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 $(a_n)_{n\geq 1}$ 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

$$\prod_{\mathcal{P}} \frac{1}{P_{\mathcal{P}}(|\mathcal{P}|^{-s})}$$

où $P_{\mathcal{P}}$ est un polynôme de coefficient constant égal à 1 et où $|\mathcal{P}|$ est l'entier > 0 tel que la norme absolue de $\mathcal{P}$ soit $|\mathcal{P}|\mathbf{Z}$ ($|\mathcal{P}|$ est parfois noté $N_{\mathcal{P}}$ dans ces notes). 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 ; eslle 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 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 commun 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

$$F_K(s) = \prod_{\mathcal{P}} \frac{1}{1 - |\mathcal{P}|^{-s}}$$

où $\mathcal{P}$ parcourt les idéaux maximaux de $\mathcal{O}_K$. Etudions la convergence de ce produit. On a

$$\log(F_K(s)) = \sum_{\mathcal{P}} \sum_{n=1}^{\infty} \frac{1}{n|\mathcal{P}|^{ns}}.$$

Rappelons qu'on a $|\mathcal{P}| = p^{f_{\mathcal{P}}}$ 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 $|\mathcal{P}| \geq p$ et

$$\sum_{\mathcal{P}|p} 1 \leq \sum_{\mathcal{P}|p} f_{\mathcal{P}} e_{\mathcal{P}} = d.$$

On a donc

$$|\log(F_K(s))| = |\sum_{p} \sum_{\mathcal{P}|p} \sum_{n} \frac{1}{np^{f_{\mathcal{P}} s}}| \leq \sum_{p} \sum_{n} \frac{d}{np^{\Re(s)}} = d \log(\zeta(\Re(s))).$$

On en déduit la convergence normale de $F_K(s)$ sur $D_{1+\delta}$ (δ nombre réel > 0) et donc la convergence sur D_0.

Par le théorème de factorisation des idéaux dans $\mathcal{O}_K$ et par multiplicativité de la norme, on a

$$\zeta_K(s) = \sum_{\mathcal{P}} \sum_{n=1}^{\infty} \frac{1}{|\mathcal{P}|^{ns}}.$$

Cette dernière quantité coïncide avec $F_K(s)$. Cela achève de prouver la proposition.

Remarque . — On retiendra le développement en produit eulerien

$$\zeta_K(s) = \prod_{\mathcal{P}} \frac{1}{1 - \frac{1}{|\mathcal{P}|^s}}.$$

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. r_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

$$b_1 + b_2 + ... + b_n = A_n - \frac{2^{r_1}(2\pi)^{r_2}\mathrm{reg}(K)}{\omega_K|\mathcal{D}_K|^{1/2}} n = O(t^{1-1/d}).$$

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

$$\mathcal{M} = \prod_{v\in\Omega_K} \mathcal{P}_v^{n_v}$$

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 $\Omega_{K,\infty}$ tels que $n_v=1$. Posons

$$\mathcal{M}_\infty = \prod_{v\in\Omega_{K,\infty}} \mathcal{P}_v^{n_v}$$

et

$$\mathcal{M}_0 = \prod_{v \in \Omega_K - \Omega_{K,\infty}} \mathcal{P}_v^{n_v}.$$

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 définit pour démontrer le théorème des unités. Considérons un plongement logarithmique un peu différent

$$\Lambda : \qquad K^* \longrightarrow \mathbf{R}^{r_1+r_2}$$

$$x \mapsto (\log(x_1), ..., \log(x_{r_1}), 2\log(x_{r_1+1}), ..., 2\log(x_{r_1+r_2})).$$

Au vu des conventions adoptées pour les normalisations des valeurs absolues complexes, cette définition est plus naturelle que celle utilisée dans la leçon VI. 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 $n(R,t)$ nombre 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 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 $\Lambda(\alpha/(\mathrm{N}_{K/\mathbf{Q}}\alpha)^{1/d}) \in \Lambda(\mathcal{O}_\mathcal{M})$ et donc $\Lambda(\alpha) \in \Lambda(\mathcal{O}_\mathcal{M}) + \mathbf{R}W$.

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 donnée 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 égale à un réseau translaté.

L'ensemble $I_0 \cap K_\mathcal{M}$ est l'intersection de 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 paramétrisables par des cubes et du fait que Λ est un difféomorphisme sur $\Gamma_{\mathcal{M}}$. Les applications $\lambda\phi$ définissent des paramétrisations $d-1$-Lipschitzienne. 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 t^{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

$$n(R,t) = \frac{\mathrm{vol}(\Gamma'_{\mathcal{M}})2^{r_2}}{N_{\mathcal{M}_0}|\mathcal{D}_K|^{1/2}\omega_K}t + O(t^{1-1/d}).$$

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

$$n(R,t) = \frac{2^{r_1}(2\pi)^{r_2}\mathrm{vol}(\Gamma^+_{\mathcal{M}})2^{r_2}}{N_{\mathcal{M}}|\mathcal{D}_K|^{1/2}\omega_K}t + O(t^{1-1/d}).$$

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 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'idéal de rayon $\mathcal{M}$.

6. Compléments

Rappelons que la fonction Γ d'Euler d'une variable complexe s est donnée par la formule

$$\Gamma(s)=\int_0^\infty e^{-t}t^s\,\frac{dt}{t}.$$

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.