Math 422/501: Problem set 11 (due 25/11/09)

The discriminant

Let L/K be a separable extension, and let N/K be its normal closure. Let $n = [L:K] = \#\mathrm{Hom}_K(L,N)$, with an enumeration $\mathrm{Hom}_K(L,N) = \{\mu_i\}_{i=1}^n$. Given $\left\{\omega_j\right\}_{j=1}^n \subset L$ let $\Omega \in M_n(L)$ be the matrix with $\Omega_{i,j} = \mu_i(\omega_j)$ and set:

$$d_{L/K}(\omega_1, \ldots, \omega_n) = (\det \Omega)^2 .$$

In particular, write $d_{L/K}(\alpha) = d_{L/K}\left(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\right)$.

1. Let $\left\{\omega_j\right\}_{j=1}^n \subset L$.
   (a) Show that $d_{L/K}(\omega_1, \ldots, \omega_n) \in K$.
   (b) Show that $d_{L/K}(\omega_1, \ldots, \omega_n) \neq 0$ iff $\left\{\omega_j\right\}_{j=1}^n$ is a basis for L over K.
   (c) Show that $d_{L/K}(\alpha) \neq 0$ iff $L = K(\alpha)$.
   (d) Show that if $d_{L/K}(\alpha) \neq 0$ then it is the discriminant of the minimal polynomial of α.

2. (The case $K = \mathbb{Q}$) Let L be a number field of degree n over $\mathbb{Q}$. Let $\{\omega_i\}_{i=1}^n, \left\{\omega_j'\right\}_{j=1}^n \subset L$ be Q-bases of L so that the abelian groups $M = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n$ and $N = \mathbb{Z}\omega_1' \oplus \cdots \oplus \mathbb{Z}\omega_n'$ satisfy $N \subset M$.
   (a) Show that the sum $\oplus_{i=1}^n (\mathbb{Z}\omega_i)$ is indeed direct.
   (b) Show that $d_{L/\mathbb{Q}}(\omega_1', \ldots, \omega_n') = D d_{L/\mathbb{Q}}(\omega_1, \ldots, \omega_n)$ for some positive integer D.
   Hint: Relate the matrices Ω and Ω'.
   (c) Show that when $M = N$ we have $d_{L/\mathbb{Q}}(\omega_1, \ldots, \omega_n) = d_{L/\mathbb{Q}}(\omega_1', \ldots, \omega_n')$, in other words that the discriminant of a basis is really a function of the Z-module generated by that basis.
   (d) Say $\omega_j' = a_j \omega_j$ for some $a_j \in \mathbb{Z}$. Show that $D = [M:N]^2$.
   REMARK (c),(d) are special cases of the general identity $d_{L/\mathbb{Q}}(N) = [M:N]^2 d_{L/\mathbb{Q}}(M)$.

Rings of integers

FACT. *(Integral basis Theorem) Let K be a number field of degree n (that is, $[K:\mathbb{Q}] = n$), and let $\mathscr{O}_K \subset K$ be the set of algebraic integers in K. Then there exists a basis $\{\alpha_i\}_{i=1}^n$ of K over $\mathbb{Q}$ so that $\mathscr{O}_K = \oplus_{i=1}^n \mathbb{Z}\alpha_i$. Moreover, $d_K \stackrel{def}{=} d_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$ is an integer.*

3. Let D be a square-free integer (this means a product of distinct primes up to sign) and let $K = \mathbb{Q}(\sqrt{D})$.
   (a) Let $\alpha \in K$. Show that α is an algebraic integer iff $\mathrm{Tr}\,\alpha, N\alpha \in \mathbb{Z}$ (trace and norm from K to $\mathbb{Q}$).
   (b) Show that $\frac{1+\sqrt{D}}{2}$ is an algebraic integer iff $D \equiv 1\,(4)$.
   (c) Show that $\mathbb{Z}[\sqrt{D}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{D} \subset \mathscr{O}_K \subset \mathbb{Z}\frac{1}{2} \oplus \mathbb{Z}\frac{\sqrt{D}}{2}$.
   Hint: write $\alpha \in K$ in the form $a + b\sqrt{D}$ for $a, b \in \mathbb{Q}$.
   (d) By considering the equation $x^2 - y^2 D \equiv 0\,(4)$ in $\mathbb{Z}/4\mathbb{Z}$, show that if $D \equiv 2,3\,(4)$ then $\mathscr{O}_K = \mathbb{Z}[\sqrt{D}] = \left\{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\right\}$.

(e) Show that when $D \equiv 1\,(4)$ $\mathscr{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] = \left\{\frac{a+b\sqrt{D}}{2} \mid a,b \in \mathbb{Z},\, a \equiv b\,(2)\right\}$.

— What about $D \equiv 0\,(4)$?

4. (Dedekind) Let $K = \mathbb{Q}(\theta)$ where θ is a root of $f(x) = x^3 - x^2 - 2x - 8$.
   (a) Show that f is irreducible over $\mathbb{Q}$ and find its Galois group.
   (b) Show that $1, \theta, \theta^2$ are all algebraic integers.
   (c) Let $\eta = \frac{\theta^2+\theta}{2}$. Show that $\eta^3 - 3\eta^2 - 10\eta - 8 = 0$ and conclude that is an algebraic integer a well.
   (d) Show that $1, \theta, \eta$ are linearly independent over $\mathbb{Q}$.
   (e) Let $M = \mathbb{Z} \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\eta$ and let $N = \mathbb{Z}[\theta] = \mathbb{Z} \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\theta^2$. Show that $N \subset M$.
   (f) Show that $d_{K/\mathbb{Q}}(\theta) = \Delta(f) = -4 \cdot 503$.
   (g) Find $d_{K/\mathbb{Q}}(1, \theta, \eta)$.
   Hint: You can be confident in your answer by consulting 2(a).
   (h) Show that $\{1, \theta, \eta\}$ is an integral basis.
   Hint: Let $\{\alpha, \beta, \gamma\}$ be an integral basis and consider $\frac{d_{K/\mathbb{Q}}(1,\theta,\eta)}{d_{K/\mathbb{Q}}(\alpha,\beta,\gamma)}$.
   (i) Let $\delta = A + B\theta + C\eta$ with $A, B, C \in \mathbb{Z}$. Show that $2 | d_{K/\mathbb{Q}}(\delta)$. Conclude that the set of algebraic integers of K is not of the form $\mathbb{Z}[\delta]$.