18.785 Number Theory **Fall 2018**

Problem Set #10 **Due: 11/28/2018**

Description

These problems are related to the material covered in Lectures 19-22. Your solutions are to be written up in latex and submitted as a pdf-file with a filename of the form `SurnamePset10.pdf` via e-mail to `drew@math.mit.edu` by **noon** on the date due. Collaboration is permitted/encouraged, but you must identify your collaborators, and any references you consulted. If there are none, write "**Sources consulted: none**" at the top of your problem set. The first person to spot each non-trivial typo/error in any of the problem sets or lecture notes will receive 1-5 points of extra credit.

Instructions: First do the warm up problems, then pick 2 of the problems 1-4 to solve and write up your answers in latex, then complete the survey problem 5.

Problem 0.

These are warm up problems that do not need to be turned in.

(a) Prove that for each integer $n > 1$ there are infinitely many $(\mathbb{Z}/n\mathbb{Z})$-extensions of $\mathbb{Q}$ ramified at only one prime.

(b) Prove that for each integer $n > 2$ there are no $(\mathbb{Z}/n\mathbb{Z})^2$-extensions of $\mathbb{Q}$ ramified at only one prime. Why does this not contradict the fact that $(\mathbb{Z}/p\mathbb{Z})^2$-extensions of $\mathbb{Q}_p$ exists for every p?

(c) In class we proved that in any finite extension of number fields infinitely many primes split completely. Must infinitely many primes remain inert?

(d) Let K be a real quadratic field and let ∞ denote the modulus supported on the real place of K. Show that if the fundamental unit of K has norm -1 then $\mathrm{Cl}_K^\infty = \mathrm{Cl}_K$ and otherwise Cl_K^∞ is larger than Cl_K by a factor of 2.

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 α.

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 ith *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

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

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:

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

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 $B/\mathfrak{q}$.

(d) Fix $i \ge 0$. Show that for each $\sigma \in G_i$ we have $\sigma(\pi)/\pi \in U_i$, and the map $\sigma \mapsto \sigma(\pi)/\pi$ induces an injective group homomorphism $\theta_i \colon G_i/G_{i+1} \hookrightarrow U_i/U_{i+1}$.

(e) Let $i \ge 1$. Show that for $\sigma \in G_0$ and $\tau \in G_i/G_{i+1}$ we have $\theta_i(\sigma\tau\sigma^{-1}) = \theta_0(\sigma)^i\theta_i(\tau)$ (first show that both sides of this equality actually make sense, you may wish to invoke (c) when doing so). Then show $\sigma\tau\sigma^{-1}\tau^{-1} \in G_{i+1} \Leftrightarrow \sigma^i \in G_1$ or $\tau \in G_{i+1}$.

(f) Prove that for $i, j \ge 1$, if $\sigma \in G_i$ and $\tau \in G_j$ then $\sigma\tau\sigma^{-1}\tau^{-1} \in G_{i+j+1}$. Using this, show that the integers $i \ge 1$ for which $G_i \ne G_{i+1}$ are all congruent modulo p.

Now fix $K = \mathbb{Q}_p$, and let $L/\mathbb{Q}_p$ be a finite Galois extension as above.

(g) Show that if $L/\mathbb{Q}_p$ is totally ramified of odd degree p then $v_{\mathfrak{q}}(\mathcal{D}) = 2p - 2$, and that if $L/\mathbb{Q}_p$ is totally ramified of odd degree p^2 then $v_{\mathfrak{q}}(\mathcal{D}) = 3p^2 - p - 2$.

(h) Show that if $L/\mathbb{Q}_p$ is totally ramified of odd degree p^2 then G is cyclic. Conclude that no extension of $\mathbb{Q}_p$ has Galois group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^3$.

Problem 2. The p-adic logarithm (49 points)

The *p-adic exponential* is defined by

$$\exp(x) := \sum_{n \ge 0} \tfrac{x^n}{n!} \in \mathbb{Q}_p[[x]];$$

we may view it as a function on $\mathbb{C}_p$ (the completion of the algebraic closure of $\mathbb{Q}_p$ whose absolute value $|\ |_p$ extends the p-adic absolute value on $\mathbb{Q}_p$). For any power series over $\mathbb{C}_p$, we define its *radius of convergence* r in the usual way:

$$1/r := \limsup_{n \to \infty} |a_n|_p^{1/n}.$$

(a) Show that for any power series $f \in \mathbb{C}_p[[x]]$ with radius of convergence r, the series converges on $|x|_p < r$, diverges on $|x|_p > r$, and either converges for all x with $|x|_p = r$, or diverges for all x with $|x|_p = r$.

(b) Show that $v_p(n!) = \frac{n-s_n}{p-1}$, where s_n is the sum of the digits of n when written in base p, and use this to compute the radius of convergence of $\exp(x)$.

We now define the *p-adic logarithm* by

$$\log(1+x) = \sum_{n\geq 1}(-1)^{n+1}\tfrac{x^n}{n}.$$

Let $\mathfrak{m} := \{x \in \mathbb{C}_p : |x| < 1\}$ (this is the maximal ideal of the valuation ring of $\mathbb{C}_p$).

(c) Show that the power series defining $\log(1+x)$ has radius of convergence 1; conclude that it gives a well defined function for $x \in \mathfrak{m}$.

(d) Show that $\log\big((1+x)(1+y)\big) = \log(1+x) + \log(1+y)$ for $x, y \in \mathfrak{m}$.

(e) Let r be the radius of convergence of exp you computed in (b). Prove that log and exp are inverse isomorphisms between the multiplicative group of the open disc of radius r about 1 and the additive group of the open disc of radius r about 0.

We are now in a position to fill in one of the missing details in our proof of the Kronecker-Weber theorem. Let ζ_p denote a primitive pth-root of unity, let $\pi = 1 - \zeta_p$, and let U_1 denote the subgroup of $\mathbb{Q}_p(\zeta_p)^\times$ congruent to 1 modulo π, and let U_1^p be the group of pth powers in U_1. We showed in lecture that the p-power maps sends U_1 to a subset U_1^p of $\{u \equiv 1 \bmod \pi^{p+1}\}$, but we actually used the fact that this map is surjective. With the p-adic logarithm we can easily invert the p-power map.

(f) Show that the function $f(x) := \exp\big(\frac{1}{p}\log x\big)$ maps each $v \equiv 1 \bmod \pi^{p+1}$ to an element $u \in U_1$ for which $u^p = v$, thus $U_1^p = \{u \equiv 1 \bmod \pi^{p+1}\}$.

Following Iwasawa, we now extend log to a function on $\mathbb{C}_p^\times$ by (arbitrarily) defining $\log p = 0$, and for $x \in \mathfrak{m}$ and $n \in \mathbb{Z}$ we define

$$\log(p^n(1+x)) := \log(1+x).$$

This extends log to the subgroup $G := p^{\mathbb{Z}}(1+\mathfrak{m})$ of $\mathbb{C}_p^\times$. For $x \in \mathbb{C}_p^\times$ with $x^n \in G$, let

$$\log(x) := \tfrac{1}{n}\log(x^n).$$

(g) Show that for every $x \in \mathbb{C}_p^\times$ there is an integer n for which $x^n \in G$ (thus our definition above covers all of $\mathbb{C}_p^\times$).

(h) Prove that $\log\colon \mathbb{C}_p^\times \to \mathbb{C}_p$ is a homomorphism whose kernel is the subgroup of $\mathbb{C}_p^\times$ generated by all roots of unity and all roots of p.

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 $\#C/\#G$.[1] In this problem you will prove the *Frobenius density theorem*, which says essentially the same thing, but with a different notion of conjugacy.

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

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, 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 that map $\mathfrak{p}' \mapsto \mathfrak{p}' \cap \mathcal{O}_K$ defines a surjective map $\pi\colon S' \to S$.

(f) Show that the fibers of π 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 principal ideal theorem (49 points)

The following theorem describes another remarkable (but not unique) property of the Hilbert class field.

Theorem. *Let K be a number field and let L be its Hilbert class field. Every $\mathcal{O}_K$-ideal generates a principal $\mathcal{O}_L$-ideal.*

This theorem was conjectured by Hilbert in 1900 and later reduced to a group theoretic question by Emil Artin that was finally proved by Furtwangler in 1930. One needs Artin reciprocity in order to prove it, so we will take this as given.

(a) Show that the Hilbert class field M of L is a Galois extension of K and that $\mathrm{Gal}(L/K)$ is the maximal abelian quotient of $\mathrm{Gal}(M/K)$ (thus M/K is nonabelian unless $M = L$).

Recall that for a finite group G, the maximal abelian quotient of G is $G^{\mathrm{ab}} := G/G'$, the quotient of G by its commutator subgroup $G' := \{ghg^{-1}h^{-1} : g, h \in G\}$. If H is a (not necessarily normal) subgroup of G, there is a natural map $V\colon G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ called the *transfer map* (*Verlagerung* in German) which is defined as follows. Let $S := \{g_1, \ldots, g_n\}$ be a set of left coset representatives of H in G, define $\phi\colon G \to S$ by $g \in \phi(g)H$, and put

$$V(g) := \prod_{i=1}^{n} \phi(gg_i)^{-1} gg_i.$$

(b) Show that V induces a canonical homomorphism $V\colon G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ by showing that (i) $V(g) \in H$ for all $g \in G$, (ii) the induced map $G \to H^{\mathrm{ab}}$ is a homomorphism with G' in its kernel, (iii) this homomorphism does not depend on the choice of S.

The Artin map $\psi_{L/K}$ induces an isomorphism $\mathrm{Cl}(K) \xrightarrow{\sim} \mathrm{Gal}(L/K)$, and the Artin map $\psi_{M/L}$ induces an isomorphism $\mathrm{Cl}(M) \xrightarrow{\sim} \mathrm{Gal}(M/L)$. The groups $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(M/L)$ are both abelian, hence equal to their maximal abelian quotients, We have a diagram of group homomorphisms

$$\begin{array}{ccc}
\mathrm{Cl}(K) & \xrightarrow{\sim} & \mathrm{Gal}(L/K) = \mathrm{Gal}(M/K)^{\mathrm{ab}} \\
\downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle V} \\
\mathrm{Cl}(L) & \xrightarrow{\sim} & \mathrm{Gal}(M/L) = \mathrm{Gal}(M/L)^{\mathrm{ab}}
\end{array}$$

where π is the map $[\mathfrak{a}] \mapsto [\mathfrak{a}\mathcal{O}_L]$. To prove the principal ideal theorem we need to show (1) this diagram commutes, and (2) the image of V on the RHS is trivial.

Put $G := \mathrm{Gal}(M/K)$ and $H := \mathrm{Gal}(M/L)$ so that $G/H \simeq \mathrm{Gal}(L/K) = \mathrm{Gal}(M/K)^{\mathrm{ab}}$ (thus $H = G'$, so it is not unreasonable to think $V\colon G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ should be trivial).

Let $\mathfrak{p}$ be a prime of K and let $\mathfrak{p}\mathcal{O}_K = \mathfrak{q}_1 \cdots \mathfrak{q}_r$ be its factorization into primes of L. Fix a prime $\mathfrak{r}|\mathfrak{q}|\mathfrak{p}$ of M above a prime $\mathfrak{q}|\mathfrak{p}$ of L (say $\mathfrak{q} = \mathfrak{q}_1$), define τ_i by $\tau_i(\mathfrak{q}_i) = \mathfrak{q}$), let $D \subseteq G$ be the decomposition group of $\mathfrak{r}$ over K, and let $g := \sigma_{\mathfrak{r}} \in G$ be the Frobenius element at $\mathfrak{r}$.

(c) Show that the image of $\mathfrak{p}$ in H under $\psi_{M/L} \circ \pi$ is $\prod_i \psi_{M/L}(\mathfrak{q}_i)$ and that the double cosets $D\tau_i H$ are distinct and cover G.

(d) Define $g_{ij} := g^j \tau_i$ for $0 \le j < m$, where m is the order of $\psi_{L/K}(\mathfrak{p})$, and show that $S := \{g_{ij}\}$ is a unique set of left coset representatives for H.

(e) Using $S := \{g_{ij}\}$ to define the maps ϕ and V above, show that for each $\mathfrak{q}_i|\mathfrak{p}$ we have

$$\psi_{M/L}(\mathfrak{q}_i) = \prod_{j=0}^{m-1} \phi(gg_{ij})^{-1} gg_{ij}$$

and conclude that the diagram above commutes.

(f) Let $\mathbb{Z}[G]$ be the (noncommutative) group algebra of G (formal sums $\sum n_g[g]$ over $\{[g] : g \in G\}$ with $[g][h] = [gh]$). Let I_G be the *augmentation ideal* of sums $\sum n_g[g]$ for which $\sum n_g = 0$, and let

$$\delta\colon H/H' \to (I_H + I_G I_H)/(I_G I_H)$$

be the homomorphism that sends the class of $h \in H$ in H/H' to the class of $[h]-1$ in $(I_H+I_GI_H)/(I_GI_H)$ (here 1 is the identity in $\mathbb{Z}[G]$). Prove that δ is an isomorphism (hint: show that $\{[g]([h]-1) : g \in S, h \in H\}$ is a basis for $I_H+I_GI_H$ as a $\mathbb{Z}$-module).

(g) Prove that the diagram

$$\begin{tikzcd} G/G' \arrow[r, "V"] \arrow[d, "\delta"] & H/H' \arrow[d, "\delta"] \\ I_G/I_G^2 \arrow[r, "\varphi"] & (I_H + I_GI_H)/(I_GI_H) \end{tikzcd}$$

commutes, where $\varphi(x) = x([g_1] + \cdots + [g_n])$.

(h) Prove that if G is a finite group and $H = G'$ then $V\colon G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ has trivial image (hint: quotient by H' to reduce to the case that H is abelian then write $G/H = G/G'$ as a product of cyclic groups and go from there; if you get stuck feel free to consult [1, Theorem VI.7.6] for further details on how to proceed).

Problem 5. Class fields of $\mathbb{Q}$ (49 points)

(a) Show that the ray class fields of $\mathbb{Q}$ consist of the cyclotomic fields $\mathbb{Q}(\zeta_m)$ and their maximal real subfields $\mathbb{Q}(\zeta_m)^+ := \mathbb{Q}(\zeta_m + \zeta_m^{-1})$. For integers $m > 2$ show that $[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m)^+] = 2$ and that $\mathbb{Q}(\zeta_m)$ is *totally complex* (its archimedean places are all complex) while $\mathbb{Q}(\zeta_m)^+$ is *totally real* (its archimedean places are all real).

(b) Solve the abelian inverse Galois problem over $\mathbb{Q}$ by showing that every finite abelian group is isomorphic to the Galois group of an extension of $\mathbb{Q}$.

(c) Does (b) still hold if we restrict to totally real extensions of $\mathbb{Q}$?

Recall that the *conductor* of a congruence subgroup is the minimal modulus that appears in its equivalence class; it follows from the Artin reciprocity law that the conductor of the corresponding abelian extension L/K is the minimal modulus $\mathfrak{m}$ of a ray class field $K(\mathfrak{m})$ that contains L. Our next goal is to determine the set of conductors for abelian extensions of $K = \mathbb{Q}$, but we will initially work in greater generality.

Let $\mathfrak{p}_2$ denote a prime of K of absolute norm $\mathrm{N}(\mathfrak{p}_2) = 2$ (if one exists) and suppose $\mathfrak{m}$ is the conductor of some congruence subgroup for K.

(d) Show that if $\mathfrak{m}_0$ is trivial then $\#\mathfrak{m}_\infty \neq 1$.

(e) Show that if $\mathfrak{p}_2|\mathfrak{m}$ then $\mathfrak{p}_2^2|\mathfrak{m}$.

(f) Show that if $\mathfrak{m} = \mathfrak{p}_2^2$ then $\mathfrak{p}_2$ is ramified in $K/\mathbb{Q}$.

(g) Show that $\#\mathfrak{m}_\infty = 0$ then $\mathrm{N}(\mathfrak{m}_0) \neq 3$.

(h) Show that the only moduli that are not conductors of an abelian extension of $\mathbb{Q}$ are those ruled out be (d)–(g), namely: ∞, (3), (4), (m) and $(m)\infty$, for all $m \equiv 2 \bmod 4$.

Problem 6. Survey

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			

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
11/19	Kronecker–Weber theorem				
11/21	Intro to class field theory				
11/26	Statements of 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] Jürgen Neukirch, *Algebraic number theory*, Springer-Verlag, 1999.