Math 676. Homework 5

1. (i) For an odd prime p, use Galois theory to prove that $\mathbf{Q}(\zeta_p)$ contains a unique quadratic subfield K, and use considerations with discriminants to prove that $\mathrm{disc}(\mathscr{O}_K/\mathbf{Z}) = \pm p$. Conclude that $K = \mathbf{Q}(\sqrt{(-1|p)p})$, where $(-1|p) = (-1)^{(p-1)/2}$ is the Legendre symbol.

(ii) Use discriminants to determine all three quadratic subfields of $\mathbf{Q}(\zeta_8)$.

(iii) Let p and q be distinct *positive* odd primes, and let $\phi_q \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) = (\mathbf{Z}/p\mathbf{Z})^\times$ be the residue class of q mod p. Prove that ϕ_q preserves all primes $\mathfrak{Q}$ of $\mathbf{Z}[\zeta_p]$ over q, and hence $\phi_q|_K$ preserves the primes of $\mathscr{O}_K$ over q for K as in (i). By studying Galois-actions on *finite* residue fields and on primes over $q\mathbf{Z}$ in $\mathscr{O}_K$, prove that ϕ_q has trivial image in $\mathrm{Gal}(K/\mathbf{Q})$ if and only if $q\mathbf{Z}$ is split in $\mathscr{O}_K$. (Hint: check that ϕ_q induces the qth-power automorphism on $\mathbf{Z}[\zeta_p]/\mathfrak{Q}$ for every prime $\mathfrak{Q}$ over $q\mathbf{Z}$, and so $\phi_q|_K$ does the same on $\mathscr{O}_K/\mathfrak{q}$ for all $\mathfrak{q}$ over $q\mathbf{Z}$ in $\mathscr{O}_K$.) Also prove that $\phi_q|_K = 1$ if and only if q is a square modulo $p\mathbf{Z}$. Deduce quadratic reciprocity for odd primes; where does your argument use that p and q are *positive*?

(iv) Modify the method in (iii) by means of (ii) to prove the Legendre-symbol formula $(2|p) = (-1)^{(p^2-1)/8}$.

2. (i) Compute the discriminant for $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ (that is, compute $\mathrm{disc}(\mathbf{Z}[\zeta_n]/\mathbf{Z})$).

(ii) Choose an integer $n > 2$, and show that $K = \mathbf{Q}(\zeta_n)$ is a CM field with maximal totally real subfield $K^+ = \mathbf{Q}(\zeta_n + \zeta_n^{-1})$. Use your knowledge of $\mathscr{O}_K$ to prove $\mathscr{O}_{K^+} = \mathbf{Z}[\zeta_n + \zeta_n^{-1}]$. (Hint: $[K^+ : \mathbf{Q}] = [K : \mathbf{Q}]/2$.)

(iii) For $p = 31$, explain why $\mathbf{Q}(\zeta_p)$ contains a unique subfield L with degree 6 over $\mathbf{Q}$, and by studying the action of $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) = (\mathbf{Z}/p\mathbf{Z})^\times$ on ζ_p, prove that the prime $2\mathbf{Z}$ is totally split in $\mathscr{O}_L$. (Hint: it suffices to prove triviality of a certain extension of *finite* residue fields, and note that $2^{\phi(p)/6} \equiv 1 \bmod p$ for $p = 31$.) Use the fact that $\mathbf{F}_2[X]$ does not contain 6 distinct monic linear polynomials to infer that $\mathscr{O}_L$ is *not* monogenic over $\mathbf{Z}$ (that is, $\mathscr{O}_L \neq \mathbf{Z}[\alpha]$ for all $\alpha \in \mathscr{O}_L$).

3. Let A be a Dedekind domain whose residue fields at all maximal ideals are *finite*, and let F be the fraction field of A. The Dedekind domains of most interest in number theory have this property.

(i) Prove that if F'/F is a finite separable extension and A' is the integral closure of A in F' then A' has finite residue fields at all maximal ideals. Also prove that this finiteness property is inherited by all localizations $S^{-1}A$ that are Dedekind (that is, $S^{-1}A \neq F$).

(ii) Let $\mathfrak{m}$ be a maximal ideal of A and let $M = \mathfrak{m}A_{\mathfrak{m}}$. Recall from class that the natural map $A/\mathfrak{m}^e \to A_{\mathfrak{m}}/M^e$ is an isomorphism carrying $\mathfrak{m}^i/\mathfrak{m}^e$ over onto M^i/M^e for $0 \le i \le e$. Deduce from the fact that $A_{\mathfrak{m}}$ is a discrete valuation ring with residue field $A/\mathfrak{m}$ that $A/\mathfrak{m}^e$ is finite with size $|A/\mathfrak{m}|^e$. Use the Chinese Remainder Theorem to conclude that if $I \subseteq A$ is a nonzero ideal then the quotient ring A/I is *finite*. We write $\mathrm{N}(I)$ to denote its cardinality, and this is called the *absolute norm* of I.

(iii) Prove that $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$ for any two nonzero ideals I and J of A, and in the setup of (i) prove that $\mathrm{N}(IA') = \mathrm{N}(I)^{[F':F]}$ for any nonzero ideal I of A'. In the special case that $A = \mathbf{Z}$ and $A' = \mathscr{O}_K$ for a number field K, prove $\mathrm{N}(I) = |\mathrm{N}_{K/\mathbf{Q}}(I)|$ for all nonzero ideals I of A' (hint: reduce to the case when $K/\mathbf{Q}$ is Galois). Prove an analogous relationship between absolute norm and ring-theoretic norm in the case when $A = k[X]$ for a finite field k and A' is its integral closure in a finite separable extension of $F = \mathrm{Frac}(A)$.

4. Let A be a Dedekind domain with fraction field F, and let $A_0 \subseteq A$ be a subring with fraction field F such that A is a finitely generated A_0-module. We call such an A_0 an *order* in A. The purpose of this exercise and the next one is to define the concept of *class group* for orders and to relate them to the class group of A.

(i) Explain why the above definition of "order" recovers our earlier notion of order (as a subring with finite lattice-index) in the case when A is the ring of integers of a number field, and in general prove that all nonzero prime ideals of A_0 are maximal and that A is the integral closure of A_0 in F (so A is intrinsic to A_0). Construct a nonzero $a \in A$ such that $aA \subseteq A_0$, so $A_0[1/a] = A[1/a]$, and define the *conductor* of A_0 to be

$$\mathfrak{c} = \mathfrak{c}_{A/A_0} = \{a \in A \mid aA \subseteq A_0\},$$

so $\mathfrak{c} \neq 0$. Show that $\mathfrak{c}$ is an ideal of A that is contained in A_0 (so it has the peculiar property of being an ideal in both A_0 and A), and show that all ideals of A contained in A_0 are in fact contained in $\mathfrak{c}$ (so $\mathfrak{c}_{A/A_0} = A$

if and only if $A_0 = A$). If $\mathscr{O}$ is the order of index f in the ring of integers $\mathscr{O}_K$ of a quadratic field K, prove that $\mathfrak{c}_{\mathscr{O}_K/\mathscr{O}} = f\mathscr{O}_K$.

(*ii*) Let S be a multiplicative set of A_0 that is disjoint from some maximal ideal of A_0 (that is, $S^{-1}A_0 \neq F$), so $S^{-1}A$ is the integral closure of $S^{-1}A_0$ and is a finitely generated $S^{-1}A_0$-module (so $S^{-1}A$ is Dedekind). Show that $S^{-1}\mathfrak{c}_{A/A_0} = \mathfrak{c}_{S^{-1}A/S^{-1}A_0}$ as ideals of $S^{-1}A$ (or of $S^{-1}A_0$).

(*iii*) Prove that $\overline{A}_0 = A_0/\mathfrak{c}$ is a subring of $\overline{A} = A/\mathfrak{c}$ such that $\overline{A}_0$ is a finitely generated $\overline{A}$-module and such that no nonzero principal ideals of $\overline{A}$ lie in $\overline{A}_0$ and A_0 is the preimage of $\overline{A}$ under the projection $A \to \overline{A}$. Show that this observation is "universal" in the sense that for any nonzero ideal I of A and any subring $\overline{R}$ of A/I such that $\overline{R}$ does not contain nonzero principal ideals of A/I and such that A/I is finitely generated as an $\overline{R}$-module, the preimage R of $\overline{R}$ in A is an order of A with conductor equal to I. In this sense, all orders can be "described" by ring-theoretic congruence conditions. Deduce in particular that $A_0^\times = A_0 \cap A^\times$, and that if A has finite residue fields at all maximal ideals then for any nonzero ideal I of A there exist only *finitely many* orders A_0 of A such that $\mathfrak{c}_{A/A_0}|I$.

5. A nonzero ideal I in a noetherian domain R is *invertible* if $I_\mathfrak{m} = IR_\mathfrak{m}$ is principal for all maximal ideals $\mathfrak{m}$ of R, and a *fractional ideal* of R is an R-submodule $\mathscr{I}$ of $K = \mathrm{Frac}(R)$ having the form cI for $c \in K^\times$ and I an ordinary ideal of R. Two fractional ideals I and I' of R are *linearly equivalent* if $I = cI'$ for some $c \in K^\times$.

(*i*) Prove that if $\mathscr{I}$ is a nonzero fractional ideal of R then $\mathscr{I}' = \{x \in K \,|\, x\mathscr{I} \subseteq R\}$ is also a nonzero fractional ideal of R. We say that $\mathscr{I}$ is *invertible* if $\mathscr{I}\mathscr{I}' = R$; prove that this condition is unaffected by linear equivalence and that it recovers the initial notion of invertibility when $\mathscr{I}$ is an ordinary ideal of R.

(*ii*) Prove that if $\mathscr{I}_1$ and $\mathscr{I}_2$ are invertible fractional ideals of R then so is $\mathscr{I}_1\mathscr{I}_2$, and that in fact $\mathscr{I}_1 \otimes_R \mathscr{I}_2$ is a torsion-free R-module such that the natural map $\mathscr{I}_1 \otimes_R \mathscr{I}_2 \to \mathscr{I}_1\mathscr{I}_2$ is an isomorphism. Explain how the set $\mathrm{Pic}(R)$ of linear equivalence classes of invertible fractional ideals of R forms an abelian group via tensor products and dualization (over R). This is the *class group* of R.

(*iii*) In the special case when $R = A_0$ is an order in a Dedekind domain A, use weak approximation for A to prove that every invertible fractional ideal of A_0 is linearly equivalent to an invertible ordinary ideal I_0 of A_0 that is coprime to $\mathfrak{c}_{A/A_0}$ in the sense that $I_0 + \mathfrak{c}_{A/A_0} = A_0$.

(*iv*) Prove that $I_0 \mapsto I_0A$ and $I \mapsto I \cap A_0$ are inverse bijections between the set of invertible ordinary ideals of A_0 coprime to $\mathfrak{c} = \mathfrak{c}_{A/A_0}$ and invertible ordinary ideals of A coprime to $\mathfrak{c}$, and that these bijections are compatible with formation of products of such ideals. (Hint: Use gluing of ideals and (*ii*) to reduce to the case when A_0 is local and A is semi-local, so A is a PID whose maximal ideals all contain $\mathfrak{c}$ if $A_0 \neq A$). Deduce that if $\mathfrak{m}_0$ is a maximal ideal of A_0 then the following are equivalent: $\mathfrak{m}_0$ is coprime to $\mathfrak{c}$, $\mathfrak{m}_0$ is invertible, and $(A_0)_{\mathfrak{m}_0}$ is integrally closed (and hence is a discrete valuation ring).

(*v*) Use the bijection with ideals of A, in conjunction with (*iii*), to define an exact sequence of abelian groups

$$1 \to A^\times/A_0^\times \to (A/\mathfrak{c})^\times/(A_0/\mathfrak{c})^\times \to \mathrm{Pic}(A_0) \to \mathrm{Pic}(A) \to 1,$$

and deduce that if all residue fields of A are *finite* and $\mathrm{Pic}(A)$ is finite then $\mathrm{Pic}(A_0)$ is finite for every order A_0 of A.