18.785 Number Theory **Fall 2016**

Problem Set #5

Description

These problems are related to material covered in Lectures 9-11. Your solutions are to be written up in latex and submitted as a pdf-file via e-mail to the instructor on the due date. Collaboration is permitted/encouraged, but you must identify your collaborators, and any references consulted other than the lecture notes. If there are none, write

Sources consulted: none at the top of your problem set. The first person to spot each typo/error in the problem set or lecture notes will receive 1-5 points of extra credit.

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

Problem 0.

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

(a) Prove (1) all local fields have the same cardinality, (2) all global fields have the same cardinality, (3) completing an uncountable field does not change its cardinality, (4) taking the algebraic closure of an infinite field does not change its cardinality.

(b) Prove that an open subgroup of a topological group is always closed, but a closed subgroup need not be open (give an explicit example).

(c) Prove that $\mathbb{Q}_7(\sqrt[3]{2}) \simeq \mathbb{Q}_7(\zeta_{342})$, where ζ_{342} is a primitive 342th root of unity.

(d) Prove that there are exactly two non-isomorphic cubic extensions of $\mathbb{Q}_2$.

Problem 1. Complete algebraically closed fields (50 points)

The field of complex numbers has the virtue of being both complete and algebraically closed. One might ask whether there are any nonarchimedean fields with this property. We proved in lecture that every finite extension of $\mathbb{Q}_p$ is a local field, and in particular, complete. In this problem you will prove that the algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ is not complete, but the completion $\mathbb{C}_p$ of $\overline{\mathbb{Q}}_p$ is both complete algebraically closed.

(a) Prove that if K is a complete perfect field with nonarchimedean absolute value $|\ |$ and algebraic closure $\overline{K}$ then there is a unique absolute value on $\overline{K}$ that restricts to $|\ |$ (so we may unambiguously view $\overline{K}$ as a field with absolute value $|\ |$). You may assume that (all variants of) Hensel's lemma hold for any complete field with a nonarchimedean absolute value (the valuation ring need not be discrete).

(b) Let $\overline{\mathbb{Z}}_p := \{x \in \overline{\mathbb{Q}}_p : |x|_p \le 1\}$ be the valuation ring of $\overline{\mathbb{Q}}_p$, with maximal ideal $\mathfrak{m} := \{x \in \overline{\mathbb{Q}}_p : |x|_p < 1\}$. Prove that $\overline{\mathbb{Z}}_p/\mathfrak{m}$ is an infinite algebraic extension of $\mathbb{F}_p$, and that it is algebraically closed (hence we may denote it $\overline{\mathbb{F}}_p$).

(c) Prove that the image of $|\ |_p \colon \overline{\mathbb{Q}}_p^\times \to \mathbb{R}_{>0}$ is the set $p^{\mathbb{Q}}$ of fractional powers of p. Conclude that $\overline{\mathbb{Z}}_p$ is not a DVR.

(d) Prove that $\overline{\mathbb{Z}}_p$ is not compact and that $\overline{\mathbb{Q}}_p$ is therefore not locally compact, hence not a local field.

Recall that a *Baire space* is a topological space in which every countable intersection of open dense sets is dense. The Baire Category Theorem states that every complete metric space (and also every locally compact Hausdorff space) is a Baire space.

(e) Let $X_n := \{x \in \overline{\mathbb{Q}}_p : [\mathbb{Q}_p(x) : \mathbb{Q}_p] \leq n\}$. Show that X_n is a closed set whose interior is empty. Conclude that $\overline{\mathbb{Q}}_p$ is not a Baire space and therefore not complete.

(f) Prove the following form of *Krasner's Lemma*: Let K be a complete perfect field with nontrivial nonarchimedean absolute value $|\ |$ and algebraic closure $\overline{K}$, let $\alpha \in \overline{K}$, and let

$$\epsilon := \min\left\{|\alpha - \sigma(\alpha)| : \sigma \in \mathrm{Gal}(\overline{K}/K), \sigma(\alpha) \neq \alpha\right\}.$$

Then $K(\alpha) \subseteq K(\beta)$ for all $\beta \in B_{<\epsilon}(\alpha)$.

(g) Prove the following form of *Continuity of Roots*: Let K be a complete perfect field with nontrivial nonarchimedean absolute value $|\ |$ and algebraic closure $\overline{K}$, and let $\alpha \in \overline{K}$ have minimal polynomial $f(x) = \sum_{i=0}^{n} f_i x^i \in K[x]$. Prove that for every $\epsilon > 0$ there is a $\delta > 0$ such that if $g(x) = \sum_{i=0}^{n} g_i x^i \in K[x]$ is a monic polynomial with $\sum_i |g_i - f_i| < \delta$ then $g(x)$ has a root β for which $|\alpha - \beta| < \epsilon$.

(h) Prove that if K is a complete perfect field with a nontrivial nonarchimedean absolute value then the completion of its algebraic closure is algebraically closed (so in particular, $\mathbb{C}_p$ is algebraically closed).

Remark: The simplifying assumption that K is perfect is not necessary; one can prove alternative versions of (f) and (g) that do not assume K is perfect but still imply (h).

Problem 2. Finite extensions of local fields (50 points)

If K is an archimedean local field, then either $K = \mathbb{R}$, in which case K has exactly one nontrivial finite extension (up to isomorphism), or $K = \mathbb{C}$, in which case K has no nontrivial finite extensions. So let us assume that K is a nonarchimedean local field; then K is a finite extension of $\mathbb{Q}_p$ or a finite extension of $\mathbb{F}_p((t))$. For a positive integer n, we wish to determine the number of degree-n extensions of K (which we count only up to isomorphism). Let A be the valuation ring of K, and let E_n be the set of Eisenstein polynomials $f \in A[x]$ of degree n.

First consider the case where K is a finite extension of $\mathbb{Q}_p$:

(a) Show that there is a natural topology on E_n induced by the topology on A and that E_n is compact in this topology.

(b) Prove that for any finite extension L/K, the set

$$\{f \in E_n : K[x]/(f(x)) \simeq L\}$$

is open in the topology on E_n.

(c) Prove that K has only finitely many totally ramified extensions of degree n.

(d) Prove that K has only finitely many extensions of degree n.

(e) Derive a formula for the number of degree-q extensions of $\mathbb{Q}_p$ (up to isomorphism), where p and q are distinct primes.

Now consider the case where K if a finite extension of $\mathbb{F}_p((t))$:

(f) Show that K has infinitely many non-isomorphic extensions of degree n, for some n.

(g) Why does your proof above for finite extensions of $\mathbb{Q}_p$ not apply here? Pinpoint exactly where the proof breaks down when $\mathbb{Q}_p$ is replaced by $\mathbb{F}_p((t))$.

Problem 3. The absolute Galois group of $\mathbb{F}_q$ (50 points)

Let $\mathbb{F}_q$ be a finite field with q elements, let $\overline{\mathbb{F}}_q$ be a fixed algebraic closure of $\mathbb{F}_q$, and for every positive integer n let us fix the finite field

$$\mathbb{F}_{q^n} := \{x \in \overline{\mathbb{F}}_q : x^{q^n} = x\}$$

with q^n elements. For any set S (finite or infinite), we use $\#S$ to denote its cardinality (isomorphism class in the category of sets), and if L/K is any field extension, $[L : K]$ denotes the the cardinality of any K-basis for L (i.e. $\dim_K L$). Recall that cardinals are ordered by monomorphisms of representative sets (so $\#S \leq \#T$ if and only if an injection $f\colon S \to T$ exists), and for any set S we have the strict inequality $2^{\#S} > \#S$ (here $2^{\#S}$ denotes the cardinality of the set of all subsets of S). We also note the standard cardinals $\beth_0 := \aleph_0 := \#\mathbb{Z}$, $\beth_1 := 2^{\beth_0} = \#\mathbb{R}$, and $\beth_{n+1} := 2^{\beth_n}$.

(a) Prove that $\overline{\mathbb{F}}_q = \bigcup_{n\geq 1} \mathbb{F}_{q^n}$.

(b) Compute the cardinals $\#\overline{\mathbb{F}}_q$ and $[\overline{\mathbb{F}}_q : \mathbb{F}_q]$.

Let $\mathbb{N}$ denote the set of positive integers partially ordered by divisibility. Consider the inverse system of groups

$$\big(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)\big)_{n\in\mathbb{N}},$$

where for $m|n$ the homomorphism $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \to \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is induced by restriction (the image of $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is obtained by restricting its domain to $\mathbb{F}_{q^m}$).

(c) Prove that we have group isomorphisms

$$\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \varprojlim_{n\in\mathbb{N}} \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}. \tag{1}$$

Conclude that $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ is abelian (so all of its subgroups are normal).

(d) The inverse limit $\widehat{\mathbb{Z}} := \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$ on the RHS of (1) is not only an inverse limit of abelian groups, it is also an inverse limit of rings (for $m|n$ the reduction map $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is a ring homomorphism). Prove that there is a ring isomorphism

$$\widehat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p.$$

(e) Compute the cardinality of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Conclude that $\#\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \neq [\overline{\mathbb{F}}_q : \mathbb{F}_q]$.

(f) Compute the cardinality of the set of subgroups of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ and the cardinality of the set of subfields $k \subseteq \overline{\mathbb{F}}_q$ that contain $\mathbb{F}_q$. Conclude that the Galois correspondence does not hold for $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$; in particular, many different subgroups of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ have the same fixed field k (ridiculously many, in fact).

(g) For any subgroup $G \subseteq$ of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, let $\overline{G}$ be the subgroup generated by the union of all subgroups of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ with the same fixed field as G. Call G *closed* if $G = \overline{G}$ (we will see in later lectures that $\overline{G}$ is in fact the closure of G with respect to the *Krull topology* on $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$). Show that there is a one-to-one inclusion-reversing correspondence between closed subgroups $G \subseteq \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ and intermediate fields $\mathbb{F}_q \subseteq k \subseteq \overline{\mathbb{F}}_q$ such that

(i) $G = \mathrm{Gal}(\overline{\mathbb{F}}_q/k)$;
(ii) $k = \overline{\mathbb{F}}_q^{\,G}$.

Thus provided we restrict to closed subgroups of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, the main theorem of Galois theory holds.

Problem 4. Uniqueness of norms (50 points)

Let K be a field with absolute value $|\ |$ and let V be a K-vector space. The absolute value $|\ |$ induces a topology on K via the metric $d(x, y) := |x - y|$, and every norm $\|\ \|$ on V induces a topology on V via the metric $d(v, w) := \|v - w\|$.

The goal of this problem is to prove that if K is complete and V has finite dimension then the topology on V is uniquely determined by the topology on K. One can find standard proofs for $K = \mathbb{R}$ and $K = \mathbb{C}$ in most analysis textbooks, and the same proof works for any locally compact field. But the standard approach does not work in general because it relies on the assumption that closed balls are compact (as we proved in Lecture 9, this is equivalent to local compactness). Here we follow the approach of Cassels [1], which works for any complete field and any finite-dimensional vector space.

(a) Give an example of a complete field that is not locally compact.

(b) Give an example of an infinite-dimensional vector space over a complete field with two norms that induce different topologies.

Two norms $\|\ \|_1$ and $\|\ \|_2$ on V are said to be *equivalent* if there exists a constant $c \in \mathbb{R}$ such that $\|v\|_1 \leq c\|v\|_2$ and $\|v\|_2 \leq c\|v\|_1$ for all $v \in V$.

(c) Show that equivalent norms induce the same topology.

Let us now fix a complete field K and a vector space V with basis $(v_1, \ldots, v_n)$, and for $v = x_1v_1 + \cdots x_nv_n \in V$ define the sup-norm $\|v\|_\infty := \max_i |x_i|$.

(d) Show that the topology induced by the sup-norm does not depend on the basis.

(e) Prove that V is complete under the topology induced by the sup-norm.

(f) Let $c := n \max_i \|v_i\|$. Prove that if $\|\ \|$ is a norm on V then $\|v\| \leq c\|v\|_\infty$ for $v \in V$.

(g) Prove that if $\|\ \|$ is any norm on V then there is a constant $C \in \mathbb{R}$ such that $\|v\|_\infty \leq C\|v\|$ for $v \in V$ (hint: proceed by induction on n and use the fact that non-trivial subspaces of V are complete under the induction hypothesis).

Problem 5. 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			

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
10/13	Extensions of complete DVRs				
10/18	Totally ramified extensions				

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] J.W.S. Cassels, *Local Fields*, Cambridge University Press, 1986.

[2] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta function*, Springer, 1984.

18.785 Number Theory I

Fall 2016