Algebraic Number Theory 88-798
Question Sheet 2
Due Dec. 2, 2008

Please feel free to e-mail me at `mschein@math.biu.ac.il` with any questions of translation or otherwise. Throughout these exercises, K is a number field and $[K:\mathbb{Q}] = n$.

(1) Let $\alpha \in \mathcal{O}_K$. We denote by (α) the principal ideal (אידאל ראשי) generated by it. Prove that $N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$.

Hint: Here is one way to do it. Let $\omega_1, \ldots, \omega_n$ be a basis for $\mathcal{O}_K$ as $\mathbb{Z}$-module. Then $\alpha\omega_1, \ldots, \alpha\omega_n$ is a basis for (α) as $\mathbb{Z}$-module. Write $\alpha\omega_j = \sum_{i=1}^n a_{ij}\omega_i$, for $a_{ij} \in \mathbb{Z}$, and let A be the matrix $A = (a_{ij})$. Now show that $N((\alpha)) = |\det A|$ (recall that the volume of the parallelipiped spanned by the columns of a matrix A is $|\det A|$).

Prove that $\det A = N_{K/\mathbb{Q}}(\alpha)$. It may be helpful to consider K as a $\mathbb{Q}$-vector space, and consider the linear transformation $M_\alpha : K \to K$ defined by $M_\alpha(v) = v\alpha$.

The following two exercises are preparation for the proof of Minkowski's bound.

(2) Let $r, s \geq 0$ be integers such that $r + 2s = n$. Let $t \in \mathbb{R}$, and let $X_t \subset \mathbb{R}^n$ be the set

$$X_t = \left\{ (x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s) : |x_1| + \cdots + |x_r| + 2\sqrt{y_1^2 + z_1^2} + \cdots + 2\sqrt{y_s^2 + z_s^2} < t \right\}.$$

Prove that X_t is bounded, convex (קמור), and symmetric (if $(x_1, \ldots, x_r, \ldots, z_s) \in X_t$, then $(\pm x_1, \ldots, \pm z_s) \in X_t$). Recall that the volume of X_t is $\mathrm{vol}(X_t) = \int_{X_t} 1 \cdot dx_1 \cdots dz_s$. Prove that

$$\mathrm{vol}(X_t) = \frac{2^{r-s}\pi^s t^n}{n!}.$$

Hint: Change to polar coordinates and use induction on r.

(3) Let $C \subset \mathbb{R}^n$ be bounded, convex, and symmetric. Let $v_1, \ldots, v_n \in \mathbb{R}^n$ be linearly independent vectors, and let A be the $n \times n$ matrix whose columns are the vectors v_i. Suppose that $\mathrm{vol}(C) > 2^n |\det A|$. Prove that there exist $x_1, \ldots, x_n \in \mathbb{Z}$, not all zero, such that $x_1 a_1 + \cdots x_n a_n \in C$.

Hint: Consider the set $D = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_1 a_1 + \cdots x_n a_n \in C\} \in \mathbb{R}^n$. We need to show that D contains a lattice point.

For the remaining exercises you may assume Minkowski's bound. We will prove it in class next week.

(4) Let $\mathfrak{a} \subset \mathcal{O}_K$ be an ideal, and let $\mathcal{C} \in Cl_K$ be a class in the class group (חבורת המחלקות) of K. Prove that there exists an ideal $\mathfrak{b} \subset \mathcal{O}_K$ such that $\mathfrak{b} \in \mathcal{C}$ and $\mathfrak{b}$ is coprime (זר) to $\mathfrak{a}$.

(5) Find the class number of $\mathbb{Q}(\sqrt{17})$.

(6) Find the class number of $\mathbb{Q}(\sqrt{14})$.

(7) Let p be a prime number such that $p \equiv 11 (\mathrm{mod}\ 12)$. Prove that if $p > 3^m$, then the class group of $K = \mathbb{Q}(\sqrt{-p})$ contains an element of order at least m.

Hint: Let $\mathfrak{p}$ be a prime ideal that divides $3\mathcal{O}_K$. Prove that the corresponding element of Cl_K has order at least m.

(8) Prove that if K is a number field and $K \neq \mathbb{Q}$, then $|d_K| > 1$.