Math 676. Homework 7

1. Let $K = \mathbf{Q}(\zeta_{23})$ and let $\mathscr{O} = \mathscr{O}_K$. Use the following steps to prove that $\mathscr{O}$ is not a PID; note that $n = 23$ is the least n such that $\mathbf{Q}(\zeta_n)$ has class number > 1. This approach will use the arithmetic of the unique quadratic subfield $\mathbf{Q}(\sqrt{-23})$.

(*i*) Prove that $47\mathbf{Z}$ splits completely in $\mathscr{O}$.

(*ii*) Assuming $\mathscr{O}$ to be a PID, let $x \in \mathscr{O}$ be a generator of one of the 22 primes over $47\mathbf{Z}$ in $\mathscr{O}$. Let y be the norm of x down to $\mathbf{Q}(\sqrt{-23})$, and explain why $y \in \mathbf{Z}[(1+\sqrt{-23})/2]$ has norm 47 in $\mathbf{Z}$.

(*iii*) Prove that there are two primes of $\mathbf{Q}(\sqrt{-23})$ over $47\mathbf{Z}$, and show "by hand" that neither is principal. Conclude that the assumption in (*ii*) is false, so $\mathbf{Q}(\zeta_{23})$ has class number > 1.

2. Let $K = \mathbf{Q}(\zeta_{17})^+$ denote the totally real subfield of $\mathbf{Q}(\zeta_{17})$. Use the following steps to prove "by hand" that $h_K = 1$.

(*i*) For any odd prime p, you know the discriminant of $\mathbf{Q}(\zeta_p)$ and you know that there is a unique prime $(\zeta_p - 1)$ over p with trivial residue field degree (and hence ramification index $p-1$). Since this is quadratic over $\mathbf{Q}(\zeta_p)^+$, use transitivity of discriminants to compute the discriminant of $\mathbf{Q}(\zeta_p)^+$ over $\mathbf{Q}$ (the answer will be $p^{(p-3)/2}$ up to a sign that you must determine).

(*ii*) By (*i*), $\mathbf{Q}(\zeta_{17})^+/\mathbf{Q}$ has discriminant 17^7. Use Minkowski's bound to conclude that each ideal class contains an integral ideal with norm at most 48. We will show that all such ideals are principal.

(*iii*) Using the identification of $\mathrm{Gal}(\mathbf{Q}(\zeta_{17})^+/\mathbf{Q})$ with $(\mathbf{Z}/17\mathbf{Z})^\times/\langle -1\rangle$, prove that for any prime $\ell \neq 17$ with ℓ having order f in $(\mathbf{Z}/17\mathbf{Z})^\times/\langle -1\rangle$, the prime ℓ splits into $8/f$ factors in $\mathbf{Q}(\zeta_{17})^+$ with each prime of residual degree f. Also check that the prime over 17 has norm 17 and find a principal generator for this ideal.

(*iv*) Analyze the splitting in $\mathbf{Q}(\zeta_{17})^+$ of all positive rational primes $\ell \leq 48$, and conclude that the only prime ideals of $\mathbf{Q}(\zeta_{17})^+$ with norm ≤ 48 are the ones over 2 and 17; hence, we just have to show that the primes over 2 are principal.

(*v*) Show that 2 splits into two primes of $\mathbf{Q}(\zeta_{17})^+$ with residual degree 4 and norm 16. Also show that 2 splits into a product of two principal primes P and P' in the (unique) quadratic subfield $\mathbf{Q}(\sqrt{17})$; you have to find algebraic integers in $\mathbf{Q}(\sqrt{17})$ with norm ± 2.

(*vi*) Prove that P and P' remain prime in $\mathbf{Q}(\zeta_{17})^+$, and conclude the desired result.

3. Let A be the order of conductor f in a quadratic field K with discriminant D. Using the end of Exercise 5 on HW5, give a formula for the class number of A in terms of the class number h_K of $\mathscr{O}_K$:

$$\#\mathrm{Pic}(A) = \frac{h_K f}{[\mathscr{O}_K^\times : A^\times]} \cdot \prod_{p|f} \left(1 - \frac{(D|p)}{p}\right)$$

where $(D|p)$ means 0 if $p|D$ and otherwise it 1 or -1 depending respectively on whether p is split or inert in $\mathscr{O}_K$ (so it is the usual Legendre symbol for odd p, and for $p = 2$ it is 1 for $D \equiv 1 \bmod 8$ and -1 for $D \equiv 5 \bmod 8$). You should explain in particular why $\mathscr{O}_K^\times/A^\times$ is finite for any order A in the ring of integers of any number field K.

4. The purpose of this exercise is to fill in the omitted step in lecture for proving that the "abstract" measure-theoretic definition of the regulator of K coincides with the "concrete" definition as the determinant of a matrix (with one row removed).

Let $M = (x_{ij})$ be an $(n+1)\times n$-matrix over a commutative ring, and assume that the column sums $\sum_{i=1}^{n+1} x_{ij}$ vanish for all $1 \leq j \leq n$. Let $M^{(i_0)} = (x_{ij})_{i \neq i_0}$ be the $n \times n$ submatrix obtained by deleting the i_0th row. Prove $\det M^{(i_0)} = (-1)^{i_0 - 1}\det M^{(1)}$. (hint: express $\det M^{(i_0)}$ as the determinant of an $(n+1)\times(n+1)$ matrix containing M as a submatrix).

5. Let A be a finite-dimensional nonzero associative $\mathbf{R}$-algebra with identity (and with $\mathbf{R}$ in its center). Let $n = \dim_{\mathbf{R}} A > 0$.

(*i*) Define $\mathrm{N}_{A/\mathbf{R}} : A \to \mathbf{R}$ by $\mathrm{N}_{A/\mathbf{R}}(a) = \det(x \mapsto ax)$. Prove that this is a *homogeneous polynomial map* of degree n in the sense that it is given by a homogenous polynomial of degree n in the linear coordinates with respect to any choice of $\mathbf{R}$-basis of A.

(*ii*) Prove that if $aa' = 1$ for some $a' \in A$ then $a'a = 1$ as well (hint: think of the associated left-multiplication endomorphisms of A). The set of such elements is denoted $A^\times$, and is called the *unit group* of A; prove that it is a group with respect to multiplication. Prove that $A^\times = \mathrm{N}_{A/\mathbf{R}}^{-1}(\mathbf{R}^\times)$, and conclude that $A^\times$ is *open* in A. Prove that with respect to the induced topology, it is a *topological group*; explain why the laws for multiplication and inversion are even given by rational functions with denominators given by powers of the polynomial function $\mathrm{N}_{A/\mathbf{R}}$ that is non-vanishing on $A^\times$ (and so $A^\times$ is thereby naturally a Lie group).

(*iii*) If $A \simeq A'$ is an $\mathbf{R}$-algebra isomorphism between two such $\mathbf{R}$-algebras as above, prove that the induced isomorphism $A^\times \simeq {A'}^\times$ between unit groups is an isomorphism of topological groups (and even Lie groups, if you know the meaning of such things).

(*iv*) Let K be a number field. Let $\sigma_i : K \to \mathbf{R}$ ($1 \le i \le r_1$) be the real embeddings and let $\sigma_{r_1+j} : K \to \mathbf{C}$ ($1 \le j \le r_2$) be representatives for the conjugate pairs of (non-real) complex embeddings. Using these to define the familiar isomorphism $K \otimes_{\mathbf{Q}} \mathbf{R} \simeq \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$, explain why $(K \otimes_{\mathbf{Q}} \mathbf{R})^\times$ is open in $K \otimes_{\mathbf{Q}} \mathbf{R}$ and why the induced isomorphism of unit groups $(K \otimes_{\mathbf{Q}} \mathbf{R})^\times \simeq (\mathbf{R}^\times)^{r_1} \times (\mathbf{C}^\times)^{r_2}$ is an isomorphism of topological groups (using the natural topologies on each side).

6. Let K be a field, and let $\mathbf{P}^1(K)$ denote the set of K-points of the projective line over K. That is, it is the quotient set $(K^2 - \{(0,0)\})/K^\times$ for the action of $K^\times$ on $K^2 - \{(0,0)\}$, or more geometrically it is the set of lines in K^2 passing through the origin. For $(x,y) \in K^2 - \{(0,0)\}$, we write $[x,y]$ to denote the class of (x,y) in $\mathbf{P}^1(K)$ (the line joining $(0,0)$ and (x,y)).

There is a natural action of $\mathrm{GL}_2(K)$ on $\mathbf{P}^1(K)$ because the action of $\mathrm{GL}_2(K)$ on K^2 carries lines to lines and fixes the origin. We shall assume that K is the fraction field of a Dedekind domain A.

(*i*) Use the fact that every fractional ideal of A admits two generators as an A-module to conclude that $[x,y] \mapsto [xA + yA] \in \mathrm{Pic}(A)$ is a well-defined map from $\mathbf{P}^1(K)$ *onto* the class group of A.

(*ii*) Continuing in the setup of (*i*), prove that two points $[x,y], [x',y'] \in \mathbf{P}^1(K)$ map to the same ideal if and only if there are in the same orbit for the action of the subgroup $\mathrm{SL}_2(A) \subseteq \mathrm{GL}_2(K)$ on $\mathbf{P}^1(K)$. (Hint: To prove "only if", which is the nontrivial implication, use the fact that the inverse ideal $(xA + yA)^{-1}$ also admits two generators.)

(*iii*) Prove that the quotient set $\mathbf{P}^1(K)/\mathrm{SL}_2(A)$ of $\mathrm{SL}_2(A)$-orbits in $\mathbf{P}^1(K)$ is in bijection with the class group of A, and so this set of orbits is *finite* if the class group of A is finite; a notable example is $A = \mathscr{O}_K$ for K a number field, in which case this finiteness theorem is important in the study of Hilbert modular varieties over totally real number fields.