E. Dummit's Math 7315 ~ Algebraic Number Theory, Fall 2024 ~ Homework 3, due Wed Oct 30th.

Solve whichever problems you haven't seen before that interest you the most (suggestion: between 20 and 40 points' worth). Starred problems are especially recommended. Prepare to present 1-2 problems in class on the due date.

0.1 In-Lecture Exercises

0.1.1 Exercises from (Oct 7)

1. [1pt] If P is a prime ideal of $\mathcal{O}_K$ that lies above the integer prime p, show that $N(P)$ is a power of p.
2. [1pt] We have previously observed that an element $\alpha \in \mathcal{O}_K$ of norm $\pm p$ for a prime p is irreducible. Show in fact that such an element is prime.
3. [1pt] Let p be a prime. Show that $(1-\zeta_p)$ is a prime ideal of $\mathbb{Z}[\zeta_p]$ that lies above $p \in \mathbb{Z}$. [Hint: $\mathbb{Z}[\zeta_p]/(1-\zeta_p)$ is isomorphic to $\mathbb{Z}[x]/(1-x, \Phi_p(x))$.]
4. [3pts*] Let $L/K/F$ be an extension tower of number fields with R a prime ideal of $\mathcal{O}_L$ lying over the prime ideal Q of $\mathcal{O}_K$ lying over the prime ideal P of $\mathcal{O}_F$.
   (a) Show that the ramification index is multiplicative in towers: $e(R|P) = e(R|Q)e(Q|P)$.
   (b) Show that the inertial degree is multiplicative in towers: $f(R|P) = f(R|Q)f(Q|P)$.
5. [1pt] Show that if Q is a prime ideal of $\mathcal{O}_L$ lying over the prime ideal P of $\mathcal{O}_K$, then $N_L(Q) = N_K(P)^{f(Q|P)}$.

0.1.2 Exercises from (Oct 9)

1. [3pts*] Compute the prime ideal factorizations of (2), (3), (5), (7), and (11) in $\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, and $\mathbb{Q}(\sqrt{5})$. Identify which primes ramify, split, and remain inert in each case.
2. [2pts] For $K = \mathbb{Q}(\sqrt[3]{5})$, compute the prime ideal factorizations of (2), (3), (5), (7), and (11) in $\mathcal{O}_K$. (Recall that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ as noted in an earlier exercise.)
3. [2pts*] For $K = \mathbb{Q}(\alpha)$ where $\alpha^3 - \alpha + 1 = 0$, compute the prime ideal factorizations of (2), (3), (5), (7), and (23) in $\mathcal{O}_K$. (Recall that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ as noted in an earlier exercise.)

0.1.3 Exercises from (Oct 16)

1. [3pts*] For $K = \mathbb{Q}(\zeta_7)$, compute the prime ideal factorizations of (2), (3), (5), (7), and (11) in $\mathcal{O}_K$. Determine also the general factorization behavior of (p) in terms of the residue class of p modulo 7.
2. [2pts] For $K = \mathbb{Q}(\sqrt{5}, \sqrt{13})$, compare the prime ideal factorizations of (2), (3), (5), and (7) in K to those in the other two subfields $\mathbb{Q}(\sqrt{13})$ and $\mathbb{Q}(\sqrt{65})$.
3. [2pts*] For $K = \mathbb{Q}(\sqrt{3}, \sqrt{7})$, find the prime ideal factorizations of (2), (3), (5), and (7) in $\mathcal{O}_K = \mathbb{Z}[\frac{\sqrt{3}+\sqrt{7}}{2}]$. Compare these factorizations to the corresponding factorizations in $\mathcal{O}_F$ for $F = \mathbb{Q}(\sqrt{3})$.

0.1.4 Exercises from (Oct 17)

1. [1pt] Let K be a number field and let I be a nonzero ideal of $\mathcal{O}_K$ with $c \in \mathcal{O}_K$ arbitrary. Show that there are infinitely many elements $a \equiv c \pmod{I}$ such that $K = \mathbb{Q}(a)$. [Hint: Let $b \in \mathcal{O}_K$ generate $K/\mathbb{Q}$ and $N = N(I)$. Show that infinitely many $c_k = a + kNb$ for $k \in \mathbb{Z}$ are generators of $K/\mathbb{Q}$.]

2. [2pts] Let p be a prime and let $f_p(n)$ be the number of monic irreducible polynomials of degree n in $\mathbb{F}_p[x]$. Show that $f_p(n) = \frac{1}{n}\sum_{d|n}\mu(d)p^{n/d}$ where μ denotes the Möbius μ-function.

3. [1pt] Suppose that $K/\mathbb{Q}$ is an extension of degree 3. Show that if p is an odd prime, then there exists some $\alpha \in \mathcal{O}_K$ such that $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is not divisible by p. Show also that if 2 splits completely in K, then for any $\alpha \in \mathcal{O}_K$, the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is divisible by 2.

4. [2pts*] Suppose $K = \mathbb{Q}(\alpha)$ where $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Prove that an integer prime p is ramified in K if and only if p divides the discriminant $\operatorname{disc}(K)$. [Hint: Note $\operatorname{disc}(K) = \operatorname{disc}(m(x))$ where $m(x)$ is the minimal polynomial of α over $\mathbb{Q}$, and apply Dedekind-Kummer.]

0.1.5 Exercises from (Oct 21)

1. [1pt] If A is a nonzero fractional ideal of $\mathcal{O}_L$, show that $A^{**} = A$.

2. [1pt] Suppose A is a nonzero fractional ideal of $\mathcal{O}_L$. Show that $A^{-1} \subseteq A^*$.

3. [1pt*] Suppose A, B are nonzero fractional ideals of $\mathcal{O}_L$. Show that if $A \subseteq B$ then $B^{-1} \subseteq A^{-1}$ and $B^* \subseteq A^*$.

4. [1pt] In $K = \mathbb{Q}(\sqrt{-5})$, compute a basis of A^* for $A = \mathcal{O}_K$ and for $A = (2, 1+\sqrt{-5})\mathcal{O}_K$.

5. [1pt] Show that for any ideal I of $\mathcal{O}_L$, we have $D_{L/K}(I) = D_{L/K} \cdot I$: thus, we may view the notation $D_{L/K}(I)$ as representing a product or a function, interchangeably.

6. [1pt] Suppose $\alpha_1, \dots, \alpha_n$ is a basis of $K/\mathbb{Q}$ with dual basis $\alpha_1^*, \dots, \alpha_n^*$. Show that $\operatorname{disc}(\alpha_1^*, \dots, \alpha_n^*) = \operatorname{disc}(\alpha_1, \dots, \alpha_n)^{-1}$. [Hint: Show that the product of the matrices $\{\sigma_i(\alpha_j)\}_{1\le i,j\le n}$ and the transpose of $\{\sigma_i(\alpha_j^*)\}_{1\le i,j\le n}$ is the identity matrix.]

0.1.6 Exercises from (Oct 23)

1. [1pt] Suppose R is a subring of S and $d : S \to M$ is a derivation such that $d(r) = 0$ for all $r \in R$. Prove the "chain rule" for polynomials: for any $p(x) \in R[x]$ and any $a \in S$, show that $d(p(a)) = p'(a)d(a)$ where p' is the usual formal derivative of p.

2. [2pts*] Let Q be a nonzero prime ideal of $\mathcal{O}_L$. Show that the zero divisors in $\mathcal{O}_L/Q^e$ are the elements of Q/Q^e.

3. [2pts] Show that L/K is unramified if and only if $\operatorname{disc}(L) = \pm\operatorname{disc}(K)^{[L:K]}$.

4. [2pts*] Show that the extension $\mathbb{Q}(\sqrt{-3}, \sqrt{5})/\mathbb{Q}(\sqrt{-15})$ is unramified.

5. [3pts] Let $\alpha^3 - \alpha - 1 = 0$. Show that the extension $\mathbb{Q}(\alpha, \sqrt{-23})/\mathbb{Q}(\sqrt{-23})$ is unramified.

0.2 Additional Exercises

1. [10pts] The goal of this problem is to give an approach for defining the relative norm of an ideal that parallels our definition of the relative norm of an element. Let L/K be an extension of number fields.

   We first do the Galois case, so suppose L/K is Galois with Galois group G. For an ideal I of $\mathcal{O}_L$, define its relative ideal norm $N_{L/K}(I)$ to be the intersection $\mathcal{O}_K \cap \prod_{\sigma \in G} \sigma(I)$.

   (a) Show that for a prime ideal Q of $\mathcal{O}_L$ lying over a prime ideal P of $\mathcal{O}_K$, we have $N_{L/K}(Q) = P^{f(Q|P)}$. [Hint: First show that for any ideal J of $\mathcal{O}_K$ it is true that $J = J\mathcal{O}_L \cap K$.]

   (b) Show that for any ideal I of $\mathcal{O}_L$, it is true that $N_{L/K}(I)\mathcal{O}_L = \prod_{\sigma \in G} \sigma(I)$.

   (c) Show that the relative ideal norm is completely multiplicative: $N_{L/K}(IJ) = N_{L/K}(I)N_{L/K}(J)$ for any ideals I, J of $\mathcal{O}_L$.

   (d) Show that for the principal ideal $I = \alpha\mathcal{O}_L$, the norm ideal $N_{L/K}(I)$ is principal and generated by the element norm $N_{L/K}(\alpha)$.

   (e) Show that if $L/\mathbb{Q}$ is Galois, then $N_{L/\mathbb{Q}}(I)$ is the principal ideal of $\mathbb{Z}$ generated by the ideal norm $N_L(I) = [\mathcal{O}_L : I]$. (In particular, when $L = \mathbb{Q}(\sqrt{D})$, we can compute ideal norms by finding a generator for $N_{L/\mathbb{Q}}(I) = I \cdot \overline{I}$ where $\overline{I} = \{\overline{r} : r \in I\}$ is the conjugate of I.)

   In the non-Galois case, we use (a) to motivate the definition: for a prime ideal Q lying over P, we set $N_{L/K}(Q) = P^{f(Q|P)}$ and then extend multiplicatively to all ideals via their prime factorizations. Observe (trivially) that the ideal norm is completely multiplicative.

   (f) Show that if $L/K/F$ is an extension tower, then for any ideal I of $\mathcal{O}_L$ we have $N_{L/F}(I) = N_{K/F}(N_{L/K}(I))$.

   (g) Let $\hat{L}$ be the Galois closure of L/K and I be an ideal of $\mathcal{O}_L$. Show that $N_{L/K}(I) = \mathcal{O}_K \cap \prod_{\sigma \in S} \sigma(I)$, where S is a set of coset representatives for the subgroup H of $\mathrm{Gal}(\hat{L}/K)$ fixing L.

2. [4pts] The goal of this problem is to prove that in any number field extension L/K, there are infinitely many prime ideals P of $\mathcal{O}_K$ that split in $\mathcal{O}_L$ (i.e., are not inert and not ramified).

   (a) Suppose that $q(x)$ is a nonconstant polynomial with integer coefficients. Show that there are infinitely many primes for which $q(x)$ has a root modulo p. [Hint: If there are only finitely many, say $p_1, \dots, p_k$, pick some a with $q(a) = \pm p_1^{a_1} \cdots p_k^{a_k}$ and pick $b \equiv a \pmod{p_1^{a_1+1} \cdots p_k^{a_k+1}}$. If $q(b) = \pm p_1^{b_1} \cdots p_k^{b_k}$, show $b_i = a_i$ for all i.]

   (b) Show that there are infinitely many primes p that split in the Galois closure $\hat{L}/\mathbb{Q}$.

   (c) Show that there are infinitely many primes that split in L/K.

3. [4pts*] The goal of this problem is to give a lower bound on the power of p that divides the discriminant of a number field. So suppose K is a number field and p is a prime with prime ideal factorization $p\mathcal{O}_K = P_1^{e_1} \cdots P_k^{e_k}$.

   (a) Prove that $\mathrm{disc}(K)$ is divisible by p^s where $s = \sum_{i=1}^{k} [e(P_i|p) - 1] f(P_i|p)$.

   (b) Prove that if none of the primes P_i are wildly ramified, then the exact power of p dividing $\mathrm{disc}(K)$ is p^s, with s as in (a).