Assignment 2 – Parts 1, 2, & 3 – Math 661

(1) Some pure fields.

(a) Let p be an odd prime such that $p^2 \nmid 2^{p-1}-1$. Let $\alpha = 2^{1/p} \in \mathbf{R}$ and let $K = \mathbf{Q}(\alpha)$. Show that

$$\Delta(K) = (-1)^{(p-1)/2} p^p 2^{p-1}$$

and

$$\mathcal{O}_K = \mathbf{Z}[2^{1/p}].$$

(Hint: look at what we did in class for $p = 3$.)

(b) Let p be an odd prime, let $\alpha = p^{1/p} \in \mathbf{R}$, and let $K = \mathbf{Q}(\alpha)$. Show that $\Delta(K) = (-1)^{(p-1)/2} p^{2p-1}$ and $\mathcal{O}_K = \mathbf{Z}[p^{1/p}]$.

(2) As mentioned in class Theorem 4.26 of Narkiewicz says: Suppose K_1, K_2 are two number fields of degree n_1, n_2 with relatively prime discriminants. If $\alpha_1, \ldots, \alpha_{n_1}$ is an integral basis of K_1 and $\beta_1, \ldots, \beta_{n_2}$ is an integral basis of K_2, then $\{\alpha_i \beta_j\}$ is an integral basis of $K_1 K_2$ and

$$\Delta(K_1 K_2) = \Delta(K_1)^{n_2} \Delta(K_2)^{n_1}.$$

Use this to help you do the following.

(a) Let p, q be distinct odd primes that are not both congruent to 3 (mod 4). Find the discriminant and an integral basis of $K = \mathbf{Q}(\sqrt{p}, \sqrt{q})$.

(b) Find the discriminant and an integral basis of $K = \mathbf{Q}(\sqrt[3]{2}, \zeta_5)$ (where $\zeta_5 = e^{2\pi i/5}$).

(3) In class, we covered a very concrete definition of the discriminant of a number field. This exercise lays the foundation for a more conceptual definition. Let A be an integral domain with field of fractions F and let M be a free A-module of finite rank r (i.e. A has a basis of r elements). A *bilinear form* on M (or an *F-valued pairing on M*) is a map

$$\psi : M \times M \to F$$

that is A-linear in each variable, i.e. ψ is such that for all $m, m', n, n' \in M$ and $a \in A$

- $\psi(am + m', n) = a\psi(m, n) + \psi(m', n)$,
- $\psi(m, an + n') = a\psi(m, n) + \psi(m, n')$.

A bilinear form ψ is called *symmetric* if for all $m, n \in M$

$$\psi(m, n) = \psi(n, m).$$

Let $\mathcal{B} = \{e_1, \ldots, e_r\}$ be a basis of M (as an A-module). The *Gram matrix* of ψ with respect to $\mathcal{B}$, denoted $[\psi]_{\mathcal{B}}$, is the $r \times r$-matrix whose (i,j)-entry is $\psi(e_i, e_j)$.

(a) For $m \in M$, let $[m]_{\mathcal{B}}$ denote its *coefficient vector with respect to* $\mathcal{B}$, i.e. the column vector

$$[m]_{\mathcal{B}} = (a_1, \ldots, a_r)^T \in A^r \text{ such that } m = \sum_{i=1}^{r} a_i e_i.$$

Show that for all $m, n \in M$,

$$\psi(m,n) = ([m]_{\mathcal{B}}^T)[\psi]_{\mathcal{B}}[n]_{\mathcal{B}}.$$

(So that the Gram matrix of ψ represents ψ much in the same way one can represent a linear transformation by a matrix.)

(b) Conversely, given an $r \times r$-matrix G with entries in F, show that there is a bilinear form ψ such that G is the Gram matrix of ψ with respect to $\mathcal{B}$.

(c) Suppose $\mathcal{B}' = \{e_1', \ldots, e_r'\}$ is another basis and let $g \in \mathrm{GL}_r(A)$ be its change of basis matrix so that

$$(e_1', \ldots, e_r') = (e_1, \ldots, e_r)g.$$

Show that for all $m \in M$,

$$[m]_{\mathcal{B}} = g[m]_{\mathcal{B}'}$$

and hence that

$$[\psi]_{\mathcal{B}'} = g^T[\psi]_{\mathcal{B}}g.$$

(d) The *determinant* of ψ (or of M if ψ is understood) is defined to be the determinant of the Gram matrix of ψ with respect to some basis. Show that the determinant is well-defined up to multiplication by the square of a unit in A, i.e. $\det(M) \in F/(A^\times)^2$. (Hint: use the previous part.)

(e) Recall that if K/F is a finite, separable extension of degree r, then there are exactly r distinct F-embeddings $\sigma_i : K \to \overline{F}$. For $\alpha \in K$, recall that its *trace* is given by

$$\mathrm{tr}_{K/F}(\alpha) = \sum_{i=1}^{r} \sigma_i(\alpha).$$

Show that the map $T_{K/F} : K \times K \to F$ given by

$$T_{K/F}(\alpha, \beta) = \mathrm{tr}_{K/F}(\alpha\beta)$$

is a symmetric, bilinear form on K.

(4) Let $K/\mathbf{Q}$ be a number field of degree n and let $\sigma_1, \ldots, \sigma_n$ be the n embeddings of K into $\overline{\mathbf{Q}}$ (or $\mathbf{C}$ if you'd like). For $\alpha_1, \ldots, \alpha_n$, let $\mathcal{M}$ be the $n \times n$ matrix whose (i,j)-entry $\sigma_i(\alpha_j)$. We defined in class $\Delta(\alpha_1, \ldots, \alpha_n) := \det(\mathcal{M})^2$. We also used the notation $\Lambda(\alpha_1, \ldots, \alpha_n)$ for the $\mathbf{Z}$-submodule of K generated by $\alpha_1, \ldots, \alpha_n$.

(a) Suppose $\alpha_1, \ldots, \alpha_n$ is a basis of $\Lambda = \Lambda(\alpha_1, \ldots, \alpha_n)$. With the notation of Question (3) (with $A = \mathbf{Z}$ and $F = \mathbf{Q}$), let T_Λ denote the restriction of the trace form $T_{K/\mathbf{Q}}$ to $\Lambda \times \Lambda$. Show that $\mathcal{M}^T\mathcal{M}$ is the Gram matrix of T_Λ.

(b) Conclude that $\Delta(\alpha_1, \ldots, \alpha_n)$ is the determinant of T_Λ, and hence that $\Delta(K) = \det(T_{\mathcal{O}_K})$.

(5) Let A be an integral domain and let F be its field of fractions

(a) Let M be an A-submodule of F. It is called *invertible* if there is an A-submodule N of F such that $MN = A$. We showed in class that if $MN = A$, then

$$N = (A : M) := \{\beta \in F : \beta M \subseteq A\}.$$

(In class, we stated this for fractional ideals, but the proof in no way needed that). Show that if M is invertible, then it is a finitely-generated A-module, and hence a fractional ideal of A. (Hint: since $M(A : M) = A$, there are finitely many elements $m_i \in M$ and $n_i \in (A : M)$ such that

$$\sum_{i=1}^{r} m_i n_i = 1.$$

Show that $m_1, \ldots, m_r$ generates M as an A-module.)

(b) Conclude that if I is an invertible fractional ideal of A, then $(A : I)$ is also a fractional ideal.

(6) Let $A = \mathbf{Z}[\sqrt{-5}]$. Let $\mathfrak{p}_1 := (2, 1 + \sqrt{-5})$ and let $\mathfrak{p}_2 := (2, 1 - \sqrt{-5})$. In Assignment 1, Question (2b), you showed that $\mathfrak{p}_1\mathfrak{p}_2 = (2)$.

(a) Show that, in fact, $\mathfrak{p}_1 = \mathfrak{p}_2$, so that $(2) = \mathfrak{p}_1^2$.

(b) Let $\mathfrak{q}_1 := (3, 1 + \sqrt{-5})$ and let $\mathfrak{q}_2 := (3, 1 - \sqrt{-5})$. Show that $\mathfrak{q}_1\mathfrak{q}_2 = (3)$.

(c) Show that each of $\mathfrak{p}_1, \mathfrak{q}_1$, and $\mathfrak{q}_2$ are prime ideals. (Hint: think about the norm function.)

(d) Use the factorization $6 = 2 \cdot 3$, to factor $6\mathbf{Z}[\sqrt{-5}]$ into prime ideals.