

## Exercices - Feuille 2

### Finitude des groupes de classes des corps quadratiques imaginaires

#### I. Espaces quadratiques provenant des corps quadratiques imaginaires

*Rappels* : Soit  $A$  un anneau commutatif ( $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$  etc.), un espace quadratique est un pair  $(M, q)$  où  $M$  est un  $A$ -module libre de rang fini et  $q : M \rightarrow A$  est une forme quadratique, i.e.

–  $q(am) = a^2q(m), \forall a \in A, \forall m \in M$

– la flèche symétrique  $B_q : (m, m') \mapsto q(m + m') - q(m) - q(m')$  est  $A$ -bilinéaire

Si on fixe une base  $m_1, \dots, m_n$  de  $M$ , on a  $B_q(\sum x_i m_i, \sum y_j m_j) = \sum c_{ij} x_i y_j$  où

$c_{ij} = c_{ji} = B_q(m_i, m_j)$  et  $2q(\sum_i x_i m_i) = \sum_{i,j} c_{ij} x_i x_j$ .  $disc(q) := -det(c_{ij})$ , ce nombre ne dépend pas du choix de la base à un carré d'un unité près, en particulier c'est bien défini si  $A = \mathbb{Z}$ .

$(M, q)$  et  $(M', q')$  sont isomorphes s'il existe un isomorphisme de  $A$ -modules  $f : M \simeq M'$  tel que  $q' \circ f = q$ .

On ne considère que les espaces quadratiques binaires (i.e. de rang 2).

1. Considérons les espaces quadratiques définis par  $q_1(X, Y) = X^2 + 15Y^2$  et par

$q_2(X, Y) = 3X^2 + 5Y^2$ , montrer qu'ils ont le même discriminant, mais ils ne sont pas isomorphes sur  $\mathbb{Z}$ .

2. Dans cette feuille on suppose toujours que  $d$  est un nombre entier positif sans facteur carré. Le corps quadratique  $K = \mathbb{Q}(\sqrt{-d})$  a discriminant  $\Delta_d = -d$  et  $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$  si  $-d \equiv 1 \pmod{4}$ ; respectivement  $\Delta_d = -4d$  et  $\mathcal{O}_K = \mathbb{Z}[\sqrt{-d}]$  si  $-d \equiv 2, 3 \pmod{4}$ .

(1) Montrer que la forme quadratique  $q = q_{\mathcal{O}_K} : \mathcal{O}_K \rightarrow \mathbb{Z}, x \mapsto N_{K/\mathbb{Q}}(x)$  est de discriminant  $\Delta_d$ , elle est définie positive i.e.  $q(x) > 0$  pour tout  $x \neq 0$ .

(2) Vérifier que  $B_q$  associé à  $q$  est donné par  $(x, y) \mapsto Tr_{K/\mathbb{Q}}(x \cdot \sigma y) = x \cdot \sigma y + y \cdot \sigma x$ , où  $\sigma$  est l'élément non-trivial du groupe de Galois  $Gal(K/\mathbb{Q})$ .

(3) En général, soit  $I \subset \mathcal{O}_K$  un idéal, montrer que  $x \mapsto N_{K/\mathbb{Q}}(x)/N(I)$  définit une forme quadratique  $q_I : I \rightarrow \mathbb{Z}$  où  $N(I) = [\mathcal{O} : I]$ , ainsi un espace quadratique  $(I, q_I)$ . Elle est aussi définie positive après (1).

(4) Montrer que  $(I, q_I)$  est de discriminant  $\Delta_d$ .

*Allusion* : pour chaque point suivant, trouver un énoncé général pour tout espace quadratique sur  $\mathbb{Z}$  duquel il résulte

–  $disc(N(I) \cdot q_I) = N(I)^2 \cdot disc(q_I)$

–  $disc(q_{\mathcal{O}_K|I}) = [\mathcal{O}_K : I]^2 \cdot disc(q_{\mathcal{O}_K})$

(5) En déduire que  $q_I$  est primitive (une  $\mathbb{Z}$ -forme quadratique binaire  $aX^2 + bXY + cY^2$  est dite primitive si  $a, b, c$  n'ont pas de facteur commun).

(6) Montrer que la classe d'isomorphisme de  $(I, q_I)$  ne dépend que de la classe de  $I$  dans le groupe de classes  $Cl(K)$ .

#### II. Retrouver le corps quadratique à partir d'une forme

Soit  $(M, q)$  un  $\mathbb{Z}$ -espace quadratique non-dégénéré de rang 2 (c'est le cas pour  $(I, q_I)$  car  $disc = \Delta_d \neq 0$ ). Pour  $f \in End_{\mathbb{Q}}(M \otimes_{\mathbb{Z}} \mathbb{Q})$ , la théorie d'algèbre linéaire implique l'existence d'un endomorphisme adjoint  $f^\dagger \in End_{\mathbb{Q}}(M \otimes_{\mathbb{Z}} \mathbb{Q})$  tel que  $B_q(f^\dagger m, m') = B_q(m, f m')$  pour tout  $m, m' \in M \otimes_{\mathbb{Z}} \mathbb{Q}$ .

On considère  $A(M, q) = \{f \in \text{End}_{\mathbb{Z}}(M) : f^\dagger = \text{tr}(f) \cdot \text{id}_M - f\} \subseteq \text{End}_{\mathbb{Z}}(M) \simeq \text{Mat}_{2 \times 2}(\mathbb{Z})$ .

1. Vérifier que  $A(M, q)$  est un sous-anneau (pas forcément commutatif) de  $\text{End}_{\mathbb{Z}}(M)$ . (allusion : le vérifier sur  $\overline{\mathbb{Q}}$ )

2. Vérifier que  $B_q(fm, fm') = \det(f) \cdot B_q(m, m')$  pour tout  $f \in A(M, q)$  et  $m, m' \in M$ , en déduire que  $q \circ f = \det(f) \cdot q$ . (allusion : Cayley-Hamilton)

3. À partir de maintenant, supposons que la forme  $q$  est définie positive. Montrer que  $A = A(M, q)$  n'a pas de diviseur de zéro. Alors  $A \otimes \mathbb{Q}$  est une  $\mathbb{Q}$ -algèbre de dimension finie sans diviseur de zéro,  $\mathbb{Q}$  est contenu dans le centre de  $A \otimes \mathbb{Q}$ .

4. Soit  $R$  une algèbre (pas forcément commutatif) de dimension finie sur un corps  $k$  avec  $k$  contenu dans son centre. Montrer que  $R$  est une algèbre à division s'il n'a pas de diviseur de zéro.

5. Montrer que  $F = A \otimes_{\mathbb{Z}} \mathbb{Q}$  est un corps commutatif et  $[F : \mathbb{Q}] \leq 2$ . (Lemme. Soit  $A$  une algèbre simple central sur un corps  $K$  de dimension finie, alors  $\dim_K A$  est toujours un carré. En fait,  $A \otimes \overline{K}$  est isomorphe à une algèbre des matrices.)

6. De la même façon, on sait que  $F \otimes_{\mathbb{Q}} \mathbb{R} = A \otimes_{\mathbb{Z}} \mathbb{R}$  est un corps. Supposons que  $q$  est définie positive (par exemple si  $q = q_I$  pour un certain idéal  $I \subseteq \mathcal{O}_K$  avec  $K$  un corps quadratique imaginaire). Montrer que  $A \neq \mathbb{Z}$ , alors  $F \neq \mathbb{Q}$  et  $A$  est un ordre du corps quadratique  $F$  (un sous-anneau  $A$  d'un corps de nombres  $F$  est un  $\mathbb{Z}$ -module libre de type fini, il est un ordre s'il a une base  $\mathcal{B}$  telle que  $\mathcal{B} \otimes_{\mathbb{Z}} \mathbb{Q}$  est une  $\mathbb{Q}$ -base de  $F$ ). Déduire que  $F$  est imaginaire. De plus, comme l'anneau des entiers  $\mathcal{O}_F$  est l'ordre maximal de  $F$ , alors  $A \subset \mathcal{O}_F$ .

7. On part d'un corps  $K$  quadratique imaginaire de discriminant  $\Delta_d < 0$ . On pose  $(M, q) = (I, q_I)$  pour un idéal non nul,  $B_q(x, y) = \text{Tr}_{K/\mathbb{Q}}(x \cdot \sigma y) / N(I) = \frac{x \cdot \sigma y + y \cdot \sigma x}{N(I)}$ . Vérifier que  $\forall a \in \mathcal{O}_K, \forall x, y \in I$  on a  $B_q(\sigma a \cdot x, y) = B_q(x, a \cdot y)$ . Montrer que ceci définit un homomorphisme  $\mathcal{O}_K \rightarrow A(M, q)$ , montrer qu'il est injectif. Conclure que  $F = K$  et  $\mathcal{O}_K \simeq A(M, q)$ .

*Remarque.* Dans 7, il y a deux façon de définir  $\mathcal{O}_K \rightarrow A(M, q)$ , disons  $a \mapsto (a \cdot : I \rightarrow I)$  et  $a \mapsto (\sigma a \cdot : I \rightarrow I)$ , a priori, on n'a pas de préférence entre les deux, par contre on va fixer une "orientation" dans III.

### III. Finitude

Notations :  $d, K$  etc. comme ci-dessus,  $\Delta = \Delta_d$

$(M, q, \iota)$  est dit un espace quadratique  $K$ -orienté (défini positif de rang 2 de discriminant  $\Delta$ ) si  $A(M, q)$  est isomorphe à  $\mathcal{O}_K$  et on fixe un tel isomorphisme  $\iota : \mathcal{O}_K \simeq A(M, q)$ .  $(M, q, \iota)$  et  $(M', q', \iota')$  sont isomorphes s'il existe un isomorphisme  $f : (M, q) \rightarrow (M', q')$  tel que l'isomorphisme induit  $A(M, q) \simeq A(M', q')$  est compatible avec  $\iota : \mathcal{O}_K \simeq A(M, q)$  et  $\iota' : \mathcal{O}_K \simeq A(M', q')$ , autrement dit  $f : M \rightarrow M'$  est un morphisme de  $\mathcal{O}_K$ -modules.

$Q_{\Delta} = \{\text{espaces quadratiques sur } \mathbb{Z} \text{ définis positifs de rang 2 de discriminant } \Delta\} / \sim \text{isom.}$

$Q_K = \{\text{espaces quadratiques sur } \mathbb{Z} \text{ définis positifs de rang 2 de discriminant } \Delta \text{ et } K\text{-orientés}\} / \sim \text{isom.}$

$S_{\Delta} = \{\text{formes quadratiques binaires sur } \mathbb{Z} \text{ définies positives de discriminant } \Delta\} / SL_2(\mathbb{Z})$

$G_{\Delta} = \{\text{formes quadratiques binaires sur } \mathbb{Z} \text{ définies positives de discriminant } \Delta\} / GL_2(\mathbb{Z})$

1. Montrer qu'il existe les applications naturelles suivantes, en déduire la finitude de  $Q_K$  (on sait que  $S_{\Delta}$  est fini cf. le cours).

$$\begin{array}{ccc} S_{\Delta} & & Q_K \\ \downarrow & & \downarrow \\ G_{\Delta} & \xrightarrow{\simeq} & Q_{\Delta} \end{array}$$

2. D'après I.2(6) et II.7, l'application  $Cl(K) \rightarrow Q_K$  est bien définie, montrer que elle injective, alors  $Cl(K)$  est fini. (Cela résulte du théorème de structure des modules projectifs de type finis d'un anneau de Dedekind, cf. par exemple wikipédia...)

*Remarques* 1. En fait, il existe une application  $S_\Delta \rightarrow Q_K$  naturelle telle que le diagramme dans III.1 commute, en plus, cette application est une bijection. Voir des notes de Conrad pour une preuve complète. Il y a aussi une version pour les corps quadratiques réels. <http://math.stanford.edu/~conrad/676Page/handouts/picgroup.pdf> Malheureusement, cette preuve purement algébrique de la finitude de  $Cl(K)$  ne marche que pour les corps quadratiques, pour un corps de nombres général, on étudie la “géométrie des nombres”.

2. Gauss a défini une loi de composition dans  $S_\Delta$  tel qu’il devient un groupe abélien. De plus,  $Cl(K) \rightarrow S_\Delta$  est un isomorphisme de groupes. Ceci a généralisé récemment par Bhargava, cf. une série de ses articles dans *Ann. of Math.*.