Math 154. Homework 8

1. Let A be Dedekind with fraction field F, $F''/F'/F$ a tower of finite separable extensions, and $A' \subseteq F'$ and $A'' \subseteq F''$ the integral closures of A (so A'' is also the integral closure of A' in F'').

(*i*) Let $\mathfrak{p}''$ be a maximal ideal of A'', lying over $\mathfrak{p}' \subseteq A'$ and $\mathfrak{p} \subseteq A$. Use prime factorization of nonzero ideals to prove that $e(\mathfrak{p}''|\mathfrak{p}) = e(\mathfrak{p}''|\mathfrak{p}')e(\mathfrak{p}'|\mathfrak{p})$, and also prove that $f(\mathfrak{p}''|\mathfrak{p}) = f(\mathfrak{p}''|\mathfrak{p}')f(\mathfrak{p}'|\mathfrak{p})$.

(*ii*) Show $\mathfrak{p}''$ is unramified over $\mathfrak{p}$ if and only if $\mathfrak{p}''$ is unramified over $\mathfrak{p}'$ and $\mathfrak{p}'$ is unramified over $\mathfrak{p}$. Prove $\mathfrak{p}$ is totally split in F'' if and only if it is totally split in F' and each prime of F' over $\mathfrak{p}$ is totally split in F''.

(*iii*) Assume that F''/F and F'/F are Galois extension of number fields, with A, A', and A'' the corresponding rings of integers. Prove that the quotient map $\mathrm{Gal}(F''/F) \twoheadrightarrow \mathrm{Gal}(F'/F)$ carries $D(\mathfrak{p}''|\mathfrak{p})$ onto $D(\mathfrak{p}'|\mathfrak{p})$ and $I(\mathfrak{p}''|\mathfrak{p})$ into $I(\mathfrak{p}'|\mathfrak{p})$ (finer methods show this is also onto), and that if $\mathfrak{p}$ is unramified in F'' then it carries $\mathrm{Fr}(\mathfrak{p}''|\mathfrak{p})$ to $\mathrm{Fr}(\mathfrak{p}'|\mathfrak{p})$. In the unramified case, also prove that $\mathrm{Fr}(\mathfrak{p}''|\mathfrak{p}') = \mathrm{Fr}(\mathfrak{p}''|\mathfrak{p})^{f(\mathfrak{p}'|\mathfrak{p})}$. As an application, read the beautiful "algebraic number theory" proof of quadratic reciprocity in §6.5.

2. Fix a Galois extension K'/K of number fields generated by a root of a monic irreducible $f \in K[X]$.

(*i*) For a maximal ideal $\mathfrak{p}$ of $\mathscr{O}_K$ such that $f \in \mathscr{O}_{K,\mathfrak{p}}[X]$ (holds for all but finitely many $\mathfrak{p}$), if $f \bmod \mathfrak{p}$ is irreducible over $\mathscr{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathscr{O}_{K,\mathfrak{p}} = \mathscr{O}_K/\mathfrak{p}$ then prove $\mathfrak{p}' := \mathfrak{p}\mathscr{O}_{K'}$ is prime and $\mathrm{Gal}(K'/K) = D(\mathfrak{p}'|\mathfrak{p})$ (cyclic!). (Hint: Let A be a dvr (e.g., $\mathscr{O}_{K,\mathfrak{p}}$) with maximal ideal $\mathfrak{m}$, $F = \mathrm{Frac}(A)$, $f \in A[X]$ monic that is irreducible and separable over F, and A' the integral closure of A in $F' := F[X]/(f)$, so A' is a finite free A-module (A is a PID!). Assume $f \bmod \mathfrak{m}$ is irreducible over $A/\mathfrak{m}$. Prove $j : A[X]/(f) \to A'$ is an injection between finite free A-modules of the same rank, and via ring-theoretic reasons prove $j \bmod \mathfrak{m}$ is injective! Deduce "$\det(j) \in A^\times$" (using A-bases), so j is an isomorphism. Conclude that $A'/\mathfrak{m}A'$ is a *field*, so $\mathfrak{m}A'$ is *prime*.)

(*ii*) If $\mathrm{Gal}(K'/K)$ is not cyclic, show that $f \bmod \mathfrak{p}$ must be *reducible* over $\mathscr{O}_K/\mathfrak{p}$ for all but finitely many $\mathfrak{p}$. Find an irreducible quartic $f \in \mathbf{Z}[X]$ that is reducible modulo p for all but finitely many p!

3. For $p = 31$, prove $\mathbf{Q}(\zeta_p)$ contains a unique subfield L with $[L : \mathbf{Q}] = 6$ and via the action of $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) = (\mathbf{Z}/p\mathbf{Z})^\times$ on ζ_p prove $2\mathbf{Z}$ is totally split in $\mathscr{O}_L$. (Hint: it suffices to prove triviality of Frobenius at 2 for $L/\mathbf{Q}$; use Exercise 1(iii) and note that $2^{\phi(p)/6} \equiv 1 \bmod p$ for $p = 31$.) Show that $\mathbf{F}_2[X, Y]$ has fewer than 6 distinct maps to $\mathbf{F}_2$ and deduce that $\mathscr{O}_L$ requires at least three generators over $\mathbf{Z}$ (that is, $\mathscr{O}_L \neq \mathbf{Z}[\alpha, \beta]$ for all $\alpha, \beta \in \mathscr{O}_L$). Do *not* try to explicitly compute prime ideals (or $\mathscr{O}_L$)!

4. Let $K = \mathbf{Q}(\zeta_{23})$. The following shows $\mathbf{Z}[\zeta_{23}]$ is not a PID; $n = 23$ is minimal for this property.

(*i*) Prove that $47\mathbf{Z}$ splits completely in $\mathbf{Z}[\zeta_{23}]$, and that $\mathbf{Q}(\sqrt{-23})$ is the unique quadratic subfield of K.

(*ii*) Assume $\mathbf{Z}[\zeta_{23}]$ is a PID, and let $x \in \mathbf{Z}[\zeta_{23}]$ generate a prime over $47\mathbf{Z}$. Let $y = \mathrm{N}_{K/\mathbf{Q}(\sqrt{-23})}(x)$. Prove $y \in \mathbf{Z}[(1 + \sqrt{-23})/2]$ must have norm 47 in $\mathbf{Z}$, but show no $z \in \mathbf{Z}[(1 + \sqrt{-23})/2]$ has norm 47!

5. Let $K = \mathbf{Q}(\sqrt{5}, \sqrt{-1})$. Prove any $p \neq 2, 5$ is unramified in K. Use quadratic reciprocity and Exercise 1(iii) to find $\mathrm{Fr}_p \in \mathrm{Gal}(K/\mathbf{Q})$ depending on $p \bmod 20$. Prove $\mathrm{Gal}(K/\mathbf{Q})$ is the decomposition group at 2 (i.e., $g_2 = 1$), $\mathrm{Gal}(K/\mathbf{Q}(i))$ is the decomposition group at 5, and find the inertia subgroup in each.

6. Let $K = \mathbf{Q}(\alpha, i)$ with $\alpha^4 = 3$ and $i^2 = -1$, so $G := \mathrm{Gal}(K/\mathbf{Q}) \simeq D_4$ with generators s and t satisfying $s(\alpha) = i\alpha, s(i) = i,\ t(\alpha) = \alpha, t(i) = -i$ (so $s^4 = t^2 = 1$ and $tst^{-1} = s^{-1}$). Write e_p, f_p, g_p for the invariants attached to a prime p relative to $K/\mathbf{Q}$. (You *do not* need to compute any rings of integers below!)

(*i*) Using Exercise 1(*i*) applied to $K/\mathbf{Q}(\alpha)/\mathbf{Q}$ and $K/\mathbf{Q}(i)/\mathbf{Q}$, show that $e_3 = 4$ and $f_3 = 2$, so $g_3 = 1$. Deduce that the unique prime over 3 is $\mathfrak{p} := \alpha\mathscr{O}_K$, and that $D(\mathfrak{p}|3\mathbf{Z}) = G$. Prove $I(\mathfrak{p}|3\mathbf{Z}) = \langle s \rangle$.

(*ii*) Check that $T^4 - 3$ is irreducible over $\mathbf{F}_5$, and use the tower $K/\mathbf{Q}(\alpha)/\mathbf{Q}$ to show $4|f_5$. Using $K/\mathbf{Q}(i)/\mathbf{Q}$, show $2|g_5$, and conclude that $e_5 = 1$, $f_5 = 4$, and $g_5 = 2$. Hence, there are exactly two primes $\mathfrak{q}$ and $\mathfrak{q}'$ of $\mathscr{O}_K$ over $5\mathbf{Z}$, labelled with $\mathfrak{q}$ over $(1 + 2i)\mathbf{Z}[i]$ and $\mathfrak{q}'$ over $(1 - 2i)\mathbf{Z}[i]$. Explain why $\mathrm{Fr}(\mathfrak{q}|(1 + 2i)\mathbf{Z}[i]) = \mathrm{Fr}(\mathfrak{q}|5\mathbf{Z})$, and prove $\mathfrak{q} = (1 + 2i)\mathscr{O}_K$ and $\mathfrak{q}' = (1 - 2i)\mathscr{O}_K$.

(*iii*) Since 5 splits in $\mathbf{Q}(i)$, prove $D(\mathfrak{q}|5\mathbf{Z}) = D(\mathfrak{q}'|5\mathbf{Z}) = \mathrm{Gal}(K/\mathbf{Q}(i)) = \langle s \rangle$. Since $\mathrm{Fr}(\mathfrak{q}|5\mathbf{Z})$ and $\mathrm{Fr}(\mathfrak{q}'|5\mathbf{Z})$ generate this group, each is s or s^3. Figure out which is which. (Hint: $\alpha \notin \mathfrak{q}, \mathfrak{q}'$, and $\mathbf{F}_5 \simeq \mathbf{Z}[i]/(1 \pm 2i)$ identifies i with $\pm 2 \bmod 5$!) Explain why this is consistent with the fact that t swaps $\mathfrak{q}$ and $\mathfrak{q}'$.

(*iv*) Prove that 7 is unramified in K with $2|f_7$ using $K/\mathbf{Q}(\alpha)/\mathbf{Q}$. Prove that the only nontrivial $\sigma \in G$ which can satisfy $\sigma(x) \equiv x^7 \bmod \mathfrak{P}$ for a prime $\mathfrak{P}$ of $\mathscr{O}_K$ over 7 are the elements st and s^3t with order 2! (Hint: consider $x = \alpha$ and $x = i$). Deduce that $f_7 = 2$, $g_7 = 4$, and $7\mathbf{Z}[i]$ is totally split in $\mathscr{O}_K$.