Math 676, Homework 3 (Revised 2)

(*Note:* Problems 1, 2, 3, 9, 10: Marcus, Chapter 3 pp. 92-94.)

1. [Fractional Ideals and Different] Let L/K be number fields with rings of integers O_K, O_L. L can be considered both as an O_K-module and as an O_L-module. Let A be an additive subgroup of L. Define

$$\begin{aligned} A^{-1} &:= \{\alpha \in L : \alpha A \subset O_L\} \\ A^* &:= \{\alpha \in L : Tr_{L/K}(\alpha A) \subset O_K\}. \end{aligned}$$

Define the *different* $\delta(A)$ (also denoted $\mathrm{diff}(A)$) in terms of these definitions by

$$\delta(A) := (A^*)^{-1},$$

it will be an O_L-module, see below, and its definition is made with respect to the O_K-module structure on O_L given by the trace map. The different is an invariant which is related to the discriminant, see Problem 9.

Llet A, B denote additive subgroups of L and I a fractional O_L ideal in L (called hereafter a fractional L-ideal.)

(a) Show that A^{-1} is an O_L-submodule of L, and A^* is an O_K-submodule of L (i.e. $O_L A^{-1} \subset A^{-1}$ and $O_K A^* \subset A^*$.) Then show that

$$A \subset B \Rightarrow B^{-1} \subset A^{-1} \text{ and } B^* \subset A^*.$$

(b) Show that A is a fractional ideal in L if and only if

$$O_L A \subset A \text{ and } \ A^{-1} \neq \{0\}.$$

(c) For a fractional ideal I of L and additive subgroups A, B of L show that

$$I = (I^{-1})^{-1}$$

$$I^* \quad \text{is an } O_L - \text{submodule of} \ \ L$$

$$I^* \ \text{ is a fractional ideal.}$$

$$II^* \subset (O_L)^*$$

$$I^*(I^*)^* = (O_L)^*$$

$$(I^*)^* = I.$$

(d) For the different show that:

$$\delta(A) \subset (A^{-1})^{-1}$$

$$\delta(I) \subset I$$

$$\delta(I) \text{ is a fractional ideal.}$$

$$A \subset I \Rightarrow \delta(A) \quad \text{is a fractional ideal.}$$

$$I^* \subset (\delta(I))^{-1}$$

$$\delta(I) = I\delta(O_L)$$

2. [Dual Basis for Trace] Let L/K be number fields with $[L : K] = n$. Let $\{\alpha_1, ..., \alpha_n\}$ be a basis for L over K as a vector space.

(a) Prove there exist $\beta_1, ..., \beta_n \in L$ such that $Tr_{L/K}(\alpha_i \beta_j) = 1$ if $i = j$, 0 otherwise. (Hint: recall that $d(\alpha_1, ...\alpha_n) = \det[Tr_{L/K}(\alpha_1 \alpha_j)] \neq 0$.) Show that $\{\beta_1, ..., \beta_n\}$is another basis of L over K. (It is called the *dual basis* for the trace bilinear form.)

(b) Let $A = O_K\alpha_1 \oplus \cdots \oplus O_K\alpha_n \subset L$ be the free O_K-module generated by the α_i. Show that

$$A^* = B$$

where $B = O_K\beta_1 \oplus \cdots \oplus O_K\beta_n \subset L$. (Hint: Given $\gamma \in A^*$, obtain $\beta \in B$ such that $Tr_{L/K}((\gamma - \beta)A) = 0$, and show this implies $\gamma = \beta$.)

3. [Power Basis and Different] Let L/K number fields, with $L = K(\alpha)$, noting that $L = K[\alpha]$ as well. Let $f(x)$ be the monic irreducible polynomial α satisfies over K, and write $f(x) = (x - \alpha)g(x)$. Then write

$$g(x) = \gamma_{n-1}x^{n-1} + \gamma_{n-1}x^{n-2} + \cdots + \gamma_0,$$

for some $\gamma_i \in L$. This problem is to show that the dual basis to the power basis

$$A = O_K[1, \alpha, \alpha^2, \cdots \alpha^{n-1}]$$

is

$$B = O_K[\frac{\gamma_0}{f'(\alpha)}, \cdots, \frac{\gamma_{n-1}}{f'(\alpha)}]$$

(a) Let $\sigma_1, \cdots, \sigma_n$ be embeddings of L in $\mathbb{C}$ fixing K pointwise. The the $\sigma_i(\alpha)$ are the roots of $f(x)$. Show that

$$f(x) = (x - \alpha_i)g_i(x)$$

with $g_i(x)$ being the polyomial obtained from $g(x)$ by applying σ_i to its coefficients., and $\alpha_i = \sigma_i(\alpha)$.

(b) Show that $g_i(\alpha_j) = f'(\alpha_j)$ if $i = j$ and 0 otherwise. [Hint: Show $f'(\alpha_) = \prod(\alpha - \beta)$ where β runs over all roots unequal to α.]

(c) Let M be the Vandermonde matrix $M = [(\alpha_j)^{i-1}]_{ij}$. Let N be the matrix $N = [\sigma_i(\frac{\gamma_{j-1}}{f'(\alpha)})]_{ij}$. Show that $NM = I$, and conclude $N = M^{-1}$.

(d) Show that if $\alpha \in O_L$ then the O_K-module

$$B = O_K[\gamma_0, \gamma_1, \cdots \gamma_{n-1}]$$

is the ring $B = O_K[\alpha]$. (Hint: multiply out $(x - \alpha)g(x)$.)

(e) Prove that if $\alpha \in O_L$ then

$$(O_K[\alpha])^* = (f'(\alpha))^{-1} O_K[\alpha].$$

(f) Prove that if $\alpha \in O_L$ then the different

$$\delta(O_K[\alpha]) = f'(\alpha) O_L.$$

(g) Prove that if $\alpha \in O_L$ then

$$f'(\alpha) \in \delta(O_L).$$

4. [Localization and PID's] Let R be a (commutative) integral domain with unit, that is Noetherian, and contains a finite number of nonzero prime ideals.

(a) Show that if R is a Dedekind domain and has only one prime ideal, then it is a PID, i.e. all prime ideals are principal.

(b) Extend your proof in (a) to show R is a PID if is a *semi-local* Dedekind domain, i.e. it has a finite number of maximal ideals.

(c) (*) Is the PID conclusion always true without the Dedekind domain assumption? What about being a UFD?

5. [General Basis of O_K.] Let $K = \mathbb{Q}(\alpha)$ where α is an algebraic integer. We showed that the ring of integers can be written

$$O_K = \mathbb{Z}[1, \frac{f_1(\alpha)}{d_1}, \frac{f_2(\alpha)}{d_2}, \cdots, \frac{f_{n-1}(\alpha)}{d_{n-1}}] \text{ with } d_i \mid d_{i+1},$$

and $f_i(x) \in \mathbb{Z}[x]$ is a monic polynomial of degree i.

(a) Show that

$$d(\mathbb{Z}[\alpha]) = (d_1 d_2 \cdots d_{n-1})^2 \Delta_K.$$

[Hint: First show that $d(1, \alpha, \alpha^2 \cdots, \alpha^{n-1}] = d[1, f_1(\alpha), ..., f_{n-1}(\alpha).]$

(b) Show that $[O_K : \mathbb{Z}[\alpha]\ ] = d_1 d_2 \cdots d_{n-1}$.

(c) Show that $d_i d_j | d_{i+j}$ if $i + j \le n - 1$.
[Hint: Consider $\frac{f_i(\alpha) f_j(\alpha)}{d_i d_j}$.]

(d) Show that for $1 \le i \le n-1$, $(d_1)^i | \ d_i$. Conclude that

$$(d_1)^{n(n-1)} \mid d(\mathbb{Z}[\alpha]).$$

6. [Cyclotomic Field Discriminant: Sharpening of Lemma 10.1.1]. Find the discriminant of the cyclotomic field $\mathbb{Q}(\zeta_m)$.

(a) Show that the discriminant of the cyclotomic field for $m = p^k$ a prime power is $\Delta_{p^k} := \pm p^{p^{n-1}((p-1)n-1}$.

(b) Determine for which p^n the minus sign occurs in (a).

(c) Using (a), (b), prove that the discriminant of $\mathbb{Q}(\zeta_m)$ for general n is

$$\Delta_m := (-1)^{\phi(m)/2} \frac{m^{\phi(m)}}{\prod_{p|m} p^{\phi(m)/(p-1)}}.$$

7. [Quadratic Fields in Cyclotomic Fields] This exercise relates quadratic fields and cyclotomic fields.

(a) Show that every cyclotomic field $L = \mathbb{Q}(\zeta_n)$ for $n \ge 3$ contains at least one quadratic subfield $K = \mathbb{Q}(\sqrt{D})$.

(b) For each odd prime p show that this quadratic field is unique, and that it is $K = \mathbb{Q}(\sqrt{\pm p})$ so that $\pm p \equiv 1 \pmod 4$.

[Hint: Consider the discriminant of $\mathbb{Q}(\zeta_p)$ computed in problem 6. Note that the discriminant of a power basis is a square of something.]

(c) Show that $\sqrt{2}$ is in $\mathbb{Q}(\zeta_8)$.

(d) Show that every quadratic field $K = \mathbb{Q}(\sqrt{D})$ is a subfield of some cyclotomic field. Identify the smallest m that you can, given a factorization of D. (It is $m = \Delta_K$).

8. [Ideal Class Groups] (a) Use Minkowski's bounds on the norm of elements in ideal classes to prove that $\mathbb{Q}(\sqrt{-3}$ and $\mathbb{Q}(\sqrt{5})$ have trivial ideal class group (class number 1).

(b) Show $\mathbb{Q}(\sqrt{21})$ has class number 1. Do the same for $\mathbb{Q}(\sqrt{17})$. [Hint: Analyze factorization/principality of prime ideals of small norm.]

9. [Different and Ramification] Let L/K be number fields and let consider the different $\delta(O_L)$ defined with respect to O_K; it is an integral O_L-ideal. Let P be a prime ideal in O_K, and Q a prime ideal in O_L lying over P. This exercise shows that if Q is ramified with index $e = e(Q/P) \geq 2$, then $Q^{e-1} \mid \delta(O_L)$. That is, the different detects exactly which of the primes lying over P ramify.

(a) Define an O_L-ideal I by $PO_L = Q^{e-1}I$, show that P contains the ideal $Tr_{L/K}(I) = \{Tr_{L/K}(\alpha) : \alpha \in I\}$. [HInt: See the proof that a ramified prime divides discriminant.]

(b) Let P^{-1} be the inverse of P as an O_K-fractional ideal. Show that $P^{-1}O_L = (pPO_L)^{-1}$ as O_L-fractional ideals.

(c) Show that $(PO_L)^{-1}I \subset (O_L)^*$.

(d) Show that $Q^{e-1} \mid \delta(O_L) := (O_L^*)^{-1}$.

(e) Show that for any $\alpha \in O_L$ that

$$Q^{e-1}|f'(\alpha)O_L,$$

where $f(x)$ is the monic irreducible polynomial for α over O_K.

10. [Absolute Different and Discriminant]

Consider a number field $L/\mathbb{Q}$ with discriminant Δ_L. The dual module to O_L is

$O_L^* = \{\alpha \in L : Tr_{L/\mathbb{Q}}(\alpha O_L) \subset \mathbb{Z}\}$. The *absolute different* over $\mathbb{Z}$ is

$$\delta(O_L) := (O_L^*)^{-1}.$$

It is an O_L-ideal.

(a) Let $[\alpha_1, ..., \alpha_n]$ be an integral basis of O_L and let $[\beta_1, ..., \beta_n]$ be the dual basis with respect to $Tr_{L/\mathbb{Q}}$. Then $[\beta_1, ..., \beta_n]$ is a basis for O_L^* over $\mathbb{Z}$. (See Problem 2.) Show that the discriminants

$$d(\alpha_1, ..., \alpha_n)d(\beta_1, ..., \beta_n) = 1.$$

(b) Show that $|((O_L)^* : O_L] = |\Delta_L|$, the absolute discriminant of O_L. (Hint: Write the α_i in terms of the β_i.)

(c) Prove that $[O_L : \delta(O_L)] = |\Delta_L|$. (See Problem 1.)