Finitude du groupe des classes et théorème des unités.

François BRUNAULT

Groupe de travail Motifs - 24 octobre 2001

Table des matières

1 Introduction.

Dans cet exposé, nous énonçons et démontrons deux résultats fondamentaux de la théorie algébrique des nombres, à savoir la finitude du groupe des classes d'idéaux d'un corps de nombres, et le théorème des unités de Dirichlet. Nous évoquons également leur généralisation au cas d'un corps de fonctions en une variable sur un corps fini.

Nous utiliserons le formalisme géométrique “à la Arakelov” de Szpiro [Szp, pp. 12-15]. Nous verrons que dans ce cadre, la démonstration dans le cas d'un corps de nombres présente des ressemblances frappantes avec celle dans le cas d'un corps de fonctions (cf. les suites exactes (13) et (26)).

2 Énoncé des théorèmes.

Notations. Soit K un corps de nombres. Nous noterons d le degré de K sur $\mathbf{Q}$, $\mathcal{O}_K$ l'anneau des entiers de K, $\mathcal{O}_K^*$ le groupe des unités de $\mathcal{O}_K$, et μ_K le groupe des racines de l'unités dans K.

Soit Σ_K l'ensemble des places de K (classes d'équivalence de valeurs absolues sur K). Posons $\Sigma_K = \Sigma_f \cup \Sigma_\infty$, où Σ_f (resp. Σ_∞) désigne l'ensemble des places finies (resp. infinies) de K. L'ensemble Σ_f est en bijection avec l'ensemble des idéaux premiers non nuls de $\mathcal{O}_K$, c'est-à-dire avec l'ensemble des points fermés du schéma $\operatorname{Spec} \mathcal{O}_K$. L'ensemble Σ_∞ est en bijection avec le quotient de l'ensemble des plongements complexes de K, par la conjugaison complexe. Notons r_1 (resp. $2r_2$) le nombre de plongements réels (resp. complexes) de K, on a alors $\operatorname{Card} \Sigma_\infty = r_1 + r_2$.

Soit $IF(\mathcal{O}_K)$ le groupe des idéaux fractionnaires de $\mathcal{O}_K$. On définit le groupe $Cl(\mathcal{O}_K)$ des classes d'idéaux de $\mathcal{O}_K$ par la suite exacte

$$
\begin{aligned}
K^* \to IF(\mathcal{O}_K) &\to Cl(\mathcal{O}_K) \to 0 \qquad (1)\\
x \mapsto x\mathcal{O}_K. &
\end{aligned}
$$

Les deux théorèmes suivants ont eu un rôle essentiel dans le développement de la théorie algébrique des nombres au cours du 19ème siècle.

Théorème 2.1. *(Dirichlet, Dedekind).*
Le groupe $Cl(\mathcal{O}_K)$ est fini.

Théorème 2.2. *(Dirichlet, 1846).*
Le groupe $\mathcal{O}_K^*$ est isomorphe à $\mu_K \times \mathbf{Z}^{r_1+r_2-1}$, et μ_K est un groupe cyclique fini.

Deux généralisations de ces théorèmes sont possibles. La première consiste à remplacer $\mathcal{O}_K$ par l'anneau des S-entiers de K, où S est une partie finie de Σ_K contenant Σ_∞. La deuxième consiste à remplacer K par un corps de fonctions en une variable sur un corps fini, et $\mathcal{O}_K$ par une structure entière (dans un sens convenable) sur ce corps. Nous allons maintenant adopter un point de vue englobant ces deux généralisations.

Soit K un corps global, c'est-à-dire un corps de nombres ou une extension finie séparable de $\mathbf{F}_q(T)$, où $\mathbf{F}_q$ est le corps fini à q éléments. Dans le deuxième cas, nous supposerons toujours que $\mathbf{F}_q$ est algébriquement fermé dans K. Notons μ_K le groupe des racines de l'unité dans K. Notons enfin Σ_K (resp. Σ_f, Σ_∞) l'ensemble des places (resp. places finies, places infinies) de K. Lorsque K est un corps de fonctions, on a $\Sigma_\infty = \emptyset$.

Définition 2.3. *Soit S une partie finie non vide de Σ_K contenant Σ_∞. On appelle* anneau des S-entiers de K, *et l'on note $\mathcal{O}_S$, l'anneau*

$$\mathcal{O}_S = \{x \in K; \forall v \in \Sigma_K \backslash S, v(x) \geq 0\}.$$

On note $\mathcal{O}_S^*$ le groupe des éléments inversibles de $\mathcal{O}_S$. C'est le *groupe des S-unités de K*. On a

$$\mathcal{O}_S^* = \{x \in K; \forall v \in \Sigma_K \backslash S, v(x) = 0\}.$$

Notons $Cl(\mathcal{O}_S)$ le groupe des classes d'idéaux de l'anneau de Dedekind $\mathcal{O}_S$. Les théorèmes (2.1) et (2.2) se généralisent ainsi :

Théorème 2.4. *Le groupe $Cl(\mathcal{O}_S)$ est fini.*

Théorème 2.5. *Le groupe $\mathcal{O}_S$ est isomorphe à $\mu_K \times \mathbf{Z}^{\mathrm{Card}\, S-1}$, et μ_K est un groupe cyclique fini (égal à $\mathbf{F}_q^*$ dans le cas d'un corps de fonctions).*

Il existe une version plus précise du théorème (2.5). Pour l'énoncer, nous avons besoin de quelques définitions supplémentaires.

Pour toute place $v \in \Sigma_K$, notons K_v le complété de K en v. Définissons une valeur absolue normalisée $||.||_{K_v}$ sur K_v, de la manière suivante. Dans le cas où v est une place finie, notons $k(v)$ le corps résiduel (fini) de K en v et $\mathrm{N}\, v = \mathrm{Card}\, k(v)$ la norme de v. Identifions v à une valuation discrète normalisée sur K et posons

$$||x||_{K_v} = (\mathrm{N}\, v)^{-v(x)}. \qquad (2)$$

Dans le cas où v est une place infinie (K est donc un corps de nombres et $K_v = \mathbf{R}$ ou $\mathbf{C}$), posons

$$
\begin{aligned}
||x||_{\mathbf{R}} &= |x| \\
||z||_{\mathbf{C}} &= |z|^2.
\end{aligned} \tag{3}
$$

Il est à noter que lorsque $K_v = \mathbf{C}$, l'application $||.||_{\mathbf{C}}$ ainsi définie est seulement *équivalente* à une valeur absolue... Avec cette normalisation, la formule du produit s'écrit :

$$
\text{Pour tout } x \in K^*, \qquad \prod_{v \in \Sigma_K} ||x||_{K_v} = 1. \tag{4}
$$

Définition 2.6. *Le* plongement logarithmique r_S *de* $\mathcal{O}_S^*$ *(ou* application régulateur *de* $\mathcal{O}_S^*$*) est défini par*

$$
\begin{aligned}
r_S : \mathcal{O}_S^* &\to \mathbf{R}^S \\
x &\mapsto (\log ||x||_{K_v})_{v \in S}.
\end{aligned} \tag{5}
$$

Notons H_S l'hyperplan de $\mathbf{R}^S$ défini par l'équation $\sum_{v \in S} \lambda_v = 0$. La formule du produit (4) donne alors $r_S(\mathcal{O}_S^*) \subset H_S$. Le théorème (2.5) peut être affiné de la manière suivante.

Théorème 2.7. *L'image $r_S(\mathcal{O}_S^*)$ du plongement logarithmique est un réseau complet de H_S. Le noyau de r_S dans $\mathcal{O}_S^*$ est réduit à μ_K.*

Remarque 2.8. *Le S-régulateur de K est par définition le volume du quotient $H_S/r_S(\mathcal{O}_S^*)$, pour une mesure de Haar bien choisie sur H_S (voir l'exposé suivant).*

3 Rappels de théorie algébrique des nombres.

Notations. Les d plongements complexes de K seront notés $\sigma_1, \dots, \sigma_d$, de telle sorte que $\sigma_1, \dots, \sigma_{r_1}$ soient réels, et que pour tout $j \in [r_1 + 1, r_1 + r_2]$, l'on ait $\sigma_{j+r_2} = \overline{\sigma_j}$. Par suite, Σ_∞ s'identifie à $\{\sigma_1, \dots, \sigma_{r_1+r_2}\}$.

Pour tout $\sigma \in \Sigma_\infty$, nous noterons K_σ le complété de K en σ et nous poserons $\epsilon_\sigma = [K_\sigma : \mathbf{R}]$. Pour alléger les notations, nous poserons $\epsilon_i = \epsilon_{\sigma_i}$ pour tout $i \in [1, d]$.

Définition 3.1. *Soit $(e_1, \dots, e_d)$ une base de $\mathcal{O}_K$ vu comme $\mathbf{Z}$-module. On appelle* discriminant *de K, et l'on note D_K, la quantité*

$$
D_K = (\det(\sigma_i(e_j))_{1 \le i,j \le d})^2 \in \mathbf{Z} \backslash \{0\}. \tag{6}
$$

Remarque 3.2. *Notons ϕ la forme $\mathbf{Q}$-bilinéaire (non dégénérée) sur K donnée par la trace :*

$$
\begin{aligned}
\phi : K^2 &\to \mathbf{Q} \\
(x, y) &\mapsto \mathrm{Tr}_{K/\mathbf{Q}}(xy).
\end{aligned}
$$

On a alors $D_K = \det(\phi(e_i, e_j))_{1 \le i,j \le d}$. Autrement dit, D_K s'interprète géométriquement comme le carré du covolume de $\mathcal{O}_K$ dans K, mesuré au moyen de ϕ.

Définition 3.3. *Soit I un idéal non nul de $\mathcal{O}_K$. On appelle* norme de I*, et l'on note* $\mathrm{N}\, I$*, l'entier*

$$\mathrm{N}\, I = \mathrm{Card}(\frac{\mathcal{O}_K}{I}) \in \mathbf{N}^*. \tag{7}$$

On montre que cette définition est multiplicative en I. On étend alors la définition de la norme aux idéaux fractionnaires de $\mathcal{O}_K$ en posant

$$\mathrm{N}(\frac{I}{J}) = \frac{\mathrm{N}\, I}{\mathrm{N}\, J}.$$

Proposition 3.4. *Soit m un entier ≥ 1. Il n'existe qu'un nombre fini d'idéaux entiers non nuls de $\mathcal{O}_K$ de norme m.*

Démonstration. Soit I un idéal entier non nul de $\mathcal{O}_K$ de norme m. Puisque m annule le groupe abélien $\mathcal{O}_K/I$, on a $m \in I$ puis

$$m\mathcal{O}_K \subset I \subset \mathcal{O}_K.$$

L'idéal I s'identifie donc à un idéal de $\mathcal{O}_K/m\mathcal{O}_K$. Puisque l'anneau $\mathcal{O}_K/m\mathcal{O}_K$ est fini, il n'y a qu'un nombre fini de possibilités pour I.

□

Définition 3.5. *On appelle* plongement canonique de K*, et l'on note* ψ_K*, l'homomorphisme injectif d'anneaux*

$$\begin{aligned} \psi_K : K &\to \prod_{\sigma \in \Sigma_\infty} K_\sigma \\ x &\mapsto (\sigma(x))_{\sigma \in \Sigma_\infty} \end{aligned} \tag{8}$$

où K_σ désigne le complété de K en la place σ.

Proposition 3.6. *Le groupe $\psi_K(\mathcal{O}_K)$ est un réseau complet de $\prod_{\sigma \in \Sigma_\infty} K_\sigma \cong \mathbf{R}^d$. De plus on a, pour la métrique euclidienne usuelle sur $\mathbf{R}^d$:*

$$\mathrm{Vol}(\frac{\mathbf{R}^d}{\psi_K(\mathcal{O}_K)}) = 2^{-r_2}|D_K|^{\frac{1}{2}}. \tag{9}$$

Démonstration. Soit $(e_1, \ldots, e_d)$ une base de $\mathcal{O}_K$ sur $\mathbf{Z}$ et V le déterminant

$$V = \begin{vmatrix} \vdots & & \vdots \\ \sigma_i(e_1) & \ldots & \sigma_i(e_d) \\ \vdots & & \vdots \\ \vdots & & \vdots \\ \mathrm{Re}\, \sigma_j(e_1) & \ldots & \mathrm{Re}\, \sigma_j(e_d) \\ \mathrm{Im}\, \sigma_j(e_1) & \ldots & \mathrm{Im}\, \sigma_j(e_d) \\ \vdots & & \vdots \end{vmatrix}_{1 \leq i \leq r_1,\ r_1+1 \leq j \leq r_1+r_2} . \tag{10}$$

En utilisant le fait que $\mathrm{Re}\, \sigma_j = \frac{1}{2}(\sigma_j + \overline{\sigma_j})$ et $\mathrm{Im}\, \sigma_j = \frac{1}{2i}(\sigma_j - \overline{s_j})$, ainsi que la linéarité du déterminant par rapport aux lignes, il vient

$$V = (-\frac{1}{2i})^{r_2} \begin{vmatrix} \vdots & & \vdots \\ \sigma_i(e_1) & \dots & \sigma_i(e_d) \\ \vdots & & \vdots \\ \vdots & & \vdots \\ \sigma_j(e_1) & \dots & \sigma_j(e_d) \\ \overline{\sigma_j}(e_1) & \dots & \overline{\sigma_j}(e_d) \\ \vdots & & \vdots \end{vmatrix}_{1\leq i\leq r_1,\ r_1+1\leq j\leq r_1+r_2} . \tag{11}$$

On a donc $|V| = 2^{-r_2}|D_K|^{1/2}$. En particulier, V est non nul et $\psi_K(\mathcal{O}_K)$ est un réseau de $\mathbf{R}^d$. Enfin, on a par définition même du volume $\mathrm{Vol}(\frac{\mathbf{R}^d}{\psi_K(\mathcal{O}_K)}) = |V| = 2^{-r_2}|D_K|^{1/2}$.

$\square$

Corollaire 3.7. *Soit I un idéal fractionnaire de $\mathcal{O}_K$. Le groupe $\psi_K(I)$ est un réseau complet de $\mathbf{R}^d$. De plus on a :*

$$\mathrm{Vol}(\frac{\mathbf{R}^d}{\psi_K(I)}) = 2^{-r_2}|D_K|^{\frac{1}{2}}\,\mathrm{N}\,I. \tag{12}$$

4 Le groupe de Picard compactifié.

Nous allons construire un groupe abélien $\mathrm{Pic}_c(\mathcal{O}_K)$ localement compact muni d'une suite exacte de groupes abéliens

$$1 \to \mu_K \to \mathcal{O}_K^* \xrightarrow{r_K} \mathbf{R}^{r_1+r_2} \to \mathrm{Pic}_c(\mathcal{O}_K) \xrightarrow{\pi} \mathrm{Cl}(\mathcal{O}_K) \to 0 \tag{13}$$

où $\mu_K, \mathcal{O}_K^*$ et $\mathrm{Cl}(\mathcal{O}_K)$ sont munis de la topologie discrète.

Définition 4.1. *On appelle* groupe des diviseurs compactifiés sur $\mathcal{O}_K$*, et l'on note* $\mathrm{Div}_c(\mathcal{O}_K)$*, le groupe des diviseurs de la forme*

$$D = \sum_{\mathfrak{p}\in\Sigma_f} n_{\mathfrak{p}}\{\mathfrak{p}\} + \sum_{\sigma\in\Sigma_\infty} \lambda_\sigma\{\sigma\} \tag{14}$$

avec $n_{\mathfrak{p}} \in \mathbf{Z}$ et $\lambda_\sigma \in \mathbf{R}$. Le degré *d'un tel diviseur est la quantité*

$$\deg D = \sum_{\mathfrak{p}\in\Sigma_f} n_{\mathfrak{p}} \log(\mathrm{N}\,\mathfrak{p}) + \sum_{\sigma\in\Sigma_\infty} \lambda_\sigma.$$

Nous noterons $\mathrm{Div}_c^0(\mathcal{O}_K) \subset \mathrm{Div}_c(\mathcal{O}_K)$ le sous-groupe des diviseurs de degré 0.

Définition 4.2. *Le* diviseur principal associé à $x \in K^*$ *est le diviseur compactifié*

$$\mathrm{div}(x) = -\sum_{\mathfrak{p}\in\Sigma_f} v_{\mathfrak{p}}(x)\{\mathfrak{p}\} + \sum_{\sigma\in\Sigma_\infty} \epsilon_\sigma \log|\sigma(x)|\{\sigma\}$$

(rappelons que l'on a posé $\epsilon_\sigma = [K_\sigma : \mathbf{R}]$). On note $\mathrm{Pr}_c(\mathcal{O}_K) \subset \mathrm{Div}_c(\mathcal{O}_K)$ le sous-groupe des diviseurs principaux. Remarquons que tout diviseur principal est de degré 0, autrement dit $Pr_c(\mathcal{O}_K) \subset \mathrm{Div}_c^0(\mathcal{O}_K)$.

Définition 4.3. *Un* faisceau inversible compactifié sur $\mathcal{O}_K$ *est un $\mathcal{O}_K$-module L, projectif de rang 1 (i.e. L est facteur direct d'un $\mathcal{O}_K$-module libre, et $\dim_K(L \otimes_{\mathcal{O}_K} K) = 1$), muni pour chaque $\sigma \in \Sigma_\infty$ d'une métrique hermitienne définie positive $|.|_\sigma$ sur $L_\sigma := L \otimes_{\mathcal{O}_K} K_\sigma$. Les métriques $|.|_\sigma$ sont appelées* métriques à l'infini de L.

Remarque 4.4. *Si L est un $\mathcal{O}_K$-module projectif de rang 1, alors L_σ est un K_σ-espace vectoriel de dimension 1. Lorsque $K_\sigma = \mathbf{R}$ (resp. $K_\sigma = \mathbf{C}$), se donner une métrique hermitienne définie positive sur L_σ revient à se donner un élément de norme 1 dans L_σ (resp. se donner un cercle unité dans L_σ).*

Définition 4.5. *Deux faisceaux inversibles compactifiés L_1 et L_2 sont dits* isomorphes *lorsqu'il existe un isomorphisme de $\mathcal{O}_K$-modules de L_1 vers L_2 respectant les métriques à l'infini.*

Exemple. Lorsque $L = \mathcal{O}_K$ est muni des métriques standard à l'infini, définies par $|1|_\sigma = 1$, on parle du *faisceau inversible compactifié trivial.*

Remarque 4.6. *Les $\mathcal{O}_K$-modules projectifs de rang 1 sont exactement les idéaux fractionnaires de $\mathcal{O}_K$ (à $\mathcal{O}_K$-isomorphisme près). On peut donc toujours supposer, lorsque L est un faisceau inversible compactifié sur $\mathcal{O}_K$, que l'on a $L \subset K$. Cette inclusion induit un isomorphisme $L_\sigma \cong K_\sigma$ (attention : cet isomorphisme ne transporte pas la métrique à l'infini de L vers la métrique standard à l'infini de $\mathcal{O}_K$).*

Définition 4.7. *Deux faisceaux inversibles compactifiés $(L_1, |.|_{1,\sigma})$ et $(L_2, |.|_{2,\sigma})$ sont dits* isométriques *lorsqu'il existe un isomorphisme de $\mathcal{O}_K$-modules $\phi : L_1 \to L_2$ et une unité $u \in \mathcal{O}_K^*$ tels que pour tout $\sigma \in \Sigma_\infty$,*

$$\phi^* |.|_{2,\sigma} = |\sigma(u)| \, |.|_{1,\sigma} \tag{15}$$

Définition 4.8. *Nous appellerons* groupe de Picard compatifié de $\mathcal{O}_K$, *et nous noterons* $\mathrm{Pic}_c(\mathcal{O}_K)$, *l'ensemble des classes d'isométrie de faisceaux inversibles compactifiés. C'est un groupe abélien pour la loi*

$$(L_1, |.|_{1,\sigma}) + (L_2, |.|_{2,\sigma}) := (L_1 \otimes_{\mathcal{O}_K} L_2, |.|_{1,\sigma} \otimes |.|_{2,\sigma}), \tag{16}$$

l'élément neutre étant la classe du faisceau inversible compactifié trivial.

Proposition 4.9. *On a un isomorphisme*

$$\mathrm{Pic}_c(\mathcal{O}_K) \cong \frac{\mathrm{Div}_c(\mathcal{O}_K)}{\mathrm{Pr}_c(\mathcal{O}_K)}.$$

Démonstration. Indiquons comment construire cet isomorphisme.

Soit $D = \sum_{\mathfrak{p} \in \Sigma_f} n_\mathfrak{p} \{\mathfrak{p}\} + \sum_{\sigma \in \Sigma_\infty} \lambda_\sigma \{\sigma\}$ un diviseur compactifié sur $\mathcal{O}_K$. On lui associe l'idéal fractionnaire

$$L = \prod_{\mathfrak{p} \in \Sigma_f} \mathfrak{p}^{-n_\mathfrak{p}}$$

muni des métriques à l'infini $|.|_\sigma$ définies par

$$|1|_\sigma = \exp\left(\frac{-\lambda_\sigma}{\epsilon_\sigma}\right).$$

Cela fournit un homomorphisme de groupes $\mathrm{Div}_c(\mathcal{O}_K)/\,\mathrm{Pr}_c(\mathcal{O}_K) \to \mathrm{Pic}_c(\mathcal{O}_K)$ (on pourra remarquer que si I, J sont deux idéaux fractionnaires de $\mathcal{O}_K$, on a $I \otimes_{\mathcal{O}_K} J \cong IJ$).

Réciproquement, soit L un faisceau inversible compactifié sur $\mathcal{O}_K$. D'après une remarque précédente, L est isomorphe à un idéal fractionnaire I de $\mathcal{O}_K$ muni de métriques à l'infini $|.|_\sigma$. On associe à L le diviseur

$$D = -\sum_{\mathfrak{p}\in\Sigma_f} v_{\mathfrak{p}}(I)\{\mathfrak{p}\} - \sum_{\sigma\in\Sigma_\infty} \epsilon_\sigma \log|1|_\sigma\{\sigma\}.$$

La classe de ce diviseur dans $\mathrm{Div}_c(\mathcal{O}_K)/\Pr_c(\mathcal{O}_K)$ ne dépend ni du choix de I, ni de la classe d'isométrie de L, ce qui fournit l'homomorphisme réciproque $\mathrm{Pic}_c(\mathcal{O}_K) \to \mathrm{Div}_c(\mathcal{O}_K)/\Pr_c(\mathcal{O}_K)$.

□

Construction de la suite exacte (13). L'homomorphisme r_K est donné par le plongement logarithmique (5) pour $S = \Sigma_\infty$. Il se réécrit de la manière suivante :

$$\begin{aligned} r_K : \mathcal{O}_K^* &\to \mathbf{R}^{r_1+r_2} \\ x &\mapsto (\epsilon_1 \log|\sigma_1(x)|, \dots, \epsilon_{r_1+r_2} \log|\sigma_{r_1+r_2}(x)|). \end{aligned} \tag{17}$$

L'homomorphisme $\mathbf{R}^{r_1+r_2} \to \mathrm{Pic}_c(\mathcal{O}_K)$ est donné par :

$$\begin{aligned} \mathbf{R}^{r_1+r_2} &\to \mathrm{Pic}_c(\mathcal{O}_K) \\ (\lambda_1,\dots,\lambda_{r_1+r_2}) &\mapsto \left[\sum_{i=1}^{r_1+r_2} \lambda_i\{\sigma_i\}\right] = \left[\left(\mathcal{O}_K, |1|_{\sigma_i} = \exp(\frac{-\lambda_i}{\epsilon_i})\right)\right]. \end{aligned} \tag{18}$$

L'homomorphisme $\mathrm{Pic}_c(\mathcal{O}_K) \to \mathrm{Cl}(\mathcal{O}_K)$ est donné par *l'oubli des métriques à l'infini*. Étant donné un faisceau inversible compactifié L isomorphe à un idéal fractionnaire I (muni de métriques à l'infini), on associe à L la classe de I dans $\mathrm{Cl}(\mathcal{O}_K)$:

$$\begin{aligned} \mathrm{Pic}_c(\mathcal{O}_K) &\to \mathrm{Cl}(\mathcal{O}_K) \\ [(I, |.|_\sigma)] &\mapsto [I]. \end{aligned} \tag{19}$$

Proposition 4.10. *La suite (13) est exacte en $\mathcal{O}_K^*$.*

Démonstration. Il est évident que $r_K(\mu_K) = 0$. Réciproquement, posons

$$N := \{x \in \mathcal{O}_K^*, r_K(x) = 0\}.$$

En utilisant le fait que $\psi_K(\mathcal{O}_K)$ est un réseau de $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$, on montre que pour tout nombre réel M, l'ensemble

$$E_M := \{x \in \mathcal{O}_K, \text{pour tout } i \in [1, r_1+r_2], |\sigma_i(x)| \leq M\}$$

est fini. Puisque $N \subset E_1$, on a que N est fini. D'autre part, puisque N est un groupe, on obtient $N \subset \mu_K$, ce qui achève de démontrer la proposition.

□

L'exactitude de (13) en les autres termes est laissée en exercice. On obtient ainsi :

Proposition 4.11. *La suite (13) est une suite exacte de groupes abéliens.*

On munit $\mathrm{Pic}_c(\mathcal{O}_K)$ de l'unique topologie rendant la suite exacte (13) continue. La suite (13) devient une suite exacte de groupes abéliens localement compacts.

Définition 4.12. *Soit L un faisceau inversible compactifié. On appelle ensemble des sections de L, et l'on note $H^0(L)$, l'ensemble*

$$H^0(L) = \{s \in L; \forall \sigma, |s|_\sigma \leq 1\}. \tag{20}$$

C'est un ensemble fini (cf. proposition 3.6 et démonstration de la proposition 4.10).

Définition 4.13. *Soit L un faisceau inversible compactifié. On appelle caractéristique d'Euler-Poincaré de L, et l'on note $\chi(L)$, la quantité*

$$\chi(L) = -\log \mathrm{Vol}(\frac{\bigoplus_\sigma L_\sigma}{L}). \tag{21}$$

(En effet, L est un réseau de $\bigoplus_\sigma L_\sigma$, d'après le corollaire 3.7 et la remarque 4.6).
On appelle caractéristique d'Euler-Poincaré modifiée de L, la quantité

$$\chi'(L) = \chi(L) - \log \frac{2^d}{2^{r_1}\pi^{r_2}}. \tag{22}$$

Proposition 4.14. *On a les identités*

$$\chi(L) = \chi(\mathcal{O}_K) + \deg L \quad \textit{et} \quad \chi'(L) = \chi'(\mathcal{O}_K) + \deg L. \tag{23}$$

Démonstration. Écrivons $L = (I, |.|_\sigma)$ avec I idéal fractionnaire de $\mathcal{O}_K$ et $|.|_\sigma$ métrique sur K_σ. On a :

$$\begin{aligned}\chi(L) &= -\log \mathrm{Vol}(\frac{\bigoplus_\sigma L_\sigma}{L}) = -\log \mathrm{Vol}(\frac{\bigoplus_\sigma K_\sigma}{I}) - \log \prod_\sigma |1|_\sigma^{\epsilon_\sigma} \\ &= -\log(2^{-r_2}|D_K|^{1/2} NI) - \sum_\sigma \epsilon_\sigma \log |1|_\sigma\end{aligned}$$

d'après (12). Le même calcul conduit à

$$\chi(\mathcal{O}_K) = -\log(2^{-r_2}|D_K|^{1/2}).$$

En utilisant la correspondance entre les (classes de) diviseurs compactifiés et les faisceaux inversibles compactifiés, ainsi que la définition (4.1) du degré, on en déduit la proposition.

□

Proposition 4.15. *Soit L un faisceau inversible compactifié tel que* $\deg L < 0$*, alors $H^0(L) = \{0\}$.*

Proposition 4.16. *Soit L un faisceau inversible compactifié tel que $\chi'(L) \geq 0$, alors $H^0(L) \neq \{0\}$.*

Démonstration. Notons $|.|_\sigma$ les métriques à l'infini de L. Soit

$$B = \{x \in \bigoplus_\sigma L_\sigma; \forall \sigma, |x|_\sigma \leq 1\}.$$

B est une partie compacte convexe de $\bigoplus_\sigma L_\sigma$, et l'on a $B = -B$. Notons μ la mesure sur $\bigoplus_\sigma L_\sigma$ associée aux métriques à l'infini. On a évidemment

$$\mu(B) = 2^{r_1}\pi^{r_2}.$$

De plus

$$\mathrm{Vol}(\frac{\bigoplus_\sigma L_\sigma}{L}) = \exp(-\chi(L)) = \frac{2^{r_1}\pi^{r_2}}{2^d}\exp(-\chi'(L)) \leq \frac{2^{r_1}\pi^{r_2}}{2^d}.$$

Il reste alors à appliquer le lemme de Minkowski ci-dessous.

□

Lemme 4.17. *(Minkowski)*

Soit Λ un réseau complet de $\mathbf{R}^d$, et B une partie compacte convexe de $\mathbf{R}^d$ vérifiant $B = -B$. Si $\mu(B) \geq 2^d\mu(\frac{\mathbf{R}^d}{\Lambda})$ (pour n'importe quelle mesure de Haar μ sur $\mathbf{R}^d$), alors $B \cap \Lambda \supsetneq \{0\}$.

5 Démonstrations des théorèmes.

5.1 Cas de la caractéristique p

Soit K une extension finie séparable de $k(T)$, où k est un corps fini de caractéristique p. Nous supposerons k algébriquement fermé dans K (quitte à changer k, on peut toujours se ramener à ce cas-là). Notons X l'unique courbe projective lisse sur k telle que $K = k(X)$.

Soit S un ensemble fini non vide de points fermés de X. Posons $U = X \setminus S$, c'est un ouvert affine de X. On a $\mathcal{O}_S = \mathcal{O}_X(U)$ (cf. définition (2.3)) et $U = \operatorname{Spec}\mathcal{O}_S$. L'anneau $\mathcal{O}_S$ est un anneau de Dedekind, de corps des fractions K.

Définition 5.1. *Nous appellerons groupe de Picard de X/k (resp. groupe de Picard de U/k), et nous noterons* $\mathrm{Pic}(X)$ *(resp.* $\mathrm{Pic}(U)$*), le groupe abélien défini de la manière suivante :*

$$\mathrm{Pic}(X) = \frac{\{\textit{Diviseurs } k-\textit{rationnels sur } X\}}{\{\textit{Diviseurs } k-\textit{rationnels principaux}\}} \tag{24}$$

$$\textit{resp. } \mathrm{Pic}(U) = \frac{\{\textit{Diviseurs } k-\textit{rationnels sur } U\}}{\{\textit{Diviseurs } k-\textit{rationnels principaux}\}}.$$

Le groupe $\mathrm{Pic}(U)$ s'identifie au groupe $\mathrm{Cl}(\mathcal{O}_S)$ des classes d'idéaux de l'anneau de Dedekind $\mathcal{O}_S$. Quant au groupe $\mathrm{Pic}(X)$, on peut le décrire de la manière suivante.

Lemme 5.2. *Soit* $\mathrm{Pic}^0(X)$ *le sous-groupe de* $\mathrm{Pic}(X)$ *défini par la suite exacte*

$$0 \to \mathrm{Pic}^0(X) \to \mathrm{Pic}(X) \xrightarrow{\deg} \mathbf{Z} \to 0 \tag{25}$$

Alors $\mathrm{Pic}^0(X)$ *est un groupe fini.*

Démonstration. La suite exacte (25) résulte de l'existence d'un 0-cycle k-rationnel de degré 1 sur X.

Le groupe $\mathrm{Pic}^0(X)$ s'identifie au groupe des points k-rationnels de la jacobienne de X, qui est une courbe projective sur k, d'où le fait que $\mathrm{Pic}^0(X)$ est fini.

□

Proposition 5.3. *On a une suite exacte*

$$1 \to (k')^* \to \mathcal{O}_S^* \xrightarrow{\mathrm{div}} \mathbf{Z}^S \to \mathrm{Pic}(X) \to \mathrm{Pic}(U) \to 0 \tag{26}$$

Rappelons seulement la définition des différentes flèches.

L'application $\mathcal{O}_S^* \to \mathbf{Z}^S$ associe à toute fonction $f \in OS^*$ la restriction à S du diviseur principal $\operatorname{div} f$. L'application $\mathbf{Z}^S \to \operatorname{Pic}(X)$ associe à tout diviseur sur S sa classe dans $\operatorname{Pic}(X)$. L'application $\operatorname{Pic}(X) \to \operatorname{Pic}(U)$ consiste en la restriction des diviseurs de X à U.

Théorème 5.4. *(cf. théorème 2.4) Le groupe* $\operatorname{Cl}(\mathcal{O}_S) = \operatorname{Pic}(U)$ *est fini.*

Démonstration. On sait que $\operatorname{Pic}(X)$ est de type fini (cf. (25)). Par conséquent $\operatorname{Pic}(U)$ est de type fini (cf. (26). D'autre part, soit $s \in S$. Posons $m = \deg s$ et $n = \operatorname{Card} \operatorname{Pic}^0(X)$. En utilisant la suite exacte (26), on constate que $\operatorname{Pic}(U)$ est annulé par mn. Autrement dit $\operatorname{Pic}(U)$ est de type fini et d'exposant fini, c'est donc un groupe fini.

□

Théorème 5.5. *(cf. théorème 2.5) Le groupe* $\mathcal{O}_S^*$ *est un groupe abélien de type fini, de rang* $\operatorname{Card} S - 1$.

Démonstration. La type-finitude de $\mathcal{O}_S^*$ est conséquence de la suite exacte (26). De plus, si l'on tensorise cette suite exacte par $\mathbf{Q}$, on obtient (par exactitude de la localisation)

$$1 \to \mathcal{O}_S^* \otimes_{\mathbf{Z}} \mathbf{Q} \to \mathbf{Q}^S \to \mathbf{Q} \to 0,$$

ce qui montre que le rang de $\mathcal{O}_S^*$ est égal à $\operatorname{Card} S - 1$.

□

5.2 Cas de la caractéristique 0

Soit K un corps de nombres. Nous allons nous contenter de démontrer les théorèmes 2.1 et 2.2 (autrement dit nous nous placerons dans le cas $S = \Sigma_\infty$). Nous nous appuierons sur la suite exacte (13), que nous reproduisons ici:

$$1 \to \mu_K \to \mathcal{O}_K^* \xrightarrow{r_K} \mathbf{R}^{r_1+r_2} \to \operatorname{Pic}_c(\mathcal{O}_K) \xrightarrow{\pi} \operatorname{Cl}(\mathcal{O}_K) \to 0.$$

On notera la ressemblance avec la suite exacte (26). On peut rendre cette ressemblance encore plus évidente, de la manière suivante. Soit U le schéma affine $U = \operatorname{Spec} \mathcal{O}_K$. Posons $X = U \cup \Sigma_\infty$. Heuristiquement, X est une compactification de U et $\operatorname{Pic}_c(\mathcal{O}_K) = \operatorname{Pic}(X)$.

Soit H l'hyperplan de $\mathbf{R}^{r_1+r_2}$ défini par la suite exacte

$$\begin{array}{l} 0 \to H \to \mathbf{R}^{r_1+r_2} \to \mathbf{R} \to 0 \\ \qquad\qquad\quad (\lambda_i)_i \mapsto \displaystyle\sum_{i=1}^{r_1+r_2} \lambda_i. \end{array}$$

Posons $\operatorname{Pic}_c^0(\mathcal{O}_K) = \operatorname{Div}_c^0(\mathcal{O}_K)/\operatorname{Pr}_c(\mathcal{O}_K)$. On a donc une suite exacte

$$0 \to \operatorname{Pic}_c^0(\mathcal{O}_K) \to \operatorname{Pic}_c(\mathcal{O}_K) \xrightarrow{\deg} \mathbf{R} \to 0.$$

La formule du produit donne $r_K(\mathcal{O}_K^*) \subset H$. On a donc en fait une suite exacte

$$1 \to \mu_K \to \mathcal{O}_K^* \xrightarrow{r_K} H \to \operatorname{Pic}_c^0(\mathcal{O}_K) \xrightarrow{\pi} \operatorname{Cl}(\mathcal{O}_K) \to 0.$$

Démonstration du théorème 2.1. Soit L un idéal fractionnaire de $\mathcal{O}_K$. Nous allons montrer que L est équivalent à un idéal entier non nul I de $\mathcal{O}_K$ de norme inférieure ou égale à $\exp(-\chi'(\mathcal{O}_K))$, ce qui concluera d'après la proposition 3.4.

Munissons L^{-1} de métriques à l'infini $|.|_\sigma$ de telle façon que $\deg(L^{-1}) = -\chi'(\mathcal{O}_K)$. On a donc $\chi'(L^{-1}) = 0$. D'après le lemme 4.16, on a $H^0(L^{-1}) \neq \{0\}$. Soit donc $x \in L^{-1}$ tel que pour tout $\sigma \in \Sigma_\infty$, on ait $|x|_\sigma \leq 1$. Posons $I = xL$, c'est un idéal entier non nul de $\mathcal{O}_K$. On a alors

$$\begin{aligned}
\mathbf{N}I &= |\mathbf{N}_{K/\mathbf{Q}}x|\mathbf{N}L \\
&= (\prod_\sigma |\sigma(x)|^{\epsilon_\sigma})\mathbf{N}L \\
&= (\prod_\sigma (\frac{|x|_\sigma}{|1|_\sigma})^{\epsilon_\sigma})\mathbf{N}L \\
&\leq (\prod_\sigma (\frac{1}{|1|_\sigma})^{\epsilon_\sigma})\mathbf{N}L \\
&\leq (\prod_\sigma (\frac{1}{|1|_\sigma})^{\epsilon_\sigma})\mathbf{N}L^{-1} \\
&\leq \exp(\deg L^{-1}) \qquad \text{par définition du degré} \\
&\leq \exp(-\chi'(\mathcal{O}_K)).
\end{aligned}$$

□

Remarque 5.6. *On peut en fait améliorer la constante* $\exp(-\chi'(\mathcal{O}_K))$ *(c'est utile pour démontrer le théorème d'Hermite, qui dit qu'il n'y a qu'un nombre fini de corps de nombres de discriminant donné).*

Démonstration du théorème 2.2. Nous allons démontrer que $r_K(\mathcal{O}_K^*)$ est un réseau de H. Clairement cela entraîne le théorème 2.2.

Lemme 5.7. *Le sous-groupe* $r_K(\mathcal{O}_K^*)$ *est discret dans* H.

Démonstration du lemme 5.7. Il suffit de montrer que pour toute partie bornée B de H, l'ensemble $B \cap r_K(\mathcal{O}_K^*)$ est fini. Soit $E = \{x \in \mathcal{O}_K^*; r_K(x) \in B\}$. D'après la proposition 3.6, l'ensemble E est fini (cf. démonstration de la proposition 4.10). Le lemme suit.

□

Pour montrer que $r_K(\mathcal{O}_K^*)$ est un réseau de H il suffit maintenant de démontrer que $\mathrm{Pic}_c^0(\mathcal{O}_K)$ est quasi-compact. Pour cela il suffit de démontrer que l'ensemble

$$Y = \{L \in \mathrm{Pic}_c(\mathcal{O}_K); \deg L = -\chi'(\mathcal{O}_K) \text{ et } \pi(L) = 0\} \tag{27}$$

est quasi-compact.

Soit $(L_n)_n$ une suite d'éléments de Y. On peut supposer que L_n est représenté par le faisceau inversible compactifié $(\mathcal{O}_K, |.|_{n,\sigma})$. On a $\deg(L_n) = -\chi'(\mathcal{O}_K)$ d'où $\chi'(L_n) = 0$.

Par le lemme 4.16, il existe $x_n \in L_n, x_n \neq 0$ tel que pour tout σ, on ait $|x_n|_{n,\sigma} \leq 1$. Par un calcul similaire à celui de la démonstration du théorème 2.1, il vient $\mathbf{N}_{K/\mathbf{Q}}(x_n) \leq \exp(-\chi'(\mathcal{O}_K))$.

Quitte à extraire une sous-suite de (x_n), on peut donc supposer que pour tout n, on a $x_n\mathcal{O}_K = x\mathcal{O}_K$ avec $x \in K^*$. Posons $x_n = u_n x$ avec $u_n \in \mathcal{O}_K^*$. Soit

$$D_n = \sum_\sigma \lambda_{n,\sigma}\{\sigma\}$$

le diviseur compactifié associé à L_n (on a donc $|1|_{n,\sigma} = \exp(-\lambda_{n,\sigma}/\epsilon_\sigma))$. Alors L_n est équivalent à

$$L'_n = \sum_\sigma (\lambda_{n,\sigma} - \epsilon_\sigma \log|\sigma(u_n)|)\{\sigma\}.$$

Montrons que $(lambda'_{n,\sigma})_n := (\lambda_{n,\sigma} - \epsilon_\sigma \log|\sigma(u_n)|)_n$ est une suite bornée. On a

$$\begin{aligned} lambda'_{n,\sigma} &= -\epsilon_\sigma \log|1|_{n,\sigma} - \epsilon_\sigma \log|x_n|_{n,\sigma} + \epsilon_\sigma \log|x|_{n,\sigma} \\ &= -\epsilon_\sigma \log|x_n|_{n,\sigma} + \epsilon_\sigma \log|\sigma(x)| \\ &\geq \epsilon_\sigma \log|\sigma(x)| \text{ par hypothèse sur les } x_n. \end{aligned}$$

La suite $(lambda'_{n,\sigma})_n$ est donc minorée. Puisque

$$\sum_\sigma \lambda'_{n,\sigma} = -\chi'(\mathcal{O}_K)$$

elle est également majorée. Quitte à extraire une sous-suite on peut donc supposer que pour tout σ, on a $\lambda'_{n,\sigma} \to \lambda'_\sigma \in \mathbf{R}$. D'où $L_n \to [\sum_\sigma \lambda'_\sigma\{\sigma\}] \in Y$.

$\square$

Remarque 5.8. *On peut résumer les énoncés 2.1 et 2.2 en disant que le groupe* $\mathrm{Pic}^0_c(\mathcal{O}_K)$ *est compact.*

Références.

[Szp] Szpiro L., Degré, intersections, hauteurs. In *Séminaire sur les pinceaux arithmétiques : la conjecture de Mordell*, Astérisque No. 127, Société Mathématique de France, Paris (1985), pp. 11-28.