Exercise sheet 8
Geometry of numbers and the group of units

Exercise 1. [Minkowski bound]

(a) Let K be a number field of degree d, discriminant D_K and with r_1 real and r_2 pairs of conjugate complex embedding. Recall the Minkowski bound G.

(b) Deduce that $|D_K| \geq 2$ unless $K = \mathbb{Q}$.

(c) Give the Minkowski bound when $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field. Deduce that $\mathcal{O}_K$ is principal for $d = -11, -7, 5, 13$.

Exercise 2. [Quadratic fields with class number 1]

Let $d < 0$ a squarefree integer and $K = \mathbb{Q}(\sqrt{d})$.

(a) If $d \equiv 2, 3 \mod 4$, prove that for every prime number $p < |d|$, there is no $\alpha \in \mathcal{O}_K$ of norm p. Deduce that $\mathcal{O}_K$ is principal if and only if $\left(\frac{d}{p}\right) = -1$ for every such prime p (with the Minkowski bound for the converse).

(b) Prove a similar statement for $p < |d|/4$ in the case $d \equiv 1 \mod 4$.

Exercise 3. [Rabinowitz's theorem]

We fix $q \geq 2$ such that q and $4q - 1$ are squarefree, and $K = \mathbb{Q}(\sqrt{1-4q})$, $\theta = (1 + \sqrt{1-4q})/2$. Define also $P(X) = X^2 + X + q$.

(a) For every $x, y \in \mathbb{Q}$, compute $N_{K/\mathbb{Q}}(x + \theta y)$ and deduce that if for $z \in \mathcal{O}_K$, $p = N_{K/\mathbb{Q}}(z)$ is prime, then $p \geq q$.

(c) For $a \in \{0, \cdots, q-2\}$ such that $P(a)$ is not prime, prove there exists a prime number $p \leq q - 1$ such that $P(a) = 0 \mod p$.

(d) Assume $\mathcal{O}_K$ is principal. For $a \in \{0, \cdots, q-2\}$, use that $P(a) = N_{K/\mathbb{Q}}(a+\theta)$ to prove that $P(a)$ must be prime.

(e) Conversely, assume that $P(a)$ is prime for every $a \in \{0, \cdots, q-2\}$. Prove that every prime $p < q$ is inert in $\mathcal{O}_K$, in particular principal. Deduce with Minkowski's bound that $\mathcal{O}_K$ is principal. Can we improve the hypothesis on the a's ?

Exercise 4. [Diverse results]

(a) Let K be a number field. For any integer $m \geq 1$, recall why $\mathcal{O}_K/m\mathcal{O}_K$ is finite and deduce there are finitely many ideals of $\mathcal{O}_K$ of norm at most m.

(b) Let $M \in M_n(\mathbb{R})$ with strictly positive diagonal coefficients and strictly negative coefficients elsewhere, whose lines all have sum zero. For $X \in \operatorname{Ker} M$, by considering its coordinate of maximal modulus, prove that $X \in \operatorname{Vect} {}^t(1, \cdots, 1)$. Deduce that M has rank exactly $n-1$ and that all the determinants of its minors of size $n-1$ are equal up to sign.

(c) Let K be a number field, r_1 its number of real embeddings and r_2 its number of pairs of complex conjugate embeddings. Consider a basis $(u_1, \cdots, u_{r_1+r_2-1}) \in \mathcal{O}_K^*$ whose images by Log generate a basis of the lattice $\operatorname{Log} \mathcal{O}_K^*$ of the hyperplane H of zero sum of coordinates in $\mathbb{R}^n$.

By adding a vector orthonormal to H in $\mathbb{R}^n$ to $\operatorname{Log} \mathcal{O}_K^*$, prove that

$$\operatorname{vol}(\operatorname{Log} \mathcal{O}_K^*) = \sqrt{r_1 + r_2} \cdot R_K.$$

Exercise 5. [Fundamental units]

(a) Let $d > 0$ such that $d \equiv 2, 3 \mod 4$ and $K = \mathbb{Q}(\sqrt{d})$.

Consider $x = a + b\sqrt{d} \in \mathcal{O}_K$. Prove that $x \in \mathcal{O}_K^*$ if and only if $a^2 - db^2 = \pm 1$, which we assume now.

(b) Assume that $x \neq \{\pm 1\}$. Prove that amongst $x, x^{-1}, -x, -x^{-1}$, one of these satisfies $a > 0, b > 0$. We rename it x, and define a_n, b_n by

$$a_n + b_n\sqrt{d} = (a + b\sqrt{d})^n.$$

(c) By studying the growth of these sequences, prove that x is the fundamental unit if and only if $b > 0$ is the smallest integer such that $db^2 + 1$ or $db^2 - 1$ is a square a^2.

(d) Compute the fundamental units for $d = 2, 3, 6, 7, 10, 11$.

(e) For $d > 0$ such that $d \equiv 1 \mod 4$, adapt the arguments and the method.