Exercise sheet 7
Quadratic forms and discrete subgroups

Exercise 1. [Class groups and quadratic forms with positive discriminant]

Let K be a quadratic field with discriminant $D > 0$. The group $\mathrm{Cl}^+(\mathcal{O}_K)$ is the group of (fractional) ideals up to *strict equivalence*: two ideals I and J are said strictly equivalent if $I = zJ$ for some $z \in K^*$ such that $N_{K/\mathbb{Q}}(\alpha) > 0$.

Define $\alpha = \frac{\sqrt{D}}{2}$ if $D \equiv 0 \mod 4$ and $\alpha = \frac{1+\sqrt{D}}{2}$ if $D \equiv 1 \mod 4$.

For I a nonzero fractional ideal of K and (u, v) a $\mathbb{Z}$-basis of I (direct with respect to $(1, \alpha)$), define $q_{u,v}(x, y) = N_{K/\mathbb{Q}}(ux + vy)/N(I)$ for all $x, y \in \mathbb{Z}$.

(a) Prove that it is a binary quadratic form of discriminant D, whose proper equivalence class does not depend of the choice of (u, v).

(b) Prove that for any $z \in K^*$ such that $N_{K/\mathbb{Q}}(z) > 0$, with the previous notations, (zu, zv) is a direct $\mathbb{Z}$-basis of zI. Deduce that the morphism $\mathrm{Cl}^+(\mathcal{O}_K) \to \mathrm{Cl}(D)$ is well-defined.

(c) Build the inverse morphism $\mathrm{Cl}(D) \to \mathrm{Cl}^+(\mathcal{O}_K)$ as in the case $D < 0$.

Exercise 2. [Reduced quadratic forms for positive discriminants]

Fix $D > 0$ a nonsquare discriminant. A form (a, b, c) with discriminant D is *reduced* if

$$|\sqrt{D} - 2|a|| < b < \sqrt{D}$$

(a) Prove that if (a, b, c) is reduced, then $ac < 0$, $b > 0$ and $|a|$ and b are smaller than $\sqrt{D}$. Separating between the cases $a < 0$ and $a > 0$, prove also that $|c| < \sqrt{D}$.

(b) Prove that (a, b, c) is reduced if and only if (c, b, a) is.

For integers $c \neq 0, b \in \mathbb{Z}$, define $r = r(b, c)$ the unique integer such that $r \equiv -b \mod 2c$, and $-|c| < r \leq |c|$ (if $|c| > \sqrt{D}$) or $\sqrt{D} - 2|c| < r < \sqrt{D}$ (if $|c| < \sqrt{D}$).

The reduction operator ρ on forms (a, b, c) of discriminant D is then defined by

$$\rho(a, b, c) = (a', b', c') := \left(c, r(b, c), \frac{r(b, c)^2 - D}{4c}\right).$$

(c) Prove that (a', b', c') is still of discriminant D and that $|c'| \leq |c|/2$ if $|c| > \sqrt{D}$.

(d) Prove that after finitely many iterations starting from a form (a, b, c), one has $|c'| < \sqrt{D}$. Prove that after one more iteration, we have

$$\sqrt{D} - 2|a'| < b' < \sqrt{D}, \quad \max(|a'|, b, |c'|) < \sqrt{D}.$$

(e) Use if necessary one more iteration to prove that one finally gets a reduced form.

(f) Prove finally that ρ sends reduced forms to reduced forms.

Exercise 3. [Closed subgroups of $\mathbb{R}^n$]

The aim of this exercise is to describe all the closed topological subgroups G of $\mathbb{R}^n$.

(a) For $n = 1$, describe all the possible groups G.

(b) Assume now that $G \subset \mathbb{R}^n$ is not discrete, prove that 0 is an accumulation point of G.

(c) Deduce that there is a sequence $(g_k)_{k\in\mathbb{N}}$ of nonzero elements of G such that $g_k/\|g_k\|$ converges towards a point e of the unit sphere.

(d) Fix $t \neq 0$ a real number and $\varepsilon > 0$. Prove that there exists $k \in \mathbb{N}$ such that $\|g_k\| \leq \varepsilon/2$ and $\|g_k/\|g_k\| - e\| \leq \varepsilon/(2|t|)$. Prove that there is an integer $m \in \mathbb{N}$ such that $\|mg_k - te\| \leq \varepsilon$. Deduce that $\mathbb{R}e$ is included in G.

(e) Use this to prove by induction on the dimension n that for every closed topological subgroup G of $\mathbb{R}^n$, if W is the largest vector subspace contained in G and $\pi : \mathbb{R}^n \to \mathbb{R}^n/W$ the canonical projection, $G = \pi^{-1}(G')$ where G' is a discrete subgroup of $\mathbb{R}^n/W$.

(f) Use this criterion to prove that a subgroup G of $\mathbb{R}^n$ is dense if and only if there is no nonzero linear form ℓ on $\mathbb{R}^n$ such that $\ell(G) \subset \mathbb{Z}$.

(g) Use this lemma to prove that for any $(a_1, \cdots, a_n) \in \mathbb{R}^n$, its image in $\mathbb{R}^n/\mathbb{Z}^n$ generates a dense subgroup of $\mathbb{R}^n/\mathbb{Z}^n$ if $1, a_1, \cdots, a_n$ are $\mathbb{Q}$-linearly independent.