Math 676. Homework 6

1. Let A be a Dedekind domain.

(*i*) Prove that A is a UFD if and only if A is a PID.

(*ii*) For any multiplicative set S of A (with $0 \notin S$), prove that $[\mathscr{I}] \mapsto [S^{-1}\mathscr{I}]$ is a well-defined and surjective group map $\mathrm{Pic}(A) \to \mathrm{Pic}(S^{-1}A)$ whose kernel is generated by the ideal classes $[\mathfrak{p}]$ of primes of A such that $\mathfrak{p}$ meets S. In particular, if $\mathrm{Pic}(A)$ is finite then so is $\mathrm{Pic}(S^{-1}A)$ for any S. (Hint: reduce to the case $S = \{1, a, a^2, \dots\}$ by using "denominator-chasing" to show that if $S^{-1}\mathscr{I}$ is a principal fractional ideal of $S^{-1}A$ then for some $a \in S$ the fractional ideal $\mathscr{I}[1/a]$ of $A[1/a]$ is principal).

(*iii*) Prove that $\mathrm{Pic}(A)$ is generated by the classes $[\mathfrak{p}]$ of nonzero prime ideals of A, and if $\Sigma = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ is a finite set of nonzero primes of A such that each $[\mathfrak{p}_i]$ has finite order in $\mathrm{Pic}(A)$ (an automatic condition when $\mathrm{Pic}(A)$ is finite) then construct a nonzero $a \in A$ whose prime factors are exactly the $\mathfrak{p}_i$'s. For such an a, prove that $\mathrm{Pic}(A[1/a])$ is identified with the quotient of $\mathrm{Pic}(A)$ by the subgroup generated by the classes of the primes in Σ.

(*iv*) Assume that $\mathrm{Pic}(A)$ is finitely generated. For every maximal ideal $\mathfrak{m}$ of A, use weak approximation to find a nonzero $a \in A$ with $a \notin \mathfrak{m}$ such that $A[1/a]$ is a PID. Conclude that there exist nonzero $a_1, \dots, a_n \in A$ generating 1 such that $A[1/a_i]$ is a PID for all i. Conversely, if A is Dedekind and $A[1/a]$ is a PID for some nonzero $a \in A$ then deduce that $\mathrm{Pic}(A)$ is finitely generated.

2. Let $K = \mathbf{Q}(\sqrt{d})$ with d squarefree and $d \equiv 1 \bmod 4$ (and $d \neq 1$). Let $h(d)$ be the class number of $\mathscr{O}_K$.

(*i*) Prove that $\mathscr{O}_K$ contains a principal ideal with norm 2 if and only if one of the equations $X^2 - dY^2 = \pm 8$ has a solution in $\mathbf{Z}$.

(*ii*) Prove $h(17) = h(33) = 1$, but $h(-15) = 2$ (with 2 splitting in $\mathbf{Q}(\sqrt{-15})$).

(*iii*) Prove $h(-23) = 3$. (Hint: In $\mathscr{O}_K$, prove $(2) = \mathfrak{p}\mathfrak{p}'$ and $(3) = \mathfrak{q}\mathfrak{q}'$ with non-principal prime ideals. Letting $x = (3 + \sqrt{-23})/2$ and $y = x - 1$ be elements with respective norms 8 and 6, study the prime factorizations of (x) and (y).)

3. Let $K = \mathbf{Q}(\alpha)$ with $\alpha^5 - \alpha + 1 = 0$. Prove $\mathrm{disc}(\mathbf{Z}[\alpha]/\mathbf{Z}) = 19 \cdot 151$, so $\mathbf{Z}[\alpha] = \mathscr{O}_K$. Check that the Minkowski constant λ_K is < 4, and by studying $\mathscr{O}_K/(2)$ and $\mathscr{O}_K/(3)$ show that there does not exist a prime ideal $\mathfrak{p}$ of $\mathscr{O}_K$ with norm 2 or 3. Deduce $h_K = 1$.

4. Let A be a Dedekind domain with fraction field F, and let F'/F be a finite Galois extension with Galois group G. Let A' be the integral closure of A in F'.

(*i*) Let $\mathfrak{p}'$ be a maximal ideal of A' lying over a maximal ideal $\mathfrak{p}$ of A (that is, $\mathfrak{p}' \cap A = \mathfrak{p}$). Let $e = e(\mathfrak{p}'|\mathfrak{p})$ and $f = f(\mathfrak{p}'|\mathfrak{p})$. Using Exercise 1 on Homework 4, show that the *decomposition group at* $\mathfrak{p}'$

$$D(\mathfrak{p}'|\mathfrak{p}) = \{g \in G \,|\, g(\mathfrak{p}') = \mathfrak{p}'\}$$

has order ef and that $D(g(\mathfrak{p}')|\mathfrak{p}) = gD(\mathfrak{p}'|\mathfrak{p})g^{-1}$ for all $g \in G$. Conclude that the *conjugacy class* of this subgroup of G is intrinsic to $\mathfrak{p}$, and in particular if G is *abelian* then $D(\mathfrak{p}'|\mathfrak{p})$ depends only on $\mathfrak{p}$ and not on the prime over it in A'; in this case we call this common decomposition group at primes over $\mathfrak{p}$ the *decomposition group at* $\mathfrak{p}$ and denote it $D_{\mathfrak{p}}$. See Exercise 5 for a worked example.

(*ii*) Construct a natural map of groups $D(\mathfrak{p}'|\mathfrak{p}) \to \mathrm{Aut}(\kappa(\mathfrak{p}')/\kappa(\mathfrak{p}))$; its kernel $I(\mathfrak{p}'|\mathfrak{p})$ is the *inertia group* at $\mathfrak{p}'$. Prove that this is a normal subgroup of $D(\mathfrak{p}'|\mathfrak{p})$ and that $I(g(\mathfrak{p}')|\mathfrak{p}) = gI(\mathfrak{p}'|\mathfrak{p})g^{-1}$ for all $g \in G$, so if G is abelian then $I(\mathfrak{p}'|\mathfrak{p})$ likewise only depends on $\mathfrak{p}$ (in which case it is called the *inertia group at* $\mathfrak{p}$ and is denoted $I_{\mathfrak{p}}$). See Exercise 5 for a worked example.

(*iii*) The fixed field F'_{d} of $D(\mathfrak{p}'|\mathfrak{p})$ is called the *decomposition field* for $\mathfrak{p}'$, and the fixed field F'_{i} of $I(\mathfrak{p}'|\mathfrak{p})$ is called the *inertia field* for $\mathfrak{p}'$, so $F'_{\mathrm{d}} \subseteq F'_{\mathrm{i}}$. Let A'_{d} and A'_{i} denote the corresponding integral closures of A in F'_{d} and F'_{i}, and let $\mathfrak{p}'_{\mathrm{d}}$ and $\mathfrak{p}'_{\mathrm{i}}$ be the associated primes under $\mathfrak{p}'$ (and over $\mathfrak{p}$).

Prove that $\mathfrak{p}'$ is the unique prime of A' over $\mathfrak{p}'_{\mathrm{d}}$ (so $D(\mathfrak{p}'|\mathfrak{p}'_{\mathrm{d}}) = \mathrm{Gal}(F'/F'_{\mathrm{d}}) = D(\mathfrak{p}'|\mathfrak{p})$) and that $e(\mathfrak{p}'|\mathfrak{p}'_{\mathrm{d}}) = e$ and $f(\mathfrak{p}'|\mathfrak{p}'_{\mathrm{d}}) = f$ (hint: multiply these hypothetical equations), and deduce that $\mathfrak{p}'_{\mathrm{d}}$ appears in the factorization of $\mathfrak{p}A'_{\mathrm{d}}$ with multiplicity 1 and trivial residue field degree. Prove the following maximality property of the decomposition field: if K is any intermediate field for which the prime below $\mathfrak{p}'$ (in the integral closure of A) has trivial ramification and residue-field degrees over $\mathfrak{p}$ then $K \subseteq F'_{\mathrm{d}}$. Discuss how F'_{d} and F'_{i} change as $\mathfrak{p}'$ varies over $\mathfrak{p}$.

(*iv*) Renaming F'_{d} as F and $\mathfrak{p}'_{\mathrm{d}}$ as $\mathfrak{p}$, suppose $D(\mathfrak{p}'|\mathfrak{p}) = G$. Prove that $\mathfrak{p}'$ is the unique prime of A' over $\mathfrak{p}$, and that the inertia field F'_{i} is Galois over F with Galois group $D(\mathfrak{p}'|\mathfrak{p})/I(\mathfrak{p}'|\mathfrak{p})$ that is identified with a subgroup of $\mathrm{Aut}(\kappa(\mathfrak{p}'_{\mathrm{i}})/\kappa(\mathfrak{p}))$. Recall from field theory that if K'/K is a finite extension then $\#\mathrm{Aut}(K'/K) \leq [K' : K]$ with equality if and only if K'/K is Galois. Deduce that the inclusion

$$\mathrm{Gal}(F'_{\mathrm{i}}/F) \hookrightarrow \mathrm{Aut}(\kappa(\mathfrak{p}'_{\mathrm{i}})/\kappa(\mathfrak{p}))$$

is an equality, so $\kappa(\mathfrak{p}'_{\mathrm{i}})/\kappa(\mathfrak{p})$ is *Galois* (in particular, separable!) and

$$[D(\mathfrak{p}'|\mathfrak{p}) : I(\mathfrak{p}'|\mathfrak{p})] = [\kappa(\mathfrak{p}'_{\mathrm{i}}) : \kappa(\mathfrak{p})] | f(\mathfrak{p}'|\mathfrak{p}).$$

Conclude that $\mathfrak{p}'_{\mathrm{i}}$ is unramified over $\mathfrak{p}$, and that the unique maximal subfield of F' unramified over $\mathfrak{p}$ (why does this exist?) is *Galois* over $F = F'_{\mathrm{d}}$ (use maximality!) and consequently is *equal* to F'_{i}.

(*v*) Continuing with the hypothesis $F'_{\mathrm{d}} = F$, pick an element $\overline{\theta} \in \kappa(\mathfrak{p}')$ and let $\overline{f} \in \kappa(\mathfrak{p})[X]$ be its minimal polynomial. Choose $\theta \in A'$ lifting $\overline{\theta}$ and let $f \in A[X]$ be its minimal polynomial over F. Prove that $\overline{f}$ divides f mod $\mathfrak{p}$, and use the Galois property of F'/F to infer that $\overline{f}$ splits over $\kappa(\mathfrak{p}')$; hence, the extension $\kappa(\mathfrak{p}')/\kappa(\mathfrak{p})$ is normal. By taking $\overline{\theta}$ to be a primitive element for the (Galois!) maximal separable subextension k, deduce that the map

$$\mathrm{Gal}(F'/F) = D(\mathfrak{p}'|\mathfrak{p}) \to \mathrm{Aut}(\kappa(\mathfrak{p}')/\kappa(\mathfrak{p})) = \mathrm{Gal}(k/\kappa(\mathfrak{p}))$$

is surjective with kernel $I(\mathfrak{p}'|\mathfrak{p})$.

(*vi*) Using the results in (*iv*), deduce in general (without requiring $F'_{\mathrm{d}} = F$) that $\mathfrak{p}'_{\mathrm{i}}$ is unramified over $\mathfrak{p}$ and that F'_{i} is maximal with respect to this property in the sense that if $K \subseteq F'$ is an subextension over F in which the prime below $\mathfrak{p}'$ is unramified over $\mathfrak{p}$ (so KF'_{d} has the property too!) then $K \subseteq F'_{\mathrm{i}}$. Also use (*iv*) to deduce that in general $\kappa(\mathfrak{p}')/\kappa(\mathfrak{p})$ is normal with $\kappa(\mathfrak{p}'_{\mathrm{i}})$ as its maximal separable subextension, and that $D(\mathfrak{p}'|\mathfrak{p}) \to \mathrm{Aut}(\kappa(\mathfrak{p}')/\kappa(\mathfrak{p}))$ is *surjective*, so $e(\mathfrak{p}'|\mathfrak{p})|\#I(\mathfrak{p}'|\mathfrak{p})$ with equality if and only if the finite normal extension $\kappa(\mathfrak{p}')/\kappa(\mathfrak{p})$ is *separable* (and hence Galois); note that this latter condition always holds if $\kappa(\mathfrak{p})$ is perfect (*e.g.*, finite).

5. Let $K = \mathbf{Q}(\sqrt{5}, \sqrt{-1})$ be a splitting field of $(X^2 - 5)(X^2 + 1)$ over $\mathbf{Q}$.

(*i*) Prove $K/\mathbf{Q}$ is Galois with Galois group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

(*ii*) Let $A = \mathbf{Z}[\sqrt{-1}, (1 + \sqrt{5})/2]$. Show that A is an order in $\mathscr{O}_K$, and compute the nonzero discriminant $\mathrm{disc}(A/\mathbf{Z}[\sqrt{-1}]) \in \mathbf{Z}[\sqrt{-1}]$ (which is well-defined up to sign, as $\mathbf{Z}[\sqrt{-1}]$ is a PID whose unit squares are ± 1). Check that this is squarefree in the PID $\mathbf{Z}[\sqrt{-1}]$, and infer that $\mathscr{O}_K = A$.

(*iii*) Compute $\mathrm{disc}(\mathscr{O}_K/\mathbf{Z})$, and deduce that 2 and 5 are the primes of $\mathbf{Z}$ that ramify in $\mathscr{O}_K$, and the associated ramification degrees e_2 and e_5 (for all primes of $\mathscr{O}_K$ over 2 and 5 respectively) each equal 2.

(*iv*) (This uses Exercise 4.) For all $p \neq 2, 5$, observe that the decomposition group $D_p \subseteq \mathrm{Gal}(K/\mathbf{Q})$ is equal to D_p/I_p since I_p is trivial. Hence, for such p we may identify D_p with the Galois group of a Galois extension of *finite* residue fields, so it has a canonical Frobenius generator Frob_p. (Recall that if κ'/κ is a finite extension of finite fields, the *arithmetic Frobenius* generator of $\mathrm{Gal}(\kappa'/\kappa)$ is $x \mapsto x^{|\kappa|}$). Compute the element $\mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbf{Q})$ for all $p \neq 2, 5$, and determine the decomposition field as well. For $p \in \{2, 5\}$ compute the associated decomposition and inertia groups at p in $\mathrm{Gal}(K/\mathbf{Q})$, as well as the decomposition and inertia fields K_{d} and K_{i}, and compute the Frobenius generator for $D_p/I_p \simeq \mathrm{Gal}(K_{\mathrm{i}}/K_{\mathrm{d}})$ at the primes of K_{d} over $p\mathbf{Z}$.