Math 676, Homework 4

(Do 5 problems of 10)

1. [Norm of Lattices Proof] Prove that the region

$$\tilde{T}_t = \{(x_1, ..., x_n) \ : \ |x_1| + \cdots + |x_r| + 2(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \cdots + \sqrt{x_{r+2s-1}^2 + x_{r+2s}^2}) \leq t\}$$

defines a compact convex body in $\mathbb{R}^n$, with positive volume.

(*Hint:* For convexity, reduce the problem to proving that the midpoint of any segment connecting two points in the body is in the body. Then that the midpoint of two points in the body, using $\sqrt{a^2+b^2+c^2+d^2} \leq \sqrt{a^2+b^2} + \sqrt{c^2+d^2}$.)

2. [Norm Map on Ideal Classes] Let K and L be number fields, and let C_K, C_L be the ideal class groups of their rings of integers. Assume as known that C_K, C_L are finite abelian groups.

(a) Show that the norm map $N_{L/K} : C_L \to C_K$ which sends an ideal A of O_L to $N_{L/K}(A)$ is well-defined and gives a homomorphism.

(b) Let P be a prime ideal of O_K and Q a prime ideal of O_L lying over P. Let a_P be the order of P in the ideal class group C_K, and a_Q the order of Q in C_L. Show the divisibility relation

$$a_P \mid a_Q f(Q/P),$$

where $f(Q/P)$ is the inertial degree of Q over P, i.e. $f(Q/P) = [O_L/Q : O_K/P]$.

3. [Non-trivial Ideal Classes in Cyclotomic Field $\mathbb{Q}(\zeta_{23})$]
Let $L = \mathbb{Q}(\zeta_{23})$, with $(\zeta_{23})^{23} = 1$, and let $K = \mathbb{Q}(\sqrt{-23})$.

(a) Show that $K \subset L$. [Hint: Recall that the discriminant $\Delta_{\mathbb{Q}(\zeta_p)} = (-1)^{\frac{p-1}{2}} p^{p-2}$ from problem 6 of Problem Set 3, and recall that the discriminant of a power basis is a square of something.]

(b) Let P be one of the primes of K lying over (2), for definiteness take $P = (2, \theta)$ with $\theta = \frac{1+\sqrt{-23}}{2}$. Let Q be a prime of L lying over P. Show that

$$f(Q/P) = 11.$$

Conclude that $Q = (2, \theta)O_L$. [Hint: Use known results on splitting of primes in cyclotomic fields.]

(c) Show that $P^3 = (\theta - 2)$, but that P is not principal in O_K. Thus O_K has class number at least three. Hint: To show non-principal, note the index $N_{K/\mathbb{Q}}(P) = [O_K : P]$, so if P were principal this would be norm of some element $N_{K/\mathbb{Q}}(\frac{a+b\sqrt{-23}}{2})$].

(d) Show that O_K has class number equal to 3. [Hint: Maybe the Minkowski bound is useful here.]

(e) Show that Q is not principal in O_L. [Hint: Use result on norm map on ideal classes, Problem 8 on Problem Set 3.]

(f) Show that if $2 = \alpha\beta$ in $\mathbb{Z}[\zeta_{23}]$, then one of α and β must be a unit in $\mathbb{Z}[\zeta_{23}]$.

4. [Extended Minkowski Convex Body Theorem]

(a) Prove that for each integer $k \geq 1$ that if a centrally symmetric convex body T (with nonempty interior) has volume $vol(T) > k2^n$ then T contains at least $2k$ nonzero integer lattice points $\{v_i : 1 \leq i \leq k\}$. [Note: These points need not be linearly independent over $\mathbb{R}$.

(b) If T is compact, show that $vol(T) \geq k2^n$ suffices for the conclusion.

(c) Find examples showing that the result is best possible.

5. [Dual Lattice] Given a lattice L in $V = \mathbb{R}^n$, the *dual lattice* or *reciprocal lattice* is

$$L^* := \{y \in \mathbb{R}^n :< x, y >\in \mathbb{Z}, \text{for all } x \in L\}$$

Here $< x, y >= x_1y_1 + \cdots + x_ny_n$ is the standard (real) scalar product.

(i) Show that is B is a basis of L then $(B^T)^{-1}$ is a basis of L^*. Deduce that $\det(L)\det(L^*) = 1$.

(ii) Show that the (Euclidean norm) successive minima of L and L^* satisfy

$$\lambda_i\lambda^*_{n-i+1} \geq 1.$$

[HInt: Let $[v_1, ..., v_n]$ be vectors in L giving successive minima, and $[w_1, ..., w_n]$ vectors in

L^* giving successive minima. Show that among $[v_1, ..., v_i], [w_1, w_2, ..., w_{n-i+1}]$ there must be some $< v_i, w_j > \neq 0$.]

(iii) [Hard] Show there is a constant C_n depending only on $n = \dim(V)$ such that

$$\lambda_i \lambda^*_{n-i+1} \leq C_n.$$

[Hint: Use Minkowski's second fundamental theorem (as a black box) to bound above $\lambda_1 \cdots \lambda_n)(\lambda^*_1 \cdots \lambda^*_n)$ by a constant depending on n. What constant do you get?]

6. [Some Real Quadratic Field Class Numbers.]

Show that $K = \mathbb{Q}(\sqrt{m})$ has ring of integers of class number one (PID) for the three choices $m = 6, m = 173, m = 293$.

[Hint: For $m = 6$ observe $2O_K = (2, \sqrt{6})^2$. Show the latter is a principal ideal by finding an element of norm 2.]

7. [Class Number of Real Cyclotomic Field for $n = 11$.]

Let $\theta_{11} := \zeta_{11} + \zeta_{11}^{-1}$ so that $K = \mathbb{Q}(\theta_{11})$ is the real subfield of the cyclotomic field $L = \mathbb{Q}(\zeta_{11})$. Prove that K has class number one. [Hint: Make use of known splitting formulas for prime ideals in L to get information on how small prime ideals in K split.]

8. [Unit Bound in Non-Totally Real Cubic Field]

Let K be a real cubic field whose two conjugate fields are complex. Let $u > 1$ be the fundamental unit in K (unit rank $r + s - 1 = 1$), all units of form $\pm u^k$. The object is to find a lower bound for u.

(a) Let $u, re^{i\theta}, re^{-i\theta}$ be the conjugates of u. Show that $u = r^{-1}$ and that

$$disc(\mathbb{Z}[1, u, u^2]) = -4(\sin\theta)^2(r^3 + r^{-3} - 2\cos\theta)^2.$$

[Hint: Use a formula for discriminant of power basis in terms of product of differences of conjugates.]

(b) Show that

$$|disc((\mathbb{Z}[1, u, u^2])| \leq 4(u^2 + u^{-3} + 6).$$

[HInt: Set $x = r^3 + r^{-3}$, $c = \cos\theta$ and for fixed $-1 \leq c \leq 1$ find the minimum value of $f(x) = (1 - c^2)(x - 2c)^2 - x^2$.]

(c) Conclude the lower bound

$$u^3 > \frac{\Delta_K}{4} - 6 - u^{-3} > \frac{1}{4}\Delta_k - 7.$$

9. [Fundamental Unit of Field of Cube Root of 2] Determine the fundamental unit of $K = \mathbb{Q}(\alpha)$ with $\alpha = 2^{1/3}$, as follows.

(a) Given that $O_K = \mathbb{Q}[\alpha]$, show that $\Delta_K = -108$. (Can you prove O_K is the full ring of integers?)

(b) Show that $u^3 > 20$. [Hint: Use the result of Problem 8.]

(c) Then show that

$$\beta = (\alpha - 1)^{-1}$$

is a unit between 1 and u^2, and conclude $\beta = u$.

10.[Quintic Trinomial Ring of Integers] Let $f(x) = x^5 + ax + b$, with $a, b \in \mathbb{Z}$, and suppose it is irreducible over $\mathbb{Q}$. (Thus $b \neq 0$.)

(a) Show that the discriminant

$$d(\mathbb{Z}[\alpha]) = Disc(f(x)) = 4^4a^5 + 5^5b^4.$$

[Hint: Try the case of a cubic: $g(x) = x^3 + ax + b$, where $d(ZZ[\alpha]) = 2^2a^3 - 3^2b^2$ $g'(\alpha) = -\frac{2a\alpha+3b}{\alpha}$. Now note $2\alpha a + 3b$ is a root of $(\frac{x-3b}{2a})^3 + a(\frac{x-3b}{2a}) + b = 0$, and use this to find $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(2a\alpha + 3b)$.]

(b) Let a be squarefree and not ± 1, and consider $a = b$, so that $x^5 + ax + a$ is an Eisenstein polynomial, hence irreducible. Let α be a root and let the integral basis of $K = \mathbb{Q}(\alpha)$ be written

$$O_K = \mathbb{Z}[1, \frac{f_1(\alpha)}{d_1}, \frac{f_2(\alpha)}{d_2}, \frac{f_3(\alpha)}{d_3}, \frac{f_4(\alpha)}{d_4}] \quad \text{with} \quad d_i | d_{i+1}.$$

Show that if $4^4a + 5^5b$ is squarefree, then one has

$$d_1 = d_2 = 1, \quad \text{and} \quad d_3d_4 | a^2.$$

[Hints: For the d_i, use results in Problem Set 3, Problem 5. The conditions in (b) are known to hold for $a = -2, -3, -6. - 7. - 10, -11, -13, -15.$]

(c) Let α be as in part (b). Prove that $\alpha + 1$ is a unit in O_K. [Hint: Write $\alpha^5 = -a(\alpha + 1)$ and take norms.]