Math 248A. Homework 4

Read the handout on examples of vertical factorization.

1. Let $A$ be a Dedekind domain with fraction field $F$ and let $F'/F$ be a finite separable extension. Let $A'$ be the integral closure of $A$ in $F'$. We assume that $F'/F$ is Galois with Galois group $\Gamma$.

   (i) Prove that the action of $\Gamma$ on $F'$ carries $A'$ back into itself and that the $\Gamma$-invariant elements in $A'$ are exactly the elements of $A$. Also show that for any $\gamma \in \Gamma$ and maximal ideal $p'$ of $A'$, $\gamma(p')$ is a maximal ideal of $A'$. (We say that the maximal ideal $\gamma(p')$ is a $\Gamma$-conjugate of $p'$.)

   (ii) Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ and $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_s$ be two finite sets of pairwise distinct maximal ideals of $A'$ such that every $\Gamma$-conjugate of a $\mathfrak{P}_i$ is a $\mathfrak{P}_j$ and every $\Gamma$-conjugate of a $\mathfrak{Q}_i$ is a $\mathfrak{Q}_j$. Use weak approximation to construct $x' \in A'$ such that $\gamma(x') \in \prod_i \mathfrak{P}_i$ for all $\gamma \in \Gamma$ but $\gamma(x') \notin \mathfrak{Q}_j$ for all $\gamma \in \Gamma$ and for all $j$.

   (iii) Let $p$ be a nonzero prime ideal of $A$, and let $\{p'_1, \ldots, p'_j\}$ be the finite set of primes of $A'$ over $A$, with $p A' = \prod p'_i$; let $f_i = [A'/p'_i : A/p]$ be the associated residue-field degrees. Prove that the action of $\Gamma$ on $A'$ permutes the set of $p'_i$'s, and that if $\gamma$ carries $p'_i$ to $p'_j$ then $e_i = e_j$ and $\gamma$ induces an isomorphism $A'/p'_i \cong A'/p'_j$ as extensions of $A/p$ (so $f_i = f_j$).

   (iv) Prove that the action of $\Gamma$ on the set of $p'_i$'s is transitive, so in fact $p A' = (\prod p'_i)^c$ with a common ramification degree $e = e_i$ for all $i$ and a common residue field degree $f = f_i$ for all $i$. (Hint: Suppose that the set of $p'_i$'s is not a single $\Gamma$-orbit, and use (ii) to construct $x' \in A'$ such that $N_{F'/F}(x') = \prod_{\gamma \in \Gamma} \gamma(x') \in A$ lies in the $p'_i$'s from one $\Gamma$-orbit but not in any of the $p'_i$'s from some other $\Gamma$-orbit. Check that $N_{F'/F}(x') \in p$ and deduce a contradiction.)

2. Let $K/Q$ be a quadratic field with discriminant $D$, and let $p \in \mathbb{Z}$ be a prime. Let $\mathcal{O}_K$ be the ring of integers of $K$. The following extends Exercise 3 in Homework 3.

   (i) If $p$ is odd, prove that $p\mathcal{O}_K$ is prime (that is, $p\mathbb{Z}$ is inert in $\mathcal{O}_K$) if and only if $p \nmid D$ with $D$ a nonsquare modulo $p\mathbb{Z}$, that $p\mathcal{O}_K = p_1p_2$ is a product of two distinct primes (that is, $p\mathbb{Z}$ is split in $\mathcal{O}_K$) if and only if $p \nmid D$ with $D$ a square modulo $p\mathbb{Z}$, and that $p\mathcal{O}_K = p^2$ (that is, $p\mathbb{Z}$ is ramified in $\mathcal{O}_K$) if and only if $p | D$.

   (ii) Give analogous criteria for $p = 2$.

   (iii) Use the method of proof of Exercise 3 in Homework 3 to explicitly factor $p\mathbb{Z}$ in the rings of integers $\mathbb{Z}[(\sqrt{7})]$ and $\mathbb{Z}[(1 + \sqrt{-15})/2]$ (with respective discriminants $D = 28$ and $-15$) for all $p \in \{2, 3, 5, 7, 11\}$, expressing each prime ideal in the form $(p, \theta)$. Later methods will show that neither of these rings is a PID (or you can try to directly verify that specific prime ideals are not principal).

   (iv) Using quadratic reciprocity, determine all primes $p$ that are split in $\mathbb{Z}[(\sqrt{11})]$.

3. Let $A$ be a Dedekind domain, with fraction field $F$. The following uses Exercise 5 from Homework 3.

   (i) Let $I$ and $I'$ be nonzero ideals of $A$. Prove that the natural map $I \otimes_A I' \to A$ induced by multiplication is an isomorphism onto $II'$. (use localization and functoriality to reduce to the case of discrete valuation rings).

   (ii) Let $M$ be a finitely generated and torsion-free $A$-module, and let $M_F = F \otimes_A M$. Define the dual module to be $M^\vee = \text{Hom}_A(M, A)$, so this is again finitely generated and torsion-free. Prove that $(M^\vee)_F$ is naturally identified with the $F$-dual space to $M_F$, and use localization at maximal ideals to prove that the natural map $M \otimes_A M^\vee \to A$ defined by $m \otimes \ell \mapsto \ell(m)$ is an isomorphism if $\dim_F M_F = 1$.

   (iii) Let $\text{Pic}(A)$ denote the set of isomorphism classes $[M]$ of finitely generated and torsion-free $A$-modules $M$ such that $\dim_F M_F = 1$. Prove that every nonzero ideal $I$ of $A$ satisfies these conditions on $M$, and that the operation of tensor product gives $\text{Pic}(A)$ a natural structure of commutative group (called the class group of $A$, or the Picard group of Spec $A$ in the language of schemes) with identity $[A]$ and with inversion $- [M] = [M^\vee]$. Prove that every element of $\text{Pic}(A)$ has the form $[I]$ for a nonzero ideal $I$ of $A$, with $[I] = [I']$ if and only if $I = cI'$ for some $c \in F^\times$. Deduce that the group $\text{Pic}(A)$ is trivial if and only if $A$ is a PID.

   (iv) We define a fractional ideal of $A$ to be a finitely generated nonzero $A$-submodule $\mathcal{I}$ of $F$, and two fractional ideals $\mathcal{I}$ and $\mathcal{I}'$ of $A$ are linearly equivalent if $\mathcal{I} = c\mathcal{I}'$ for some $c \in F^\times$. The product of two fractional ideals $\mathcal{I}$ and $\mathcal{I}'$ of $A$ is defined to be

   \[ \mathcal{I} \mathcal{I}' = \{ y \in F \mid y = x_1x'_1 + \cdots + x_nx'_n, \ x_i \in \mathcal{I}, x'_i \in \mathcal{I}' \}. \]
why is this a fractional ideal? Prove that every fractional ideal of $A$ is linearly equivalent to a nonzero ordinary ideal of $A$, that the isomorphism $F \otimes_F F \simeq F$ induced by multiplication induces an isomorphism $\mathcal{I} \otimes_A \mathcal{I}' \simeq \mathcal{I} \mathcal{I}'$, and that

$$\mathcal{I}^{-1} \overset{\text{def}}{=} \{ x \in F \mid x \mathcal{I} \subseteq A \}$$

is a fractional ideal that is naturally identified with the dual module $\mathcal{I}^\vee$. Deduce that Pic($A$) may be described using only the classical language of fractional ideals of $A$ (without mentioning tensor products or dual modules): it is the monoid of fractional ideals up to linear equivalence, with group law given by the product as above and with inversion given by $\mathcal{I}^{-1}$ as above.

4. (optional) Let $A$ be a Dedekind domain. If $I$ and $I'$ are ideals in $A$, we say $I$ divides $I'$ if $I' = IK$ for an ideal $K$ of $A$ (so all ideals divide $(0)$).

(i) If $I$ and $J$ are ideals in $A$, prove that $I + J$ is the unique smallest ideal that divides $I$ and $J$.

(ii) Using weak approximation, prove that every ideal in $A$ admits one or two generators.

5. (optional) Let $I, I', J$ be nonzero ideals of $A$. Prove that if $I \oplus J$ and $I \oplus J'$ are abstractly isomorphic as $A$-modules then $[J] = [J']$ in Pic($A$). (Hint: Prove that the natural $A$-linear map $I \otimes_A J \rightarrow \wedge^2(I \oplus J)$ defined by $x \otimes y \mapsto (x, 0) \wedge (0, y)$ is an isomorphism by using localization to reduce to the case when $A$ is a discrete valuation ring. You must of course show that the exterior power really is torsion-free.)