ALGEBRAIC NUMBER THEORY W4043

1. Homework, week 4, due October 4

I. The first part of this assignment establishes some of the basic properties of quadratic forms attached to ideals in imaginary quadratic fields. A *quadratic space* of rank n over $\mathbb{Z}$ is a pair (M, q), where M is a free rank n $\mathbb{Z}$-module (free abelian group on n generators) and $q : M \to \mathbb{Z}$ is a quadratic form, i.e. a function satisfying

(1) $q(am) = a^2 q(m)$, $a \in \mathbb{Z}, m \in M$;
(2) The function $B_q : M \times M \to \mathbb{Z}$, defined by $B_q(m, m') = q(m+m') - q(m) - q(m')$ is a bilinear form, i.e.
(3) $B_q(m, m') = B_q(m', m)$;
(4) $B_q(am + bm', m") = aB_q(m, m") + bB_q(m', m")$.

We only consider the case $n = 2$ and identify M with $\mathbb{Z}^2$. If $\{e_1, e_2\}$ is the standard $\mathbb{Z}$-basis of $\mathbb{Z}^2$, B_q is determined by the 2×2 symmetric matrix (b_{ij}) where $B_q(e_i, e_j) = b_{ij}$ (and you can check that this in turn determines $q(m) = \frac{B_q(m,m)}{2}$). We identify q with a polynomial in two variables (X, Y) by setting

$$q(X, Y) = q(Xe_1 + Ye_2).$$

A (binary) quadratic form $q(X, Y) = aX^2 + bXY + cY^2$

Say (M, q) and (M', q') are isomorphic if there is an isomorphism $f : M \to M'$ of abelian groups such that $q' \circ f = q$. Define the *discriminant* of the quadratic form q by $\Delta(q) = -\det(b_{ij})$ and check for yourselves (without writing it down) that two isomorphic quadratic spaces have the same discriminant.

1. Consider $q_1(X, Y) = X^2 + 15Y^2$, $q_2(X, Y) = 3X^2 + 5Y^2$. Show that q_1 and q_2 have the same discriminant but don't define isomorphic quadratic spaces. 2. Let d be a positive squarefree integer. Let $K = \mathbb{Q}(\sqrt{-d})$, with integer ring $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$ if $d \equiv 3 \pmod 4$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{-d}]$ if $d \equiv 1, 2 \pmod 4$. We write $\Delta_d = -d$ if $d \equiv 3 \pmod 4$ and $\Delta_d = -4d$ if $d \equiv 1, 2 \pmod 4$ (this is the *discriminant* of the field K).

(a) Show that the quadratic form $q = q_{\mathcal{O}_K}$ on the rank 2 $\mathbb{Z}$-module $\mathcal{O}_K$, defined by $q(x) = N_{K/\mathbb{Q}}(x)$, has discriminant Δ_d. Moreover, q is *positive definite*: $q(x) > 0$ for all $x \neq 0$.

(b) Show that the bilinear form B_q associated to q is given by

$$B_q(x, y) = Tr_{K/\mathbb{Q}}(x\sigma(y)) = x\sigma(y) + \sigma(x)y$$

where $\sigma \in Gal(K/\mathbb{Q})$ is the non-trivial element.

(c) In general, let $I \subset \mathcal{O}_K$ be an ideal, $N(I) = [\mathcal{O}_K : I] = |\mathcal{O}_K/I|$. Define $q_I : I \to \mathbb{Q}$ by $q_I(x) = N_{K/\mathbb{Q}}(x)/N(I)$. Show that q_I takes values in $\mathbb{Z}$ and the pair (I, q_I) is a quadratic space over $\mathbb{Z}$.

(d) Show that (I, q_I) is of discriminant Δ_d.

There will be additional exercises on quadratic forms in subsequent homework.

II. 1. Do exercise 6.15, p. 120 from Hindry's book.

2. Let $v_1, \ldots, v_n \in \mathbb{R}^n$ be n linearly independent vectors. Let

$$G = \{\sum_{i=1}^{n} a_i v_i, a_i \in \mathbb{Z}\}$$

be the subgroup of $\mathbb{R}^n$ generated by the set of v_i. Define the *fundamental domain* $D \subset \mathbb{R}^n$ to be the set

$$D = \sum_{i=1}^{n} d_i v_i, 0 \leq d_i < 1\}.$$

(a) Show that every element $v \in \mathbb{R}^n$ can be written uniquely as a sum $d + g$ where $d \in D$ and $g \in G$.

(b) For any $r > 0$, let $B(r)$ be the ball of radius r around 0:

$$B(r) = \{v \in \mathbb{R}^n \mid ||v|| \leq r\}.$$

For any $h \in G$, let $D_h = h + D = \{h + d \mid d \in D\}$ (in other words, h is fixed but d varies in D). Show that the set of $h \in G$ such that $B(r) \cap D_h \neq \emptyset$ is finite.