**18.785 Number Theory** **Fall 2025**
**Problem Set #11** **Due: 12/5/2025**

---

### Description

These problems are related to Lectures 18–20. Your solutions should be written up in latex and submitted as a pdf-file to Gradescope by midnight on the date due.

**Instructions:** Solve any combination of problems that sum to 100 points, or **alternatively, solve any combination of problems that sum to 200 points to receive credit for two problem sets**. Collaboration is permitted/encouraged, but you must identify your collaborators (including any LLMs you consulted) and any references you consulted outside the course syllabus. Include this information after the **Collaborators/Sources** prompt at the end of the problem set (if there are none, you should enter "none", do not leave it blank). Note that each student is expected to write their own solutions; it is fine to discuss problems with others, but your writing must be your own.

### Problem 1. Higher ramification groups (49 points)

Let $A$ be a complete DVR with finite residue field; its fraction field $K$ is a nonarchimedean local field (Prop. 9.6). Let $L$ be a finite Galois extension of $K$, let $G := \mathrm{Gal}(L/K)$, and let $B$ be the integral closure of $A$ in $L$, with maximal ideal $\mathfrak{q} = (\pi)$. Fix $\alpha \in B$ so that $B = A[\alpha]$ (via Theorem 10.14), and let $f \in A[x]$ be the minimal polynomial of $\alpha$.

The decomposition group $D_\mathfrak{q}$ is equal to $G$ (since $\sigma(\mathfrak{q}) = \mathfrak{q}$ for all $\sigma \in G$), and the inertia subgroup is $I_\mathfrak{q} := \{\sigma \in G : \sigma(x) \equiv x \bmod \mathfrak{q} \text{ for all } x \in L\}$ with order equal to the ramification index $e := e_\mathfrak{q}$. For any integer $i \geq -1$ define

$$G_i := \{\sigma \in G : \sigma(x) \equiv x \bmod \mathfrak{q}^{i+1} \text{ for all } x \in B\},$$

so that $G_{-1} = G$ and $G_0$ is the inertia subgroup. The group $G_i$ is the $i$th *ramification group* of $G$ (in the lower numbering). Define $i_G : G \to \mathbb{Z} \cup \{\infty\}$ by $i_G(\sigma) := v_\mathfrak{q}(\sigma(\alpha) - \alpha)$.

**(a)** Prove that $G_i = \{\sigma \in G : i_G(\sigma) \geq i + 1\}$, show that $G_{i+1}$ is a normal subgroup of $G_i$, and show that the groups $G_i$ are trivial for all sufficiently large $i$.

Recall that the different ideal $\mathcal{D} := \mathcal{D}_{B/A}$ is equal to $(f'(\alpha))$ and satisfies the bounds

$$e - 1 \leq v_\mathfrak{q}(\mathcal{D}) \leq e - 1 + v_\mathfrak{q}(e),$$

with $e - 1 = v_\mathfrak{q}(\mathcal{D})$ if and only if $v_\mathfrak{q}(e) = 0$, by Proposition 12.23 and Theorem 12.26.

**(b)** Prove Hilbert's *different formula*:

$$v_\mathfrak{q}(\mathcal{D}) = \sum_{\sigma \neq 1} i_G(\sigma) = \sum_{i \geq 0} (\#G_i - 1).$$

Let $U_0 := B^\times$ be the unit group of $B$, and for $i > 0$ define

$$U_i := 1 + \mathfrak{q}^i = \{x \in U_0 : x \equiv 1 \bmod \mathfrak{q}^i\}.$$

**(c)** Show that $U_0/U_1 \simeq (B/\mathfrak{q})^\times$ and that for $i > 0$ we have $U_i/U_{i+1} \simeq \mathfrak{q}^i/\mathfrak{q}^{i+1}$ isomorphic to the additive group of $B/\mathfrak{q}$. Conclude that $L/K$ is tamely ramified if and only if $G_1$ is trivial and totally wildly ramified if and only if $G = G_1$.[1]

**(d)** Show that for $i \geq 0$ the map $\phi\colon \sigma \mapsto \sigma(\pi)/\pi$ defines a homomorphism $\phi_i\colon G_i \to U_i$ that induces an injection $G_i/G_{i+1} \hookrightarrow U_i/U_{i+1}$ (in other words, the composition of $\phi_i$ with the quotient map $U_i \to U_i/U_{i+1}$ has kernel $G_{i+1}$). Conclude that (i) $G_0/G_1$ is cyclic of order prime to $p$, (ii) $G_1$ is the unique $p$-Sylow subgroup of $G_0$, (iii) $G_i/G_{i+1}$ an abelian $p$-group for all $i \geq 1$, and (iv) $G = \mathrm{Gal}(L/K)$ is solvable.

**(e)** Suppose that $\sigma \in G_i - G_{i+1}$ and $\tau \in G_j - G_{j+1}$ with $1 \leq i \leq j$. Show that $\phi(\sigma\tau) - \phi(\tau\sigma) \equiv (j-i)u\pi^{i+j} \bmod \mathfrak{q}^{i+j+1}$ for some $u \in U_0$ and that this implies $\phi(\sigma\tau\sigma^{-1}\tau^{-1}) \equiv 1 + (j-i)u\pi^{i+j} \bmod \mathfrak{q}^{i+j+1}$. Then use this to show $i \equiv j \bmod p$.

Let $K = \mathbb{Q}_p$ with $p$ odd, and let $L/\mathbb{Q}_p$ be a totally wildly ramified abelian extension, so in the notation above, $\mathrm{Gal}(L/K) = G = G_0 = G_1$, and $\mathcal{D}$ is the different ideal.

**(f)** Show that $v_\mathfrak{q}(\mathcal{D}) = 2p-2$ if $[L:K] = p$ and $v_\mathfrak{q}(\mathcal{D}) = 3p^2 - p - 2$ if $[L:K] = p^2$.

**(g)** Prove that $G$ is cyclic (hint: reduce to $[L:K] = p^2$ then show that if $H \leq G$ has order $p$ then $H = G_{p+1}$ by computing the different of $L/L^H$ using **(b)** and **(f)**).

## Problem 2. Polar density (49 points)

Let $K$ be a number field and let $S$ be a set of primes of $K$. Recall the *Dirichlet density*

$$d(S) := \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} \mathrm{N}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} \mathrm{N}(\mathfrak{p})^{-s}} = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} \mathrm{N}(\mathfrak{p})^{-s}}{\log \frac{1}{s-1}},$$

and the *natural density*

$$\delta(S) := \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in S : \mathrm{N}(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{p} : \mathrm{N}(\mathfrak{p}) \leq x\}},$$

which are defined whenever these limits exist. As shown on Problem Set 9, if $\delta(S)$ exists then so does $d(S) = \delta(S)$ (you may use this fact even if you did not prove it).

**Definition.** The *partial Dedekind zeta function* associated to $S$ is the complex function

$$\zeta_{K,S}(s) := \prod_{\mathfrak{p}\in S} (1 - \mathrm{N}(\mathfrak{p})^{-s})^{-1}.$$

If for some integer $n \geq 1$ the function $\zeta_{K,S}^n$ extends to a meromorphic function on a neighborhood of 1, the *polar density* of $S$ is defined by

$$\rho(S) := \frac{m}{n}, \qquad m = -\operatorname{ord}_{s=1} \zeta_{K,S}^n(s).$$

**(a)** Show that $\rho(S)$ is well defined (so $m/n$ does not depend on the choice of $n$).

**(b)** Prove that $\delta(S) = d(S) = \rho(S)$ whenever $\rho(S)$ exists.

[1] The group $G_1$ is sometimes called the *wild inertia group*.

**(c)** Show that $\rho(S)=0$ when $S$ is finite and $\rho(S)=1$ when $S$ is cofinite.

**(d)** Show that $S\subseteq T$ implies $\rho(S)\le\rho(T)$ whenever both densities exist.

**(e)** Let $\mathcal{P}_1$ denote the set of degree-1 primes of $K$ (those of prime norm). Prove that $\rho(\mathcal{P}_1)=1$ and $\rho(S\cap\mathcal{P}_1)=\rho(S)$ whenever $S$ has a polar density.

**(f)** Let $L/K$ be a Galois extension and let $\mathrm{Spl}(L/K)$ be the set of primes of $K$ that split completely in $L$. Prove that $\rho(\mathrm{Spl}(L/K))=1/[L:K]$. Conclude that for $G=\mathrm{Gal}(L/K)$ and any normal subgroup $H\subseteq G$, the set $S$ of primes $\mathfrak{p}$ of $K$ for which the Frobenius conjugacy class $\mathrm{Frob}_{\mathfrak{p}}$ lies in $H$ has polar density $\rho(S)=\#H/\#G$.

**(g)** Prove that if $L/K$ and $M/K$ are Galois extensions of $K$ then $\mathrm{Spl}(M)=\mathrm{Spl}(L)$ if and only if $M=L$.

## Problem 3. The Frobenius density theorem (49 points)

Let $L/K$ be a Galois extension of number fields of finite degree $n$ with Galois group $G:=\mathrm{Gal}(L/K)$. Recall that for each unramified prime $\mathfrak{p}$ of $K$, the *Frobenius class* $\mathrm{Frob}_{\mathfrak{p}}$ is the conjugacy class of the Frobenius elements $\sigma_{\mathfrak{q}}$ for $\mathfrak{q}|\mathfrak{p}$.

The *Chebotarev density theorem* states that for any set $C\subseteq G$ stable under conjugation (a union of conjugacy classes), the set of unramified primes $\mathfrak{p}$ with $\mathrm{Frob}_{\mathfrak{p}}\subseteq C$ has Dirichlet density $\#C/\#G$.[2] In this problem you will prove the *Frobenius density theorem*, which says essentially the same thing, but with a different notion of conjugacy.

**Definition.** Two elements $g$ and $h$ of a group $G$ are *quasi-conjugate* if they generate conjugate subgroups $\langle g\rangle$ and $\langle h\rangle$.

**(a)** Show that quasi-conjugacy is an equivalence relation and that each quasi-conjugacy class in a group is a union of conjugacy classes.

**(b)** Show that in the symmetric group $S_n$, each quasi-conjugacy class is actually a conjugacy class (so the Frobenius density theorem implies the Chebotarev density theorem in this case), but that this is generally not true for the alternating group $A_n$.

**(c)** Suppose $G$ is cyclic. For each $d|n$, let $S_d$ be the set of primes $\mathfrak{p}$ of $K$ for which the primes $\mathfrak{q}|\mathfrak{p}$ have inertia degree $f_{\mathfrak{q}}=d$. Prove that the set $S_d$ has polar density $\rho(S_d)=\phi(d)/[L\!:\!K]$ and conclude that infinitely many primes of $K$ are inert in $L$.

Fix $\sigma\in G$, let $K'=L^\sigma$ be its fixed field, let $H=\langle\sigma\rangle\subseteq G$, and let $d=\#H$. Recall that in any number field, a *degree-1 prime* is a prime whose absolute norm is prime. For each prime $\mathfrak{p}$ of $K$ (resp. $K'$) that is unramified in $L$, let $\overline{\mathrm{Frob}}_{\mathfrak{p}}$ denote the quasi-conjugacy class in $G$ (resp. $H$) that contains the conjugacy class $\mathrm{Frob}_{\mathfrak{p}}$.

**(d)** Let $S'$ be the set of degree-1 primes $\mathfrak{p}'$ of $K'$ for which $\mathfrak{p}=\mathfrak{p}'\cap\mathcal{O}_K$ is unramified in $L$ and for which $\sigma\in\overline{\mathrm{Frob}}_{\mathfrak{p}'}$. Prove that $S'$ has polar density $\rho(S')=\phi(d)/d$.

**(e)** Let $S$ be the set of unramified degree-1 primes $\mathfrak{p}$ of $K$ for which $\sigma\in\overline{\mathrm{Frob}}_{\mathfrak{p}}$. Show that map $\mathfrak{p}'\mapsto\mathfrak{p}'\cap\mathcal{O}_K$ defines a surjective map $\pi\colon S'\to S$.

[2] It also has this natural density, but this was proved later.

**(f)** Show that the fibers of $\pi$ all have cardinality $[K' : K]/c$, where $c$ is the number of distinct conjugates of $H$ in $G$.

**(g)** Show that $S$ has polar density

$$\rho(S) = \frac{c\phi(d)}{[L:K]}.$$

**(h)** Prove that for any set $C \subseteq G$ stable under quasi-conjugation the set of unramified primes $\mathfrak{p}$ of $K$ with $\overline{\mathrm{Frob}_\mathfrak{p}} \subseteq C$ has polar density $\#C/\#G$.

## Problem 4. The Hilbert symbol (98 points)

Let $K$ be a local field whose characteristic is not 2.

**Definition.** The *local Hilbert symbol* is the map $(\cdot,\cdot)\colon K^\times/K^{\times 2} \times K^\times/K^{\times 2} \to \{\pm 1\}$

$$(a,b) := \begin{cases} 1 & \text{if } ax^2 + by^2 = 1 \text{ has a solution in } K, \\ -1 & \text{otherwise.} \end{cases}$$

Here and throughout this problem $a, b \in K^\times$ are understood to represent elements of $K^\times/K^{\times 2}$ whenever the context requires it.

**(a)** Prove that the Hilbert symbol satisfies:

- **(i)** $(a,b) = (b,a)$ (symmetry);
- **(ii)** $(a,bc) = (a,b)(a,c)$ and $(ab,c) = (a,c)(b,c)$ (bilinearity);
- **(iii)** For any $a \in K^\times$, if $(a,b) = 1$ for all $b \in K^\times$ then $a \in K^{\times 2}$ (nondegeneracy).
- **(iv)** $(a, 1-a) = 1$ (for $a \neq 1$) and $(a,-a) = 1$ (Steinberg relations).

**(b)** In part (a) where (if anywhere) did you use the fact that $K$ is a local field? Determine which of (i)-(iv) hold for all fields whose characteristic is not 2, and for those that do not, give explicit counterexamples.

**(c)** Prove that for $a \notin K^{\times 2}$ we have $(a,b) = 1$ if and only if $b \in \mathrm{N}_{K(\sqrt{a})/K}(K(\sqrt{a})^\times)$.

**(d)** Let $L/K$ be an abelian extension. Let $r_{L/K}\colon K^\times/\mathrm{N}_{L/K}(L^\times) \to \mathrm{Gal}(L/K)$ be the isomorphism given by Artin reciprocity, and $\langle\cdot,\cdot\rangle := \mathrm{Gal}(\overline{K}/K) \times K^\times/K^{\times 2} \to \{\pm 1\}$ the Kummer pairing $\langle \sigma, a\rangle := \sigma(\sqrt{a})/\sqrt{a}$ (which can be applied to $\sigma \in \mathrm{Gal}(L/K)$ whenever $L \subset \overline{K}$ contains $\sqrt{a}$). Prove that the Hilbert symbol satisfies

$$(a,b) = \left\langle r_{K(\sqrt{b})/K}(a), b \right\rangle.$$

**(e)** For $a, b, c \in K^\times$ prove $ax^2 + by^2 = c$ has a solution if and only if $(-ab, c) = (a,b)$.

**(f)** For $a, b \in K^\times$ define the quaternion algebra $H_{a,b}$ as the $K$-algebra $K(i,j)$ with $i^2 = a$, $j^2 = b$, $ij = -ji$. Show that $(a,b) = 1$ if and only if $H_{a,b} \simeq \mathrm{M}_2(K)$, the $2 \times 2$ matrix algebra over $K$ (such quaternion algebras are said to *split*). Then show that $H_{a,b} \simeq H_{a,c}$ if and only if $[b] = [c]$ in $K^\times/N_{K(\sqrt{a})/K}(K(\sqrt{a})^\times)$ and deduce that the isomorphism class of $H_{a,b}$ depends only on the Hilbert symbol $(a,b)$.

**(g)** Show that for archimedean $K$ we have $(a, b) = -1$ if and only if $K \simeq \mathbb{R}$ and $a, b < 0$.

**(h)** Suppose that $K$ is nonarchimedean with residue field of odd cardinality $q$. Let $\mathcal{O}$ be its valuation ring, $\pi$ a uniformizer for $\mathcal{O}$. Define the residue symbol

$$\left(\frac{a}{\pi}\right) := \begin{cases} 1 & \text{if } \bar{a} \in \mathbb{F}_q^{\times 2}, \\ -1 & \text{if } \bar{a} \notin \mathbb{F}_q^{\times 2}, \end{cases}$$

where $\mathbb{F}_q := \mathcal{O}/(\pi)$ is the residue field (which does not depend on the choice of $\pi$). For $a, b \in K^\times$, let $a = u_a\pi^\alpha$, $b = u_b\pi^\beta$ with $u_a, u_b \in \mathcal{O}^\times$. Prove the *reciprocity law*:

$$(a, b) = (-1)^{\alpha\beta(q-1)/2} \left(\frac{u_a}{\pi}\right)^\beta \left(\frac{u_b}{\pi}\right)^\alpha.$$

**(i)** Now let $K$ be a global field of characteristic not 2, and for each place $v$ of $K$ let $(a, b)_v$ denote the Hilbert symbol of the completion of $K$ at $v$. Prove the *product formula*, which states that

$$\prod_v (a, b)_v = 1$$

for all $a, b \in K^\times$ (and in particular, $(a, b)_v = 1$ for all but finitely many places $v$).

Useful references for this problem if you get stuck are [4, Ch. III] and [5, §5.6].

## Problem 5. Profinite groups (98 points)

Recall that a topological space is *totally disconnected* if every pair of distinct points can be separated by open neighborhoods that partition the space; totally disconnected spaces are obviously Hausdorff.

**(a)** Show that products and inverse limits of totally disconnected compact topological spaces are totally disconnected and compact. Conclude that every profinite group is a totally disconnected compact group.

Let $G$ be a totally disconnected compact group, let $\widehat{G} := \varprojlim G/N$ be its profinite completion (so $N$ varies over finite index open normal subgroups of $G$ ordered by containment), and let $\phi\colon G \to \widehat{G}$ be the natural map that sends each $g \in G$ to its images in the finite quotients $G/N$.

**(b)** Show that every open subgroup of $G$ has finite index and contains an open normal subgroup (which necessarily also has finite index).

**(c)** Show that $\phi(G)$ is both dense in $\widehat{G}$ and closed, hence equal to $\widehat{G}$; thus $\phi$ is surjective.

**(d)** Show that to prove that $\phi$ is injective it suffices to show that the intersection of all open subgroups of $G$ is trivial. Then show that for every $g \in G - \{1\}$ there is a neighborhood $U$ of 1 that is both open and closed and does not contain $g$, and it is enough to show that every such $U$ contains an open subgroup $H$.

**(e)** Let $U$ be a neighborhood of 1 that is both open and closed. Show that $U$ contains an open neighborhood of 1 that is closed under multiplication and inversion, hence a subgroup (this requires some work; you will need to use the fact that the multiplication map $G \times G \to G$ is continuous and that $U$ is compact).

**(f)** Show that $\phi$ is a continuous open map, hence a homeomorphism. Conclude that $G$ is isomorphic to its profinite completion, and in particular, a profinite group.

**(g)** Show that for a profinite group $G$ the following are equivalent: (i) the topology of $G$ is induced by a metric, (ii) $G \simeq \varprojlim G_n$, with $n \in \mathbb{Z}_{\geq 1}$, the $G_n$ finite, and $G_{n+1} \to G_n$ surjective, (iii) the number of open subgroups of $G$ is countable.

**(h)** Show that the equivalent conditions (i)-(iii) in (g) imply that $G$ contains a countable dense subset (so $G$ is *separable* as a topological space), and give an example showing that the converse does not hold.

**(i)** Let $p$ be prime, let $\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$, and let $G_p := \prod_n \mathbb{Z}/p^n\mathbb{Z}$. Show that $G_p$ and $\mathbb{Z}_p \times (G_p/\mathbb{Z}_p)$ are isomorphic as groups. Are they isomorphic as topological groups?

**(j)** Show that $\widehat{\mathbb{Z}}^\times \simeq \widehat{\mathbb{Z}} \times \prod_n \mathbb{Z}/n\mathbb{Z}$ as topological groups.

A useful reference for this problem if you get stuck is Ribes and Zalesskii [3].

### Problem 6. Arithmetically equivalent number fields (98 points)

Two number fields are said to be *arithmetically equivalent* if their Dedekind zeta functions coincide. Isomorphic number fields obviously have the same zeta functions, but as proved by Gassmann [1], the converse need not hold. A particularly simple example is given by the fields $\mathbb{Q}(\sqrt[8]{a})$ and $\mathbb{Q}(\sqrt[8]{16a})$; as shown by Perlis [2], for $a \in \mathbb{Z}$ not square and not twice a square, these fields are arithmetically equivalent but nonisomorphic (they have the same Galois closure, which is obtained by adjoining a primitive 8th root of unity).

**(a)** Show that arithmetically equivalent number fields must have the same Galois closure (up to isomorphism). Conclude that if $K/\mathbb{Q}$ is Galois then $K'$ is arithmetically equivalent to $K$ if and only if $K' \simeq K$.

In view of (a) we now consider two non-Galois extensions $K$ and $K'$ of $\mathbb{Q}$ with Galois closure $L/\mathbb{Q}$. Let $G := \mathrm{Gal}(L/\mathbb{Q})$ and put $H := \mathrm{Gal}(L/K)$ and $H' := \mathrm{Gal}(L/K')$.

**(b)** Show that if $K$ and $K'$ are arithmetically equivalent number fields then for every prime $p$ there is a bijection between the primes of $K$ lying above $p$ and the primes of $K'$ lying above $p$ that preserves inertia degrees. Conclude that $K$ and $K'$ must have the same degree.

**(c)** Given a cyclic $C \subseteq G$, we can partition $G$ into double cosets $H\sigma_1 C, \ldots, H\sigma_g C$. When $H$ is not normal these cosets need not have the same size; each will have cardinality $f_i \cdot \#H$ for some integer $f_i \geq 1$. Assume the $f_i$ are in increasing order and call the tuple $(f_1, \ldots, f_g)$ the *coset type* of the pair $(H, C)$. Prove that if $p$ is a prime that is unramified in $L$ and $C$ is any decomposition group of $p$ in $G$, then the coset type of $(H, C)$ is equal to the tuple of inertia degrees of the primes of $K$ lying above $p$ when arranged in increasing order. Conclude that if $K$ and $K'$ are arithmetically equivalent then $(H, C)$ and $(H', C)$ have the same coset type for every cyclic subgroup $C$ of $G$.

**(d)** Two subgroups $H$ and $H'$ of a finite group $G$ are said to be *Gassmann equivalent* if for conjugacy class $c$ of elements in $G$ the sets $c \cap H$ and $c \cap H'$ have the same cardinality. Show that this holds if and only if for every cyclic group $C$ the coset types of $(H, C)$ and $(H', C)$ coincide.

**(e)** Suppose $H$ and $H'$ are Gassmann equivalent. Show that $K$ and $K'$ have the same number of real and complex places (hint: consider the "decomposition group" of the prime $p = \infty$ in $G$).

Like the Riemann zeta function, the Dedekind zeta function has a meromorphic continuation to $\mathbb{C}$ that satisfies a functional equation. Define $\Gamma_{\mathbb{R}}(s) := \pi^{-s/2}\Gamma(s/2)$ and $\Gamma_{\mathbb{C}}(s) := 2(2\pi)^{-s}\Gamma(s)$, and let

$$Z_K(s) := |D_K|^{s/2}\Gamma_{\mathbb{R}}(s)^{n_1}\Gamma_{\mathbb{C}}(s)^{n_2}\zeta_K(s),$$

where $n_1$ and $n_2$ are the number of real and complex places of $K$, respectively. Then

$$Z_K(s) = Z_K(1-s)$$

as meromorphic functions on $\mathbb{C}$ (you may assume this in what follows).

**(f)** Let $f(s) = f_1(s)/f_2(s)$ be a ratio of Euler products over a finite set of primes that extends to a meromorphic function on $\mathbb{C}$ that satisfies a functional equation $f(s) = g(s)f(1-s)$ for some meromorphic function $g(s)$ whose zeros and poles do not coincide with any zero or pole of $f$. Prove that $g(s) = 1$, then use this and the functional equations for $\zeta_K(s)$ and $\zeta_{K'}(s)$ to prove that if $H$ and $H'$ are Gassmann equivalent then $K$ and $K'$ are arithmetically equivalent.

**(g)** A *Gassmann triple* (or *Gassmann-Sunada triple*) is a triple $(G, X, Y)$ in which $G$ is a group that acts faithfully on sets $X$ and $Y$ such that every element of $G$ fixes the same number of elements in $X$ and $Y$ but $X$ and $Y$ are not isomorphic as $G$-sets. Show that $K$ and $K'$ are arithmetically equivalent but not isomorphic if and only if $(G, G/H, G/H')$ is a Gassmann triple, where $G/H$ and $G/H'$ denote sets of cosets (for consistency with part (c), use right cosets and put the $G$-action on the right).

**(h)** Show that if $K$ and $K'$ are arithmetically equivalent then they have the same normal core (largest subfield that is a normal extension of $\mathbb{Q}$). Use this to show that $K$ and $K'$ contain the same roots of unity and conclude that the unit groups $\mathcal{O}_K^\times$ and $\mathcal{O}_{K'}^\times$ are isomorphic as abelian groups.

**(i)** Show that if $K$ and $K'$ are arithmetically equivalent then $|\operatorname{disc}\mathcal{O}_K| = |\operatorname{disc}\mathcal{O}_{K'}|$ and conclude that $h_K R_K = h_{K'} R_{K'}$, where $h_K := \#\operatorname{Cl}\mathcal{O}_K$ is the class number and $R_K$ is the regulator of $K$ (and similarly for $K'$).

It is natural to ask whether the class numbers and regulators must also match. This is not the case; the arithmetically equivalent fields $K := \mathbb{Q}(\sqrt[8]{-15})$ and $K' := \mathbb{Q}(\sqrt[8]{-240})$ have class numbers 8 and 4, respectively (you do not need to prove this).

**(j)** You showed in (b) that in arithmetically equivalent fields the multisets of inertia degrees above any prime $p$ must match (including at ramified primes); it is natural to ask whether the same is true of the ramification indices. Show that this is not the case by showing that the polynomials $x^8 - 97$ and $x^8 - 16 \cdot 97$ (which you may assume define arithmetically equivalent fields $K$ and $K'$), do not have the same factorization pattern in $\mathbb{Q}_2[x]$. Conclude that the different ideals $\mathcal{D}_{K/\mathbb{Q}}$ and $\mathcal{D}_{K'/\mathbb{Q}}$ do not necessarily have the same factorization pattern, even though the discriminant ideals $D_{K/\mathbb{Q}} := \mathrm{N}_{K/\mathbb{Q}}(\mathcal{D}_{K/\mathbb{Q}})$ and $D_{K'/\mathbb{Q}} := \mathrm{N}_{K'/\mathbb{Q}}(\mathcal{D}_{K'/\mathbb{Q}})$ do.

A useful reference for this problem if you get stuck is Perlis' paper [2].

### Problem 7. Survey (2 points)

Complete the following survey by rating each problem you attempted on a scale of 1 to 10 according to how interesting you found it (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found it (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem to the nearest half hour.

| | Interest | Difficulty | Time Spent |
|---|---|---|---|
| Problem 1 | | | |
| Problem 2 | | | |
| Problem 3 | | | |
| Problem 4 | | | |
| Problem 5 | | | |
| Problem 6 | | | |

Please feel free to record any additional comments you have on the problem sets and the lectures, in particular, ways in which they might be improved.

**Collaborators/Sources**

## References


[1] F. Gassmann, *Bemerkungen zu der vorstehenden Arbeit von Hurwitz* (comments on *Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe*, by Hurwitz) Math. Z. **25** (1926), 655-665.

[2] R. Perlis, *On the equation $\zeta_K(s) = \zeta_{K'(s)}$*, J. Number Theory **9** (1977), 342–360.

[3] L. Ribes and P. Zalesskii, *Profinite groups*, 2nd edition, Springer, 2010.

[4] J.-P. Serre, *A course in arithmetic*, Springer, 1973.

[5] J. Voight, *Quaternion algebras*, Springer, 2021.