18.785 Number Theory **Fall 2021**

Problem Set #11

Description

These problems are related to the material covered in Lectures 23-27. Your solutions should be submitted as a pdf-file by midnight on the date due.

Collaboration is permitted/encouraged, but you must identify your collaborators or the name of your group on, as well any references you consulted that are not listed in the course syllabus. If there are none write "**Sources consulted: none**" at the top of your solution. Note that each student is expected to write their own solutions; it is fine to discuss the problems with others, but your work must be your own.

The first person to spot each typo/error in any of the problem sets or lecture notes will receive 1–5 points of extra credit, depending on the severity of the error.

Instructions: Solve 1 of the first 4 problems, then complete the survey problem 5.

Problem 1. The conductor ideal (96 points)

The goal of this problem is to analyze the conductor of an abelian extension of number fields (without assuming the results of class field theory). Recall that the conductor of an abelian extension L/K of number fields is a modulus for K whose values are defined in terms of local conductors

$$\mathfrak{c}(L/K)(v) := \mathfrak{c}(L_w/K_v) \in \mathbb{Z}_{\geq 0}$$

where v ranges over the places of K and w is any place of L that extends v. We can view $\mathfrak{c} := \mathfrak{c}(L/K)$ as a product of powers of places whose finite part is the $\mathcal{O}_K$-ideal $\prod_{\mathfrak{p}} \mathfrak{p}^{\mathfrak{c}(\mathfrak{p})}$.

The conductor of an extension of archimedean local fields has value 1 if it is non-trivial (isomorphic to $\mathbb{C}/\mathbb{R}$) and 0 otherwise. The conductor of a finite extension of nonarchimedean local fields L/K is the least integer n for which

$$U_K^n \subseteq \mathrm{N}_{L/K}(\mathcal{O}_L^\times)$$

where the groups $U_K^n \subseteq \mathcal{O}_K^\times$ are defined by $U_K^0 := \mathcal{O}_K^\times$ and $U_K^n := 1 + \mathfrak{p}^n$ for $n > 0$; here $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}_K$.

(a) Verify that the conductor of an abelian extension of number fields is well defined by showing that (1) it does not depend on the choice of the w's extending v, and (2) if L/K is a finite extension of nonarchimedean local fields then there is an integer n for which $U_K^n \subseteq \mathrm{N}_{L/K}(\mathcal{O}_L^\times)$. To prove (2), show that the groups U_K^n form a fundamental system of neighborhoods of the identity in the topological group $\mathcal{O}_K^\times$ (this means the cosets of the U_K^n form a basis for the topology).

(b) Show that if L/K is an abelian extension of number fields then the local extensions L_w/K_v are all abelian. Does the converse hold? That is, if L/K is a Galois extension of number fields for which L_w/K_v is abelian for every $v \in M_K$, is L/K necessarily abelian? (if your answer is no, give an explicit counter example).

(c) While not directly relevant to computing conductors, its worth noting that if you replace "abelian" with "solvable" in (b) the converse does not hold. Prove that in fact every Galois extension of local fields is solvable, even though many (most) extensions of number fields are not solvable.

Now let L/K be an abelian extension of local fields. The archimedean case is clear, so we assume L/K is nonarchimedean. Let $\mathbb{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$ denote the residue field.

(d) Show that $K^\times \simeq \mathbb{Z} \times U_K^0$, and that the reduction map $\mathcal{O}_K \to \mathbb{F}_\mathfrak{p}$ induces isomorphisms $U_K^0/U_K^1 \simeq \mathbb{F}_\mathfrak{p}^\times$ and $U_K^n/U_K^{n+1} \simeq \mathbb{F}_\mathfrak{p}$ for $n \geq 1$.

(e) Prove that if L/K is unramified then $\mathrm{N}_{L/K}(\mathcal{O}_L^\times) = \mathcal{O}_K^\times$ but $\mathrm{N}_{L/K}(L^\times) \neq K^\times$ unless $L = K$. Show that in fact $K^\times/\mathrm{N}_{L/K}(L^\times) \simeq \mathrm{Gal}(L/K)$ and both groups are cyclic.

(f) Prove that if L/K is totally ramified then $K^\times/\mathrm{N}_{L/K}(L^\times) \simeq \mathcal{O}_K^\times/\mathrm{N}_{L/K}(\mathcal{O}_L^\times)$.

(g) Prove that if L/K is totally tamely ramified then $\mathrm{N}_{L/K}(U_L^1) = U_K^1$ and the ramification index divides $\#\mathbb{F}_\mathfrak{p}^\times$.

(h) Prove that if L/K is totally wildly ramified then $\mathrm{N}_{L/K}(U_L^1) \neq U_K^1$.

(i) Show that the conductor of L/K takes the value 0 if and only if L/K is unramified, and otherwise takes the value 1 if and only if L/K is tamely ramified.

Useful references for this problem if you get stuck are [1, Ch. III] and [6, Ch. V].

Problem 2. The Hilbert symbol (96 points)

Let K be a local field whose characteristic is not 2.[1]

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 counter examples.

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

[1] Note that this excludes only extensions of $\mathbb{F}_2(t)$; extensions of $\mathbb{Q}_2$ are fine.

(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 $\langle\cdot,\cdot\rangle := \mathrm{Gal}(\overline{K}/K) \times K/K^{\times 2} \to \{\pm 1\}$ 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 2×2 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, π a uniformizer for $\mathcal{O}$. Define the residue symbol

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

where $\mathbb{F}_q := \mathcal{O}/(\pi)$ is the residue field (which does not depend on the choice of π). 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 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 [5, Ch. III] and [7, §5.6].

Problem 3. Profinite groups (96 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 ϕ is surjective.

(d) Show that to prove that ϕ 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 ϕ 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 [4].

Problem 4. Arithmetically equivalent number fields (96 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 [2], 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 [3], 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 $f_1 \cdot \#H$ 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 $\delta_{K/\mathbb{Q}}$ and $\delta_{K'/\mathbb{Q}}$ do not necessarily have the same factorization pattern, even though the discriminant ideals $D_{K/\mathbb{Q}} := \mathrm{N}_{K/\mathbb{Q}}(\delta_{K/\mathbb{Q}})$ and $D_{K'/\mathbb{Q}} := \mathrm{N}_{K'/\mathbb{Q}}(\delta_{K'/\mathbb{Q}})$, do.

A useful reference for this problem if you get stuck is Perlis' paper [3].

Problem 5. Survey (4 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			

Please rate each of the following lectures that you attended, according to the quality of the material (1="useless", 10="fascinating"), the quality of the presentation (1="epic fail", 10="perfection"), the pace (1="way too slow", 10="way too fast", 5="just right") and the novelty of the material to you (1="old hat", 10="all new").

Date	Lecture Topic	Material	Presentation	Pace	Novelty
12/6	Local class field theory				
12/8	Global class field theory				

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.

References

[1] I.B. Fesenko and S.V. Vostokov, *Local fields and their extensions*, second edition, AMS Translations of Mathematics Monographs **121**, 2002.

[2] 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.

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

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

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

[6] J.-P. Serre, *Local fields*, Springer, 1979.

[7] J. Voight, *Quaternion algebras*, preprint, 2018.

18.785 Number Theory I
Fall 2021