Université Paris Sud — Année 2008-2009

M1 — Arithmétique

TD n° VI

Exercice A. −Finitude du groupe de Picard d'un corps de nombres

Soit K un corps de nombres c'est-à-dire une extension finie de $\mathbb{Q}$. On notera d son degré, et $\mathcal{O}_K$ son anneau d'entiers.

On pourra fixer d $\mathbb{Q}$-plongements deux à deux distincts $\sigma_{i\ ,1\leq i\leq d}$ de K dans une clôture algébrique de $\mathbb{Q}$. Pour tout $x \in K$, on notera alors

$$\mathrm{N}_{K/\mathbb{Q}}(x) \ = \ \prod_{i=1}^{d} \sigma_i(x) \text{ (cf. III.3.2.2.iii.)}$$

On notera encore

$$\mathrm{N}_{K/\mathbb{Q}}) \ : \ \mathcal{I}(\mathcal{O}_K) \ \to \ \mathcal{I}(\mathbb{Z})$$

l'application définie en III.3.2.4.

1) Donner un sens à la notation

$$N(\mathfrak{I}) \ := \ |\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{I})| \, \forall \, \mathfrak{I} \ \in \ \mathcal{I}(\mathcal{O}_K) \, .$$

2) Soit $(e_1, \ldots, e_d)$ une $\mathbb{Q}$-base de K. Montrer qu'il existe $c \ > \ 0$ tel que pour tout d-uplet $a_{i\ ,1\leq i\leq d} \in \mathbb{Q}$ d'éléments de $\mathbb{Q}$,

$$|\mathrm{N}_{L/K}(\sum_{i=1}^{d} a_i e_i)| \ \leq \ c \sup\{|a_i|^d\}_{1\leq i\leq d} \, .$$

3) Soit $(e_1, \ldots, e_d)$ une $\mathbb{Z}$-base de $\mathcal{O}_K$. Pour tout idéal $\mathfrak{I} \ \subset \ \mathcal{O}_K$ de $\mathcal{O}_K$, notons

$$E \ := \ \{\sum_{i=1}^{d} a_i e_i \mid a_i \in \mathbb{Z} \text{ et } 0 \leq a_i \leq N(\mathfrak{I})^{\frac{1}{d}}\} \, .$$

a) Montrer que

$$\#(E) \ > \ N(\mathfrak{I}) \, .$$

b) Montrer que $\mathcal{O}_K/\mathfrak{I}$ est un ensemble fini et que

$$\#(\mathcal{O}_K/\mathfrak{I}) \;=\; N(\mathfrak{I})\,.$$

c) En déduire qu'il existe des éléments α et β de E avec

$$\alpha \;\neq\; \beta \,\text{et}\, \beta-\alpha \;\in\; \mathfrak{I}\,.$$

d) Montrer finalement qu'il existe $c>0$ tel que pour tout idéal $\mathfrak{I}\subset\mathcal{O}_K$ de $\mathcal{O}_K$, il existe $\gamma\in\mathfrak{I}$ tel que

$$|\mathrm{N}_{K/\mathbb{Q}}(\gamma)| \;\leq\; cN(\mathfrak{I})\,.$$

4) On note encore c la constante définie en 3.d. Soit $\mathfrak{I}\in\mathcal{I}(\mathcal{O}_K)$ un idéal fractionnaire de $\mathcal{O}_K$.

a) Rappeler qu'il existe $\alpha\in\mathcal{O}_K$ tel que $\alpha\mathfrak{I}$ est un idéal de $\mathcal{O}_K$.

b) En déduire qu'il existe $\gamma\in\alpha\mathfrak{I}$, $\gamma\neq 0$, tel que

$$|\mathrm{N}_{K/\mathbb{Q}}(\gamma)| \;\leq\; cN(\alpha\mathfrak{I})\,.$$

c) Si on pose

$$\mathfrak{J} \;:=\; \gamma\alpha^{-1}\mathfrak{I}^{-1},$$

montrer que

$$N(\mathfrak{J}) \;\leq\; c\,.$$

5) On rappelle qu'un idéal fractionnaire $\mathfrak{I}\in\mathcal{I}(\mathcal{O}_K)$ de $\mathcal{O}_K$ est *principal* s'il existe $a\in K^*$ tel que

$$\mathfrak{I} \;= a\mathcal{O}_K\,.$$

On a ainsi un morphisme naturel injectif de groupes abéliens $K^*\;\hookrightarrow\;\mathcal{I}(\mathcal{O}_K)$. Le quotient

$$\mathrm{Pic}(\mathcal{O}_K) \;:=\; \mathcal{O}_K/K^*$$

est appelé *groupe de Picard* ou *groupe des classes d'idéaux* de K.

a) Soit $c>0$ la constante définie en 3.d. Montrer qu'on peut définir une application injective

$$\mathrm{Pic}(\mathcal{O}_K) \;\hookrightarrow\; \mathcal{I}(\mathcal{O}_K)^c$$

où $\mathcal{I}(\mathcal{O}_K)^c$ est l'ensemble des idéaux $\mathfrak{I}\subset\mathcal{O}_K$ de $\mathcal{O}_K$ tels que $N(\mathfrak{I})\leq c$.

b) Montrer que $\mathcal{I}(\mathcal{O}_K)^c$ est un ensemble fini et en déduire finalement que $\mathrm{Pic}(\mathcal{O}_K)$ est un groupe fini.

Exercice B

Soit L/K une extension finie de corps de nombres. On veut montrer qu'il existe une infinité d'idéaux maximaux $\mathfrak{p}$ de $\mathcal{O}_K$ totalement décomposés dans L, c'est-à-dire tels que $\mathfrak{p}\mathcal{O}_L$ est un produit fini d'idéaux maximaux distincts de $\mathcal{O}_L$:

$$\mathfrak{p}\mathcal{O}_L \;=\; \prod_{i=1}^{g} \mathfrak{p}_i,$$

où $\mathcal{O}_L/\mathfrak{p}_i \;\cong\; \mathcal{O}_K/\mathfrak{p}$ pour tout i.

1) Montrer qu'il suffit de traiter le cas $K = \mathbb{Q}$, L un corps de nombres galoisien. On se place dorénavant dans ce cadre.

2) Pour tout polynôme $P \in \mathbb{Z}[X]$, montrer qu'il existe une infinité de nombres premiers $p \in \mathbb{Z}$ tels que P a une racine dans $\mathbb{F}_p$.

3) On écrit $L = \mathbb{Q}(\alpha)$, où α est entier de polynôme minimal P. Montrer que si p est tel que P ait une racine dans $\mathbb{F}_p$ et soit sans facteur carré modulo p, alors P est un produit de facteurs linéaires dans $\mathbb{F}_p[X]$.

4) Conclure.

Exercice C

Soient D un entier strictement négatif et sans facteur carré et $K \;:=\; \mathbb{Q}[X]/(X^2 - D) \;=\; \mathbb{Q}(\sqrt{D})$. On dit que K est un *corps quadratique imaginaire*.

1 .a) Montrer que tout idéal $\mathfrak{I}$ de $\mathcal{O}_K$ peut s'écrire

$$\mathfrak{I} \;=\; \delta\big(a\mathbb{Z} + \frac{b+\sqrt{D}}{2}\mathbb{Z}\big)$$

où

$$(a, b, \delta) \in \mathbb{Z}^3 \;,\; a > 0 \;,\; b^2 \;\equiv\; D\;[4a] \text{ et } |b| \leq a \;.$$

b) Réciproquement montrer qu'un $\mathbb{Z}$-module comme ci-dessus est un idéal de $\mathcal{O}_K$, et qu'on a :

$$N(\mathfrak{I}) \;=\; a\delta^2 \text{ et } \mathfrak{I} \;\cap\; \mathbb{Z} \;=\; \delta a\mathbb{Z} \;.$$

2) Avec les notations de la question précédente, on note

$$c \;:=\; \frac{b^2 - D}{4a} \;.$$

a) Montrer que $\big(c, \frac{-b+\sqrt{D}}{2}\big)$ est dans la même classe d'idéaux que $\mathfrak{I}$.

b) En déduire que toute classe d'idéaux contient un idéal $\mathfrak{J} \;=\; a\mathbb{Z} \;+\; \frac{b+\sqrt{D}}{2}\mathbb{Z}$ avec

$$|b| \leq a \leq c \;:=\; \frac{b^2 - D}{4a} \in \mathbb{Z},$$

et que l'on peut supposer $b \geq 0$ si l'une des inégalités est une égalité. Un idéal possédant une telle base est dit *réduit*.

c) Montrer que $N(\mathfrak{J}) = a \leq \sqrt{\frac{|D|}{3}}$.

3 .a) Montrer que

$$N(aX + \frac{b+\sqrt{D}}{2}Y) \ = \ a(aX^2 \ + \ bXY \ + \ cY^2) \, ,$$

pour $(X, Y) \in \mathbb{Q}^2$.
b) En déduire que $a^2 = \min N(x)$ quand x parcourt $\mathfrak{J} \setminus \{0\}$. **Indication** *Pour tout X, Y entiers non tout deux nuls, on a $X^2 - |XY| + Y^2 \geq 1$.*

c) Montrer qu'il y a un unique idéal réduit dans chaque classe d'idéaux. **Indication** *Montrer que $ac = \min N(x)$, quand x parcourt $\mathfrak{J} \setminus \mathbb{Z}$.*

d) En déduire que les classes d'idéaux de K sont en bijection avec les triplets (a, b, c) satisfaisant $b^2 - 4ac = D$, $|b| \leq a \leq c$ et $b \geq 0$ si $|b| = a$ ou $a = c$.

e) Calculer $h\big(\mathbb{Q}(\sqrt{-d})\big)$ pour $d = 3, 4, 7, 8, 11, 12, 15, 16, 19, 20, 43, 48, 163$.

f) Donner la structure du groupe de classes d'idéaux de $\mathcal{O}_K$ pour $K = \mathbb{Q}(\sqrt{-21})$ et $K = \mathbb{Q}(\sqrt{-23})$.