E. Dummit's Math 7315 ~ Algebraic Number Theory, Fall 2024 ~ Homework 5, due Thu Dec 5th.

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 (Nov 13)

1. [2pts*] Find the decomposition and inertia groups for the primes $(\sqrt{-2})$, $(1+\sqrt{-2})$, and (5) of $\mathbb{Q}(\sqrt{-2})$.
2. [2pts] Suppose L/K is a Galois extension with Galois group G and Q is a prime of $\mathcal{O}_L$ lying over P. Show that $D(Q|P) = G$ if and only if Q is the unique prime of $\mathcal{O}_L$ lying over P.
3. [3pts] Show that if D is a normal subgroup of G, then P is totally split from K to L_D, and if E is also normal, then each of the primes $Q_D^{(i)}$ of L_D above P are totally inert from L_D to L_E and then are totally ramified from L_E to L. (Thus, we obtain all of the splitting of P in the decomposition field, and then all of the inertia of P in the inertia field, whence the names for these fields.)

0.1.2 Exercises from (Nov 14)

1. [3pts*] Let $L = \mathbb{Q}(i, \sqrt{3})$. Analyze the factorization type of the primes 2, 3, and 5 in $\mathcal{O}_L$, and find the decomposition and inertia groups and fields for each associated prime.
2. [3pts] Suppose L/K is Galois and Q is a prime of $\mathcal{O}_L$ lying over the prime P of $\mathcal{O}_K$. Show that if $\sigma \in \mathrm{Gal}(L/K)$, then $D(\sigma Q|P) = \sigma D(Q|P)\sigma^{-1}$ and $E(\sigma Q|P) = \sigma E(Q|P)\sigma^{-1}$. Deduce that when G is abelian, all primes of $\mathcal{O}_L$ lying over P have the decomposition and the same inertia subgroups and subfields.
3. [3pts] Let $L = \mathbb{Q}(10^{1/3}, \zeta_3)$. Analyze the factorization types of the primes 2, 3, and 5 in $\mathcal{O}_L$, and find the decomposition and inertia groups and fields for each associated prime.
4. [2pts] Let p be a prime and H be a subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Show that $\alpha = \sum_{\sigma \in H} \sigma(\zeta_p)$ is a generator for the fixed field of H.
5. [2pts] Let $L = \mathbb{Q}(\zeta_{31})$. Analyze the factorization types of the primes 2, 5, and 7 in $\mathcal{O}_L$, and find the decomposition and inertia groups and fields for each associated prime.

0.1.3 Exercises from (Nov 20)

1. [2pts] Suppose L/K is a number field extension and P is a prime of $\mathcal{O}_K$. Suppose that P is totally split / inert / ramified in L. Show that P is totally split / inert / ramified (respectively) in every subfield of L.
2. [3pts*] Let $K = \mathbb{Q}(\sqrt{D})$ have discriminant Δ and let p be an odd prime. Show the following equivalences:

   (a) p is ramified in $\mathbb{Q}(\sqrt{D}) \iff \Delta$ is zero mod $p \iff$ the Legendre symbol $\left(\frac{\Delta}{p}\right) = 0$.

   (b) p is split in $\mathbb{Q}(\sqrt{D}) \iff \Delta$ is a nonzero square mod $p \iff$ the Legendre symbol $\left(\frac{\Delta}{p}\right) = +1$.

   (c) p is inert in $\mathbb{Q}(\sqrt{D}) \iff \Delta$ is a nonsquare mod $p \iff$ the Legendre symbol $\left(\frac{\Delta}{p}\right) = -1$.
3. [1pt] If u is a primitive root modulo p and d divides $p-1$, show that the dth powers modulo p are u^d, u^{2d}, ... , u^{p-1}. Deduce again that a is a dth power mod p if and only if the order of a divides $(p-1)/d$.
4. [3pts] By comparing the splitting of p in $\mathbb{Q}(\zeta_8)$ to that of 2 in $\mathbb{Q}(\sqrt{p^*})$, show that $\left(\frac{2}{p}\right) = +1$ when $p \equiv 1, 3 \pmod 8$ and $\left(\frac{2}{p}\right) = -1$ when $p \equiv 5, 7 \pmod 8$.

0.1.4 Exercises from (Nov 21)

1. [2pts] Suppose L/K is Galois with Q of $\mathcal{O}_L$ lying over P of $\mathcal{O}_K$. Show that if $Q' = \sigma(Q)$ is another prime lying above P for some $\sigma \in \mathrm{Gal}(L/K)$, then the corresponding Frobenius element for $\sigma Q|P$ is given by the conjugate $\varphi_{\sigma Q|P} = \sigma \varphi_{Q|P} \sigma^{-1}$.

2. [3pts*] Suppose $n = p^v k$ where p is prime and does not divide k, and let $K = \mathbb{Q}(\zeta_n)$ and P be a prime of $\mathcal{O}_K$ lying above p.

   (a) Show that the inertia field of $P|p$ is $\mathbb{Q}(\zeta_k)$. [Hint: Consider ramification.]

   (b) Suppose that K' is a subfield of K in which p is unramified. Show that $K \subseteq \mathbb{Q}(\zeta_k)$.

   (c) Show that the decomposition field of $P|p$ is the subfield of $\mathbb{Q}(\zeta_k)$ fixed by the automorphism $\zeta_k \mapsto \zeta_k^p$. [Hint: This is the Frobenius element.]

3. [3pts] Suppose n is not a prime power. For $K = \mathbb{Q}(\zeta_n)$ and $K_+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, show that the extension K/K_+ is unramified at finite primes, so that the different $d_{K/K_+} = 1$. [Hint: Write $n = p^v k$ where $k > 1$. If P is a prime of K lying over P_+ in K_+ lying over p in $\mathbb{Q}$, observe that $E(P|P_+) = E(P|p) \cap \{1, \sigma\}$ where σ is complex conjugation. Use the exercise above and $k > 1$ to see that $\sigma \notin E(P|p)$.]

4. [2pts] Suppose $\hat{L}$ is the Galois closure of L/K and $\hat{Q}$ is an unramified prime of $\hat{L}$ lying over Q of $\mathcal{O}_L$ lying over P of $\mathcal{O}_K$. Show that $\varphi_{\hat{Q}|Q} = \varphi_{\hat{Q}|P}^{f(Q|P)}$. [Hint: Both Frobenius elements act as power maps. How are the powers related?]

5. [2pts] Let L/K be a Galois extension with Galois closure $\hat{L}$. Show that the prime P of $\mathcal{O}_K$ splits completely in L if and only if the Frobenius conjugacy class for P is trivial. [Hint: Consider the sizes of the orbits.]

6. [3pts*] Let $m \geq 3$ and let a be relatively prime to m. Apply the Chebotarev density theorem to the element $a \in (\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ to conclude that the natural and analytic density of primes p with $p \equiv a \pmod{m}$ is $1/\varphi(m)$.

7. [2pts] Let $g(x)$ be a polynomial irreducible over $\mathbb{Q}$. Prove that the discriminant of g is a square if and only if the Galois group of $g(x)$ is a subgroup of A_n.

8. [5pts] Find the probable Galois group for each polynomial below, given its factorization modulo the 100 smallest primes not dividing its discriminant Δ:

   (a) $g(x) = x^5 - x^2 - 2x - 3$, with $\Delta = 17^2 \cdot 29^2$.

Factorization Type	1	2,2	3	5
# Appearances	1	20	30	49

   (b) $g(x) = x^5 - 5x^3 + 5x - 20$, with $\Delta = 2^4 \cdot 3^4 \cdot 5^5 \cdot 11^2$.

Factorization Type	1	2,2	4	5
# Appearances	3	26	52	19

   (c) $g(x) = x^6 + x^4 + 23$, with $\Delta = -2^6 \cdot 23^3$.

Factorization Type	1	2,2	2,2,2	3,3	4
# Appearances	3	9	27	36	24

   (d) $g(x) = x^6 - 6x^3 - 6x^2 - 6x - 2$, with $\Delta = 2^6 \cdot 3^6 \cdot 13^2$.

Factorization Type	2,2	2,4	3	3,3	5
# Appearances	8	24	13	14	41

   (e) $g(x) = x^7 - 14x^5 + 56x^3 - 56x - 22$, with $\Delta = 2^6 \cdot 7^{10}$.

Factorization Type	1	3,3	7
# Appearances	2	68	30

9. [5pts] Suppose that $q(x) \in \mathbb{Z}[x]$ is an irreducible monic polynomial of degree n.

   (a) Suppose that the Galois group over $\mathbb{Q}$, considered as a subgroup of S_n, contains no n-cycles. Prove that $q(x)$ is reducible modulo p for every prime p. Show that $x^4 + 1$ is an example of such a polynomial.

   (b) Suppose that n is even and the discriminant of $q(x)$ is a perfect square. Prove that q is reducible modulo p for every prime p.

0.1.5 Exercises from (Nov 25)

1. [2pts] Suppose L/K is a number field extension and Q is a prime of $\mathcal{O}_L$ that is wildly ramified over the prime P of $\mathcal{O}_K$. If Q (and P) lie over the integer prime p, show that $p \leq [L:K]$.

2. [2pts*] Show that the only prime that can be wildly ramified in a quadratic extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ is 2, and that this occurs if and only if $D \equiv 3 \pmod 4$.

3. [1pt] Suppose that $\psi : G \to R$ is a function from a group G to a ring R with 1 such that $\psi(g_1 g_2) = \psi(g_1)\psi(g_2)$ for all $g_1, g_2 \in G$ and $\psi(1_G) = 1_R$. Show that ψ is a group homomorphism of G into the unit group of R.

4. [2pts] Let L/K be a Galois extension of number fields with Q a prime of $\mathcal{O}_L$ lying above the prime P of $\mathcal{O}_K$. Show that the decomposition and inertia groups $D(Q|P)$ and $E(Q|P)$ are solvable groups.

5. [2pts] Let L/K be a Galois extension whose Galois group is not solvable (e.g., S_5) and let P be a prime of $\mathcal{O}_K$. Show that P cannot be totally inert or totally ramified in L.

6. [1pt] Let L/K be a Galois extension with Q a prime of $\mathcal{O}_L$. Let $\pi \in Q \backslash Q^2$ and define $S_{-1} = G \backslash V_0$ and $S_m = V_m \backslash V_{m+1}$ for each $m \geq 0$. For any $\sigma \in S_m$, show that the exact power of Q dividing $\pi - \sigma(\pi)$ is Q^m. [Hint: Apply higher ramification group property (4).]

7. [4pts] Let L/K be a Galois extension with Q a totally ramified prime of $\mathcal{O}_L$. Suppose $\pi \in Q \backslash Q^2$ has $L = K(\pi)$ and π has minimal polynomial $m(x) \in \mathcal{O}_K[x]$ over K. Show that the exact power of Q dividing the different $D_{L/K}$ is the same as that dividing $m'(\pi)$. [Hint: Let $A = \mathbb{Z} \oplus \mathbb{Z}\pi \oplus \cdots \oplus \mathbb{Z}\pi^{n-1}$ where $n = [L:K]$ and let $I = \{r \in \mathcal{O}_K : r\mathcal{O}_L \subseteq A\}$. Show that $\mathcal{O}_L^* \subseteq A^* \subseteq (I\mathcal{O}_L)^*$ and deduce that $D_{L/K}$ divides $(A^*)^{-1} = (m'(\pi))$ divides $D_{L/K} I$. Finish by using total ramification to see that Q does not divide I.]

8. [2pts] Verify Hilbert's formula for the ramified primes $(1+i)$ in $\mathbb{Q}(i)$, $(\sqrt{5})$ in $\mathbb{Q}(\sqrt{5})$, and $(1-\zeta_9)$ in $\mathbb{Q}(\zeta_9)/\mathbb{Q}$.

9. [4pts] Let $p^d > 2$ be a prime power and let $K = \mathbb{Q}(\zeta_{p^d})$ and $Q = (1-\zeta_{p^d})$ be the totally ramified prime above p, which is the only ramified prime of K.

   (a) Find the ramification groups V_0 and V_1. [Hint: Sylow p-subgroup.]

   (b) Show that $\mathrm{disc}(K) = \pm p^{d\varphi(p^d) - p^{d-1}}$. [Hint: Adapt the calculation of $\mathrm{disc}(\mathbb{Q}(\zeta_p))$.]

   (c) Show that each of the quotients V_m/V_{m+1} is either trivial or cyclic of order p.

   (d) For fixed p and with $d = 2$, find the order of each group V_m for $m \geq 0$.

0.1.6 Exercises from (Dec 2)

0.1.7 Exercises from (Dec 4)

To be added

0.2 Additional Exercises

1. [7pts] The goal of this problem is to prove that there are only finitely many number fields with a given discriminant X, a result originally due to Hermite. Suppose that K is a number field of signature (r, s) and discriminant Δ with real embeddings $\sigma_1, \ldots, \sigma_r$ and nonreal embeddings $\tau_1, \overline{\tau_1}, \ldots, \tau_s, \overline{\tau_s}$.

   (a) Suppose $r > 0$. Show that there exists an element $\alpha \in \mathcal{O}_K$ such that $|\sigma_1(\alpha)| \leq \frac{1}{2}(\frac{\pi}{2})^{-s}\sqrt{\Delta}$, $|\sigma_i(\alpha)| \leq \frac{1}{2}$ for $2 \leq i \leq r$, and $|\tau_j(\alpha)| \leq \frac{1}{2}$ for all $1 \leq j \leq s$, and that $K = \mathbb{Q}(\alpha)$. [Hint: Note that all other conjugates of α other than $\sigma_1(\alpha)$ have absolute value less than 1, so they cannot equal α.]

   (b) Suppose $r = 0$. Show that there exists an element $\alpha \in \mathcal{O}_K$ such that $|\mathrm{Re}(\tau_1(\alpha))| \leq \frac{1}{2}$, $|\mathrm{Im}(\tau_1(\alpha))| \leq \frac{1}{2}(\frac{\pi}{2})^{-2}\sqrt{\Delta}$, and $|\tau_j(\alpha)| \leq \frac{1}{2}$ for all $2 \leq j \leq s$, and that $K = \mathbb{Q}(\alpha)$.

   (c) Suppose that $\alpha \in \mathcal{O}_K$ has all of its absolute values bounded by a constant M. Show that there are only finitely many possible α.

   (d) Show that there are finitely many number fields of signature (r, s) with discriminant X. Deduce that there are finitely many number fields with discriminant X.

   Remark: Let $N_n(X)$ denote the number of degree-n number fields with absolute discriminant at most X, up to isomorphism. Results establishing $N_n(X) \sim X$ for $n = 2$ are classical, for $n = 3$ are due to Davenport and Heilbronn, for $n = 4$ are due to Cohen and Diaz y Diaz, and for $n = 5$ are due to Bhargava and Shankar. For arbitrary n the estimate $N_n(X) \ll X^{(n+2)/4}$ is due to Schmidt, and has subsequently been improved for by Ellenberg and Venkatesh, Couveignes, and Thorne and Lemke Oliver. More precise heuristics for the number of extensions $N_n(X; G)$ whose Galois group is isomorphic to G are due to Kluners and Malle, subsequently generalized by Bhargava and others, and improvements in these bounds over those for general degree-n extensions for general G and specific classes of G have been made by Ellenberg, Venkatesh, Bhargava, Shankar, X. Wang, Matchett Wood, Dummit, Alberts, J. Wang, Mehta, Lemke Oliver, and numerous others.

2. [12pts*] The goal of this problem is to study the possible splitting behaviors of a prime in a biquadratic extension $\mathbb{Q}(\sqrt{a}, \sqrt{b})$. So let a and b be distinct squarefree integers and set $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$.

   (a) Show that $L/\mathbb{Q}$ is a Galois extension of degree 4 with Galois group isomorphic to the Klein 4-group and with generators σ, τ with $\sigma(\sqrt{a}, \sqrt{b}) = (-\sqrt{a}, \sqrt{b})$ and $\tau(\sqrt{a}, \sqrt{b}) = (\sqrt{a}, -\sqrt{b})$.

   (b) Deduce that L has three quadratic subfields given by $\mathbb{Q}(\sqrt{a})$,$\mathbb{Q}(\sqrt{b})$, and $\mathbb{Q}(\sqrt{ab}) = \mathbb{Q}(\sqrt{ab/\gcd(a,b)^2})$.

   Now let p be an integer prime and Q be a prime of $\mathcal{O}_L$ lying over p. We would like to identify all of the possible factorization behaviors for p in the three quadratic subfields, and in L.

   (c) Show that p cannot ramify in only one of the quadratic subfields. [Hint: Consider discriminants. The argument involves some casework for $p = 2$.]

   (d) Show that if p is ramified in all three quadratic subfields, then $p = 2$ and $(p) = Q^4$ in $\mathcal{O}_L$. Give an example where this occurs.

   (e) Show that if p is ramified in two quadratic subfields and inert in the other then $(p) = Q^2$ in $\mathcal{O}_L$, and give an example. [Hint: For inertness, make $(\frac{D}{p}) = -1$ where D is the discriminant of the unramified field.]

   (f) Show that if p is ramified in two quadratic subfields and split in the other then $(p) = Q_1^2 Q_2^2$ in $\mathcal{O}_L$, and give an example.

   (g) Show that if p is unramified in L, then it must be inert in either 0 or 2 of the quadratic subfields. [Hint: Use multiplicativity of the Legendre symbol for odd p, and the fact that the discriminants must be 1 mod 4 for $p = 2$.]

   (h) If p splits in all three quadratic subfields, show that $(p) = Q_1 Q_2 Q_3 Q_4$ in $\mathcal{O}_L$, and give an example.

   (i) If p is inert in two quadratic subfields and splits in one, show $(p) = Q_1 Q_2$ in $\mathcal{O}_L$, and give an example.

   (j) Show that the cases listed above exhaust all of the possibilities.

3. [5pts] The gosl of this problem is to demonstrate a connection between totally ramified primes and Eisenstein-irreducible polynomials. So suppose L/K is an extension of number fields and let P be a prime of $\mathcal{O}_K$ lying under Q in $\mathcal{O}_L$. We say a monic polynomial $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ in $\mathcal{O}_K[x]$ is Eisenstein at P when each $a_i \in P$ and $a_0 \notin P^2$; the theorem of Eisenstein-Schonemann shows that such polynomials are irreducible.

   (a) Suppose that $\alpha \in \mathcal{O}_L$ has $L = K(\alpha)$ and that the minimal polynomial $m(x)$ for α over K is Eisenstein at the prime ideal P. Show that P is totally ramified in L. [Hint: Use m to see $\alpha^n \in P$ hence $\alpha \in P$ hence Q^e divides all a_i. If $[L : K] \geq e(Q|P) + 1$ show $a_0 = -(\alpha^n + \cdots + a_1\alpha) \in Q^{e+1}$, contradicting $a_0 \notin P^2$.]

   (b) Conversely, suppose that P is totally ramified in L and suppose $\alpha \in Q \backslash Q^2$ has $L = K(\alpha)$. Show that the minimal polynomial $m(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ of α is Eisenstein at P. [Hint: Note that $m(x) = \prod_\sigma (x - \sigma(\alpha))$ and all $\sigma(\alpha) \in Q$; deduce each $a_i \in P$ and that since $\alpha \notin Q^2$ that $\prod_\sigma \sigma(\alpha) \notin P^2$.]

4. [8pts] The goal of this problem is to prove the following result: If a and b are integers such that $m(x) = x^3 + ax + b$ is irreducible and $\Delta = -4a^3 - 27b^2$ is squarefree, then the class number of the field $\mathbb{Q}(\sqrt{\Delta})$ is divisible by 3. So let α be a root of $m(x)$ with $K = \mathbb{Q}(\alpha)$ and let L be the Galois closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$.

   (a) Show that L has degree 6 over $\mathbb{Q}$, the Galois group of $L/\mathbb{Q}$ is S_3, the extension $L/\mathbb{Q}(\sqrt{\Delta})$ is abelian, and that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

   (b) Show that the infinite primes are unramified in $L/\mathbb{Q}(\sqrt{\Delta})$. [Hint: Show that if Δ is negative, $\mathbb{Q}(\alpha)$ has one real and two complex embeddings, and if Δ is positive, it has three real embeddings.]

   (c) Show that the finite primes are unramified in $L/\mathbb{Q}(\sqrt{\Delta})$. [Hint: If P is a finite prime lying above $p \in \mathbb{Z}$ that ramifies, show it is totally ramified and deduce $3|e(P|p)$. Conclude $p\mathcal{O}_k = Q^3$ for some ideal Q and then that p^2 divides Δ.]

   (d) Conclude that the Hilbert class field of $Q(\sqrt{\Delta})$ contains L, and deduce that the class number of $Q(\sqrt{\Delta})$ is divisible by 3.

   (e) Find five examples of discriminants Δ meeting the criteria of this problem.