide bien la topologie de produit restreint sur $\mathbf{A}_K$ relativement aux Ω_{S_P}, où S_P est constitué des places de K au-dessus de P et de la place archimédienne. En effet l'application $K \otimes_{\mathbf{Q}} \mathbf{A}_{\mathbf{Q}} \longrightarrow \mathbf{A}_K$ considérée dans la proposition induit une bijection de Ω_P sur Ω_{S_P} d'après les isomorphismes énoncés ci-dessus.

Cela prouve qu'on a un isomorphisme continu d'espaces topologiques

$$\Omega_P \simeq \Omega_{S_P}.$$

Par ailleurs la topologie de produit restreint sur $\mathbf{A}_K$ coïncide avec avec la topologie de produit restreint relativement Ω_{S_P}, puisque tout ensemble fini de places de K est contenu dans un ensembles S_P pour P ensemble de nombres premiers approprié. Les espaces topologiques $K \otimes_{\mathbf{Q}} \mathbf{A}_{\mathbf{Q}}$ et $\mathbf{A}_K$ sont donc isomorphes. On vérifie sans peine que cette bijection est K-linéaire.

La proposition 2 permet de ramener l'étude de la topologie de $\mathbf{A}_K$ à $\mathbf{A}_{\mathbf{Q}}$ dans la démonstration de la proposition suivante.

PROPOSITION 3. — *a) L'espace topologique $\mathbf{A}_K$ est localement compact.*

b) Le corps K est discret dans $\mathbf{A}_K$.

c) Le quotient $\mathbf{A}_K/K$, muni de la topologie quotient, est compact.

Démonstration. — Soit $(e_i)_{i=1,\dots,n}$ une base de K comme $\mathbf{Q}$-espace vectoriel. C'est aussi une base de $\mathbf{A}_K$ comme $\mathbf{A}_\mathbf{Q}$-module (proposition 2). On a donc $\mathbf{A}_K \simeq \mathbf{A}_\mathbf{Q}^n$ et $K \simeq \mathbf{Q}^n$, avec $n = [K : \mathbf{Q}]$. Il suffit donc de prouver les assertions de la proposition 3 dans le cas $K = \mathbf{Q}$.

Vérifions que $\mathbf{A}_\mathbf{Q}$ est localement compact. L'ouvert $\mathbf{R} \times \prod_p \mathbf{Z}_p$ est localement compact (car c'est le produit d'espaces localement compacts) et est un voisinage de 0. On en déduit par translation que tout point admet un voisinage contenu dans un compact.

Pour voir que sous-groupe $\mathbf{Q}$ de $\mathbf{A}_\mathbf{Q}$ est discret il suffit d'établir que tout point de $\mathbf{Q}$ est isolé. Par translation il suffit de prouver que 0 est isolé. C'est le cas puisque l'ouvert $]-\frac{1}{2}, \frac{1}{2}[\times \prod_p \mathbf{Z}_p$ (en effet c'est un ouvert de $\Omega_\emptyset$) ne contient que 0 comme nombre rationnel.

Vérifions la troisième assertion de la proposition 3. Tout élément de $\mathbf{A}_\mathbf{Q}/\mathbf{Q}$ admet un représentant dans $[0,1] \times \prod_p \mathbf{Z}_p \subset BR \times \prod_p \mathbf{Z}_p$. En effet cela se voit en remarquant qu'en ajoutant des éléments de $\mathbf{Z}[\frac{1}{p}]$ on respecte l'intégralité en toutes les places sauf p et en remarquant qu'on a $\mathbf{Z}[\frac{1}{p}] + \mathbf{Z}_p = \mathbf{Q}_p$ de sorte qu'on peut détruire les dénominateurs un à un. En translatant par des entiers on voit ensuite que tout élément de $\mathbf{A}_\mathbf{Q}/\mathbf{Q}$ admet un représentant dans $[0,1[\times \prod_p \mathbf{Z}_p \subset [0,1] \times \prod_p \mathbf{Z}_p$. Comme ce dernier ensemble est compact, $\mathbf{A}_\mathbf{Q}/\mathbf{Q}$ est compact.

Exercice . — Vérifier que $\prod_{v \in S_\infty} K_v$ s'identifie à $\mathbf{R} \otimes K$. Soit $(e_i)_{i=1,\dots,n}$ une base de $\mathcal{O}_K$ comme $\mathbf{Z}$-module. Notons P_∞ l'image dans $\prod_{v \in S_\infty} K_v$ du sous-ensemble de $\mathbf{R} \otimes K$ formé par les éléments de la forme $\sum_i t_i \otimes e_i$ avec t_i nombre réel vérifiant $0 \leq t_i < 1$. Démontrer que

$$\prod_{v \in S - S_\infty} \mathcal{O}_v \times P_\infty$$

est un système de représentants de $\mathbf{A}_K/K$ (on dit que le produit

$$\prod_{v \in S - S_\infty} \mathcal{O}_v \times \bar{P}_\infty,$$

où $\bar{P}_\infty$ est l'adhérence de P_∞ dans $\mathbf{R} \otimes K$, est un *domaine fondamental* de $\mathbf{A}_K/K$ pour l'action de K).

Remarques. — Un groupe localement compact est muni d'une mesure de Haar. Cette mesure est obtenue comme produit des mesures de Haar sur les composantes locales. Comme K est discret, l'espace quotient $\mathbf{A}_K/K$ hérite de la mesure de Haar de $\mathbf{A}_K$. Comme il est compact, sa mesure de Haar est bien définie : elle coïncide avec le volume d'un domaine fondamental.

Pour saisir la topologie des adèles, il est commode d'avoir à l'esprit que la situation de $\mathbf{Q}$ dans $\mathbf{A}_\mathbf{Q}$ est analogue à la situation de $\mathbf{Z}$ dans $\mathbf{R}$ (*i.e.* $\mathbf{R}$ est localement compact, $\mathbf{Z}$ est discret dans $\mathbf{R}$ et $\mathbf{R}/\mathbf{Z}$ est compact).

4. Idèles d'un corps de nombres

Reprenons les notations de la section précédente. Les groupe des *idèles* de K est le groupe des éléments inversibles de l'anneau $\mathbf{A}_K$. Notons-le, comme il se doit, $\mathbf{A}_K^*$. Il coïncide avec l'ensemble des éléments $(x_v)_{v\in S_K}$ de $\prod_{v\in S_K} K_v^*$ tels que $x_v \in \mathcal{O}_v^*$ pour presque tout $v \in S_K$. C'est donc un produit restreint.

Il est muni de la topologie (de produit restreint) pour laquelle les les ensembles $\Lambda_S = \prod_{v\in S} K_v^* \times \prod_{v\notin S} \mathcal{O}_v^*$, pour S sous-ensemble fini de S_K contenant S_∞, eux-mêmes munis de la topologie produit sont ouverts. C'est un groupe topologique (*i.e.* la multiplication et le passage à l'inverse sont des applications continues).

Attention : la topologie de $\mathbf{A}_K^*$ n'est pas induite par la topologie de $\mathbf{A}_K$ (phénomène général : le groupe des éléments inversibles d'un anneau topologique n'est pas forcément un groupe topologique pour la topologie induite car l'application $x \mapsto x^{-1}$ n'est pas forcément continue). Elle est plus fine que la topologie induite par $\mathbf{A}_K$: tout voisinage pour la topologie des adèles d'un point contient un voisinage du même point pour la topologie des idèles. Elle définit donc strictement moins de compacts et strictement plus d'ensembles discrets.

L'ensemble Λ_S est un sous-groupe de $\mathbf{A}_K^*$ que l'on appelle *groupe des S-idèles*. On a un homomorphisme injectif de groupes $K^* \longrightarrow \mathbf{A}_K^*$ induit par le plongement $K \longrightarrow \mathbf{A}_K$. Cela permet d'identifier K à un sous-groupe de $\mathbf{A}_K^*$. Le groupe Λ_S contient l'image par cet homomorphisme du groupe des S-unités, qui est même l'intersection de Λ_S et K dans $\mathbf{A}_K^*$.

De plus K^* est un sous-groupe discret de $\mathbf{A}_K^*$, puisque c'est un sous-ensemble discret de $\mathbf{A}_K$. C'est le sous-groupe des *idèles principales* de K. Le groupe quotient $\mathbf{A}_K^*/K^*$ est le groupe des *classes d'idèles* de K.

On a une application *norme* (on dit aussi *valeur absolue* ; c'est d'ailleurs préférable pour éviter toute ambiguïté) $\mathbf{A}_K^* \longrightarrow \mathbf{R}_+^*$ qui à $x = (x_v)_{v\in S}$ associe

$$||x|| = \prod_v |x_v|_v,$$

où $|x|_v$ est la valeur absolue normalisée associée à la place v. Cette formule est bien définie car pour presque tout $v \in S$ on a $|x|_v = 1$.

Proposition 6. — *La valeur absolue est un homomorphisme surjectif et continu de groupes. Soit $x \in K^*$. On a la* formule du produit *:*

$$||x|| = 1.$$

Démonstration. — La multiplicativité de la norme se vérifie composante par composante. La surjectivité résulte de du plongement canonique de $\mathbf{R}^*$ dans $\mathbf{A}_K^*$.

La formule du produit résulte de la formule

$$||x|| = ||\mathrm{N}_{K/\mathbf{Q}}(x)||,$$

que l'on vérifie composante par composante (corollaire 3 de la proposition VII-5 et corollaire 2 de la proposition VII-6), et de la formule du produit pour $\mathbf{Q}$ (qui résulte du théorème d'Ostrowski).

On a remarqué au passage l'existence d'une application norme (pour $L|K$ extension finie de corps de nombres)

$$\mathrm{N}_{L/K} \quad : \quad \mathbf{A}_L \longrightarrow \mathbf{A}_K,$$

définie en prolongeant la norme coordonnée par coordonnée. Nous reviendrons sur cette application.

Le groupe $\mathbf{A}_K^*/K^*$, muni de la topologie quotient, n'est pas compact puisque la norme est surjective sur $\mathbf{R}^*$ et continue. Notons $\mathbf{A}_{K^*}^0$ le sous-groupe de $\mathbf{A}_K^*$ formé par les éléments de valeur absolue 1.

THÉORÈME 1. — *Le groupe $\mathbf{A}_{\mathbf{K}}^{*\,0}/K^*$ est compact.*

Démonstration. — Nous allons voir que c'est une reformulation du théorème de finitude du nombre de classe combinée avec le théorème des unités.

Posons $\mathbf{I}_\infty = \prod_{v\in S_\infty} K_v^*$ et $\mathbf{I}_\infty^0 = \mathbf{I}_\infty \cap \mathbf{A}_{\mathbf{K}}^{*\,0}$. Ce dernier groupe est l'ensemble des éléments de $(x_v)_{v\in S_\infty} \in \mathbf{I}_\infty$ tels que $\prod_v |x_v|_v = 1$. Le sous-groupe $\mathbf{I}_\infty^0 \times \prod_{v\in S_K - S_\infty} \mathcal{O}_v^*$ est ouvert dans $\mathbf{A}_{\mathbf{K}}^{*\,0}$, puisque $\mathbf{I}_\infty \times \prod_{v\in S_K - S_\infty} \mathcal{O}_v^*$ est un produit d'ouverts. Pour démontrer le théorème il (faut et il) suffit de démontrer que d'une part l'ensemble $\mathbf{A}_{\mathbf{K}}^{*\,0}/K^*(\mathbf{I}_\infty^0 \times \prod_{v\in S_K - S_\infty} \mathcal{O}_v^*)$ est fini et que d'autre part l'espace $K^*(\mathbf{I}_\infty^0 \times \prod_{v\in S_K - S_\infty} \mathcal{O}_v^*)/K^*$ est compact.

L'injection $\mathbf{A}_{\mathbf{K}}^{*\,0} \longrightarrow \mathbf{A}_K^*$ définit un isomorphisme de groupes

$$\mathbf{A}_{\mathbf{K}}^{*\,0}/\mathbf{I}_\infty^0 \longrightarrow \mathbf{A}_K^*/\mathbf{I}_\infty.$$

La finitude de $\mathbf{A}_{\mathbf{K}}^{*\,0}/K^*(\mathbf{I}_\infty^0 \times \prod_{v\in S_K - S_\infty} \mathcal{O}_v^*)$ équivaut donc à la finitude $\mathbf{A}_K^*/K^*(\mathbf{I}_\infty \times \prod_{v\in S_K - S_\infty} \mathcal{O}_v^*)$. Cela équivaut à la finitude du groupe des classes de K en raison du lemme suivant.

Lemme 1. — *L'homomorphisme de groupes $\mathbf{A}_K^* \longrightarrow \mathcal{I}(K)$ qui à $x = (x_v)_{v\in S}$ associe l'idéal fractionnaire $\prod_{v\in S - S_\infty} \mathcal{P}_v^{v(x_v)}$ définit par passage aux quotients un isomorphisme de groupes*

$$\mathbf{A}_K^*/K^*(\mathbf{I}_\infty \times \prod_{v\in S_K - S_\infty} \mathcal{O}_v^*) \simeq \mathcal{C}l(K).$$

Démonstration. — Notons ψ cette application $\mathbf{A}_K^* \longrightarrow \mathcal{I}(K)$. C'est un homomorphisme surjectif de groupes puisque tout idéal fractionnaire se décompose en produit d'idéaux premiers. Son noyau est l'ensemble des $x = (x_v)_{v\in S}$ tels que $x_v \in \mathcal{O}_v^*$ pour tout $v \notin S_\infty$.

C'est donc $\mathbf{I}_\infty \times \prod_{v\in S_K - S_\infty} \mathcal{O}_v^*$. L'ensemble des idéaux principaux coïncide avec $\phi(K^*)$. L'image réciproque par ψ du sous-groupe de $\mathcal{I}(K)$ formé par les idéaux principaux est donc égale à $K^*(\mathbf{I}_\infty \times \prod_{v\in S_K - S_\infty} \mathcal{O}_v^*)$. Cela prouve le lemme 1.

Revenons à la preuve du théorème 1. Le groupe $K^*(\mathbf{I}_\infty^0 \times \prod_{v\in S_K - S_\infty} \mathcal{O}_v^*)/K^*$ s'identifie à

$$(\mathbf{I}_\infty^0 \times \prod_{v\in S_K - S_\infty} \mathcal{O}_v^*)/(K^* \cap \prod_{v\in S_K - S_\infty} \mathcal{O}_v^*) = (\mathbf{I}_\infty^0 \times \prod_{v\in S_K - S_\infty} \mathcal{O}_v^*)/\mathcal{O}_K^*.$$

Comme $\mathcal{O}_v^*$ est compact, $(\mathbf{I}_\infty^0 \times \prod_{v\in S_K - S_\infty} \mathcal{O}_v^*)/\mathcal{O}_K^*$ est compact si et seulement si $\mathbf{I}_\infty^0/\mathcal{O}_K^*$ est compact. Considérons l'application $\phi : \mathbf{I}_\infty^0 \longrightarrow \mathbf{R}^{r_1+r_2}$ qui à $(x_v)_{v\in S_\infty}$ associe $(\log(|x_v|_v))_{v\in S_\infty}$. C'est une application continue. Notons N le noyau de ϕ. D'après le théorème des unités, $\phi(\mathcal{O}_K^*)$ est un réseau de l'hyperplan image de ϕ et le groupe $N \cap \mathcal{O}_K^*$, qui est constitué par les racines de l'unité de K, est fini. Cela prouve que $\mathbf{I}_\infty^0/\mathcal{O}_K^*$ est compact.

Remarque . — On verra un énoncé plus général que le lemme 1 dans la prochaine leçon. Ce type d'énoncé faisant le lien entre classes d'idèles et classes d'idéaux permet de formuler la théorie du corps de classe de différentes façons.

5. Théorèmes d'approximations

Il existe deux types de théorèmes d'approximation. Il sont dits *faible* et *fort*. Le théorème d'approximation faible suivant est très proche du lemme d'approximation (*i.e.* le théorème chinois).

THÉORÈME 2. — *Soit K un corps. Soient $|.|_1$, $|.|_2$, ..., $|.|_n$ des valeurs absolues non triviales et deux à deux non équivalentes de K. Notons K_1, ..., K_n les complétés de K pour ces valeurs absolues. Alors l'application diagonale*

$$K \longrightarrow \prod_i K_i$$

est d'image dense (pour la topologie produit).

Démonstration. — Le théorème revient à vérifier la chose suivante : soit $(\alpha_1, \alpha_2, ..., \alpha_n) \in K_1 \times K_2 \times ... \times K_n$; pour tout nombre réel $\epsilon > 0$, il existe $\beta \in K$ tel que pour tout $i \in \{1, 2, ..., n\}$ on ait $|\beta - \alpha_i|_i < \epsilon$. C'est ce que nous allons démontrer.

Il suffit de trouver pour tout $i \in \{1, 2, ..., n\}$ un élément $\theta_i \in K$ tel que $|\theta_i|_i > 1$ et $|\theta_i|_j < 1$ pour $i \neq j$. En effet, la suite $\theta_i^r/(1+\theta_i^r)$ tend vers 1 (resp. 0) lorsque r tend vers l'infini pour $|.|_i$ (resp. $|.|_j$, $i \neq j$), si bien que la suite

$$\beta_r = \sum_{i=1}^{n} \frac{\theta_i^r}{(1+\theta_i^r)} \alpha_i$$

tend vers α_i pour $|.|_i$ lorsque r tend vers l'infini. Cela autorise à prendre $\beta = \beta_r$ pour r assez grand.

Sans nuire à la généralité, pour démontrer le théorème il suffit d'établir l'existence d'un élément $\theta \in K$ tel que $|\theta|_1 > 1$ et tel que $|\theta|_i < 1$ $(i > 1)$. Nous allons le montrer par récurrence sur n.

Etudions d'abord le cas $n = 2$. Comme $|.|_1$ et $|.|_2$ ne sont pas équivalentes, il existe α, $\beta \in K$ tels que $\log(|\alpha|_1)/\log(|\alpha|_2)$ soit distinct de $\log(|\beta|_1)/\log(|\beta|_2)$. Par conséquent, lorsque les entiers n et m varient, les signes des nombres réels $m\log(|\alpha|_1) + n\log(|\beta|_1)$ et $m\log(|\alpha|_2) + n\log(|\beta|_2)$ ne sont pas toujours identiques. En posant μ, $\lambda = \alpha^m\beta^n$, pour des valeurs judicieuses des entiers n et m on obtient qu'il existe λ, $\mu \in K$ tels que $|\lambda|_1 < 1$, $|\lambda|_2 \geq 1$, $|\mu|_1 \geq 1$ et $|\mu|_2 < 1$. On pose alors $\theta = \lambda/\mu$.

Lorsque $n \geq 3$, il existe, par hypothèse de récurrence, $\theta' \in K$ tel que $|\theta'|_1 > 1$ et tel que $|\theta'|_i < 1$ $(n > i > 1)$. De plus il existe, en raison de l'étude du cas $n = 2$, $\theta'' \in K$ tel que $|\theta''|_1 > 1$ et tel que $|\theta''|_n < 1$. On pose alors $\theta = \theta'$ si $|\theta'|_n < 1$, $\theta = \theta'^r\theta''$ si $|\theta'|_n = 1$ (pour r entier assez grand) et $\theta = \theta'^r\theta''/(1 + \theta'^r)$ si $|\theta'|_n > 1$ (pour r entier assez grand). Cela achève de prouver le théorème.

Corollaire . — *Soient deux valeurs absolues non équivalentes $|.|_1$ et $|.|_2$ de K. Elles ne définissent pas la même topologie sur K.*
Démonstration. — Si ces valeurs absolues définissaient la même topologie, les boules de K définies par $|.|_1$ et $|.|_2$ seraient identiques puisqu'on a $|a| < 1$ si et seulement si la suite a^n tend vers 0. Dans ce cas nos deux valeurs absolues définiraient les même suites de Cauchy, si bien que les corps K_1 et K_2 seraient égaux. Dans ce cas l'adhérence de K dans $K_1 \times K_2$ serait égale au plongement diagonal de K_1 dans $K_1 \times K_1 = K_1 \times K_2$. L'image de ce plongement étant distincte de $K_1 \times K_2$, cela contredit le théorème 2.

Supposons maintenant que K soit un corps de nombres. Soit S un sous-ensemble (éventuellement infini) de S_K distinct de S_K. Notons $\mathbf{A}_S$ le sous-anneau de $\prod_{v\in S} K_v$ formé par les éléments de la forme $(x_v)_{v\in S}$ avec $x_v \in \mathcal{O}_v$ pour toute place $v \in S$ excepté un nombre fini d'entre elles. C'est donc le produit restreint relativement aux sous-groupes $\mathcal{O}_v$ des corps K_v lorsque v parcourt S. C'est canoniquement un sous-anneau de $\mathbf{A}_K$ (on complète en les places en dehors de S par des zéros). Il est muni de la topologie de produit restreint, qui coïncide avec la topologie induite par la topologie de $\mathbf{A}_K$. Nous sommes maintenant en mesure d'énoncer le théorème d'approximation forte.

Théorème 3. — *L'image dans $\mathbf{A}_S$ de l'homomorphisme diagonal $K \longrightarrow \mathbf{A}_S$ est dense.*
Démonstration. — Le théorème se ramène à l'assertion suivante : soient S' un sous-ensemble fini de S, ϵ un nombre réel > 0 et une famille $(a_v)_{v\in S'}$ avec $a_v \in K_v$; il existe $c \in K$ tel que $|c - a_v|_v < \epsilon$ $(v \in S')$ et $|c|_v \leq 1$ $(v \in S - S')$. Cela revient à dire qu'on a l'inclusion

$$\mathbf{A}_K \subset K + \prod_{v\in S'} B(0,\epsilon) \times \prod_{v\in S-S'} B(0,1) \times \prod_{v\in S_K-S} K_v^*.$$

Utilisons le fait que $\mathbf{A}_K/K$ est compact. Il existe un système de représentants de ce quotient dans $\mathbf{A}_K$ qui est compact. Ce système de représentant R est donc contenu

dans un produit compact de boules fermées $\prod_{v\in S_K} B(0,\delta_v)$ avec $\delta_v = 1$ pour presque tout $v \in S_K$ (rappelons qu'on a $B(0,1) = \mathcal{O}_v$).

Lemme 2. — *Il existe un nombre réel C_K ne dépendant que de K vérifiant la condition suivante. Soit $x = (x_v)_{v\in S_K} \in \mathbf{A}_K$ tel que $\prod_v |x_v|_v > C_K$. Alors il existe $y \in K^*$ tel qu'on ait $|y|_v \leq |x_v|_v$ $(v \in S_K)$.*

Démonstration. — Considérons la mesure de Haar μ sur $\mathbf{A}_K$ (définie comme mesure produit sur chacune des coordonnées). Elle définit une mesure de Haar encore notée μ par passage au quotient sur $\mathbf{A}_K/K$. Posons $D_7 = \prod_{v\in S_K - S_\infty} B(0,1) \times \prod_{v\in S_\infty} B(0,1/7)$. Nous allons voir que la constante

$$C_K = \frac{\mu(\mathbf{A}_K/K)}{\mu(D_7)}$$

convient pour le lemme.

Posons

$$T_7 = \prod_{v\in S_K - S_\infty} B(0,|x_v|_v) \times \prod_{v\in S_\infty} B(0,|x_v|_v/7).$$

On a

$$\mu(T_7) = \mu(D_7) \prod_{v\in S_K} |x_v|_v > \mu(D_7) C_K = \mu(\mathbf{A}_K/K).$$

Il existe donc deux éléments distincts u et u' de T_7 congrus modulo K. Posons alors $y = u - u' \in K$. Ce nombre vérifie les inégalités demandées : cela se voit en les places non-archimédiennes en utilisant l'inégalité ultramétrique et en les places archimédiennes grâce à l'inégalité triangulaire.

Revenons à la démonstration du théorème. Appliquons le lemme 2 à un élément $x = (x_v)_{v\in S_K} \in \mathbf{A}_K$ tel que
ι) $|x_v|_v \geq 1/\delta_v$ $(v \in S - S')$,
$\iota\iota$) $|x_v|_v > \epsilon/\delta_v$ $(v \in S')$ et
$\iota\iota\iota$ $\prod_{v\in S_K - S} |x_v| > C_K/(\epsilon^{|S'|} \prod_{v\in S} \delta_v)$
(ces conditions entraînent $\prod_v |x_v|_v > C_K$) ; un tel élément x existe puisque S est strictement contenu dans S_K. Il existe donc $y \in K^*$ tel que $|y|_v < \epsilon/\delta_v$ $(v \in S')$ et $|y|_v \leq 1$.

Comme R est un système de représentants de $\mathbf{A}_K/K$, on a $\mathbf{A}_K = R + K$. On a donc les égalités d'ensembles

$$\mathbf{A}_K = y\mathbf{A}_K = yR + yK = yR + K.$$

Comme on a, par construction de y,

$$yR \subset \prod_{v\in S'} B(0,\epsilon) \times \prod_{v\in S - S'} B(0,1) \times \prod_{v\in S_K - S} K_v^*,$$

l'approximation cherchée s'en suit.

Remarque . — Le théorème 3 appliqué au cas où S est fini donne le théorème 2 pour les corps de nombres, d'où la terminologie faible/fort. Bien entendu, le théorème 2 ne se réduit pas au théorème 3, puisqu'il s'applique à des corps quelconques.

L'énoncé du théorème 3 est faux lorsque $S = S_K$, puisque K est discret dans $\mathbf{A}_K$. D'où l'intérêt de considérer toutes les places de K.

IX
Les énoncés de la théorie du corps de classe

1. Compléments sur les corps p-adiques

Soit p un nombre premier. Soit K un *corps p-adique*. C'est-à-dire une extension finie de $\mathbf{Q}_p$ (attention le terme corps p-adique peut désigner, suivant les auteurs, des extensions infinies de $\mathbf{Q}_p$). Notons $\mathcal{O}_K$ l'anneau des entiers de K, v la valuation discrète de K, $\mathcal{P}$ l'idéal premier non nul de $\mathcal{O}_K$, k le corps résiduel et q le nombre d'éléments de k. Posons $U_K^{(n)} = 1 + \mathcal{P}^n\mathcal{O}_K$ lorsque n est un entier > 0 et $U_K^{(0)} = \mathcal{O}_K^*$.

On a la suite décroissante de sous-groupes ouverts :

$$... \subset U_K^{(n+1)} \subset U_K^{(n)} \subset ... \subset U_K^{(1)} = 1 + \mathcal{P}\mathcal{O}_K \subset U_K^{(0)} = \mathcal{O}_K^*.$$

Soit π une uniformisante de $\mathcal{P}$. Notons (π) le sous-groupe de K^* engendré par π. Il est isomorphe à $\mathbf{Z}$.

Proposition 1. — *On a les isomorphismes canoniques de groupes*

$$K^* \simeq (\pi) \times \mathcal{O}_K^*,$$

et

$$U_K^{(0)}/U_K^{(1)} \simeq k^*.$$

De plus le groupe quotient $U_K^{(n)}/U_K^{(n+1)}$ est un k-espace vectoriel de dimension 1.

Démonstration. — La première assertion résulte du fait que la valuation discrète v définit une suite exacte de groupes abéliens

$$0 \longrightarrow \mathcal{O}_K^* \longrightarrow K^* \longrightarrow \mathbf{Z} \longrightarrow 0,$$

et qu'on a $v(\pi) = 1$.

Le deuxième isomorphisme provient de l'homomorphisme de groupes canonique et surjectif $\mathcal{O}_K^* \longrightarrow k^*$. Le noyau de cet homomorphisme est $U_K^{(1)}$.

On a un isomorphisme canonique de k-espaces vectoriels entre $U_K^{(n)}/U_K^{n+1)}$ et k déduit de l'application $U_K^{(n)} \longrightarrow k$ qui à $1 + a\pi^n$ associe $a + \mathcal{P}$. Cette dernière application est un homomorphisme surjectif de groupes de noyau $U_K^{(n+1)}$.

Remarque . — On a même un isomorphisme canonique de groupes

$$K^* \simeq (\pi) \times \mu_{q-1} \times U_K^{(1)}.$$

L'isomorphisme d'espaces vectoriels $U_K^{(n)}/U_K^{n+1)} \simeq k$ construit dans la démonstration de la proposition 1 est non canonique puisqu'il dépend du choix d'une uniformisante de $\mathcal{P}$. Lorsque K est égal à $\mathbf{Q}_p$, on dispose d'une uniformisante canonique de $p\mathbf{Z}_p$, c'est-à-dire p.

Soit $L|K$ une extension finie. On dispose de l'homomorphisme norme $\mathrm{N}_{L/K} : L^* \longrightarrow K^*$. D'après le corollaire 3 de la proposition VII-5, on a $\mathrm{N}_{L/K}(\mathcal{O}_L^*) \subset \mathcal{O}_K^*$.

Proposition 2. — *Si l'extension $L|K$ est non ramifiée, on a $\mathrm{N}_{L/K}(\mathcal{O}_L^*) = \mathcal{O}_K^*$.*

Démonstration. — Comme $\cap_{n\geq 0} U_K^{(n)} = 0$, il suffit de prouver que $\mathrm{N}_{L/K}$ composée avec l'application canonique $\mathcal{O}_L^* \longrightarrow \mathcal{O}_L^*/U_K^{(n)}$ est surjective. Pour cela montrons que $N_{L/K}$ définit des surjections $U_L^{(n)}/U_L^{(n+1)} \longrightarrow U_K^{(n)}/U_K^{(n+1)}$ (n entier ≥ 0).

Pour $n = 0$, en notant k_K et k_L les corps résiduels de K et L respectivement, cela revient à dire que la norme $k_L^* \longrightarrow k_K^*$ est surjective. Or la norme d'un générateur de k_L^* est un générateur de k_K^*.

Pour $n \geq 1$, considérons une uniformisante π de l'idéal maximal $\mathcal{Q}$ de $\mathcal{O}_K$; c'est aussi une unifomisante de l'idéal maximal $\mathcal{P}$ de $\mathcal{O}_L$, puisque l'extension $L|K$ est non ramifiée. Soit $x \in \mathcal{O}_L$ Or on a

$$\mathrm{N}_{L/K}(1 + x\pi^n) = \prod_y (1 + y\pi^n),$$

où y parcourt les conjugué de x dans L, et donc,

$$\mathrm{N}_{L/K}(1 + x\pi^n) \equiv 1 + \mathrm{Tr}_{L/K}(x)\pi^n \pmod{\mathcal{Q}^{n+1}}.$$

Cela montre que $\mathrm{N}_{L/K}(U_L^{(n)}) \subset U_K^{(n)}$. Comme de plus l'application $\mathrm{Tr}_{L/K}$ est surjective (puisque $L|K$ est séparable), l'application $U_L^{(n)}/U_L^{(n+1)} \longrightarrow U_K^{(n)}/U_K^{(n+1)}$ déduite de la norme est surjective. Cela achève la démonstration.

2. Les groupes de classe de rayon et les cycles arithmétiques

Soit K un corps de nombres. On appelle *cycle arithmétique* un produit formel

$$\prod_{v \in S_K} \mathcal{P}_v^{n_v}$$

où n_v est un entier ≥ 0 lorsque v est une place non archimédienne, où $n_v \in \{0, 1\}$ lorsque v est une place archimédienne réelle, $n_v = 0$ lorsque v est une place archimédienne non réelle et où $\mathcal{P}_v$ est l'idéal maximal de $\mathcal{O}_K$ associé à v lorsque v est une place non archimédienne et où on a $n_v = 0$ pour presque tout $v \in S_K$. Le *support* d'un cycle arithmétique est l'ensemble des places v telles que $n_v \neq 0$.

Attention la terminologie cycle arithmétique n'est pas standard. Le terme utilisé par Hasse en allemand est "Erklärungsmodul".

Cette notion de cycle étend la notion d'idéal entier, puisque tout idéal entier de $\mathcal{O}_K$ est produit d'idéaux premier et s'identifie donc à un cycle arithmétique à support dans les places non archimédiennes.

On a une relation de divisibilité évidente entre les cycles arithmétiques de K qui prolonge la relation de divisibilité des idéaux : soient $\mathcal{M} = \prod_{v \in S_K} \mathcal{P}_v^{n_v}$ et $\mathcal{M}' = \prod_{v \in S_K} \mathcal{P}_v^{n'_v}$ deux cycles arithmétiques. On dira que $\mathcal{M}$ divise $\mathcal{M}'$ si on a $n_v \leq n'_v$ $(v \in S_K)$. On dira que ces deux cycles sont premiers entre eux si on a $n_v n'_v = 0$ $(v \in S_K)$. On peut parler de plus petit commun diviseur etc.

On note 1 le cycle arithmétique à support vide.

Soit $\mathcal{M} = \prod_{v \in S_K} \mathcal{P}_v^{n_v}$. Posons alors

$$U_v^{n_v} = U_{K_v}^{(n_v)}$$

lorsque v est une place non archimédienne,

$$U_v^{n_v} = \mathbf{R}_+^*,$$

lorsque v est une place réelle et $n_v = 1$,

$$U_v^{n_v} = \mathbf{R}^*$$

lorsque v est une place réelle et $n_v = 0$ et

$$U_v^{n_v} = \mathbf{C}^*,$$

lorsque v est une place complexe.

Pour $x \in K_v^*$, on note $x \equiv 1 \pmod{\mathcal{P}_v^{n_v}}$ lorsqu'on a $x \in U_v^{n_v}$ (cela coïncide avec la notation usuelle lorsque v est non archimédienne). On généralise cette notation à $x = (x_v)_{v \in S_K} \in \mathbf{A}_K$ en posant $x \equiv 1 \pmod{\mathcal{M}}$ lorsqu'on a $x_v \equiv 1 \pmod{\mathcal{P}_v^{n_v}}$ $(v \in S_K)$.

Posons alors

$$\mathbf{A}_K^*(\mathcal{M}) = \{x \in \mathbf{A}_K^* / x \equiv 1 \pmod{\mathcal{M}}\}.$$

On a $\mathbf{A}_K^*(\mathcal{M}) \subset \mathbf{A}_K^*(\mathcal{M}')$ lorsque $\mathcal{M}' | \mathcal{M}$. On a

$$\mathbf{A}_K^*(1) = \prod_{v \in S_\infty} K_v^* \times \prod_{v \in S_K - S_\infty} \mathcal{O}_v^*.$$

C'est l'ensemble des S_∞-idèles.

Le sous-groupe

$$C_K^{\mathcal{M}} = \mathbf{A}_K^*(\mathcal{M}) K^* / K^*$$

du groupe C_K des classes d'idèles est le *sous-groupe de congruence de niveau* $\mathcal{M}$ de C_K. L'application qui à $\mathcal{M}$ associe $C_K^{\mathcal{M}}$ est décroissante.

On note $\mathcal{I}(K)^{\mathcal{M}}$ le sous-groupe du groupe $\mathcal{I}(K)$ des idéaux fractionnaires de K engendré par les idéaux de $\mathcal{O}_K$ premiers à $\mathcal{M}$. On note $\mathcal{P}(K)^{\mathcal{M}}$ le sous-groupe de $\mathcal{I}(K)^{\mathcal{M}}$ engendré par les idéaux principaux de K de la forme $a\mathcal{O}_K$ avec $a \equiv 1 \pmod{\mathcal{M}}$ et $a \in K^*$.

Le groupe quotient

$$\mathcal{C}\ell(K)^{\mathcal{M}} = \mathcal{I}(K)^{\mathcal{M}}/\mathcal{P}(K)^{\mathcal{M}}$$

est le *groupe des classes d'idéaux de rayon* $\mathcal{M}$. Lorsque $\mathcal{M} = 1$, on retrouve le groupe des classes au sens habituel.

PROPOSITION 3. — *L'homomorphisme de groupes*

$$\mathbf{A}_K^* \longrightarrow \mathcal{I}(K)$$

qui à $(x_v)_{v\in S_K}$ *associe* $\prod_{v\notin S_\infty} \mathcal{P}_v^{v(x)}$ *induit après passages aux quotients un isomorphisme de groupes*

$$C_K/C_K^{\mathcal{M}} \simeq \mathcal{C}\ell(K)^{\mathcal{M}}.$$

Démonstration. — Posons

$$\mathbf{A}_K^* < \mathcal{M} >= \{x = (x_v)_{v\in S_K} \in \mathbf{A}_K^*/x_v = 1(\mathcal{P}_v \not| \mathcal{M})\}.$$

Soit $\alpha = (\alpha_v)_{v\in S_K} \in \mathbf{A}_K^*$. D'après le théorème d'approximation faible, il existe $a \in K^*$ tel que

$$a\alpha_v \equiv 1 \pmod{\mathcal{P}_v}$$

pour tout $\mathcal{P}_v|\mathcal{M}$. Posons alors

$$a\alpha_v = \beta_v\gamma_v$$

avec $\beta_v = 1$ (si $\mathcal{P}_v \not| \mathcal{M}$), $\beta_v = \alpha_v a$ (si $\mathcal{P}_v|\mathcal{M}$), avec $\gamma_v = 1$ (si $\mathcal{P}_v|\mathcal{M}$) et $\gamma_v = \alpha_v a$ (si $\mathcal{P}_v \not| \mathcal{M}$). Posons $\beta = (\beta_v)_{v\in S_K} \in \mathbf{A}_K^*$ et $\gamma = (\gamma_v)_{v\in S_K} \in \mathbf{A}_K^*$. On a alors $\beta \in \mathbf{A}_K^* < \mathcal{M} >$ et $\gamma \in \mathbf{A}_K^*(\mathcal{M})$. On a

$$\alpha = \beta\gamma a^{-1} \in \mathbf{A}_K^* < \mathcal{M} > .\mathbf{A}_K^*(\mathcal{M}).K^*.$$

Cela prouve qu'on a

$$\mathbf{A}_K^* = \mathbf{A}_K^* < \mathcal{M} > .\mathbf{A}_K^*(\mathcal{M}).K^*.$$

On a alors

$$\begin{aligned} C_K/C_K^{\mathcal{M}} &= \mathbf{A}_K^* < \mathcal{M} > .\mathbf{A}_K^*(\mathcal{M}).K^*/\mathbf{A}_K^*(\mathcal{M}).K^* \\ &= \mathbf{A}_K^* < \mathcal{M} > /(\mathbf{A}_K^* < \mathcal{M} > \cap \mathbf{A}_K^*(\mathcal{M}).K^*). \end{aligned}$$

L'homomorphisme de groupes $\mathbf{A}_K^* \longrightarrow \mathcal{I}(K)$ qui à $(x_v)_{v\in S_K}$ associe $\prod_{v\notin S_\infty} \mathcal{P}_v^{v(x)}$ induit un homomorphisme de groupes

$$\mathbf{A}_K^* < \mathcal{M} > \longrightarrow \mathcal{I}(K)$$

dont l'image est $\mathcal{I}(K)^{\mathcal{M}}$. Il définit par passage au quotient un homomorphisme surjectif de groupes

$$\mathbf{A}_K^* < \mathcal{M} > \longrightarrow \mathcal{I}(K)^{\mathcal{M}}/\mathcal{P}(K)^{\mathcal{M}}.$$

Le noyau de ce dernier homomorphisme coïncide avec $\mathbf{A}_K^* < \mathcal{M} > \cap \mathbf{A}_K^*(\mathcal{M}).K^*$. Cela prouve qu'on a l'isomorphisme cherché.

Remarques. — La proposition 3 permet d'appeler sans ambiguïté le groupe $C_K/C_K^{\mathcal{M}}$ *groupe des classes d'idèles de rayon* $\mathcal{M}$.

Le sous-groupe

$$K_{\mathcal{M}} = K \cap \mathbf{A}_K^*(\mathcal{M})$$

de K^* est le *rayon* modulo $\mathcal{M}$.

Certains auteurs ont considèré des notions un peu plus générales que les cycles arithmétiques : des produits formels de la forme

$$\prod_{v \in S_K} \mathcal{P}_v^{n_v}$$

où $n_v \in \mathbf{Z}$ si v est non archimédienne et $n_v \in \mathbf{R}$ si v est archimédienne. Ce sont des *diviseurs compactifiés* de $\mathcal{O}_K$.

Cette terminologie inspirée par la géométrie algébrique.

Proposition 3. — *Soit* $\mathcal{M} = \prod_v \mathcal{P}_v^{n_v}$ *un cycle arithmétique. Les groupes* $C_K/C_K^{\mathcal{M}}$ *et* $\mathcal{C}\ell(K)^{\mathcal{M}}$ *sont finis.*

Démonstration. — Il suffit de le vérifier pour $C_K/C_K^{\mathcal{M}}$ d'après la proposition 2. Par ailleurs le groupe des classe ordinaire, qui s'identifie à C_K/C_K^1 (voir le lemme VIII–1), est fini. Il suffit donc de prouver la finitude du groupe quotient

$$C_K^1/C_K^{\mathcal{M}} \simeq \mathbf{A}_K^*(1)K^*/\mathbf{A}_K^*(\mathcal{M})K^*$$

et donc du quotient

$$\mathbf{A}_K^*(1)/\mathbf{A}_K^*(\mathcal{M}) \simeq \prod_{v \in S_K} \mathcal{O}_v^*/U_v^{n_v}.$$

Les facteurs de ce dernier quotient sont le groupe trivial lorsque $n_v = 0$, c'est-à-dire pour presque tout $v \in S_K$; les facteurs non triviaux sont finis d'après la proposition 1. Cela prouve la finitude cherchée.

Remarque . — On a démontré au passage que l'indice de $C_K^{\mathcal{M}}$ dans C_K est égal au produit du nombre de classes et de l'indice de $C_K^{\mathcal{M}}$ dans C_K^1. Ce dernier indice est égal au produit des indices locaux $U_v^{n_v}$ dans U_v^0. C'est donc

$$N_{\mathcal{M}} = 2^{r_0} N_{\mathcal{M}_0},$$

où r_0 est le nombre de places réelles v telles que $n_v \neq 0$ et où $N_{\mathcal{M}_0}$ est la norme de l'idéal formé par la partie non archimédienne de $\mathcal{M}$.

PROPOSITION 4. — *Tout sous-groupe d'indice fini de C_K contient un sous-groupe de congruence.*

Démonstration. — Un tel sous-groupe correspond à un sous-groupe G d'indice fini de $\mathbf{A}_K^*$ contenant K^*. Comme on a $\mathbf{A}_K^* = \mathbf{A}_K^*(1).K^*$ et $K^* \cap \mathbf{A}_K^*(1) = \mathcal{O}_K^*$, il définit un sous-groupe H d'indice fini de $\mathbf{A}_K^*(1)$ contenant $\mathcal{O}_K^*$. La projection de H dans chaque composante de

$$\mathbf{A}_K^*(1) = \prod_{v \in S_\infty} K_v^* \times \prod_{v \in S_K - S_\infty} \mathcal{O}_v^*$$

est d'indice fini.

Un sous groupe d'indice fini de $\mathbf{C}^*$ ne peut être que $\mathbf{C}^*$ lui-même. Un sous-groupe d'indice fini de $\mathbf{R}^*$ est égal à $\mathbf{R}^*$ ou $\mathbf{R}_+^*$. Enfin un sous-groupe d'indice fini de $\mathcal{O}_\mathcal{P}^*$ contient un sous-groupe de la forme $U_{\mathcal{P}_v}^n$ (voir la structure de $\mathcal{O}_\mathcal{P}^*$ donnée par la proposition 1).

On en déduit que H contient un groupe de la forme

$$\prod_{v \in S_K} U_v^{n_v}.$$

Comme H est d'indice fini, on en déduit que $n_v = 0$ pour presque tout $v \in S_K$. En posant $\mathcal{M} = \prod_v \mathcal{P}_v^{n_v}$, on obtient que H contient $\mathbf{A}_K^*(\mathcal{M})$.

Le groupe G contient donc $\mathbf{A}_K^*(\mathcal{M})K^*$. Cela achève de prouver la proposition.

3. Extensions abéliennes

Soit $L|K$ une extension de corps. On dit qu'il s'agit d'une *extension abélienne* si c'est une extension galoisienne et si le groupe de Galois $\mathrm{Gal}(L/K)$ est abélien.

On voit facilement que la composée de deux extensions abéliennes (contenues dans un corps commun) est abélienne. De plus l'intersection de deux extensions abéliennes est abélienne.

Tout groupe G admet un plus grand groupe quotient abélien G^{ab}. C'est l'*abélianisé* de G. Il est obtenu comme quotient de G par son sous-groupe des commutateurs. Il en résulte que toute extension galoisienne $L|K$ admet une plus grande sous extension $L'|K$ qui est abélienne de groupe de Galois $\mathrm{Gal}(L/K)^{\mathrm{ab}}$.

La théorie du corps de classe vise à étudier les extensions abéliennes de K lorsque K est un corps p-adique ou un corps de nombres (signalons qu'il existe des généralisations de cette théorie dans diverses directions, mentionnons tout spécialement la théorie du corps de classe pour les corps de fonctions).

4. La théorie du corps de classe local

Soit p un nombre premier. Soit K un corps p-adique.

Le théorème principal est la loi de réciprocité locale. On peut rendre le théorème 1 ci-dessous plus explicite par la théorie de Lubin-Tate. On peut le rendre plus précis en faisant intervenir les groupes de ramifications.

THÉORÈME 1. — *L'application qui à L associe $\mathrm{N}_{L/K} L^*$ est une correspondance bijective et décroissante entre les extensions abéliennes finies de K et les sous-groupes d'indice finis de K^*.*

Soit L/K une extension abélienne et finie. On a un isomorphisme de groupes

$$\mathrm{Gal}(L/K) \longrightarrow K^*/\mathrm{N}_{L/K} L^*.$$

De plus on a

$$\mathrm{N}_{L_1L_2/K} (L_1L_2)^* = \mathrm{N}_{L_1/K} L_1^* \cap \mathrm{N}_{L_2/K} L_2^*$$

et

$$\mathrm{N}_{L_1\cap L_2/K} (L_1 \cap L_2)^* = (\mathrm{N}_{L_1/K} L_1^*)(\mathrm{N}_{L_1/K} L_2^*)$$

(L_1, L_2 extensions abéliennes de K).

L'homomorphisme de groupes $K^*/\mathrm{N}_{L/K} L^* \longrightarrow \mathrm{Gal}(L/K)$ réciproque de celui dont il est question dans le théorème est l'*homomorphisme de reste normique*, ou *isomorphisme de réciprocité* ou *homomorphisme d'Artin local*. Chronologiquement la théorie du corps de classe global a précédé la théorie du corps de classe local. Mais il est plus naturel d'établir d'abord la théorie locale avant de l'utiliser comme ingrédient pour la théorie globale.

Lorsque K est non plus un corps local, mais une extension finie de $\mathbf{R}$ (c'est-à-dire $\mathbf{R}$ ou $\mathbf{C}$) le théorème 1 est encore vrai en le sens suivant. Soit L une extension finie de K (*i.e.* on a $K = L$ sauf lorsque $K = \mathbf{R}$ et $L = \mathbf{C}$). Le groupe $\mathrm{Gal}(L/K)$ est canoniquement isomorphe à $K^*/\mathrm{N}_{L/K} L^*$. En effet ces deux groupes sont triviaux sauf lorsque $K = \mathbf{R}$ et $L = \mathbf{C}$; dans ce dernier cas les groupes $\mathrm{Gal}(L/K)$ et $K^*/\mathrm{N}_{L/K} L^*$ sont d'ordre 2, puisqu'on a $\mathrm{N}_{\mathbf{C}/\mathbf{R}} \mathbf{C}^* = \mathbf{R}_+^*$. L'isomorphisme canonique

$$\mathrm{Gal}(L/K) \longrightarrow K^*/\mathrm{N}_{L/K} L^*$$

s'appelle encore homomorphisme d'Artin.

Remarques. — Soit $L|K$ une extension finie et non ramifiée. L'image de l'application norme $\mathrm{N}_{L/K}$ contient $\mathcal{O}_K^*$.

Lorsque $L|K$ est abélienne, l'image inverse d'une substitution de Frobenius par l'homomorphisme de restes normiques est un générateur de $K^*/\mathrm{N}_{L/K} L^*$. Cela résulte directement de l'homomorphisme de réciprocité local et du fait que la substitution de Frobenius est un générateur du groupe de Galois dans le cas non ramifié.

On normalise l'homomorphisme de restes normiques de telle sorte que l'image d'une uniformisante de K soit égale à la subsitution de Frobenius.

Lorsque $L|K$ est encore abélienne et finie mais pas nécessairement non ramifiée, l'image de l'application norme est d'indice fini dans K^*. Elle contient donc un sous-groupe $U_K^{(n)}$, pour n entier minimal. Cet entier n est le *conducteur* (au sens additif) de l'extension $L|K$. On peut aussi appeler conducteur l'idéal $\mathcal{P}^n$ de $\mathcal{O}_K$. Lorsque l'extension $L|K$ est non ramifiée on a $n = 0$. On verra le lien entre l'entier n et les groupes de ramification de l'extension $L|K$.

5. La théorie du corps de classe global

On considère maintenant K un corps de nombres. Soient $L|K$ une extension abélienne et finie. Soit v et w des places de K et L. Notons K_v et L_w leurs complétés respectifs en ces places. Le groupe $\mathrm{Gal}(L_w/K_v)$ s'identifie à un sous-groupe (de décomposition en w si v est non-archimédienne) de $\mathrm{Gal}(L/K)$ (voir la leçon sur les extensions de corps complets). Lorsque w varie parmis les places au-dessus de v ces sous-groupes de $\mathrm{Gal}(L/K)$ sont conjugués les uns des autres, et donc égaux puisque $\mathrm{Gal}(L/K)$ est un groupe abélien. Notons ψ_v l'homomorphisme d'Artin local correspondant.

Notons C_K et C_L les groupes de classes d'idèles de K et L. Rappelons que, pour toute place w de L, L_w^* s'identifie à un sous-groupe de C_L via le plongement $L_w^* \longrightarrow \mathbf{A}_K^*$. On a une application norme $\mathrm{N}_{L/K} : C_L \longrightarrow C_K$ déduite de l'application norme $\mathbf{A}_L* \longrightarrow \mathbf{A}_K^*$ (elle-même définie par la norme sur chaque composante ; attention au conflit de terminologie entre cette application norme et celle qui s'appelle aussi valeur absolue). La composante en w de $\mathrm{N}_{L/K}\, C_L$ n'est autre que $\mathrm{N}_{L/K}\, L_w^*$.

THÉORÈME 2. — *L'application qui à L associe $\mathrm{N}_{L/K}\, C_L$ est une correspondance bijective et décroissante entre les extensions abéliennes finies de K et les sous-groupes fermés d'indice fini de C_K.*

Soit L/K une extension abélienne et finie. On a un isomorphisme de groupes

$$\mathrm{Gal}(L/K) \longrightarrow C_K/\mathrm{N}_{L/K}\, C_L$$

compatible aux homomorphismes de restes normiques et aux plongements locaux. De plus on a

$$\mathrm{N}_{L_1L_2/K}\, C_{L_1L_2} = \mathrm{N}_{L_1/K}\, C_{L_1} \cap \mathrm{N}_{L_2/K}\, C_{L_2}$$

et

$$\mathrm{N}_{L_1\cap L_2/K}\, C_{L_1\cap L_2} = (\mathrm{N}_{L_1/K}\, C_{L_1})(\mathrm{N}_{L_1/K}\, C_{L_2})$$

(L_1, L_2 extensions abéliennes de K).

Ce théorème est dû à Artin, à la suite des travaux de nombreux mathématiciens antérieurs. La formulation en termes de classes d'idèles est postérieure et est due à Chevalley.

L'extension abélienne associée à un sous-groupe fermé et d'indice fini G de C_K est le *corps de classe* de G. L'homomorphisme $\psi : C_K/\mathrm{N}_{L/K}\, C_L \longrightarrow \mathrm{Gal}(L/K)$ inverse de celui du théorème 2 est *l'homomorphisme d'Artin*. Le fait qu'il soit compatible aux homomorphismes de restes normiques signifie que pour toute place v de K, la restriction de ψ à $K_v^*/\mathrm{N}_{L_w/K_v} L_w^*$ n'est autre que ψ_v lorsqu'on identifie $\mathrm{Gal}(L_w/K_v)$ à un sous-groupe de $\mathrm{Gal}(L/K)$ et $K_v^*/\mathrm{N}_{L_w/K_v} L_w^*$ à un sous-groupe de $C_K/\mathrm{N}_{L/K}\, C_L$. Autrement dit on a un diagramme commutatif d'homomorphismes de groupes

$$\begin{array}{ccc} \mathrm{Gal}(L_w/K_v) & \simeq & K_v^*/\mathrm{N}_{L_w/K_v} L_w^* \\ \downarrow & & \downarrow \end{array}$$

$$\mathrm{Gal}(L/K) \simeq C_K/\mathrm{N}_{L/K} C_L,$$

où les flèches horizontales sont les isomorphismes de réciprocité et les flèches verticales sont des injections.

Remarque . — La donnée des homomorphismes d'Artin locaux en chaque place v de K suffit à prouver l'existence de $\psi : \mathbf{A}_K^*/\mathrm{N}_{L/K}\,\mathbf{A}_L^* \longrightarrow \mathrm{Gal}(L/K)$. En effet soit $x = (x_v)_{v\in S_K} \in \mathbf{A}_K^*$. Pour presque tout v on a $x_v \in \mathcal{O}_v^*$ et $L|K$ non ramifiée en v. On a donc $\psi_v(x_v) = 1$ pour presque tout v (voir la remarque à la fin de la section précédente). La fonction $\psi = \prod_{v\in S_K} \psi_v : \mathbf{A}_K^* \longrightarrow \mathrm{Gal}(L/K)$ est donc bien définie. Son noyau contient $\mathrm{N}_{L/K}\,\mathbf{A}_L^*$ puisque le noyau de ψ_v contient $\mathrm{N}_{L/K}\,L_w$. Mais il n'est pas clair *a priori* qu'il contienne K^*. C'est même l'un des points essentiels de la théorie. Néanmoins, retenons que la donnée de tous les homomorphismes d'Artin locaux détermine l'homomorphisme d'Artin global.

Une extension abélienne $L|K$ admet un *conducteur* qui est l'idéal de $\mathcal{O}_K$ défini comme le produit (fini car on a $n_v = 0$ pour presque tout v)

$$\prod_{v\in S_K - S_\infty} \mathcal{P}_v^{n_v}$$

où n_v est le conducteur de l'extension locale $L_w|K_v$. On peut même définir une composante archimédienne du conducteur pour obtenir un cycle arithmétique. Cette composante est donnée comme le produit des places réelles de K au dessus desquelles l'extension $L|K$ est non réelle.

6. Point de vue élémentaire et corps de classe

Soit $L|K$ une extension abélienne de corps de nombres. Soit $\mathcal{P}$ un idéal maximal de $\mathcal{O}_L$ au dessus d'un idéal maximal $\mathcal{Q}$ de $\mathcal{O}_K$ telle que l'extension $L|K$ soit non ramifiée en $\mathcal{P}$. La substitution de Frobenius en $\mathcal{P}$ ne dépend que de $\mathcal{Q}$. C'est donc un élément de $\mathrm{Gal}(L/K)$ qui l'on appelle *symbole d'Artin* et que l'on note $(\mathcal{Q}, L/K)$. Cette définition se généralise par multiplicativité à tout idéal fractionnaire I de K qui est à support en dehors des idéaux premiers ramifiés de l'extension L/K.

On trouve dans certains ouvrages la formulation suivante de la loi de réciprocité d'Artin.

Théorème 3. — *Soient K un corps de nombres et L une extension abélienne de K. Notons A l'anneau des entiers de K. Il existe une famille de nombres entiers $n_\mathcal{Q}$ indexée par les idéaux premiers de A telle qu'on ait la propriété suivante. Soit $x \in K$ tel que $x \in 1 + \mathcal{P}^{n_\mathcal{P}}$ ($\mathcal{P}$ idéal ramifié de L/K) et $i(x) > 0$ pour tout homomorphisme de corps $i : K \longrightarrow \mathbf{R}$ qui ne se prolonge pas en un homomorphisme de corps $L \longrightarrow \mathbf{C}$. On a $(xA, L/K) = 1$.*

Par ailleurs tout élément de $\mathrm{Gal}(L/K)$ est de la forme $(\mathcal{P}, L/K)$ pour une infinité d'idéaux premiers $\mathcal{P}$ de A.

On pourra essayer de faire le lien entre la première assertion du théorème 3 et le théorème 2. La deuxième assertion du théorème 3 est une conséquence du théorème de densité de Chebotarev.

Soit $\mathcal{M}$ un cycle arithmétique de K. Le sous-groupe de congruence de niveau $\mathcal{M}$ de C_K est fermé et d'indice fini. Il lui correspond donc une extension abélienne $H^{\mathcal{M}}$ de K par la loi de réciprocité d'Artin. Cette extension s'appelle le *corps de classe de rayon* $\mathcal{M}$. On a donc

$$\mathrm{Gal}(H^{\mathcal{M}}/K) \simeq C_K/C_K^{\mathcal{M}} \simeq \mathcal{C}\ell(K)^{\mathcal{M}},$$

où le dernier isomorphisme est déduit de la proposition 1.

Lorsque $\mathcal{M} = 1$, le corps de classe de rayon $\mathcal{M}$ est le *corps de classe de Hilbert de* K. C'est la plus grande extension abélienne $H|K$ qui est partout non ramifiée et telle que toute place réelle de K reste réelle dans H. On a alors un isomorphisme de groupes

$$\mathrm{Gal}(H/K) \simeq \mathcal{C}\ell(K).$$

Lorsque $\mathcal{M} = \prod_{v\in S_\infty} \mathcal{P}_v$, le corps de classe de rayon $\mathcal{M}$ est le *corps de classe de Hilbert étendu de* K. C'est la plus grande extension abélienne et partout non ramifiée de K.

Ces assertions se vérifient facilement (en admettant tout ce qui précède) en comparant les lois de réciprocités locales et globales et en utilisant le critère de non ramification.

Mentionnons sans démonstration que tout idéal de K devient principal dans le corps de classe de Hilbert de K. C'est le *Hauptidealsatz* de Hilbert. La démonstration repose principalement sur des arguments de théorie des groupes.

X
La formule du nombre de classes

1. Séries de Dirichlet

Une *série de Dirichlet* est une série de la forme

$$\sum_{n\geq 1} \frac{a_n}{n^s},$$

où $(a_n)_{n\geq 1}$ est une suite de nombres complexes (on s'accordera à dire que ce sont les coefficients de la série) et s est une variable complexe.

Ces fonctions jouent un grand rôle en théorie des nombres, où elle apparaissent parfois sous la forme d'un *produit eulerien*, c'est-à-dire un produit infini de la forme

$$\prod_p \frac{1}{P_p(p^{-s})}$$

où p parcourt les nombres premiers et P_p est un polynôme de coefficient constant égal à 1. On retrouve une série de Dirichlet en développant un tel produit. Lorsqu'on a affaire à un produit eulerien, on est parfois amené à le "compléter" en ajoutant un facteur correspondant à la place à l'infini de $\mathbf{Q}$ (voir plus bas).

Plus généralement on appelle produit eulerien (relatif à un corps de nombres K) un produit portant sur les idéaux premiers de K

$$\prod_{\mathcal{P}} \frac{1}{P_{\mathcal{P}}(N_{\mathcal{P}}^{-s})}$$

où $P_{\mathcal{P}}$ est un polynôme de coefficient constant égal à 1. On complète le produit en ajoutant des facteurs correspondant aux places archimédiennes de K.

Soit $s_0 \in \mathbf{C}$. Posons

$$D_{s_0} = \{z \in \mathbf{C}/\Re(z) > \Re(s_0)\}.$$

Lemme 1. — *Soit* $s_0 \in \mathbf{C}$. *Soit*

$$F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

une série de Dirichlet qui converge en s_0. *Alors, elle converge uniformément sur tout compact contenu dans* D_{s_0}. *De plus elle converge normalement sur* $D_{s_0+1+\delta}$ *(*δ *nombre réel* > 0*).*

Démonstration. — Soit ϵ un nombre réel > 0. Posons $F_n(s) = \sum_{k=1}^{n} a_k/k^s$. Soit C un compact de D_{s_0}. Il existe alors des nombres réels $\mu > 0$ et $\lambda > 0$ tels que $\Re(s - s_0) > \mu$ et $|s - s_0| < \lambda$ $(s \in C)$. Comme la série $F(s_0)$ converge, la suite $F_n(s_0)$ est bornée en valeur absolue par un nombre réel F_0. Pour m et n entiers positifs assez grands vérifiant $n > m$ et pour $s \in C$, on a l'inégalité

$$|\frac{F_m(s_0)}{m^{s-s_0}}| < \frac{F_0}{m^\mu} < \epsilon/3.$$

On a, pour $s \in C$,

$$|F_n(s) - F_m(s)| = |\sum_{k=m+1}^{n} \frac{a_k}{k^s}| = |\sum_{k=m+1}^{n} \frac{a_k}{k^{s_0}}.\frac{1}{k^{s-s_0}}|.$$

On obtient, en utilisant la formule de sommation d'Abel,

$$|F_n(s) - F_m(s)| = |\frac{F_n(s_0)}{n^{s-s_0}} - \frac{F_{m+1}(s_0)}{(m+1)^{s-s_0}} + \sum_{k=m+1}^{n-1} F_k(s_0)(\frac{1}{k^{s-s_0}} - \frac{1}{(k+1)^{s-s_0}})|$$

$$< \epsilon/3 + \epsilon/3 + |\sum_{k=m+1}^{n-1} F_k(s_0) \int_k^{k+1} \frac{(s-s_0)}{x^{s-s_0+1}}\, dx|$$

$$\leq 2\epsilon/3 + |s - s_0| F_0 \sum_{k=m+1}^{n-1} |\frac{1}{k^{s-s_0+1}}|.$$

$$\leq 2\epsilon/3 + F_0\lambda \sum_{k=m+1}^{\infty} |\frac{1}{k^{\mu+1}}|.$$

Pour m assez grand le troisième terme est $< \epsilon/3$ pour tout $s \in C$; on a alors

$$|F_n(s) - F_m(s)| < \epsilon$$

et donc la convergence uniforme cherchée.

Comme la série $F(s_0)$ converge, la suite de terme général a_n/n^{s_0} tend vers 0. Il existe donc un nombre réel $B > 0$ tel que $|a_n| < B|n^{s_0}|$. On a donc

$$\frac{|a_n|}{n^s} \leq \frac{B}{|n^{s-s_0}|} \leq \frac{B}{n^{1+\delta}}.$$

On en déduit la convergence normale cherchée.

Lemme 2. — *Soit*

$$F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

une série de Dirichlet. Supposons qu'il existe des nombres réels σ et B qui sont > 0 tels qu'on ait, pour tout n entier ≥ 1,

$$|a_1 + a_2 + ... + a_n| \leq Bn^\sigma.$$

Alors F converge sur D_σ.
Démonstration. — Posons

$$A_n = a_1 + a_2 + ... + a_n.$$

Soient n et m deux entiers tels que $n > m$. Soit $s \in D_\sigma$. On a les inégalités

$$|\sum_{k=m+1}^{n} \frac{a_k}{k^s}| = |\frac{A_n}{n^s} - \frac{A_m}{m^s}| + |\sum_{k=m+1}^{n-1} A_k(\frac{1}{k^s} - \frac{1}{(k+1)^s}|$$

$$\leq B|n^{\sigma-s}| + B|m^{\sigma-s}| + \sum_{m+1}^{n-1} |A_k \int_k^{k+1} \frac{s}{x^{s+1}}\, dx|$$

$$\leq B|n^{\sigma-s}| + B|m^{\sigma-s}| + B\sum_{m+1}^{n-1} |s||\frac{1}{k^{1+s-\sigma}}|.$$

On en déduit la convergence cherchée.

2. La fonction ζ de Riemann

C'est la série de Dirichlet la plus célèbre qui soit ; elle est donnée par la formule suivante :

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Le théorème de décomposition des nombres entiers en produit de facteurs premiers nous permet de l'écrire comme un produit eulerien

$$\zeta(s) = \prod_p (\sum_{n=1}^{\infty} \frac{1}{p^{ns}}) = \prod_p \frac{1}{1 - \frac{1}{p^s}},$$

où les produits portent sur les nombres premiers. Le passage du premier au deuxième membre de la dernière série d'égalités demande un raisonnement de convergence. Le produit eulerien donne la formule suivante

$$\log(\zeta(s)) = -\sum_p (\log(1 - p^{-s})) = \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{ns}}$$

(où p parcourt les nombres premiers, et où s est un nombre complexe de partie réelle > 1). D'après le lemme 2, la série qui définit la fonction ζ converge sur D_1, puisque la somme des

n premiers coefficients de cette série de Dirichlet est égale à n. En réalité on a le résultat plus précis suivant.

PROPOSITION 1. — *La fonction ζ se prolonge en une fonction méromorphe sur D_0 avec un seul pôle, qui est simple, en 1. De plus le résidu de ζ en 1 est égal à 1.*
Démonstration. — Soit r un entier > 1. Considérons la série de Dirichlet

$$\zeta_r(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

où on a posé $a_n = 1$ si r ne divise pas n et $a_n = 1 - r$ sinon. On a, pour tout entier $n \geq 0$,

$$0 \leq a_1 + a_2 + ... + a_n \leq r.$$

La fonction ζ_r converge donc sur D_0 d'après le lemme 2.

On a, pour $s \in D_1$,

$$\zeta_r(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} - \sum_{n=1}^{\infty} \frac{r}{(nr)^s} = (1 - r^{1-s})\zeta(s).$$

Cela prouve que ζ admet un prolongement méromorphe sur D_0. Les pôles de ζ sont des pôles communs à toutes les fonctions $1/(1 - r^{1-s})$ lorsque r varie. Le seul pôle que ces fonctions aient en commun est en $s = 1$ (considérer par exemple les cas $r = 2$ et $r = 3$) et il est simple.

Le résidu en 1 de la fonction $s \mapsto 1 - r^{1-s}$ est égal à $\log(r)$. Par ailleurs on a

$$\zeta_r(1) = \lim_{k \longrightarrow \infty} 1 + 1/2 + 1/3 + ... + 1/kr - (1 + 1/2 + ... + 1/k).$$

En utilisant la formule asymptotique au voisinage de $+\infty$

$$\log x \simeq 1 + 1/2 + ... + 1/x,$$

on obtient

$$\zeta_r(1) = \lim_{k \longrightarrow \infty} (\log(kr) - \log(k)) = \log(r).$$

Cela prouve la formule de résidu cherchée.

3. La fonction ζ de Dedekind

Soit K un corps de nombres. Notons d le degré de l'extension $K|\mathbf{Q}$. Posons

$$\zeta_K(s) = \sum_I \frac{1}{N_I^s},$$

où I parcourt les idéaux entiers de K. C'est la *fonction ζ de Dedekind* de K. On a bien entendu

$$\zeta_{\mathbf{Q}} = \zeta.$$

Rappelons que N_I désigne la norme absolue de I vue comme un entier > 0.

Puisque ces normes sont des nombres entiers, on peut écrire la fonction ζ_K comme une série de Dirichlet

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

où a_n est le nombre (fini) d'idéaux de norme n. C'est sous cet angle que l'on va considérer les questions de convergence.

PROPOSITION 2. — *La fonction ζ_K est analytique sur D_1.*
Démonstration. — Posons

$$F_K(s) = \prod_{\mathcal{P}} \frac{1}{1 - N_{\mathcal{P}}^{-s}}$$

où $\mathcal{P}$ parcourt les idéaux maximaux de $\mathcal{O}_K$. Etudions la convergence de ce produit. On a

$$\log(F_K(s)) = \sum_{\mathcal{P}} \sum_{n=1}^{\infty} \frac{1}{n N_{\mathcal{P}}^{ns}}.$$

Rappelons qu'on a $N_{\mathcal{P}} = p^{f_{\mathcal{P}}}$ où $f_{\mathcal{P}}$ est le degré résiduel en $\mathcal{P}$ de l'extension $K|\mathbf{Q}$ et où p est le nombre premier au-dessous de $\mathcal{P}$. En particulier on a $N_{\mathcal{P}} \geq p$ et

$$\sum_{\mathcal{P}|p} 1 \leq \sum_{\mathcal{P}|p} f_{\mathcal{P}} e_{\mathcal{P}} = d.$$

On a donc

$$|\log(F_K(s))| = |\sum_{p} \sum_{\mathcal{P}|p} \sum_{n} \frac{1}{n p^{f_{\mathcal{P}} s}}| \leq \sum_{p} \sum_{n} \frac{d}{n p^{\Re(s)}} = d \log(\zeta(\Re(s))).$$

On en déduit la convergence normale de $F_K(s)$ sur $D_{1+\delta}$ (δ nombre réel > 0) et donc la convergence sur D_1.

Par le théorème de factorisation des idéaux dans $\mathcal{O}_K$ et par multiplicativité de la norme, on a

$$\zeta_K(s) = \prod_{\mathcal{P}} \sum_{n=1}^{\infty} \frac{1}{N_{\mathcal{P}}^{ns}}.$$

Cette dernière quantité coïncide avec $F_K(s)$. Cela achève de prouver la proposition.

Remarque . — On retiendra le développement en produit eulerien

$$\zeta_K(s) = \prod_{\mathcal{P}} \frac{1}{1 - \frac{1}{N_{\mathcal{P}}^s}}.$$

4. La formule du nombre de classes

Soit K un corps de nombres. On note d le degré de l'extension $K|\mathbf{Q}$, ω_K le nombre de racines de l'unité contenues dans K, h_K le nombre de classes de K, $\mathcal{D}_K$ le discriminant absolu de K, $\mathrm{reg}(K)$ le régulateur de K (voir section suivante) et r_1 (resp. $2r_2$) le nombre de plongements réels (resp. complexes non réels) de K.

THÉORÈME 1. — *La fonction ζ_K admet un prolongement méromorphe sur $D_{1-1/d}$ avec un unique pôle, qui est simple, en $s = 1$. Le résidu de ζ_K en ce pôle est donné par la formule*

$$\lim_{s \longrightarrow 1^+} (s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}\mathrm{reg}(K)h_K}{\omega_K|\mathcal{D}_K|^{1/2}}.$$

Démonstration. — Soit $R \in \mathcal{C}\ell(K)$ une classe. Posons

$$\zeta_K(R,s) = \sum_{I \in R, I \subset \mathcal{O}_K} \frac{1}{N_I^s} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Dans la formule ci-dessus, a_n est le nombre d'idéaux entiers appartenant à R de norme n. On a

$$\zeta_K(s) = \sum_{R \in \mathcal{C}\ell(K)} \zeta_K(R,s).$$

Le nombre $A_n = a_1 + a_2 + ... + a_n$ est le nombre d'éléments de R qui sont entiers et de norme $\leq n$.

Admettons, pour le moment, la formule asymptotique suivante (voir le théorème 2 ci-dessous) :

$$A_n = \frac{2^{r_1}(2\pi)^{r_2}\mathrm{reg}(K)}{\omega_K|\mathcal{D}_K|^{1/2}} n + O(n^{1-1/d}).$$

On remarquera que le terme dominant de cette dernière expression est indépendant de R.

Considérons la série de Dirichlet

$$F(s) = \zeta_K(R,s) - \frac{2^{r_1}(2\pi)^{r_2}\mathrm{reg}(K)}{\omega_K|\mathcal{D}_K|^{1/2}}\zeta(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}.$$

On a alors la formule asymptotique

$$b_1 + b_2 + ... + b_n = A_n - \frac{2^{r_1}(2\pi)^{r_2}\mathrm{reg}(K)}{\omega_K|\mathcal{D}_K|^{1/2}} n = O(n^{1-1/d}).$$

On en déduit que la série $F(s)$ converge sur $D_{1-1/d}$ d'après le lemme 2. Si bien que les séries de Dirichlet ζ_K et $\zeta_K(R,.)$ s'étendent en des fonctions méromorphes sur $D_{1-1/d}$ puisque ζ est une fonction méromorphe sur D_0.

On a de plus la formule asymptotique

$$\zeta_K(R,s) \simeq_{s=1} \frac{2^{r_1}(2\pi)^{r_2}\mathrm{reg}(K)}{\omega_K|\mathcal{D}_K|^{1/2}}\zeta(s)$$

Comme la fonction ζ admet un pôle simple en $s=1$ et de résidu 1 et comme les fonction $\zeta(R,s)$ sont à valeurs >0 lorsque s est un nombre réel >1, on a, en sommant sur les classes, la formule asymptotique

$$\zeta_K(s) \simeq_{s=1} \frac{2^{r_1}(2\pi)^{r_2}\mathrm{reg}(K)h_K}{\omega_K|\mathcal{D}_K|^{1/2}}\zeta(s).$$

Cela donne la formule cherchée.

Remarque . — La formule du nombre de classes est due à Dirichlet. Son intérêt n'est pas seulement esthétique : elle est utile pour calculer le nombre de classes d'un corps de nombres dans beaucoup de cas.

On appréciera le fait que la fonction ζ de Dedekind est bâtie (comme produit eulerien) à partir seulement du nombre d'éléments de tous les corps résiduels de K. Chacun de ses corps résiduel ne contient qu'une information infime sur K. Pourtant la fonction ζ_K donne des renseignements sur les propriétés globales de K. La propriété de prolongement analytique (voir les compléments ci-dessous) est tout aussi surprenante, puisque qu'un produit eulerien quelconque n'a guère de raison de se prolonger en une fonction analytique en dehors du domaine de convergence connu *a priori*; ce prolongement est donc le signe d'une compatibilité profonde entre les facteurs du produit eulerien, *i.e.* d'une compatibilité entre tous les corps résiduels associés au corps de nombres K.

5. Dénombrement d'idéaux dans une classe

Soit K un corps de nombres. Soit

$$\mathcal{M} = \prod_{v\in S_K} \mathcal{P}_v^{n_v}$$

un cycle arithmétique.

Notons $K_{\mathcal{M}}$ le rayon modulo $\mathcal{M}$. Posons

$$\mathcal{O}_{\mathcal{M}} = \mathcal{O}_K^* \cap K_{\mathcal{M}}.$$

C'est un sous-groupe d'indice fini de $\mathcal{O}_K^*$ puisque $\mathbf{A}_K^*(\mathcal{M})$ est un sous-groupe d'indice fini de $\mathbf{A}_K^*(1)$ (proposition IX-3).

Notons $\omega_{\mathcal{M}}$ le nombre de racines de l'unité qui sont dans $\mathcal{O}_{\mathcal{M}}$. Notons $h_{\mathcal{M}}$ le nombre de classes de rayon $\mathcal{M}$. Notons r_0 le nombre d'éléments v de S_∞ tels que $n_v=1$. Posons

$$\mathcal{M}_\infty = \prod_{v\in S_\infty} \mathcal{P}_v^{n_v}$$

et

$$\mathcal{M}_0 = \prod_{v \in S_K - S_\infty} \mathcal{P}_v^{n_v}.$$

On identifie $\mathcal{M}_0$ à un idéal de $\mathcal{O}_K$ encore noté $\mathcal{M}_0$. On pose

$$N_{\mathcal{M}} = 2^{r_0} N_{\mathcal{M}_0}.$$

Revenons sur le plongement logarithmique défini pour démontrer le théorème des unités. Considérons le plongement logarithmique

$$\Lambda : \qquad K^* \longrightarrow \mathbf{R}^{r_1+r_2}$$

$$x \mapsto (\log(|\sigma_1(x)|), ..., \log(|\sigma_{r_1}(x)|), 2\log(|\sigma_{r_1+1}(x)|), ..., 2\log(|\sigma_{r_1+r_2}(x)|)).$$

Le groupe $\Lambda(\mathcal{O}_K^*)$ est un réseau de l'hyperplan H de $\mathbf{R}^{r_1+r_2}$ formé par les éléments $(x_1, ..., x_{r_1+r_2})$ vérifiant $\sum_{i=1}^{r_1+r_2} x_i = 0$ (voir le théorème des unités). Puisque $\mathcal{O}_{\mathcal{M}}$ est un sous-groupe d'indice fini de $\mathcal{O}_K^*$, $\Lambda(\mathcal{O}_{\mathcal{M}})$ est un réseau de H. Le *régulateur* $\mathrm{reg}\,(\mathcal{M})$ est le volume de ce réseau. On peut l'écrire, si on le désire, comme déterminant déduit du plongement logarithmique d'un système fondamental d'unités de $\mathcal{O}_{\mathcal{M}}$ (c'est-à-dire une base sur $\mathbf{Z}$ de $\mathcal{O}_{\mathcal{M}}$ aux racines de l'unité près).

THÉORÈME 2. — *Soit $R \in \mathcal{C}\ell(K)^{\mathcal{M}}$. Le nombre $n(R,t)$ d'idéaux de $\mathcal{O}_K$ contenus dans R et de norme $\leq t$ est donné par la formule asymptotique*

$$n(R,t) = \frac{2^{r_1}(2\pi)^{r_2}\mathrm{reg}(\mathcal{M})}{\omega_{\mathcal{M}} N_{\mathcal{M}} |\mathcal{D}_K|^{1/2}} t + O(t^{1-1/d}).$$

Démonstration. — Soit I_0 un idéal de $\mathcal{O}_K$ qui est un élément de R^{-1}. Tout élément de R dans $\mathcal{O}_K$ est de la forme I/I_0 avec I idéal principal de $\mathcal{O}_K$ de rayon $\mathcal{M}$ engendré, disons, par un élément $\alpha \in I_0 \cap K^{\mathcal{M}}$.

Par conséquent $n(R,t)$ est le nombre d'idéaux entiers et principaux de rayon $\mathcal{M}$, $I \in R$ tels que $N_{I/I_0} \leq t$, c'est-à-dire $N_I \leq t N_{I_0}$.

Au lieu de compter ces idéaux, comptons leurs générateurs. Remarquons au préalable que deux éléments de $K_{\mathcal{M}} \cap \mathcal{O}_K$ engendrent le même idéal de $\mathcal{O}_K$ si et seulement si leur rapport est une unité. On a donc une suite exacte de groupes abéliens

$$1 \longrightarrow \mathcal{O}_{\mathcal{M}} \longrightarrow K_{\mathcal{M}} \longrightarrow \mathcal{I}(K)^{\mathcal{M}} \longrightarrow \mathcal{C}\ell(K)^{\mathcal{M}} \longrightarrow 1.$$

On en déduit que $n(R,t)$ est le nombre d'éléments de l'ensemble quotient

$$\frac{\{\alpha \in I_0 \cap K_{\mathcal{M}} / |\mathrm{N}_{K/\mathbf{Q}}\alpha| \leq t N_{I_0}\}}{\mathcal{O}_{\mathcal{M}}}.$$

Posons

$$W = (1, 1, ..., 1, 2, ..., 2) \in \mathbf{R}^{r_1+r_2},$$

où les r_1 premières coordonnées sont égales à 1. On a $\Lambda(\mathbf{Q}^*) \subset \mathbf{R}W$. Pour $\alpha \in K^*$, on a $\Lambda(\alpha) \in \Lambda(\mathcal{O}_\mathcal{M})$ et donc $\Lambda(\alpha/(\mathrm{N}_{K/\mathbf{Q}}\alpha)^{1/d}) \in \Lambda(\mathcal{O}_\mathcal{M}) + \mathbf{R}W$.

Soit $P_\mathcal{M}$ un parallélépipède fondamental de H pour le réseau $\Lambda(\mathcal{O}_\mathcal{M})$. On a par définition

$$\mathrm{reg}(\mathcal{M}) = \mathrm{vol}(P_\mathcal{M}).$$

Un représentant d'une classe de K^* modulo $\mathcal{O}_\mathcal{M}$ est donc donné par un élément α tel que $\Lambda(\alpha) \in P_\mathcal{M} + \mathbf{R}W$.

On en déduit que $\omega_\mathcal{M} n(R,t)$ est le nombre d'éléments $\alpha \in I_0 \cap K_\mathcal{M}$ vérifiant les conditions $|\mathrm{N}_{K/\mathbf{Q}}\alpha| \leq tN_{I_0}$ et $\Lambda(\alpha) \in P_\mathcal{M} + \mathbf{R}W$. La condition $|\mathrm{N}_{K/\mathbf{Q}}\alpha| \leq tN_{I_0}$ revient à

$$|\mathrm{N}_{K/\mathbf{Q}} \frac{\alpha}{(tN_{I_0})^{1/d}}| \leq 1.$$

Identifions $\mathcal{O}_K \otimes \mathbf{R}$ à $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ via les plongements archimédiens de K. Cela permet d'étendre le plongement logarithmique Λ en une fonction

$$\mathbf{R}^{*r_1} \times \mathbf{C}^{*r_2} \longrightarrow \mathbf{R}^{r_1+r_2}$$

obtenue comme somme des logarithmes des valeurs absolues.

Posons

$$\Gamma_\mathcal{M} = \{Y \in \mathcal{O}_K \otimes \mathbf{R}/0 < |\mathrm{N}_{K/\mathbf{Q}}Y| \leq 1, \Lambda(Y) \in P_\mathcal{M} + \mathbf{R}W\}.$$

C'est l'ensemble des r_1+r_2-uplets $\{(x_1, x_2, ..., x_{r_1}, z_{r_1+1}, ..., z_{r_1+r_2}) \in \mathbf{R}^{*r_1} \times \mathbf{C}^{*r_2}$ vérifiant les conditions

$$\log|x_1| + ... + \log|x_{r_1}| + 2\log|z_{r_1+1}| + ... + 2\log|z_{r_1+r_2}| < 0,$$

et

$$(\log|x_1|, ..., \log|x_{r_1}|, 2\log|z_{r_1+1}|, ..., 2\log|z_{r_1+r_2}|) \in P_\mathcal{M} + \mathbf{R}W.$$

Revenons à notre dénombrement. On a

$$\omega_\mathcal{M} n(R,t) = |I_0 \cap K_\mathcal{M} \cap (tN_{I_0})^{1/d}\Gamma_\mathcal{M}|.$$

Un *réseau translaté* d'un espace vectoriel réel V est un sous-ensemble de V de la forme $v + L$, où $v \in V$ et où L est un réseau de V. L'intersection de deux réseaux translatés contenus dans un réseau translaté commun est vide ou est un réseau translaté.

L'ensemble $I_0 \cap K_\mathcal{M}$ est l'intersection de l'ensemble des éléments de $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ ayant r_0 coordonnées > 0 (celles correspondant aux places réelles v en lesquelles on a $n_v = 1$) et de $I_0 \cap (1 + \mathcal{M}_0)$. L'ensemble $I_0 \cap (1 + \mathcal{M}_0)$ est non vide par le théorème d'approximation. C'est donc un réseau translaté de $\mathcal{O}_K \otimes \mathbf{R}$ car tous ces réseaux translatés sont contenus dans $\mathcal{O}_K$. Notons $\Gamma'_\mathcal{M}$ l'ensemble des éléments de $\Gamma_\mathcal{M}$ ayant des coordonnées > 0 en toutes les places v en lesquelles on a $n_v = 1$. On a donc

$$\omega_\mathcal{M} n(R,t) = |I_0 \cap (1 + \mathcal{M}_0) \cap (tN_{I_0})^{1/d}\Gamma'_\mathcal{M}|.$$

Lemme 1. — *Soit L un réseau translaté de $\mathcal{O}_K \otimes \mathbf{R}$. On a la formule asymptotique, lorsque λ tend vers l'infini,*

$$|L \cap \lambda\Gamma_{\mathcal{M}}| = \lambda^d \frac{\mathrm{vol}(\Gamma_{\mathcal{M}})}{\mathrm{vol}(L)} + O(\lambda^{d-1}).$$

Démonstration. — Le bord $\partial\Gamma_{\mathcal{M}}$ de $\Gamma_{\mathcal{M}}$ est l'ensemble formé par les $r_1 + r_2$-uplets $\{(x_1, x_2, ..., x_{r_1}, z_{r_1+1}, ..., z_{r_1+r_2}) \in \mathbf{R}^{*r_1} \times \mathbf{C}^{*r_2}$ vérifiant les conditions

$$\log|x_1| + ... + \log|x_{r_1}| + 2\log|z_{r_1+1}| + ... + 2\log|z_{r_1+r_2}| = 0,$$

et

$$(\log|x_1|, ..., \log|x_{r_1}|, 2\log|z_{r_1+1}|, ..., 2\log|z_{r_1+r_2}|) \in \partial P_{\mathcal{M}} + \mathbf{R}W,$$

où $\partial P_{\mathcal{M}}$ est le bord du parallélépipède $P_{\mathcal{M}}$ dans H.

Soit P un parallélépipède fondamental de L. Notons x_λ le nombre de parallélépipèdes fondamentaux de $\mathcal{O}_K \otimes \mathbf{R}$ translatés de P qui rencontrent le bord de $\lambda\Gamma_{\mathcal{M}}$. On a les inégalités

$$\mathrm{vol}(P)(|L \cap \lambda\Gamma_{\mathcal{M}}| - x_\lambda) \leq \mathrm{vol}(\lambda\Gamma_{\mathcal{M}}) \leq \mathrm{vol}(P)(|L \cap \lambda\Gamma_{\mathcal{M}}| + x_\lambda).$$

Le bord de $\Gamma_{\mathcal{M}}$ est recouvrable par les images d'un nombre fini (disons k) de paramétrisations $(d-1)$-Lipschitzienne, c'est-à-dire d'applications $\phi : \Omega \longrightarrow \Gamma_{\mathcal{M}}$ telles qu'il existe $C > 0$ avec $|\phi(x) - \phi(y)| \leq C|x - y|$, et où Ω est le cube unité de $\mathbf{R}^{d-1}$. Cela résulte du fait que le bord de $P_{\mathcal{M}}$ est constitué de 2^{d-1} parallélépipèdes qui sont tous paramétrables par des cubes et du fait que Λ est un difféomorphisme sur $\Gamma_{\mathcal{M}}$. Les applications $\lambda\phi$ définissent des paramétrisations $d-1$-Lipschitziennes. L'image de chaque paramétrisation $\lambda\phi$ est de diamètre borné par le produit du diamètre de Ω et de $C\lambda^{d-1}$. Le nombre d'éléments de L contenus dans l'image de ϕ est borné par une constante dépendant linéairement de ce diamètre. Comme il n'y a qu'un nombre fini de paramétrisations à considérer, x_λ est majoré par λ^{d-1} multiplié par une constante dépendant du nombre de paramétrisations et de C. Ceci achève la démonstration, un peu sèche, du lemme 1.

Puisque I_0 et $\mathcal{M}_0$ sont premiers entre eux, le volume du réseau translaté $I_0 \cap (1 + \mathcal{M}_0)$ est donné par la formule

$$\mathrm{vol}(I_0 \cap (1 + \mathcal{M}_0)) = \mathrm{vol}(I_0 \cap \mathcal{M}_0) = \mathrm{vol}(I_0\mathcal{M}_0).$$

D'après la théorie de Minkowski (proposition V-6), on a

$$\mathrm{vol}(I_0\mathcal{M}_0) = N_{I_0\mathcal{M}_0} 2^{-r_2} |\mathcal{D}_K|^{1/2} = N_{I_0} N_{\mathcal{M}_0} 2^{-r_2} |\mathcal{D}_K|^{1/2}.$$

On a donc

$$n(R, t) = \frac{\mathrm{vol}(\Gamma'_{\mathcal{M}}) 2^{r_2}}{N_{\mathcal{M}_0} |\mathcal{D}_K|^{1/2} \omega_{\mathcal{M}}} t + O(t^{1-1/d}).$$

Il reste à calculer le volume de $\Gamma'_{\mathcal{M}}$. Comme $\Gamma_{\mathcal{M}}$ est invariant par symétrie par rapport à tout hyperplan de coordonnées, on a

$$\mathrm{vol}(\Gamma_{\mathcal{M}}) = 2^{r_0} \mathrm{vol}(\Gamma'_{\mathcal{M}}) = N_{\mathcal{M}_\infty} \mathrm{vol}(\Gamma'_{\mathcal{M}}).$$

Comme $\Gamma_{\mathcal{M}}$ est invariant par action du groupe $\{-1,+1\}^{r_1} \times \{z \in \mathbf{C}/|z|=1\}^{r_2})$, on a

$$\mathrm{vol}(\Gamma_{\mathcal{M}}) = 2^{r_1}(2\pi)^{r_2}\mathrm{vol}(\Gamma^+_{\mathcal{M}}),$$

où on a posé

$$\Gamma^+_{\mathcal{M}} = \Gamma_{\mathcal{M}} \cap \mathbf{R}_+^{*r_1+r_2}.$$

On a donc

$$n(R,t) = \frac{2^{r_1}(2\pi)^{r_2}\mathrm{vol}(\Gamma^+_{\mathcal{M}})2^{r_2}}{N_{\mathcal{M}}|\mathcal{D}_K|^{1/2}\omega_{\mathcal{M}}}t + O(t^{1-1/d}).$$

Il reste à déterminer le volume de $\Gamma^+_{\mathcal{M}}$. Le plongement logarithmique Λ induit un difféomorphisme

$$\Gamma^+_{\mathcal{M}} \longrightarrow P_{\mathcal{M}} + \mathbf{R}_- W.$$

Le déterminant jacobien de ce difféomorphisme en $(y_1, ..., y_{r_1+r_2})$ est égal à

$$2^{-r_2} y_1 ... y_{r_1+r_2}.$$

Utilisons le changement de variables fourni par Λ pour calculer le volume de $\Gamma_{\mathcal{M}}$: on a

$$\mathrm{vol}(\Gamma^+_{\mathcal{M}}) = \int_{\Gamma^+_{\mathcal{M}}} d\mu = \int_{P_{\mathcal{M}}+\mathbf{R}W, x_1+...+x_{r_1+r_2}<0} 2^{-r_2} e^{x_1+...+x_{r_1+r_2}}\, dx_1...dx_{r_1+r_2}.$$

Ecrivons la mesure de Lebesgue de $\mathbf{R}^{r_1+r_2}$ suivant le produit $\mathbf{R}W \times H$:

$$d\mu = dx_1...dx_{r_1+r_2} = dt\, d\mu_H,$$

où $d\mu_H$ est la mesure de Lebesgue sur H. On a alors

$$\mathrm{vol}(\Gamma^+_{\mathcal{M}}) = 2^{-r_2}\int_{-\infty}^{0} e^t\, dt \int_{P_{\mathcal{M}}} d\mu_H = \mathrm{vol}(P_{\mathcal{M}}) = 2^{-r_2}\mathrm{reg}(\mathcal{M}).$$

Cela achève de prouver le théorème.

Remarque . — On a besoin seulement du cas $\mathcal{M} = 1$ pour la formule du nombre de classes.

Le théorème 2 est important pour démontrer le théorème de Chebotarev. Mais, dans ce but, on n'a pas besoin de déterminer le coefficient dominant dans la formule du théorème 2.

Cette dernière formule permet de démontrer une formule plus précise que la formule du nombre de classes :

$$\lim_{s \longrightarrow 1^+}(s-1)(\sum_{I \in R}\frac{1}{N_I^s}) = \frac{2^{r_1}(2\pi)^{r_2}\mathrm{reg}(\mathcal{M})}{\omega_{\mathcal{M}}|\mathcal{D}_K|^{1/2}N_{\mathcal{M}}},$$

où R est une classe d'idéaux de rayon $\mathcal{M}$.

6. Compléments

Rappelons que la fonction Γ d'Euler d'une variable complexe s est donnée par la formule

$$\Gamma(s) = \int_0^\infty e^{-t} t^s \, \frac{dt}{t},$$

pour s nombre complexe de partie réelle > 0 Cette fonction se prolonge en une fonction méromorphe sur $\mathbf{C}$. Posons

$$G_1(s) = \pi^{-s/2}\Gamma(s/2)$$

et

$$G_2(s) = (2\pi)^{1-s}\Gamma(s).$$

Soit K un corps de nombres. Posons

$$\xi_K(s) = G_1(s)^{r_1} G_2(s)^{r_2} \zeta_K(s).$$

Observons que si on remplace ζ_K par son produit eulerien, la formule de ξ devient un produit dont les facteurs sont en bijection avec les places de K, les fonctions G_1 et G_2 correspondant respectivement aux places réelles et complexes non réelles de K.

THÉORÈME 3. — *La fonction ξ_K se prolonge en une fonction méromorphe sur $\mathbf{C}$ avec des pôles, qui sont simples, seulement en 0 et 1. De plus elle satisfait l'équation fonctionnelle*

$$\xi_K(s) = |D_K|^{1/2-s} \xi_K(1-s).$$

Nous ne démontrerons pas ce théorème. Une démonstration fameuse en a été donnée par Tate dans sa thèse.

XI
Le théorème de densité de Chebotarev

1. La formulation par les idéaux de la théorie du corps de classe

Soit $L|K$ une extension abélienne de corps de nombres. Comme tout sous-groupe d'indice fini de C_K contient un sous-groupe de congruence $C_K^{\mathcal{M}}$, pour $\mathcal{M}$ cycle arithmétique approprié, le corps L est un sous-corps du corps de classe de rayon $\mathcal{M}$.

Considérons l'isomorphisme de groupes

$$C_K/C_K^{\mathcal{M}} \simeq \mathcal{C}\ell(K)^{\mathcal{M}}$$

Le fait que L soit contenu dans le corps de classe de rayon $\mathcal{M}$ s'exprime dans le diagramme suivant

$$1 \longrightarrow \mathrm{Gal}(H^{\mathcal{M}}/L) \longrightarrow \mathrm{Gal}(H^{\mathcal{M}}/K) \longrightarrow \mathrm{Gal}(L/K) \longrightarrow 1,$$

ce diagramme s'identifiant terme à terme à

$$1 \longrightarrow H/\mathcal{P}(K)^{\mathcal{M}} \longrightarrow \mathcal{C}\ell(K)^{\mathcal{M}} \longrightarrow \mathcal{I}(K)^{\mathcal{M}}/H \longrightarrow 1,$$

où H est un sous-groupe de $\mathcal{I}(K)^{\mathcal{M}}$ contenant $\mathcal{P}(K)^{\mathcal{M}}$.

La compatibilité locale-globale dans la théorie du corps de classe nous indique que l'extension $H^{\mathcal{M}}|K$ est non ramifiée en tout idéal premier à $\mathcal{M}$. C'est donc aussi le cas de l'extension $L|K$.

Puisque l'extension $L|K$ est abélienne, la substitution de Frobenius associée à un idéal premier $\mathcal{P}$ de L au-dessus de $\mathcal{Q}$ idéal premier de K ne dépend que de $\mathcal{Q}$. On peut donc la noter $\mathrm{Frob}_{\mathcal{Q}}$.

De plus dans l'isomorphisme de groupes

$$\mathrm{Gal}(L/K) \simeq \mathcal{I}(K)^{\mathcal{M}}/H$$

l'image de la substitution de Frobenius en $\mathcal{P}$ est la classe de l'idéal $\mathcal{P}$. Cela résulte du fait que l'isomorphisme de groupes construit par la proposition IX-2

$$C_K/C_K^{\mathcal{M}} \simeq \mathcal{C}\ell(K)^{\mathcal{M}}$$

associe à la classe d'une uniformisante en $\mathcal{P}$ (via l'homomorphisme canonique $\mathbf{K}_{\mathcal{P}}^* \longrightarrow C_K$) la classe de $\mathcal{P}$ dans le corps de classe de rayon $\mathcal{M}$.

Il résulte de cela que l'ordre d'un idéal premier $\mathcal{P}$ ne divisant pas $\mathcal{M}$ dans $\mathcal{C}\ell(K)^{\mathcal{M}}$ est égal l'ordre de la substitution de Frobenius dans $\mathrm{Gal}(H^{\mathcal{M}}/K)$ c'est-à-dire le degré résiduel

en $\mathcal{P}$ de l'extension $H^{\mathcal{M}}|K$. On en déduit encore que l'ordre de $\mathcal{P}$ dans $\mathcal{I}(K)^{\mathcal{M}}/H$ est égal au degré résiduel de l'extension $L|K$.

2. Rappels sur les caractères d'un groupe abélien fini

Soit G un groupe abélien et fini d'ordre n. Un homomorphisme de groupes

$$G \longrightarrow \{z \in \mathbf{C}/|z| = 1\}$$

s'appelle un *caractère* de G.

On note G^* le groupe des caractères de G. Rappelons-en quelques propriétés.

PROPOSITION 1. — *L'ordre de G^* est égal à n. L'homomorphisme de groupes $G \longrightarrow G^{**}$ qui à g associe $\chi \mapsto \chi(g)$ est un isomorphisme.*

Démonstration. — On remarque d'abord que pour tout sous-groupe H de G un caractère χ de H se prolonge en un caractère de G. Cela se démontre par récurrence sur l'indice de H dans G. Si cet indice est égal à 1, c'est évident. Sinon, on fait l'hypothèse de récurrence. Soit $x \in G - H$. Notons H' le sous-groupe de G engendré par x et H. On va construire un caractère χ' sur H' qui prolonge χ ; cela suffira pour conclure par hypothèse de récurrence, puisque l'indice de H' dans G est $<$ à l'indice de H dans G. Soit n le plus petit entier > 1 tel que $x^n \in H$. Posons $t = \chi(x^n)$. Soit $w \in \mathbf{C}^*$ tel que $w^n = t$. Posons, pour $k \in \mathbf{Z}$ et $h \in H$,

$$\chi'(x^k h) = w^k \chi(h).$$

Cela définit un caractère de H' prolongeant χ.

On a une application $G^* \longrightarrow H^*$ induite par la restriction à H dont le noyau est formé par les caractères triviaux sur H. On vient de voir que cette application est surjective. On a donc une suite exacte de groupes abéliens

$$1 \longrightarrow (G/H)^* \longrightarrow G^* \longrightarrow H^* \longrightarrow 1.$$

L'ordre de G^* est donc égal au produit des ordres de H^* et $(G/H)^*$.

Démontrons par récurrence sur n que G et G^* ont même ordre n. Si G est cyclique, ses caractères sont de la forme $x \mapsto \zeta^g$, où ζ est une racine n-ième de l'unité. Comme il y a n racines n-ièmes de l'unité le résultat s'en suit. Si G est non cyclique, il possède un sous-groupe cyclique H non trivial. Les ordres de H^* et $(G/H)^*$ sont égaux aux ordres de H et G/H par hypothèse de récurrence.

On a donc

$$|G| = |H||G/H| = |H^*||(G/H)^*| = |G^*|.$$

Les groupes G, G^* et G^{**} ont donc même ordre. Pour démontrer que l'application $x \mapsto (\chi \mapsto \chi(x))$ est un isomorphisme, il suffit donc de prouver qu'elle est injective. C'est-à-dire prouver que pour tout $x \in G$ il existe $\chi \in G^*$ tel que $\chi(x) \neq 1$. Un tel caractère existe lorsque G est cyclique. Dans le cas général il suffit pour cela de considérer un

prolongement à G d'un caractère χ' du sous-groupe cyclique H de G engendré par x tel que $\chi'(x) \neq 1$. Un tel caractère existe d'après ce qui précède.

On en déduit ce qui est essentiellement les relations d'orthogonalité des caractères de G.

COROLLAIRE . — *On a les deux relations suivantes, pour* $\chi \neq 1$

$$\sum_{g \in G} \chi(g) = 0$$

et pour $g \neq 1$

$$\sum_{\chi \in G^*} \chi(g) = 0.$$

De plus on a $\sum_{\chi \in G^*} 1 = g$ *et* $\sum_{g \in G} 1 = g$.
Démonstration. — Les deux dernières égalités sont évidentes compte-tenu de la proposition 1.

En raison de la dualité établie par la proposition 1, les deux premières égalités sont équivalentes. Démontrons la première. Soit $h \in G$ tel que $\chi(h) \neq 1$. On a

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(gh) = \sum_{g \in G} \chi(g).$$

La formule cherchée s'en suit.

3. Fonctions L de Dirichlet

Soit K un corps de nombres de degré d sur $\mathbf{Q}$. Soit $\mathcal{M}$ un cycle arithmétique de K. Soit χ un caractère du groupe des classes de rayon $\mathcal{M}$. On dit dans ce cas que $\mathcal{M}$ est le *niveau* du caractère χ.

Par abus de notation on note $\chi(I)$ pour l'image par χ de la classe d'un idéal I. De plus on pose $\chi(I) = 0$ lorsque I et $\mathcal{M}$ ne sont pas premiers entre eux. La fonction $I \mapsto \chi(I)$ est donc multiplicative.

La *fonction L de Dirichlet* associée à χ est la série de Dirichlet

$$L(\chi, s) = \sum_I \frac{\chi(I)}{N_I^s},$$

où I parcourt les idéaux entiers de K. On peut récrire cette série sous forme de produit eulerien :

$$L(\chi, s) = \prod_{\mathcal{P}} \frac{1}{1 - \chi(\mathcal{P}) N_{\mathcal{P}}^{-s}},$$

en utilisant la multiplicativité de χ et toujours le théorème de factorisation des idéaux. Il est facile de voir que cette série de Dirichlet converge sur D_1 (lemme X-2), puisque ses coefficients sont des nombres complexes de valeur absolue égale à 1.

PROPOSITION 2. — *Si χ est un caractère différent de 1, la fonction $L(\chi, s)$ se prolonge en une fonction holomorphe sur $D_{1-1/d}$.*
Démonstration. — Pour $R \in \mathcal{C}\ell(K)^{\mathcal{M}}$, on considère la fonction

$$\zeta(s, R) = \sum_{I \in R} \frac{1}{N_I^s},$$

où I parcourt les idéaux entiers K. Cette fonction est méromorphe sur $D_{1-1/d}$ (voir la démonstration du théorème X-1). On a

$$L(\chi, s) = \sum_{R \in \mathcal{C}\ell(K)^{\mathcal{M}}} \chi(R)\zeta(s, R).$$

Comme les fonctions $\zeta(s, R)$ n'ont des pôles qu'en 1 et comme les résidus correspondants sont tous égaux (démonstration du théorème X-1), la fonction $L(\chi, s)$ n'a pas de pôle en 1 en raison de la formule $\sum_R \chi(R) = 0$.

Considérons le corps de classe $H^{\mathcal{M}}$ de rayon $\mathcal{M}$. Notons $h_{\mathcal{M}}$ le nombre de classes de rayon $\mathcal{M}$.

PROPOSITION 3. — *On a*

$$\zeta_{H^{\mathcal{M}}}(s) = \prod_{\mathcal{P}|\mathcal{M}} \frac{1}{1 - N\mathcal{P}^{-s}} \prod_{\chi} L(\chi, s),$$

où χ parcourt les caractères du groupes des classes de rayon $\mathcal{M}$, et où $\mathcal{P}$ parcourt les idéaux premiers de $H^{\mathcal{M}}$ divisant $\mathcal{M}$.
Démonstration. — C'est un calcul direct. Dans ce qui suit, les sommes portant sur les caractères portent toutes sur tous les caractères du groupe des classes de rayon $\mathcal{M}$. Transformons les produits en sommes et utilisons le développement du logarithme :

$$\log(\prod_{\chi} L(\chi, s)) = \sum_{k=1}^{\infty} \sum_{\mathcal{Q}} \sum_{\chi} \frac{\chi(\mathcal{Q})^k}{k N_{\mathcal{Q}}^{ks}},$$

où $\mathcal{Q}$ parcourt les idéaux premiers de $\mathcal{O}_K$ ne divisant pas $\mathcal{M}$. En utilisant que χ est un homomorphisme de groupes, on obtient

$$\log(\prod_{\chi} L(\chi, s)) = \sum_{k=1}^{\infty} \sum_{\mathcal{Q}} (\sum_{\chi} \frac{\chi(\mathcal{Q}^k)}{k N_{\mathcal{Q}}^{ks}}).$$

En utilisant la formule $\sum_\chi \chi(R) = h_{\mathcal{M}}$ ou 0 suivant que R est nul ou non dans le groupe des classes de rayon $\mathcal{M}$, notre égalité devient

$$\log(\prod_\chi L(\chi, s)) = \sum_{k=1}^{\infty} \sum_{\mathcal{Q}, \mathcal{Q}^k \in \mathcal{P}(K)^{\mathcal{M}}} \frac{h_{\mathcal{M}}}{k N_{\mathcal{Q}}^{ks}}.$$

Par ailleurs $\mathcal{Q}^k$ est nul dans ce groupe des classes si et seulement si k est un multiple du degré résiduel $f_{\mathcal{Q}}$ de $\mathcal{Q}$ dans l'extension $H^{\mathcal{M}}|K$. Posons dans ce cas $k = f_{\mathcal{Q}} n$. Soit $\mathcal{P}$ l'idéal de $\mathcal{O}_K$ au-dessus de $\mathcal{Q}$. On a $N_{\mathcal{Q}}^{f_{\mathcal{P}}} = N_{\mathcal{P}}$.

On obtient

$$\log(\prod_\chi L(\chi, s)) = \sum_{\mathcal{Q}} \sum_{n=1}^{\infty} \frac{h_{\mathcal{M}}}{f_{\mathcal{P}} n N_{\mathcal{P}}^{f_{\mathcal{Q}} ns}}.$$

En utilisant la formule (et au passage le fait que $H^{\mathcal{M}}|K$ est non ramifié en $\mathcal{Q}$ par la théorie de corps de classe)

$$[H^{\mathcal{M}} : K] = h_{\mathcal{M}} = f_{\mathcal{P}} \sum_{\mathcal{P}|\mathcal{Q}} 1,$$

on obtient

$$\log(\prod_\chi L(\chi, s)) = \sum_{\mathcal{P} \not| \mathcal{M}} \sum_{n=1}^{\infty} \frac{1}{n N_{\mathcal{P}}^{ns}},$$

où $\mathcal{P}$ parcourt les idéaux premier de $H^{\mathcal{M}}$ ne divisant pas $\mathcal{M}$. Ajoutons à cette quantité

$$\log(\prod_{\mathcal{P}|\mathcal{M}} \frac{1}{1 - N_{\mathcal{P}}^{-s}}) = \sum_{\mathcal{P}|\mathcal{M}} \sum_{n=1}^{\infty} \frac{1}{n N_{\mathcal{P}}^{ns}}.$$

On obtient le logarithme de la fonction $\zeta_{H^{\mathcal{M}}}$.

Corollaire 1. — *On a, pour χ caractère du groupe des classes de rayon $\mathcal{M}$ différent de 1,*

$$L(\chi, 1) \neq 0.$$

Démonstration. — Pour $\chi = 1$, on a

$$L(\chi, s) = \zeta_K(s) \prod_{\mathcal{P}|\mathcal{M}} (1 - N_{\mathcal{P}}^{-s}).$$

Le facteur de droite de la dernière égalité est non nul en $s = 1$. On a d'après le théorème 2,

$$\zeta_{H^{\mathcal{M}}}(s) = \zeta_K(s) \prod_{\chi \neq 1} L(\chi, s) \prod_{\mathcal{P}|\mathcal{M}} (1 - N_{\mathcal{P}}^{-s}).$$

Les fonctions $\zeta_{H^{\mathcal{M}}}$ et ζ_K ont des pôles simples en $s = 1$. On en déduit le corollaire.

Soit $\mathcal{M}'$ un cycle arithmétique divisant $\mathcal{M}$. Les fonctions L de Dirichlet associées aux caractères triviaux sur les groupes de classes de rayon $\mathcal{M}$ et $\mathcal{M}'$ ne sont pas égales : leurs produits euleriens diffèrent en les idéaux premiers divisant $\mathcal{M}$ sans diviser $\mathcal{M}'$. Cela nous amène aux considérations suivantes.

On dit qu'un caractère de Dirichlet de niveau $\mathcal{M}$ est *primitif* s'il n'existe pas de caractère de Dirichlet χ' de niveau $\mathcal{M}'$ divisant strictement $\mathcal{M}$ tel que χ et χ' coïncident sur presque tout les idéaux premiers. En particulier le caractère trivial de niveau $\mathcal{M}$ n'est pas primitif, sauf si $\mathcal{M} = 1$. À tout caractère de Dirichlet χ de niveau $\mathcal{M}$ on peut associer un unique caractère de Dirichlet primitif de niveau $\mathcal{M}'$ qui coïncide avec χ en tout idéal premier ne divisant pas $\mathcal{M}$ ou divisant $\mathcal{M}'$. À tout caractère de Dirichlet χ' de niveau $\mathcal{M}'$ on peut associer un unique caractère de Dirichlet χ de niveau $\mathcal{M}$ (avec $\mathcal{M}'|\mathcal{M}$) qui coïncide avec χ en les idéaux premiers $\mathcal{P}$ ne divisant pas $\mathcal{M}$ et valant 0 en les autres idéaux premiers.

Proposition 4. — *On a*

$$\zeta_{H^{\mathcal{M}}}(s) = \prod_{\chi} L(\chi', s),$$

où χ' parcourt les caractères primitifs de niveau divisant $\mathcal{M}$.

Démonstration. — En effet, considérons la correspondance bijective $\chi' \mapsto \chi$ entre les caractère primitifs de niveau divisant $\mathcal{M}$ et les caractères de niveau $\mathcal{M}$. Les facteurs des produits euleriens de $L(\chi', s)$ et $L(\chi, s)$ sont égaux sauf ceux correspondant à $\mathcal{P}|\mathcal{M}$ et tel que $\mathcal{P}$ ne divise pas le niveau de χ'. Ces facteurs sont respectivement $1/(1 - \chi'(\mathcal{P})N_{\mathcal{P}}^{-s})$ et 1. On retrouve ainsi les facteurs manquant de la fonction $\zeta_{H^{\mathcal{M}}}$ dans l'énoncé de la proposition 3.

Remarque . — À tout caractère ϵ de $\mathrm{Gal}(\bar{K}/K)$ d'image finie correspond donc un caractère de Dirichlet en le sens suivant. Un caractère de $\mathrm{Gal}(\bar{K}/K)$ se factorise par $\mathrm{Gal}(L/K)$ où $L|K$ est une extension abélienne. Le groupe $\mathrm{Gal}(L/K)$ est un quotient de de $\mathrm{Gal}(H^{\mathcal{M}}/K)$ pour un certain rayon $\mathcal{M}$. On a donc un caractère de Dirichlet χ du corps de classe de rayon $\mathcal{M}$ tel que $\chi(\mathcal{P})$ soit égal à l'image par ϵ d'une substitution de Frobenius en $\mathcal{P}$ dans $\mathrm{Gal}(\bar{K}/K)$ (pour tout $\mathcal{P}$ idéal premier de K ne divisant pas $\mathcal{M}$). On peut donc associer une série L de Dirichlet à tout caractère d'image finie de $\mathrm{Gal}(\bar{K}/K)$. C'est

$$\prod_{\mathcal{P}} \frac{1}{1 - \chi \mathrm{Frob}_{\mathcal{P}} N_{\mathcal{P}}^{-s}}.$$

4. Densité de Dirichlet

Soit K un corps de nombres. Soit E un ensemble d'idéaux premiers de K. La limite, si elle existe, de quotients de séries de Dirichlet

$$\lim_{s \longrightarrow 1^+} \frac{\sum_{\mathcal{P} \in E} 1/N_{\mathcal{P}}^s}{\sum_{\mathcal{P}} 1/N_{\mathcal{P}}^s}$$

s'appelle la *densité de Dirichlet* de E. Un ensemble fini est de densité de Dirichlet nulle. Cette notion de densité de Dirichlet s'avère plus utile (et en un certain sens généralise) que la notion intuitive de *densité naturelle*, *i.e.* la limite, si elle existe,

$$\lim_{x\longrightarrow\infty}\frac{|\{\mathcal{P}\in E/N_{\mathcal{P}}\leq x\}|}{|\{\mathcal{P}/N_{\mathcal{P}}\leq x\}|}.$$

Proposition 5. — *La densité naturelle de E est donnée par la formule*

$$d(E)=\lim_{s\longrightarrow 1^+}\frac{\sum_{\mathcal{P}\in E}1/N_{\mathcal{P}}^s}{\log(\frac{1}{s-1})}.$$

Démonstration. — On a, avec $\mathcal{P}$ parcourant les idéaux premiers de K,

$$\log(\zeta_K(s))=\sum_{n=1}^{\infty}\sum_{\mathcal{P}}\frac{1}{nN_{\mathcal{P}}^{ns}}=\sum_{\mathcal{P}}\frac{1}{N_{\mathcal{P}}^s}+\sum_{n=2}^{\infty}\sum_{\mathcal{P}}\frac{1}{nN_{\mathcal{P}}^{ns}}.$$

Le deuxième terme du dernier membre est analytique en $s=1$; seul le premier terme compte vraiment pour définir les densités de Dirichlet.

Pour $\mathcal{P}$ idéal premier de K, notons $f_{\mathcal{P}}$ le degré résiduel absolu de K en $\mathcal{P}$. On a donc la formule asymptotique en $s=1^+$

$$\log(\zeta_K(s))\simeq\sum_{\mathcal{P}}\frac{1}{N_{\mathcal{P}}^s}\simeq\sum_{\mathcal{P},f_{\mathcal{P}}=1}\frac{1}{N_{\mathcal{P}}^s},$$

car la fonction

$$\sum_{\mathcal{P},f_{\mathcal{P}}\geq 2}\frac{1}{N_{\mathcal{P}}^s}$$

est analytique, puisqu'on a $N_{\mathcal{P}}=p^{f_{\mathcal{P}}}$. Rappelons qu'on a en 1^+ (en considérant le logarithme de $\zeta(s)$)

$$\log(\frac{1}{s-1})\simeq\sum_{\mathcal{P}}\frac{1}{p^s}.$$

Cela prouve le résultat.

On a le *théorème de densité de Dirichlet*, dont une généralisation est l'énoncé suivant.

Théorème 1. — *Soit $\mathcal{M}$ un cycle arithmétique de K. Soit H un sous-groupe de $\mathcal{I}(K)^{\mathcal{M}}$ d'indice h_0 contenant $\mathcal{P}(K)^{\mathcal{M}}$. Soit $R_0\in\mathcal{I}(K)^{\mathcal{M}}/H$. Alors on a*

$$d(R_0)=\frac{1}{h_0}.$$

Démonstration. — On a (où $\mathcal{P}$ parcourt les idéaux premiers de K)

$$h_0 \sum_{\mathcal{P}\in R_0} \frac{1}{N_{\mathcal{P}}^s} = \sum_{\mathcal{P}} (\sum_{\chi} \chi(\mathcal{P})\chi(R_0^{-1})) \frac{1}{N_{\mathcal{P}}^s} = \sum_{\chi} \chi(R_0^{-1}) \sum_{\mathcal{P}} \frac{\chi(\mathcal{P})}{N_{\mathcal{P}}^s}.$$

En isolant les termes correspondant à $\chi = 1$, cette dernière expression est équivalente en 1^+ à

$$\sum_{\mathcal{P}} \frac{1}{N_{\mathcal{P}}^s} + \sum_{\chi\neq 1} \chi(R_0^{-1}) \log(L(\chi, s)).$$

Le deuxième terme de cette dernière expression est analytique en $s = 1$ d'après le corollaire de la proposition 3. Le premier terme étant équivalent à $\log(\frac{1}{s-1})$ on en déduit le théorème.

Remarque . — Le théorème de densité de Dirichlet donne dans un cas particulier le théorème de la progression arithmétique.

5. Le théorème de Chebotarev

Soit $L|K$ une extension galoisienne de corps de nombres. Soit $\mathcal{P}$ un idéal premier de L au-dessus d'un idéal premier $\mathcal{Q}$ de K non ramifié dans l'extension $L|K$. La substitution de Frobenius en $\mathcal{P}$ ne dépend que de $\mathcal{Q}$ à conjugaison près dans $\mathrm{Gal}(L/K)$.

Soit C une classe de conjugaison de $\mathrm{Gal}(L/K)$. Notons P_C l'ensemble des idéaux premiers de K tels que la classe de conjugaison de la substitution de Frobenius en $\mathcal{P}$ soit égale à C.

Théorème 2. — *On a*

$$d(P_C) = \frac{|C|}{|\mathrm{Gal}(L/K)|}.$$

Démonstration. — On suppose d'abord que l'extension $L|K$ est cyclique et donc abélienne. On peut alors appliquer la théorie du corps de classe. Le corps L est contenu dans un corps de classe de rayon $H^{\mathcal{M}}$. Il existe un sous-groupe H de $\mathcal{I}(K)^{\mathcal{M}}$ et contenant $\mathcal{P}(K)^{\mathcal{M}}$ tel qu'on ait une suite exacte de groupes

$$1 \longrightarrow H/\mathcal{P}(K)^{\mathcal{M}} \longrightarrow \mathcal{I}(K)^{\mathcal{M}}/\mathcal{P}(K)^{\mathcal{M}} \longrightarrow \mathrm{Gal}(L/K) \longrightarrow 1.$$

Soit $\sigma \in \mathrm{Gal}(L/K)$. Puisque $\mathrm{Gal}(L/K)$ est abélien, la classe de conjugaison de σ est un singleton. Soit $R \in \mathcal{I}(K)^{\mathcal{M}}/H$ la classe associée à σ via l'isomorphisme de groupes $\mathcal{I}(K)^{\mathcal{M}}/H \simeq \mathrm{Gal}(L/K)$. On a

$$P_{\{\sigma\}} = \{\mathcal{P} \not| \mathcal{M}, \mathcal{P} \in R\}.$$

On a donc, d'après le théorème de Dirichlet,

$$d(P_{\{\sigma\}}) = \frac{1}{|\mathcal{I}(K)^{\mathcal{M}}/H|} = \frac{1}{|\mathrm{Gal}(L/K)|}.$$

Cela achève de traiter le cas cyclique.

Ne supposons plus l'extension $L|K$ cyclique. Soit $\sigma \in C$. Notons E le sous-corps de L fixé par σ. L'extension $L|E$ est cyclique. Notons $P(\sigma)$ l'ensemble des idéaux premier $\mathcal{P}$ de L tels que la substitution de Frobenius en $\mathcal{P}$ de $\mathrm{Gal}(L/K)$ coïncide avec σ.

L'application qui à $\mathcal{P}$ associe $\mathcal{P} \cap E$ définit une bijection entre $P(\sigma)$ et l'ensemble $P'(\sigma)$ formé par les idéaux premiers $\mathcal{Q}'$ de E tels que l'extension $E|K$ soit résiduellement triviale en $\mathcal{Q}'$ et tels que la substitution de Frobenius en tout idéal de L au-dessus de $\mathcal{Q}'$ soit égale à σ. L'extension $E|K$ est résiduellement triviale, si et seulement si on a, pour $\mathcal{Q}' \in P'(\sigma)$,

$$N_{\mathcal{Q}} = N_{\mathcal{Q}'},$$

où $\mathcal{Q} = \mathcal{P} \cap K$.

Par ailleurs, l'application qui à $\mathcal{P}$ associe associe $\mathcal{Q} = \mathcal{P} \cap K$ définit une application surjective de $P(\sigma)$ vers P_C (la surjectivité résulte du fait que les élements de C sont tous conjugués).

Le nombre T d'éléments de $P(\sigma)$ au dessus de $\mathcal{Q}$ est donné par la formule

$$T = |\{\tau \in \mathrm{Gal}(L/K)/\tau\sigma = \sigma\tau\}|/|D_{\mathcal{P}}|,$$

où $D_{\mathcal{P}}$ est le sous groupe de décomposition en $\mathcal{P}$ de $\mathrm{Gal}(L/K)$. Or on a par un argument direct de théorie des groupes

$$|\{\tau \in \mathrm{Gal}(L/K)/\tau\sigma = \sigma\tau\}| = |\mathrm{Gal}(L/K)|/|C|.$$

Par ailleurs on a, puisque σ engendre le sous-groupe de décomposition en $\mathcal{P}$, $D_{\mathcal{P}} = \mathrm{Gal}(L/E)$. On a donc

$$T = \frac{|\mathrm{Gal}(L/K)|}{|C||\mathrm{Gal}(L/E)|}.$$

Passons au calcul de la densité de Dirichlet de P_C. On a

$$d(P_C) = \lim_{s \longrightarrow 1^+} \frac{\sum_{\mathcal{Q} \in P_C} \frac{1}{N_{\mathcal{Q}}^s}}{\log(\frac{1}{s-1})}.$$

En comptant les idéaux de $P'(\sigma)$ on obtient

$$d(P_C) = \frac{1}{T} \lim_{s \longrightarrow 1^+} \frac{\sum_{\mathcal{Q}' \in P(\sigma)} \frac{1}{N_{\mathcal{Q}'}^s}}{\log(\frac{1}{s-1})}.$$

On a

$$\lim_{s \longrightarrow 1^+} \frac{\sum_{\mathcal{Q}' \notin P(\sigma)} \frac{1}{N_{\mathcal{Q}'}^s}}{\log(\frac{1}{s-1})} = 0,$$

puisque la série $\sum_{\mathcal{Q}' \notin P(\sigma)} \frac{1}{N_{\mathcal{Q}'}^s}$ converge en $s = 1$ (cela résulte du fait que $N_{\mathcal{Q}'}$ est une puissance ≥ 2 de $N_{\mathcal{Q}}$). On a donc, en notant $P_{\{\sigma\}}$ l'ensemble des idéaux premiers $\mathcal{Q}'$ de E tels que la substitution de Frobenius en $\mathcal{P}|\mathcal{Q}'$ soit égale à σ,

$$d(P_C) = \frac{1}{T} \lim_{s \longrightarrow 1^+} \frac{\sum_{\mathcal{Q}' \in P(\sigma)} \frac{1}{N_{\mathcal{Q}'}^s}}{\log(\frac{1}{s-1})} + \frac{\sum_{\mathcal{Q}' \in P_{\{\sigma\}} - P(\sigma)} \frac{1}{N_{\mathcal{Q}'}^s}}{\log(\frac{1}{s-1})} = \frac{1}{T} d(P_{\{\sigma\}}),$$

où la dernière densité est relative aux idéaux premiers de E. Puisque l'extension $L|E$ est cyclique, on connait cette densité, d'après le premier cas. On obtient alors

$$d(P_C) = \frac{|\mathrm{Gal}(L/E)||C|}{|\mathrm{Gal}(L/K)|} . \frac{1}{|\mathrm{Gal}(L/E)|} = \frac{|C|}{|\mathrm{Gal}(L/K)|}.$$

Remarque . — Le théorème de Chebotarev entraîne qu'il existe une infinité de substitutions de Frobenius qui coïncident avec un élément du groupe de Galois donné. Cet énoncé ne fait pas référence à des séries de Dirichlet. Toutes les démonstrations connues de ce fait utilisent les séries de Dirichlet.

XII
Les propriétés de base des corps cyclotomiques

1. Les polynômes cyclotomiques

Soit $\bar{\mathbf{Q}}$ une clôture algébrique de $\mathbf{Q}$. Tous les nombres algébriques que nous considérerons sont des éléments de ce corps.

Soit n un nombre entier. Rappelons que le *polynôme cyclotomique* $\Phi_n(X)$ est donné par la formule

$$\Phi_n(X) = \prod_{\zeta}(X - \zeta),$$

où ζ parcourt les racines primitives n-ièmes de l'unité dans $\bar{\mathbf{Q}}$. Rappelons qu'une racine primitive n-ième de l'unité est une racine n-ième de l'unité qui n'est racine d-ième de l'unité pour aucun diviseur strict d de n.

Le polynôme $\Phi_n(X)$ est à coefficients dans $\mathbf{Q}$ (puisque les racines primitives sont conjuguées les unes des autres) et même dans $\mathbf{Z}$ puisque les racines de l'unité sont des entiers algébriques. Il est de degré $\phi(n)$, où ϕ est la fonction indicatrice d'Euler.

On a, en comparant les racines des polynômes,

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Exemples. — Les premiers polynômes cyclotomiques sont donnés par les formules

$$\Phi_2(X) = X + 1, \qquad \Phi_3(X) = X^2 + X + 1, \qquad \Phi_4(X) = X^2 + 1...$$

Proposition 1. — *Le polynôme Φ_n est irréductible.*

Démonstration. — Soit ζ une racine primitive n-ième de l'unité. Les autres racines primitives n-ièmes de l'unité sont de la forme ζ^a avec $(a, n) = 1$. Il suffit donc de prouver que si $f(\zeta) = 0$ on a $f(\zeta^a) = 0$ pour tout polynôme irréductible $f \in \mathbf{Z}[X]$ divisant $X^n - 1$. Il suffit de prouver cela pour $a = p$ premier. Il suffit de prouver que $f(X)|f(X^p)$. C'est-à-dire que $f(X)$ et $f(X^p)$ ne sont pas premiers entre eux par irréductibilité de f.

Supposons qu'ils soient premiers entre eux. Considérons le polynôme g plus petit commun diviseur de $f(X)f(X^p)$ et $X^n - 1$.

Le polynome $X^n - 1$ est sans racine multiple dans $\bar{\mathbf{F}}_p$ puisque le polynôme dérivé nX^{n-1} ne s'annule en aucune racine n-ième de l'unité dans $\bar{\mathbf{F}}_p$ (car p ne divise pas n). Notons $\bar{f}$ et $\bar{g}$ les réductions modulo p de f et g. Ce sont des polynômes sans racine multiple. L'égalité $\bar{f}(X^p) = \bar{f}(X)^p$ entraîne $\bar{f}(X)|\bar{f}(X^p)$. On a donc $\bar{f}(X)^2|\bar{g}(X)$; cela contredit le fait que $\bar{g}$ soit sans racine multiple.

Soit ζ une racine primitive n-ième de l'unité dans une extension algébrique de $\mathbf{Q}$. Le corps $\mathbf{Q}(\zeta_n)$ engendré par $\mathbf{Q}$ et ζ est appelé *corps cyclotomique*. Il s'identifie à $\mathbf{Q}[X]/\Phi_n(X)$ et est donc de degré $\phi(n)$ d'après la proposition 1.

PROPOSITION 2. — *L'extension $\mathbf{Q}(\zeta_n)|\mathbf{Q}$ est abélienne de groupe de Galois isomorphe à $(\mathbf{Z}/n\mathbf{Z})^*$.*
Démonstration. — L'extension $\mathbf{Q}(\zeta_n)|\mathbf{Q}$ est galoisienne puisque les racines primitives sont conjuguées les unes des autres et se déduisent les unes des autres par passage à une puissance appropriée.

Déterminons le groupe de Galois $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$. Soit $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$. L'image par σ de ζ_n est une racine primitive de l'unité, et donc une puissance ζ_n^α de ζ_n, avec $\alpha \in \mathbf{Z}$. L'entier α est inversible modulo n, car ζ_n^α est une racine primitive. La donnée de $\alpha \in \mathbf{Z}$ détermine σ qui ne dépend que de la classe de α modulo n. Notons σ_α l'élément de $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ associé à $\alpha \in (\mathbf{Z}/n\mathbf{Z})^*$. L'application $\alpha \mapsto \sigma_\alpha$ définit un homomorphisme injectif de groupes qui est surjectif car le degré de l'extension $\mathbf{Q}(\zeta_n)|\mathbf{Q}$ est égal à $\phi(n)$ d'après la proposition 1.

2. L'étude du cas $n = p^k$

Soit p un nombre premier. Soit k un entier > 0. Posons $n = p^k$. Considérons le corps cyclotomique $\mathbf{Q}(\zeta_{p^k})$.

PROPOSITION 3. — *Le discriminant du système $(1, \zeta_{p^k}, ..., \zeta_{p^k}^{\phi(n)-1})$ est égal à*

$$(-1)^{\phi(p^k)(\phi(p^k)-1)/2} p^{p^{k-1}(kp-k-1)}.$$

Cette quantité est < 0, sauf si $p = 1 \pmod 4$ ou si n est une puissance de 2 différente de 2.
Démonstration. — Le polynôme Φ_n est donné par la formule :

$$\Phi_{p^k}(X) = \frac{X^{p^k} - 1}{X^{p^{k-1}-1}},$$

On obtient, pour tout ζ racine primitive p^k-ième de l'unité,

$$\Phi'_{p^k}(\zeta) = \frac{p^k \zeta^{-1}}{\zeta^{p^{k-1}} - 1}.$$

Utilisons la proposition IV-4 pour calculer le discriminant. En faisant le produit sur les racines primitives p^k-ièmes de l'unité on obtient :

$$\prod_\zeta \Phi'_{p^k}(\zeta) = \frac{p^{k\phi(p^k)} \prod_\zeta \zeta}{\prod_\zeta (\zeta^{p^{k-1}} - 1)}.$$

Le dénominateur de cette expression est égal à $((-1)^{p-1}\Phi_p(1))^{p^{k-1}} = (-1)^{(p-1)p^{k-1}} p^{p^{k-1}}$. Le numérateur est égal à $p^{k\phi(p^k)}(-1)^{\phi(p^k)}\Phi_{p^k}(0) = p^{k\phi(p^k)}(-1)^{\phi(p^k)}$. En combinant tout cela on obtient la formule suivante

$$D(1, \zeta_{p^k}, ..., \zeta_{p^k}^{\phi(n)-1}) = (-1)^{\phi(p^k)(\phi(p^k)-1)/2} p^{k\phi(p^k)-p^{k-1}}.$$

L'assertion sur le signe se vérifie facilement.

Corollaire 1. — *L'extension* $\mathbf{Q}(\zeta_n)|\mathbf{Q}$ *est non ramifiée en dehors de* p.
Démonstration. — Le discriminant absolu de l'extension $\mathbf{Q}(\zeta_n)|\mathbf{Q}$ divise le discriminant de tout système d'entiers. En particulier il divise le discriminant calculé dans la proposition 3 ; ce discriminant est au signe près une puissance de p. Le critère de ramification par les discriminants (théorème IV-1) permet de conclure.

Proposition 4. — *L'extension* $\mathbf{Q}(\zeta_{p^k})|\mathbf{Q}$ *est totalement ramifiée en* p. *L'idéal premier au-dessus de* p *est engendré par* $1-\zeta$ *où* ζ *est une racine primitive* p^k*-ième de l'unité.*
Démonstration. — Soient a et b deux entiers premiers à n. Soit s un entier tel que $a \equiv sb \pmod{n}$. On a

$$\frac{1-\zeta^a}{1-\zeta^b} = \frac{1-\zeta^{sb}}{1-\zeta^b} = 1 + \zeta^b + ... + \zeta^{b(s-1)}$$

qui est donc un entier. De même on montre que $(1-\zeta^b)/(1-\zeta^a)$ est entier. C'est donc une unité de $\mathbf{Q}(\zeta_n)$. Soit ζ_0 une racine primitive n-ième de l'unité. On a

$$\Phi_n(X) = \frac{X^{p^k} - 1}{X^{p^{k-1}-1}} = 1 + X^{p^{k-1}} + ... + X^{(p-1)p^{k-1}}$$

et donc

$$p = \Phi_n(1) = \prod_\zeta (1-\zeta) = (\prod_\zeta \frac{1-\zeta}{1-\zeta_0})(1-\zeta_0)^{\phi(n)},$$

où ζ parcourt les racines primitives n-ièmes de l'unité.

Soit $\mathcal{P}$ un idéal premier contenant $(1-\zeta_0)$. Il contient p d'après le calcul qui précède. Notons $v_\mathcal{P}$ la valuation associée et $e_\mathcal{P}$ l'indice de ramification en $\mathcal{P}$ de l'extension $\mathbf{Q}(\zeta_n)|\mathbf{Q}$. Rappelons que la valuation $\mathcal{P}$-adique de p est égale à $e_\mathcal{P}$. On a

$$v_\mathcal{P}(p) = v_\mathcal{P}((\prod_\zeta \frac{1-\zeta}{1-\zeta_0})(1-\zeta_0)^{\phi(n)}) = \phi(n) v_\mathcal{P}(1-\zeta_0).$$

On a donc $e_{\mathcal{P}} = v_{\mathcal{P}}(p) \leq \phi(n) = [\mathbf{Q}(\zeta_n) : \mathbf{Q}]$. Comme l'indice de ramification ne peut être $>$ au degré résiduel, on a

$$e_{\mathcal{P}} = \phi(n) = [\mathbf{Q}(\zeta_n) : \mathbf{Q}],$$

ce qui est synonyme de ramification totale. On en déduit la relation

$$v_{\mathcal{P}}(1-\zeta) = 1.$$

L'idéal principal engendré par $1-\zeta$ est égal à une puissance de $\mathcal{P}$ puisqu'il divise p et qu'il n'y a qu'un seul idéal au dessus de $\mathcal{P}$ en raison de la ramification totale. Il est en fait égal à $\mathcal{P}$ car $v_{\mathcal{P}}(1-\zeta) = 1$.

PROPOSITION 5. — *Soit ζ une racine primitive p^k-ième de l'unité. L'anneau des entiers de $\mathbf{Q}(\zeta_{p^k})$ est égal à l'anneau $\mathbf{Z}[\zeta_{p^k}] = \mathbf{Z}[\zeta]$.*
Démonstration. — Comme toute racine de l'unité est entière, l'anneau des entiers de $\mathbf{Q}(\zeta_{p^k})$ contient $\mathbf{Z}[\zeta_{p^k}]$.

Notons $\mathcal{P}$ l'idéal engendré par $1-\zeta$. C'est l'unique idéal de l'anneau des entiers de $\mathbf{Q}(\zeta_{p^k})$ divisant p d'après la proposition 4.

Soit α un élément entier de $\mathbf{Q}(\zeta_{p^k})$. Le calcul de discriminant effectué au cours de la proposition 3, le système $(1, \zeta^{p^k}, ..., \zeta^{p^k\phi(n)-1})$ est une base de $\mathbf{Q}(\zeta_{p^k})$ comme $\mathbf{Q}$-espace vectoriel. On en déduit que $(1, (1-\zeta), ..., (1-\zeta)^{\phi(n)-1})$ est une base de $\mathbf{Q}(\zeta_{p^k})$ comme $\mathbf{Q}$-espace vectoriel. Posons donc

$$\alpha = \sum_{t=0}^{\phi(n)-1} b_t(1-\zeta)^t,$$

avec $b_t \in \mathbf{Q}$. On a $v_{\mathcal{P}}((1-\zeta)^t) = t$ et $v_{\mathcal{P}}(b_t) \in \phi(n)\mathbf{Z}$. Les valuations des termes $b_t(1-\zeta)^t$ sont donc deux à deux distinctes. On a

$$v_{\mathcal{P}}(\alpha) = \min_t v_{\mathcal{P}}(b_t(1-\zeta)^t) = t + v_{\mathcal{P}}(b_t).$$

Comme on a $v_{\mathcal{P}}(\alpha) \geq 0$ et comme on a $v_{\mathcal{P}}(b_t) \in \phi(n)\mathbf{Z}$, on a $v_{\mathcal{P}}(b_t) \geq 0$. Les coefficients b_t sont donc $\mathcal{P}$-entiers.

On en déduit que dans l'écriture

$$\alpha = \sum_{t=0}^{\phi(n)-1} a_t\zeta^t,$$

les coefficients a_t sont $\mathcal{P}$-entiers. Considérons les conjugués $(\alpha_i)_{i\in(\mathbf{Z}/n\mathbf{Z})^*}$ de α. Ils s'écrivent sous la forme

$$\alpha_i = \sum_{t=0}^{\phi(n)-1} a_t\zeta^{it}.$$

Le déterminant de la matrice de passage des α_i aux a_t est un déterminant de Van der Monde associé à la famille $(\zeta^i)_{i\in(\mathbf{Z}/n\mathbf{Z})^*}$. Il est donc de la forme

$$\prod_{i\neq j}(\zeta^i-\zeta^j).$$

Comme toutes les valuations non associées à l'idéal $\mathcal{P}|p$ s'annulent en $\zeta^i-\zeta^j$, ce déterminant est une $\mathcal{P}$-unité. Par passage à la matrice inverse, peut donc exprimer a_t comme combinaison linéaire à coefficients de dénominateurs à support dans $\mathcal{P}$ des α_i. Les nombres rationnels a_t sont donc de dénominateurs à support dans p puisque les α_i sont entiers. Comme les a_t sont p-entiers, on en déduit qu'ils sont entiers. Cela achève de prouver la proposition.

Corollaire . — *Le discriminant absolu du corps $\mathbf{Q}(\zeta_{p^k})$ est donné par la formule*

$$|\mathcal{D}_{\mathbf{Q}(\zeta_{p^k})}|=p^{p^{k-1}(kp-k-1)}.$$

Démonstration. — Cela résulte du fait que le système introduit dans la démonstration de la proposition 3 est une base de $\mathbf{Z}[\zeta_{p^k}]$ comme $\mathbf{Z}$-module (voir la démonstration de la proposition 5).

3. Retour au cas général

Nous allons étendre ce qui précède aux corps cyclotomique d'ordre quelconque grâce à des propriétés d'indépendance des extensions cyclotomiques d'indices premiers entre eux.

Proposition 6. — *Soient n et m deux entiers ≥ 0 et premiers entre eux. On a*

$$\mathbf{Q}(\zeta_n)\mathbf{Q}(\zeta_m)=\mathbf{Q}(\zeta_{nm}).$$

Démonstration. — Le produit d'une racine primitive n-ième de l'unité et d'une racine primitive m-ième de l'unité est une racine primitive nm-ième de l'unité, puisque n et m sont premiers entre eux. On a donc $\mathbf{Q}(\zeta_{nm})\subset\mathbf{Q}(\zeta_n)\mathbf{Q}(\zeta_m)$. L'inclusion réciproque résulte des inclusions $\mathbf{Q}(\zeta_n)\subset\mathbf{Q}(\zeta_{mn})$ et $\mathbf{Q}(\zeta_m)\subset\mathbf{Q}(\zeta_{mn})$.

Proposition 7. — *Soit n un entier ≥ 3. Le nombre premier p est ramifié dans $\mathbf{Q}(\zeta_n)$ si et seulement si p divise n.*
Démonstration. — Si on pose $n=\prod_{i=1}^k q_i^{e_i}$. On a $\mathbf{Q}(\zeta_n)=\mathbf{Q}(\zeta_{q_1^{e_1}})...\mathbf{Q}(\zeta_{q_k^{e_k}})$. L'extension $\mathbf{Q}(\zeta_n)|\mathbf{Q}$ est non ramifiée en p si et seulement si chaque composante $\mathbf{Q}(\zeta_{q_i^{e_i}})|\mathbf{Q}$ est non ramifiée en p (la composée d'extensions non ramifiées est non ramifiée). C'est-à-dire si et seulement si p est égal à l'un des q_i d'après le corollaire 1 de la proposition 3.

PROPOSITION 8. — *Soient n et m deux entiers ≥ 0 et premiers entre eux. On a, dans $\bar{\mathbf{Q}}$,*

$$\mathbf{Q}(\zeta_n) \cap \mathbf{Q}(\zeta_m) = \mathbf{Q}.$$

Démonstration. — Posons

$$K = \mathbf{Q}(\zeta_n) \cap \mathbf{Q}(\zeta_m).$$

Supposons que ce soit une extension non triviale de $\mathbf{Q}$. Il existe alors un nombre premier p ramifié dans l'extension $K|\mathbf{Q}$ (par la théorie de Minkowski). Ce nombre premier est donc aussi ramifié dans les extensions $\mathbf{Q}(\zeta_n)|\mathbf{Q}$ et $\mathbf{Q}(\zeta_m)|\mathbf{Q}$. On a donc $p|m$ et $p|n$, ce qui est absurde.

PROPOSITION 9. — *Soit n un entier ≥ 1. L'anneau des entiers de $\mathbf{Q}(\zeta_n)$ est égal à $\mathbf{Z}[\zeta_n]$. De plus le discriminant absolu de $\mathbf{Q}(\zeta_n)$ est donné par la formule*

$$|\mathcal{D}_{\mathbf{Q}(\zeta_n)}| = \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

Démonstration. — Posons $n = \prod_{i=1}^{k} q_i^{e_i}$. On a

$$\mathbf{Q}(\zeta_n) = \mathbf{Q}(\zeta_{q_1^{e_1}}) ... \mathbf{Q}(\zeta_{q_k^{e_k}}).$$

Il s'agit d'une composition d'extensions linéairement disjointes d'après la proposition 8. L'anneau des entiers de cette composée est donc (en utilisant la proposition 5 et le corollaire 1 de la proposition IV-6)

$$\mathbf{Z}[\zeta_{q_1^{e_1}}] ... \mathbf{Z}[\zeta_{q_k^{e_k}}] = \mathbf{Z}[\zeta_n].$$

L'assertion sur le discriminant est valable dans le cas où n est une puissance d'un nombre premier d'après le corollaire de la proposition 5. Lorsque n et m sont des entiers > 1 premiers entre eux, les extensions $\mathbf{Q}(\zeta_n)$ et $\mathbf{Q}(\zeta_n)$ sont linéairement disjointes sur $\mathbf{Q}$ (proposition 8). On dispose donc de la formule (corollaire 1 de la proposition IV-6)

$$|\mathcal{D}_{\mathbf{Q}(\zeta_n)\mathbf{Q}(\zeta_m)}| = |\mathcal{D}_{\mathbf{Q}(\zeta_n)}^{[\mathbf{Q}(\zeta_m):\mathbf{Q}]}| |\mathcal{D}_{\mathbf{Q}(\zeta_m)}^{[\mathbf{Q}(\zeta_n):\mathbf{Q}]}|.$$

Supposons que la formule cherchée soit valable pour les corps $\mathbf{Q}(\zeta_n)$ et $\mathbf{Q}(\zeta_m)$. On a alors, en utilisant la multiplicativité de la fonction d'Euler,

$$|\mathcal{D}_{\mathbf{Q}(\zeta_n)\mathbf{Q}(\zeta_m)}| = \left(\frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}\right)^{\phi(m)} \left(\frac{m^{\phi(m)}}{\prod_{p|m} p^{\phi(m)/(p-1)}}\right)^{\phi(n)}$$

$$= \frac{(nm)^{\phi(nm)}}{\prod_{p|nm} p^{\phi(nm)/(p-1)}}.$$

On déduit la formule de discriminant cherchée par un raisonnement par récurrence sur le nombre de diviseurs premier de n.

4. Étude locale

L'extension $\mathbf{Q}(\zeta_n)|\mathbf{Q}$ est abélienne et non ramifiée en dehors de n, si bien qu'on peut parler sans ambiguïté de la substitution de Frobenius en tout nombre premier p ne divisant pas n.

PROPOSITION 10. — *Soit p un nombre premier ne divisant pas n. L'élément σ_p de $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ qui à une racine de l'unité ζ associe ζ^p coïncide avec la substitution de Frobenius en p.*
Démonstration. — Soit $\mathcal{P}$ un idéal de $\mathbf{Z}[\zeta_n]$ au-dessus de p. On a

$$\sigma_p(\zeta) \equiv \zeta^p \equiv \mathrm{Frob}_{\mathcal{P}}(\zeta) \pmod{cP}.$$

Cela prouve l'identité cherchée puisque ζ engendre $\mathbf{Z}[\zeta_n]$.

COROLLAIRE 1. — *Le degré résiduel en p de l'extension $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ est égal à l'ordre de p dans $(\mathbf{Z}/n\mathbf{Z})^*$.*
Démonstration. — C'est une conséquence directe du fait que le degré résiduel d'une extension galoisienne est égal à l'ordre d'une substitution de Frobenius relatif à la place considérée.

Rappelons qu'un idéal premier $\mathcal{P}$ est *totalement décomposé* dans une extension $L|K$ si l'extension est non ramifiée en $\mathcal{P}$ et si le degré résiduel est égal à 1. Cela signifie encore qu'il y a $[L : K]$ idéaux premiers conjugués de $\mathcal{P}$ dans L. L'idéal premier $\mathcal{P}$ est dit *inerte* si l'extension $L|K$ est de degré résiduel en $\mathcal{P}$ égal à $[L : K]$ (l'extension $L|K$ est alors non ramifiée).

COROLLAIRE 2. — *Le nombre premier p est totalement décomposé dans l'extension $\mathbf{Q}(\zeta_n)|\mathbf{Q}$ si et seulement si p est congru à 1 modulo n. Il est inerte si et seulement si p engendre $(\mathbf{Z}/n\mathbf{Z})^*$.*
Démonstration. — Cela résulte immédiatement du corollaire 1.

On appelle *conjugaison complexe* d'un corps de nombres K un automorphisme de K qui se prolonge par continuité vis-à-vis d'une valeur absolue archimédienne non réelle en la conjugaison complexe de $\mathbf{C}$. Il en existe une pour chaque place archimédienne et non réelle de K. On peut voir ces conjugaison complexes comme les analogues pour les places archimédiennes des substitutions de Frobenius.

PROPOSITION 11. — *Une conjugaison complexe de $\mathbf{Q}(\zeta_n)$ agit par $\zeta \mapsto \zeta^{-1}$ sur les racines de l'unité. Il n'y en a donc qu'une et elle correspond à l'élément -1 de $(\mathbf{Z}/n\mathbf{Z})^*$ par l'isomorphisme canonique*

$$(\mathbf{Z}/n\mathbf{Z})^* \simeq \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}).$$

Démonstration. — La conjugaison complexe de $\mathbf{C}$ agit par $z \mapsto z^{-1}$ sur les racines de l'unité. On en déduit la première assertion. La deuxième assertion résulte du fait que

les automorphismes de $\mathbf{Q}(\zeta_n)$ sont déterminés par leur action sur les racines de l'unité (proposition 2).

5. Le corps $\mathbf{Q}(\zeta_n)^+$

Soit n un entier ≥ 3. Considérons le sous-corps $\mathbf{Q}(\zeta_n)^+$ de $\mathbf{Q}(\zeta_n)$ formé par les éléments invariants par $\{-1,+1\} \subset (\mathbf{Z}/n\mathbf{Z})^* \simeq \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$.

PROPOSITION 12. — *Soit ζ une racine primitive n-ième de l'unité. Le corps $\mathbf{Q}(\zeta_n)^+$ est engendré par $\zeta + \zeta^{-1}$.*
Démonstration. — Le nombre $\zeta + \zeta^{-1}$ est invariant par $\{-1,+1\}$. Le corps $\mathbf{Q}(\zeta)_n^+$ est engendré comme $\mathbf{Q}$ espace vectoriel par les $\zeta^a + \zeta^{-a}$ (a entier > 0). Il suffit donc de prouver qu'on a $\zeta^a + \zeta^{-a} \in \mathbf{Q}(\zeta + \zeta^{-1})$. On démonte cela par récurrence sur a en posant

$$(\zeta + \zeta^{-1})^a = \sum_{k=0}^{a} \binom{a}{k} \zeta^{a-2k} = \zeta^a + \zeta^{-a} + \sum_{t=1, t\in 2\mathbf{Z}}^{a-1} \binom{a}{(a-t)/2} (\zeta^t + \zeta^{-t}).$$

Le membre de gauche et le deuxième terme du membre de droite étant dans $\mathbf{Q}(\zeta + \zeta^{-1})$ par hypothèse de récurrence, on a la propriété cherchée.

PROPOSITION 13. — *Soit ζ une racine primitive n-ième de l'unité. L'anneau des entiers de $\mathbf{Q}(\zeta_n)^+$ est égal à $\mathbf{Z}[\zeta + \zeta^{-1}]$.*
Démonstration. — L'anneau $\mathbf{Z}[\zeta+\zeta^{-1}]$ est formé d'éléments entiers de $\mathbf{Q}(\zeta_n)^+$. Les entiers de $\mathbf{Q}(\zeta_n)^+$ coïncident avec les entiers de $\mathbf{Q}(\zeta_n)$ qui sont invariants par l'automorphisme qui à ζ associe ζ^{-1}. On constate que les éléments de $\mathbf{Z}[\zeta_n)]$ invariants par cet automorphisme sont précisément les éléments de $\mathbf{Z}[\zeta + \zeta^{-1}]$.

Exercice . — Déterminer le discriminant absolu du corps $\mathbf{Q}(\zeta_n)^+$ (on pourra utiliser la formule des tours).

6. Cycles arithmériques de Q

Soit $\mathcal{M}$ un cycle arithmétique de $\mathbf{Q}$. Il s'écrit sous la forme

$$\mathcal{M} = p_\infty^{n_\infty} \prod_p p^{n_p},$$

où p parcourt les nombres premiers et où n_∞ est égal à 0 ou 1. Posons

$$n = \prod_p p^{n_p} \in \mathbf{Z}.$$

PROPOSITION 14. — *Le groupe des classes d'idèles de rayon $\mathcal{M}$ de $\mathbf{Q}$ est isomorphe à $(\mathbf{Z}/n\mathbf{Z})^*/\pm 1$ si $n_\infty = 0$ et à $(\mathbf{Z}/n\mathbf{Z})^*$ si $n_\infty = 1$.*
Démonstration. — Posons $\mathbf{R}^{n_\infty} = \mathbf{R}^*$ si $n_\infty = 0$ et $\mathbf{R}^{n_\infty} = \mathbf{R}_+^*$ si $n_\infty = 1$. Le groupe des classes de rayon $\mathcal{M}$ est égal à $C_\mathbf{Q}/C_\mathbf{Q}^\mathcal{M}$. Rappelons que le groupe des classes de $\mathbf{Q}$ est trivial, ce qui se traduit par la trivialité du groupe $C_\mathbf{Q}/C_\mathbf{Q}^1$. On a

$$C_\mathbf{Q}^1/C_\mathbf{Q}^\mathcal{M} = \mathbf{Q}^*.(\mathbf{R}^* \times \prod_p \mathbf{Z}_p^*)/\mathbf{Q}^*.(\mathbf{R}^{n_\infty} \times \prod_{p|n}(1+p^{n_p}\mathbf{Z}_p)\prod_{p\not|n}\mathbf{Z}_p^*).$$

Comme on a

$$\mathbf{Q}^* \cap (\mathbf{R}^* \times \prod_p \mathbf{Z}_p^*) = \{-1,+1\},$$

cela donne

$$C_\mathbf{Q}^1/C_\mathbf{Q}^\mathcal{M} \simeq (\mathbf{R}^* \times \prod_{p|n} \mathbf{Z}_p^*)/\{-1,+1\}.(\mathbf{R}^{n_\infty} \prod_{p|n}(1+p^{n_p}\mathbf{Z}_p)).$$

Comme

$$(\mathbf{Z}/n\mathbf{Z})^* \simeq \prod_{p|n} \mathbf{Z}_p^*/(1+p^{n_p}\mathbf{Z}_p),$$

on obtient la formule

$$C_\mathbf{Q}^1/C_\mathbf{Q}^\mathcal{M} \simeq (\mathbf{R}^*/\mathbf{R}^{n_\infty} \times (\mathbf{Z}/n\mathbf{Z})^*)/\{-1,+1\}.$$

Cela donne l'isomorphise cherché si $n_\infty = 0$. Si $n_\infty = 1$, on utilise le fait que l'application $(\mathbf{Z}/n\mathbf{Z})^* \longrightarrow (\mathbf{R}^*/\mathbf{R}^{n_\infty} \times (\mathbf{Z}/n\mathbf{Z})^*)$ qui à x associe $(1,x)$ définit par passage au quotient un isomorphisme de groupes

$$(\mathbf{Z}/n\mathbf{Z})^* \simeq (\mathbf{R}^*/\mathbf{R}^{n_\infty} \times (\mathbf{Z}/n\mathbf{Z})^*)/\{-1,+1\}.$$

Cela achève la démonstration.

On peut retrouver l'isomorphisme entre le groupe des classes d'idéaux de rayon $\mathcal{M}$ et $(\mathbf{Z}/n\mathbf{Z})^*/\{-1,+1\}$ ou $(\mathbf{Z}/n\mathbf{Z})^*$. En effet le groupe $\mathcal{I}(\mathbf{Q})^\mathcal{M}$ constitué des idéaux fractionnaires de la forme $a\mathbf{Z}$ avec a nombre rationnel de numérateur et dénominateur premiers à n et puisque le groupe $\mathcal{P}(\mathbf{Q})^\mathcal{M}$ est formé des idéaux de la forme $a\mathbf{Z}$ avec $a \equiv 1 \pmod{n}$ et $a > 0$ si $n_\infty = 1$. L'image de la classe de l'idéal $p\mathbf{Z}$ dans le groupe des classes de rayon $\mathcal{M}$ est donc égal à la classe de p dans $(\mathbf{Z}/n\mathbf{Z})^*/\{-1,+1\}$ ou $(\mathbf{Z}/n\mathbf{Z})^*$.

Remarque . — On a donc la série d'isomorphismes de groupes (pour $n_\infty = 1$)

$$C_\mathbf{Q}/C_\mathbf{Q}^\mathcal{M} \simeq \mathcal{C}\ell(\mathbf{Q})^\mathcal{M} \simeq (\mathbf{Z}/n\mathbf{Z})^* \simeq \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}).$$

Soit p un nombre premier ne divisant pas n. Considérons l'idèle de $\mathbf{Q}$ dont toutes les composantes sont triviales, sauf la composante en p qui est égale à p. Son image dans $\mathcal{C}\ell(\mathbf{Q})^\mathcal{M}$ via les homomorphismes de groupes

$$\mathbf{A}_\mathbf{Q}^* \longrightarrow C_\mathbf{Q}/C_\mathbf{Q}^\mathcal{M} \simeq \mathcal{C}\ell(\mathbf{Q})^\mathcal{M}$$

est égale à la classe de l'idéal $p\mathbf{Z}$. L'image de cette classe dans $(\mathbf{Z}/n\mathbf{Z})^*$ est $p + n\mathbf{Z}$, qui à son tour donne la substitution de Frobenius en p dans $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$. Tout cela est prédit par la théorie du corps de classe.

On a les assertions analogues lorsque $n_\infty = 0$.

7. Le théorème de Kronecker-Weber et la progression arithmétique

L'énoncé suivant est le *théorème de la progression arithmétique* de Dirichlet.

THÉORÈME 1. — *Soit n un entier > 0. Soit $x \in (\mathbf{Z}/n\mathbf{Z})^*$. La densité de Dirichlet de x est égale à $1/\phi(n)$.*
Démonstration. — On applique le théorème de densité de Dirichlet au groupe des classes de rayon np_∞.

On remarquera que le théorème de densité de Chebotarev pour l'extension cyclotomique $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ est équivalent au théorème de la progression arithmétique. Un examen de la démonstration du théorème de densité de Dirichlet convainc que la théorie du corps de classe n'est pas nécessaire pour traiter le cas de l'extension $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$. On peut utiliser les isomorphismes décrit dans la dernière remarque de la section précédente.

Cette remarque suggère la version précise (que nous allons admettre provisoirement) suivante de la théorie du corps de classe pour $\mathbf{Q}$.

THÉORÈME 2. — *Soit n un entier > 0. Les corps de classe de $\mathbf{Q}$ de rayon np_∞ et n sont $\mathbf{Q}(\zeta_n)$ et $\mathbf{Q}(\zeta_n)^+$.*

La conséquence suivante est le *théorème de Kronecker-Weber*.

COROLLAIRE . — *Toute extension abélienne de $\mathbf{Q}$ est contenue dans un corps cyclotomique.*
Démonstration. — Cela résulte du fait que toute extension abélienne d'un corps de nombres est contenu dans un corps de classe de rayon approprié.

Remarquons que l'extension $\mathbf{Q}(\zeta_n)|\mathbf{Q}$ satisfait la conclusion du théorème IX-3. En effet soit $I = k\mathbf{Z}$ un idéal de $\mathbf{Z}$ premier à n avec k de décomposition en produit de facteurs premiers donnée par $k = \prod_q q^{n_q}$. Le symbole d'Artin $(I, \mathbf{Q}(\zeta_n))/\mathbf{Q}) \in \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ est donné par la formule

$$(I, \mathbf{Q}(\zeta_n) = \prod_q \mathrm{Frob}_q^{n_q}.$$

Lorsqu'on identifie $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ à $(\mathbf{Z}/n\mathbf{Z})^*$, ce symbole d'Artin correspond à l'élément

$$\prod_q q^{n_q} \in (\mathbf{Z}/n\mathbf{Z})^*.$$

Il est donc trivial lorsque k est congru à 1 modulo n. La loi de réciprocité d'Artin est donc satisfaite (pour le conducteur d'Artin n). À noter que la condition sur les places réelles ne

joue aucun rôle puisque tout les places archimédiennes des corps cyclotomiques sont non réelles.

Tout élément de $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ s'écrit comme symbole d'Artin relatif à un idéal premier d'après le théorème de la progression arithmétique.

XIII
L'arithmétique des corps cyclotomiques

1. Les invariants des corps cyclotomiques

Soit m un entier > 2. Récapitulons les informations accumulées sur le corps cyclotomique $\mathbf{Q}(\zeta_m)$.

On a $d = [\mathbf{Q}(\zeta_m) : \mathbf{Q}] = \phi(m)$. Le nombre de plongements réels de $\mathbf{Q}(\zeta_m)$ est nul car il n'y pas de racine primitive m-ième de l'unité dans $\mathbf{R}$. On a donc

$$r_1 = 0 \qquad \text{et} \qquad r_2 = \phi(m)/2.$$

Le discriminant absolu de $\mathbf{Q}(\zeta_m)$ est égal à

$$\frac{n^{\phi}(m)}{\prod_{p|m} p^{\phi(m)/(p-1)}}.$$

Les racines de l'unité contenues dans $\mathbf{Q}(\zeta_m)$ sont les racines de l'unité de $\mathbf{Q}$ et les racines m-ièmes de l'unité (une racine distincte de celles-ci engendrerait un corps non contenu dans $\mathbf{Q}(\zeta_m)$ d'après la proposition XII-6). Il y a donc $2m$ (resp. m) racines de l'unité dans $\mathbf{Q}(\zeta_m)$ si m est impair (resp. pair).

Le groupe des unités de $\mathbf{Q}(\zeta_m)$ est donc isomorphe au groupe

$$(\mathbf{Z}/\frac{2m}{(m,2)}\mathbf{Z}) \times \mathbf{Z}^{\phi(m)/2-1}.$$

Il reste à étudier le nombre de classes h_m et le régulateur R_m de $\mathbf{Q}(\zeta_m)$.

Indiquons quels sont les invariants analogues du corps $\mathbf{Q}(\zeta_m)^+$. C'est un corps de degré $\phi(m)/2$ sur $\mathbf{Q}$. On a

$$r_1 = \phi(m)/2 \qquad \text{et} \qquad r_2 = 0,$$

puisque pour toute racine m-ième de l'unité ξ de $\mathbf{C}$, on a $\xi + \xi^{-1} \in \mathbf{R}$.

Les seules racines de l'unité de $\mathbf{R}$ sont 1 et -1. Le corps $\mathbf{Q}(\zeta_m)^+$ n'a donc que 2 racines de l'unité.

Le groupe des unités de $\mathbf{Q}(\zeta_m)^+$ est donc isomorphe à

$$(\mathbf{Z}/2\mathbf{Z}) \times \mathbf{Z}^{\phi(m)/2-1}.$$

On note h_m^+ le nombre de classes de $\mathbf{Q}(\zeta_m)^+$. On note R_m^+ le régulateurs de $\mathbf{Q}(\zeta_m)^+$. On pose $h_m^- = h_m/h_m^+$.

2. Unités cyclotomiques

Supposons d'abord que $m = p^k$ avec p nombre premier et k entier > 0.

PROPOSITION 1. — *Soit ζ une racine p^k-ième de l'unité. La quantité*

$$\theta_i = \frac{1-\zeta^i}{1-\zeta}$$

est une unité de $\mathbf{Q}(\zeta_{p^k})$ lorsque i est premier à p. Les θ_i engendrent un groupe de rang $\leq \phi(p^k)/2-1$ du groupe des unités de $\mathbf{Q}(\zeta_{p^k})$ modulo les racines de l'unité.
Démonstration. — La première assertion est tirée de la démonstration de la proposition XII-4. La deuxième résulte du fait que θ_i ne dépend que de la classe de i dans $(\mathbf{Z}/p^k\mathbf{Z})^*$, de la relation

$$\theta_{-i} = \frac{1-\zeta^{-i}}{1-\zeta} = -\zeta^{-i}\frac{1-\zeta^i}{1-\zeta} = -\zeta^{-i}\theta_i$$

et du fait que $\theta_1 = 1$.

Supposons maintenant que m n'est pas une puissance d'un nombre premier.

PROPOSITION 2. — *Soit ζ une racine primitive n-ième de l'unité. On a*

$$\prod_{j=1,(j,m)=1}^{m-1} (1-\zeta^j) = 1.$$

Il en résulte que $1-\zeta^j$ est une unité de $\mathbf{Q}(\zeta_m)$. Ces unités engendrent un groupe de rang $\leq \phi(m)/2-1$ du groupe des unités de $\mathbf{Q}(\zeta_m)$ modulo les racines de l'unité lorsque j parcourt les entiers inversibles modulo m.
Démonstration. — On a

$$\Phi_n(1) = \prod_{j=1,(j,m)=1}^{n-1} (1-\zeta^j).$$

Posons

$$g(X) = \frac{X^m-1}{X-1} = 1 + X + X^2 + ... + X^{m-1}.$$

On a donc $g(1) = m$. Rappelons la formule

$$g(X) = \prod_{d|m, d\neq 1} \Phi_d(X).$$

Cela entraîne, lorsque p est un nombre premier,

$$\Phi_{p^k}(X) = \frac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = 1 + X^{p^{k-1}} + ... + X^{p^{k-1}(p-1)}.$$

Mettons ces égalités ensemble :

$$\Phi_{p^k}(1) = p.$$

On a donc

$$m = g(1) = \prod_{d|m, d\neq 1} \Phi_d(1) = \prod_{p,k,p^k|m} p \prod_{d|m}{}' \Phi_d(1) = m \prod_{d|m}{}' \Phi_d(1),$$

où le produit $\prod'$ porte sur les les diviseurs d de m qui ne sont pas des puissances d'un nombre premier. Comme $\Phi_d(1)$ est un entier, on a $\Phi_d(1) = 1$ ou -1 lorsque d n'est pas une puissance d'un nombre premier. Une récurrence sur le nombre de diviseurs de m montre qu'on a $\Phi_m(1) = 1$.

L'assertion sur le rang du groupe d'unités se démontre de façon analogue à ce qui est démontré dans la proposition 1 (en utilisant la relation qui vient d'être établie entre les $1 - \zeta^j$).

Les unités construites par les propositions 1 et 2 sont les *unités cyclotomiques*. On démontre (voir ci-dessous) qu'elles engendrent un sous-groupe d'indice fini du groupe des unités. Cet indice est relié au nombre de classes des corps cyclotomiques.

3. Sommes de Gauss

Soit m un entier ≥ 3. Soit χ un caractère de Dirichlet primitif de niveau m. C'est-à-dire un homomorphisme de groupes

$$(\mathbf{Z}/m\mathbf{Z})^* \longrightarrow \mathbf{C}^*$$

qui ne se factorise par aucun homomorphisme

$$(\mathbf{Z}/m\mathbf{Z})^* \longrightarrow (\mathbf{Z}/(m/d)\mathbf{Z})^*.$$

On pose, pour $x \in \mathbf{Z}$, $\chi(x) = \chi(x + m\mathbf{Z})$ si x est premier à m et $\chi(x) = 0$ sinon.

On note $\bar{\chi}$ le caractère conjugué de χ, c'est-à-dire le caractère donné par la formule $\chi(x) = \chi(x)^{-1}$ (= conjugué complexe de x) lorsque x est inversible modulo n.

On dit qu'un caractère de Dirichlet est *pair* si on a $\chi(-1) = 1$ et qu'il est *impair* si on a $\chi(-1) = -1$.

Posons $\zeta_0 = e^{2i\pi/n} \in \mathbf{C}$. La *somme de Gauss* $\tau(\chi)$ associée à χ est le nombre complexe donné par l'expression

$$\tau(\chi) = \sum_{a=1}^{m} \chi(a)\zeta_0^a$$

(On remarquera que les termes correspondant à a non premier à m sont nuls).

PROPOSITION 3. — *Soit $b \in \mathbf{Z}$. On a*

$$\sum_{a=1}^{m} \bar{\chi}(a)\zeta_0^{ab} = \chi(b)\tau(\bar{\chi}).$$

Démonstration. — Si b est inversible modulo m, on considère les entier $c > 0$ tel que $c \equiv ab \pmod{n}$ et tel que $c \leq m$. Un changement de variable donne alors

$$\sum_{a=1}^{m} \bar{\chi}(a)\zeta_0^{ab} = \sum_{c=1}^{m} \bar{\chi}(c/b)\zeta_0^{c} = \chi(b)\sum_{c=1}^{m} \bar{\chi}(c)\zeta_0^{c}.$$

Si b n'est pas inversible modulo m le terme de droite dans l'énoncé de la proposition est nul. Démontrons que le terme de gauche est lui aussi nul. Posons $d = (m, b)$. Puisque le caractère χ est primitif, il existe $y \in \mathbf{Z}$ inversible modulo n, tel que $y \equiv 1 \pmod{m/d}$ et vérifiant $\chi(y) \neq 1$. On a $by \equiv b \pmod{m}$. Revenons au terme de gauche de la proposition. On a

$$\sum_{a=1}^{m} \bar{\chi}(a)\zeta_0^{ab} = \sum_{a=1}^{m} \bar{\chi}(a)\zeta_0^{aby} = \chi(y)\sum_{a=1}^{m} \bar{\chi}(a)\zeta_0^{ab}.$$

Le passage au dernier membre se fait par changement de variable comme ci-dessus en utilisant le fait que y est inversible. Comme $\chi(y) \neq 1$, on a $\sum_{a=1}^{m} \bar{\chi}(a)\zeta_0^{ab} = 0$.

COROLLAIRE . — *On a*

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

Démonstration. — Cela se déduit de la proposition 3 avec $b = -1$.

PROPOSITION 4. — *On a*

$$\tau(\chi)\overline{\tau(\chi)} = m.$$

Démonstration. — C'est un calcul. On a

$$\phi(m)\tau(\chi)\overline{\tau(\chi)} = \sum_{b=1}^{m} |\chi(b)\tau(\chi)|^2.$$

Utilisons la proposition 3 et son corollaire. On obtient

$$\phi(m)\tau(\chi)\overline{\tau(\chi)} = \sum_{b=1}^{m}\sum_{a=1}^{m}\chi(a)\zeta_0^{ab}\sum_{c=1}^{m}\bar{\chi}(c)\zeta_0^{-cb} = \sum_{c=1}^{m}\sum_{a=1}^{m}\chi(a)\bar{\chi}(c)\sum_{b=1}^{m}\zeta_0^{(a-c)b}.$$

La somme $\sum_{b=1}^{m}\zeta_0^{(a-c)b}$ est nulle sauf si $a=c$ auquel cas elle vaut m. On a donc

$$\phi(m)\tau(\chi)\overline{\tau(\chi)} = \sum_{a=1}^{m}\chi(a)\bar{\chi}(a) = m\phi(m).$$

Cela achève de prouver la proposition.

Remarque . — On prendra note de l'analogie formelle entre les sommes de Gauss et la fonction Γ (voit leçon X) : elles sont bâties comme des sommes, l'une portant sur $(\mathbf{Z}/m\mathbf{Z})^*$ l'autre sur $\mathbf{R}_+^*$, du produit d'un caractère additif et d'un caractère multiplicatif. De façon plus précise, il s'agit dans les deux cas de la transformée de Fourier multiplicative d'un caractère additif.

On tire du corollaire de la proposition 3 et de la proposition 4 la formule

$$\tau(\chi)\tau(\bar{\chi}) = \chi(-1)m.$$

Cela a quelques conséquences lorsque χ et $\bar{\chi}$ coïncident.

4. Les nombres de Bernoulli

Les *nombres de Bernoulli* sont des nombres rationnels définis comme les coefficients du développement formel

$$\frac{t}{e^t-1} = \sum_{k=0}^{\infty}B_k\frac{t^k}{k\,!}.$$

Le nombre B_k est le k-ième *nombre de Bernoulli*. On a $B_k = 0$ pour $k \geq 3$ impair. En effet la fonction $t/(e^t-1)+t/2 = t\coth(t/2)$ est paire.

Il est plus naturel d'introduire les polynômes de Bernoulli. Le k-ième *polynôme de Bernoulli* est donné par le développement formel

$$\frac{te^{tX}}{e^t-1} = \sum_{k=0}^{\infty}B_k(X)\frac{t^k}{k\,!}.$$

En particulier le coefficient constant du k-ième polynôme de Bernoulli est le k-ième nombre de Bernoulli.

Exemple . — En particulier on a

$$B_0(X) = 1, \qquad B_1(X) = X - 1/2, \qquad B_2(X) = X^2 - X + 1/6.$$

La membre de droite de la série génératrice des polynômes de Bernoulli est le produit de la série génératrice des nombres de Bernoulli et de e^{tX}. La formule donnant les coefficients d'un produit de séries génératrices nous donne

$$B_k(X) = \sum_{i=0}^{k} \binom{k}{i} B_i X^{k-i}.$$

En l'utilisant l'expression $\sum_{k=0}^{\infty} B'_k(X)t^k/k\,! = d/dX(te^{tX}/(e^t-1)) = t^2e^{tX}/(e^t-1)$, on obtient

$$B'_k(X) = kB_{k-1}(X).$$

En utilisant l'identité $te^{t(X+1)}/(e^t-1) - te^{tX}/(e^t-1) = te^{tX}$, on obtient la formule

$$B_k(X+1) - B_k(X) = kX^{k-1}$$

(on peut interpréter cela en disant que le k-ième polynôme de Bernoulli est une primitive discrète du polynôme kX^{k-1}). Cette formule suffit à déterminer les polynômes de Bernoulli au coefficient constant près. Par application, on a, pour $k \geq 2$,

$$B_k(1) = B_k(0).$$

De plus, comme on a $\int_0^1 te^{tX}/(e^t-1)\,dX = t$, on a la formule, pour $k \geq 1$,

$$\int_0^1 B_k(t)\,dt = 0.$$

Cela suffit à déterminer B_k par récurrence à partir des relations ci-dessus.

Soit m un entier ≥ 1. Soit χ un caractère de Dirichlet modulo m. On pose

$$B_{k,\chi} = m^{k-1} \sum_{a=1}^{m} \chi(a) B_k(\frac{a}{m}).$$

Ce sont les *nombres de Bernoulli généralisés*.

On considère souvent les polynômes de Bernoulli rendu périodiques. Le k-ième polynôme de Bernoulli rendu périodique $\bar{B}_k$ est l'unique fonction périodique de période 1, qui coïncide avec B_k sur l'intervalle $]0,1[$ et qui vérifie

$$\bar{B}_k(0) = \frac{B_k(0)+B_k(1)}{2} = \frac{\bar{B}_k(0^+)+\bar{B}_k(0^-)}{2}.$$

Cette relation est inutile si $k \geq 2$ puisqu'on a alors $B_k(0) = B_k(1)$. De plus on a $\bar{B}_1(0) = \bar{B}_1(1) = 0$.

Comme on a la relation $te^{t(1-X)}/(e^t-1) = -te^{-tX}/(e^{-t}-1)$, on obtient la formule

$$B_k(1-X) = (-1)^k B_k(X).$$

Cela entraîne que la fonction $\bar{B}_k$ est paire (resp. impaire) si k est pair (resp. impair).

PROPOSITION 5. — *Le développement en série de Fourier de la fonction $\bar{B}_k$ est donné par la formule suivante*

$$\bar{B}_k(t) = -\frac{k\,!}{(2\pi i)^k} \sum_{n=-\infty, n\neq 0}^{\infty} \frac{1}{n^k} e^{2i\pi nt}.$$

Démonstration. — Il suffit de calculer les coefficients de Fourier d'indice ≥ 0 en raison des propriétés de parité de $\bar{B}_k$.

Calculons le n-ième coefficient de Fourier de $\bar{B}_k$ par récurrence sur k. Lorsque $n = 0$, on sait qu'il est nul pour $k \neq 0$. Supposons donc $n \neq 0$. Calculons le n-ième coefficient de Fourier de $\bar{B}_1$. On a

$$\int_0^1 \bar{B}_1(t) e^{-2i\pi nt}\, dt = \int_0^1 (t - 1/2) e^{-2i\pi nt}\, dt = -\frac{1}{2\pi i n}.$$

Passons maintenant au cas général. On a, par intégration par parties,

$$\int_0^1 \bar{B}_k(t) e^{-2i\pi nt}\, dt = -\frac{1}{2i\pi n} [\bar{B}_k(t) e^{-2i\pi nt}]_0^1 + \frac{1}{2i\pi n} \int_0^1 \bar{B}'_k(t) e^{-2i\pi nt}\, dt.$$

Utilisons la relation reliant B'_k et B_{k-1} et la périodicité de $\bar{B}_k$. On obtient, pour $k \geq 2$,

$$\int_0^1 \bar{B}_k(t) e^{-2i\pi nt}\, dt = \frac{k}{2i\pi n} \int_0^1 \bar{B}_{k-1}(t) e^{-2i\pi nt}\, dt.$$

Cela donne par récurrence que le n-ième coefficient de Fourier de B_k est $-k\,!/(2i\pi n)^k$. Cela prouve la formule cherchée par la théorie des séries de Fourier.

La série de Fourier de $\bar{B}_k$ converge normalement pour $k \geq 2$. La fonction $\bar{B}_k$ est donc continue pour $k \geq 2$. Elle ne l'est pas dans le cas $k = 1$.

Si χ est un caractère pair différent de 1, la fonction $\mathbf{Z}/n\mathbf{Z} \longrightarrow \mathbf{C}$ qui à $a + n\mathbf{Z}$ associe $\bar{B}_1(a/n)\chi(a)$ est donc impaire, si bien qu'on a on a

$$B_{1,\chi} = \sum_{a=1}^{n} \bar{B}_1(a/n)\chi(a) = 0.$$

Lorsque χ est un caractère impair, on a

$$B_{1,\chi} = \frac{1}{p} \sum_{a=1}^{n} a\chi(a).$$

Remarque . — Cette quantité n'est jamais nulle. Cela résulte des considérations qui suivent sur les valeurs de fonctions L de Dirichlet. Aucune démonstration élémentaire n'en est connue.

5. Séries de Dirichlet

Soit χ un caractère de Dirichlet primitif modulo m. Rappelons que la fonction L de Dirichlet associée à χ est donnée par la formule

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

Comme c'est un cas particulier des séries de Dirichlet considérées dans la leçon XI, elle se prolonge en une fonction analytique sur le demi-plan $D_{1-\epsilon}$ pour un certain nombre réel $\epsilon > 0$.

THÉORÈME 1. — *Soit k un entier ≥ 1 tel que $\chi(-1) = (-1)^k$. On a*

$$L(\chi, k) = -(-1)^k \frac{(2\pi i)^k B_{k,\bar{\chi}} \tau(\chi)}{2k\,! m^k}$$

En particulier, lorsque χ est un caractère impair, on a

$$L(\chi, 1) = \pi i \frac{\tau(\chi)}{m} B_{1,\bar{\chi}}.$$

Démonstration. — Utilisons la proposition 5. On a (attention, lorsque $k = 1$, il n'y a pas de convergence absolue, le lecteur s'assurera de la validité de la manipulation)

$$B_{k,\bar{\chi}} = m^{k-1} \sum_{a=1}^{m} \bar{B}_k(\frac{a}{m}) = -\frac{m^{k-1} k\,!}{(2\pi i)^k} \sum_{n=-\infty, n\neq 0}^{\infty} \sum_{a=1}^{m} \frac{\bar{\chi}(a) e^{\frac{2i\pi an}{m}}}{n^k}.$$

Utilisons maintenant le fait que les termes de cette série sont invariants par $n \mapsto -n$. Par ailleurs on a (proposition 3) $\sum_{a=1}^{m} \bar{\chi}(a) e^{\frac{2i\pi an}{m}} = \chi(n)\tau(\bar{\chi})$. Cela donne

$$B_{k,\bar{\chi}} = -\frac{2k\,! m^{k-1}}{(2\pi i)^k} \tau(\bar{\chi}) \sum_{n=1}^{\infty} \frac{\chi(n)}{n^k} = -\frac{2k\,! m^{k-1}}{(2\pi i)^k} \tau(\bar{\chi}) L(\chi, k),$$

et donc

$$L(\chi, k) = -\frac{(2\pi i)^k B_{k,\bar{\chi}}}{2k\,! m^{k-1} \tau(\bar{\chi})}.$$

En utilisant la formule $\tau(\bar{\chi}) = \chi(-1)\overline{\tau}(\chi) = \chi(-1) m/\tau(\chi) = (-1)^k \tau(\chi)$ (corollaire de la proposition 3 et proposition 4) on obtient la formule cherchée.

Remarque . — Posons $\delta = 0$ si χ est pair et $\delta = 1$ si χ est impair. Les fonctions L de Dirichlet satisfont l'équation fonctionnelle

$$\Gamma(s) \cos(\pi(s-\delta)/2) L(\chi, s) = \frac{\tau(\chi)}{2i^\delta} (\frac{2\pi}{m})^s L(1-s, \chi).$$

En faisant le produit sur tous les caractères de cette formule on retrouve l'équation fonctionnelle de la fonction ζ de Dedekind de $\mathbf{Q}(\zeta_p)$.

En combinant cela avec le théorème 1, on obtient la formule

$$L(\chi, 1-k) = -\frac{B_{k,\chi}}{k}.$$

On peut comprendre cette dernière formule de la façon incorrecte suivante. Posons $m = 1$ et donc $\chi = 1$ pour simplifier ; c'est-à-dire $L(\chi, s) = \zeta(s)$. On a donc pour k et N entiers ≥ 1 (en utilisant les formules $B_k(X+1) - B_k(X) = kX^{k-1}$ et $B_k(1) = B_k$)

$$-\frac{B_k}{k} = \sum_{n=1}^{N} n^{k-1} - B_k(N) = \sum_{n=1}^{N} \frac{1}{n^{1-k}} - B_k(N).$$

Le premier terme du membre de droite est la somme partielle des termes qui définissent $\zeta(1-k)$, pour $1-k > 1$. Mais aucun des deux termes du membre de droite ne converge quand k est ≥ 1.

Rappelons qu'on a $\zeta_0 = e^{\frac{2i\pi}{m}}$.

THÉORÈME 2. — *Soit χ un caractère de Dirichlet pair modulo m. On a*

$$L(\chi, 1) = -\frac{\tau(\chi)}{m} \sum_{a=1}^{m} \bar{\chi}(a) \log|1 - \zeta_0^a|.$$

Démonstration. — On a

$$L(\chi, 1) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \frac{1}{n\tau(\bar{\chi})} \sum_{a=1}^{m} \bar{\chi}(a) e^{2i\pi an/m}.$$

L'interversion de sommes est délicate puisqu'on n'a pas ici convergence absolue de la série. Après une petite étude de la convergence laissée au lecteur, on obtient

$$L(\chi, 1) = \frac{1}{\tau(\bar{\chi})} \sum_{a=1}^{m} \bar{\chi}(a) \sum_{n=1}^{\infty} \frac{e^{2i\pi an/m}}{n} = -\frac{1}{\tau(\bar{\chi})} \sum_{a=1}^{m} \bar{\chi}(a) \log(1 - e^{2\pi i/m}),$$

où on a utilisé la détermination principale du logarithme. Faisons usage de la formule $\tau(\bar{\chi}) = \chi(-1)m/\tau(\chi) = m/\tau(\chi)$. Cela donne

$$L(\chi, 1) = -\frac{\tau(\chi)}{m} \sum_{a=1}^{m} \bar{\chi}(a) \log(1 - e^{2\pi ai/m}).$$

Utilisons la parité de χ et regroupons les termes d'indice a et $m-a$ à l'aide de la formule $\log(1 - e^{2\pi ai/m}) + \log(1 - e^{-2\pi ai/m}) = 2\log|1 - e^{2\pi ai/m}|$. Cela donne la formule cherchée.

Remarques. — La démonstration du théorème 2 permet d'obtenir aussi le théorème 1 pour $k = 1$.

Lorsque k est un entier ≥ 2 et que χ est de parité opposée à celle de k, on ne dispose pas d'une formule analogue à la formule du nombre de classe. Autrement dit, on n'a pas d'interprétation arithmétique du nombre $L(\chi, k)$.

6. La formule du nombres de classes

Supposons maintenant, pour simplifier, que m soit un nombre premier $p \geq 3$. Les caractères de Dirichlet non triviaux modulo p sont primitifs. Notons X^+ l'ensemble des caractères de Dirichlet primitifs et pairs de niveau p et X^- l'ensemble des caractères de Dirichlet impairs de niveau p. Ces ensembles ont respectivement $(p-3)/2$ et $(p-1)/2$ éléments. Posons

$$R'_p = \prod_{\chi \in X^+} (\sum_{a=1}^{p} -\bar{\chi}(a) \log |1 - \zeta_0^a|).$$

C'est le *régulateur cyclotomique*.

THÉORÈME 3. — On a

$$h_p = 2p \frac{R'_p}{R_p} \prod_{\chi \in X^-} (-\frac{1}{2} B_{1,\chi}).$$

Démonstration. — Nous ne démontrerons cette formule qu'au signe près.

Étudions ce que devient la formule du nombre de classes pour le corps $\mathbf{Q}(\zeta_p)$. On a, compte-tenu des calculs déja effectués des invariants des corps cyclotomiques,

$$(\frac{\zeta_{\mathbf{Q}(\zeta_p)}(s)}{\zeta_{\mathbf{Q}}(s)})_{s=1} = \frac{(2\pi)^{(p-1)/2} h_p R_p}{(2p)\sqrt{p^{p-2}}}.$$

Par ailleurs on a

$$(\frac{\zeta_{\mathbf{Q}(\zeta_p)}(s)}{\zeta_{\mathbf{Q}}(s)})_{s=1} = \prod_{\chi \neq 1} L(\chi, 1),$$

où le produit porte sur les caractères de Dirichlet primitifs de niveau p, c'est-à-dire les caractères non triviaux modulo p.

Utilisons les théorèmes 1 et 2. On obtient

$$\prod_{\chi \neq 1} L(\chi, 1) = \prod_{\chi \in X^+} -\frac{\tau(\chi)}{p} \sum_{a=1}^{p} \bar{\chi}(a) \log |1 - \zeta_0^a| \prod_{\chi \in X^-} \pi i \frac{\tau(\chi)}{p} B_{1,\bar{\chi}}$$

$$= -\frac{(2\pi)^{(p-1)/2} i^{(p-1)/2} (-1)^{(p-3)/2} R'_p}{p^{p-2}} \prod_{\chi \in X^+ \cup X^-} \tau(\chi) \prod_{\chi \in X^-} (-\frac{B_{1,\chi}}{2}).$$

Procédons par regroupement des caractères par paires conjuguées.

Puisque $(\mathbf{Z}/p\mathbf{Z})^*$ est un groupe cyclique, il n'existe qu'un seul caractère non trivial égal à son conjugué. Notons-le χ_0.

La valeur absolue de $\tau(\chi_0)$ est égale à $\sqrt{p}$ puisqu'on a $\tau(\chi)\tau(\bar{\chi}) = \chi(-1)p$. On a donc $\tau(\chi_0) \in \{\sqrt{p}, \sqrt{-p}\}$ si χ_0 est pair et $\tau(\chi_0) \in \{i\sqrt{p}, i\sqrt{-p}\}$ χ_0 est impair. Nous admettrons que ces valeurs sont $\sqrt{p}$ et $i\sqrt{p}$ respectivement (Cela résulte notamment de l'équation fonctionnelle satisfaite par la fonction ζ de Dedekind de $\mathbf{Q}(\zeta_p)$ et de la formule du conducteur-discriminant).

On obtient, en rassemblant les caractères par paires conjuguées et en utilisant les informations qui précèdent sur χ_0,

$$\prod_{\chi \in X^+ \cup X^-} \tau(\chi) = \tau(\chi_0) \prod_{\chi \in X^+ \cup X^-, \chi \neq \chi_0} \tau(\chi) = (i\sqrt{p})^{|X^-|} \sqrt{p}^{|X^+|} = i^{(p-1)/2} p^{(p-2)/2}.$$

Cela permet d'obtenir

$$\prod_{\chi \neq 1} L(\chi, 1) = -\frac{(2\pi)^{(p-1)/2}(-1)^{(p-1)/2}(-1)^{(p-3)/2} R'_p}{p^{(p-2)/2}} \prod_{\chi \in X^-} (-\frac{B_{1,\chi}}{2})$$

En comparant avec la formule du nombre de classes donnée au début de la démonstration on obtient

$$\frac{(2\pi)^{(p-1)/2} R'_p}{p^{(p-2)/2}} \prod_{\chi \in X^-} (-\frac{B_{1,\chi}}{2}) = \frac{(2\pi)^{(p-1)/2} h_p R_p}{(2p)\sqrt{p^{p-2}}}.$$

Une simplification évidente donne la formule cherchée.

Corollaire . — *Les unités cyclotomiques engendrent un sous-groupe d'indice fini du groupe des unités de $\mathbf{Q}(\zeta_p)$. Cet indice est égal à R'_p/R_p.*
Démonstration. — Soit ζ une racine primitive p-ième de l'unité. Posons

$$\theta_i = \frac{1-\zeta^i}{1-\zeta}$$

D'après les formules établies au cours de la proposition 1, le groupe engendré par les θ_i contient toutes les racines de l'unité de $\mathbf{Q}(\zeta_p)$. Il suffit donc de prouver que R'_p/R_p est l'indice du groupe engendré par le plongement logarithmique des unités cyclotomiques dans le plongement logarithmique du groupes des unités de $\mathbf{Q}(\zeta_p)$.

Puisque les plongements complexes de $\mathbf{Q}(\zeta_p)$ sont donnés par $\zeta \mapsto \zeta_0^v$ pour v parcourant $(\mathbf{Z}/p\mathbf{Z})^*$, le plongement logarithmique du groupe engendré par les unités cyclotomiques est engendré par les vecteurs de la forme

$$x_u = (\log|\frac{1-\zeta_0^{uv}}{1-\zeta_0^v}|)_v$$

où u et v parcourent $(\mathbf{Z}/p\mathbf{Z})^*/\{-1,+1\}$ et $u \neq 1$. On a

$$R'_p = \prod_{\chi \neq 1} \sum_u (-2\chi(u) \log |\frac{1-\zeta_0^{uv}}{1-\zeta_0^v}|)$$

car $\sum_{a=1}^p \chi(a) \log |1-\zeta_0^a| = 0$. Par ailleurs le déterminant de la matrice dont les lignes sont les x_u privés de la coordonnées correspondant à $v = 1$ est un déterminant circulant et donc égal à R'_p.

Par ailleurs ce déterminant divisé par le régulateur de $\mathbf{Q}(\zeta_p)$ est l'indice cherché par un argument de covolume.

Remarque . — Il est traditionnel de séparer en deux parties la formule figurant dans le théorème 3. On démontre, à l'aide de la théorie du corps de classe, que h_p^+ divise h_p et que le régulateur de $\mathbf{Q}(\zeta_p)^+$ est égal au régulateur de $\mathbf{Q}(\zeta_p)$. On a en fait

$$h_p^+ = \frac{R'_p}{R_p}$$

et donc

$$h_p^- = 2p \prod_{\chi \in X^-} (-\frac{1}{2} B_{1,\chi}).$$

Ces formules permettent effectivement de calculer des nombres de classes.

7. Compléments

Reprenons la situation laissée dans la section précédente. Le groupe $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ opère sur les idéaux fractionnaires de $\mathbf{Q}(\zeta_p)$ et laisse stable les idéaux principaux. Il opère donc sur le groupe des classes $\mathcal{C}\ell(\mathbf{Q}(\zeta_p))$. Par ailleurs il opère sur le groupe des unités $\mathbf{Z}[\zeta_p]$ et laisse stable le groupe engendré par les unités cyclotomiques.

On a la situation analogue pour le corps de $\mathbf{Q}(\zeta_p)^+$. D'après la dernière remarque de la section précédente le groupe des classes de $\mathbf{Q}(\zeta_p)^+$ et le groupe fini obtenu comme quotient du groupe des unités de de $\mathbf{Q}(\zeta_p)^+$ par le groupe engendré par les unités cyclotomiques ont même ordre. La conjecture d'Iwasawa prédit un lien plus fin entre les structures de ces $\mathrm{Gal}(\mathbf{Q}(\zeta_p)^+/\mathbf{Q})$-modules.

Soit ω l'homomorphisme canonique de groupes $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \longrightarrow \mathbf{F}_p^*$. Tout homomorphisme de groupes $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \longrightarrow \mathbf{F}_p^*$ s'écrit sous la forme ω^i, avec $i \in \{0, 1, ..., p-1\}$. Soit A un $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$-module d'exposant p. Posons

$$A_i = \{a \in A / \sigma(a) = \omega^i a, \sigma(a) \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})\}.$$

On a une décomposition en somme directe

$$A = \oplus_i A_i.$$

Appliquons cela à $A = \mathcal{C}\ell(\mathbf{Q}(\zeta_p))/p\mathcal{C}\ell(\mathbf{Q}(\zeta_p))$. Posons

$$\mathcal{C}\ell(\mathbf{Q}(\zeta_p))_i = A_i.$$

On a donc

$$\mathcal{C}\ell(\mathbf{Q}(\zeta_p))/p\mathcal{C}\ell(\mathbf{Q}(\zeta_p)) = \oplus_i \mathcal{C}\ell(\mathbf{Q}(\zeta_p))_i.$$

Si p divise h_p^-, on peut tirer de la formule du nombre de classe que p divise le produit $\prod_\chi B_{1,\chi}$ où χ parcourt les caractères impairs. Or on a

$$\prod_\chi B_{1,\chi} \equiv \prod_i B_{p-i} \pmod{p}$$

où χ parcourt les caractères impairs et i parcourt les entiers impairs ≥ 1 et $\leq p$.

Si p divise h_p^-, p divise l'un des nombres B_{p-i} pour i impair. En fait on a le résultat plus précis suivant.

THÉORÈME . — *Soit i un entier impair. On a $p \not| B_{p-i}$ si et seulement si le $\mathbf{F}_p$-espace vectoriel $\mathcal{C}\ell(\mathbf{Q}(\zeta_p))_i$ est trivial.*

L'implication est due à Herbrand. L'implication réciproque est beaucoup plus récente et est due à Ribet. Ce type de décomposition en morceaux des groupes de classes et d'unités a culminé dans la démonstration de la conjecture d'Iwasawa.

Pour finir citons la célèbre conjecture de Vandiver : *pour tout nombre premier $p \geq 3$ on a $p \not| h_p^-$*. Signalons qu'il n'existe guère de raison théorique de croire en cette conjecture. La conjecture a été vérifiée pour $p \leq 4000000$; cela ne donne pourtant pas une indication suffisamment probante.