HOMEWORK FOR FALL 2019 CLASS FIELD THEORY

Last Modified August 22, 2019

There are hints in the latex comments. (Just change the extension of this URL to .tex)

Some notes on class + lectures:

(1) **Expectations**: Taken from Tony Varilly's syllabus: "In my experience as a student, most people do not follow all the details of a Math lecture in real time. During lecture, you should expect to witness the big picture of what's going on. You should pay attention to the lecturer's advice on what is important and what isn't. A lecturer spends a long time thinking on how to deliver a presentation of an immense amount of material; they do not expect you to follow every step, but they do expect you to go home and fill in the gaps in your understanding."

(2) Please do all of the following.

   (a) After each class, review all of the lecture notes.

   (b) Before the next class, briefly review again. (Make sure that you come to each lecture knowing at least the definitions and statements from the last lecture.)

   (c) Sit down at least once on your own to attempt the homework.

   (d) Later, meet with other students, and approach me, to make more progress on the homework and material from the lectures.

(1) **Topological groups.**

Let G be a topological group with identity element e. Prove the following.

(a) If U is an open neighborhood of e then there exists a symmetric open neighborhood V of e such that $V \cdot V \subset U$ (where V is said to be symmetric if $V^{-1} = V$).

(b) If H is a subgroup of G then its closure $\overline{H}$ is again a subgroup, and if H is normal then $\overline{H}$ is normal.

(c) An open subgroup of G is closed, and a finite-index closed subgroup of G is open.

(d) An open subgroup of a compact group has finite index.

(e) If $K, K' \subset G$ are compact sets then so is $K \cdot K'$.

(f) G is Hausdorff if and only if $\{e\}$ is closed in G. (In other words, if G is T_1 then it is Hausdorff.)

(2) **Profinite groups, Galois groups, topology, etc.**

(a) A topological group is said to be topologically cyclic (resp. topologically finitely generated) if it contains a dense cyclic subgroup (resp. dense finitely generated abelian group). Show that $\widehat{\mathbb{Z}}$ and $\mathbb{Z}_p$ are topologically cyclic. Similarly, show that the image of $k[x]$ in $k[\![x]\!]$ is dense. Show that $G_{\mathbb{Q}}$ is not topologically finitely generated.

(b) Show that a profinite group is compact, Hausdorff, and totally disconnected (i.e. any subset with at least two elements can be represented as the union of two or more disjoint nonempty open subsets). Show that an infinite profinite group is uncountable.

(c) Show that $\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$.

(d) Let G be a profinite group. Show that the image of a continuous homomorphism $G \to \mathbb{Z}$ (where $\mathbb{Z}$ has the discrete topology) is trivial. Show that the image of a continuous homomorphism $G \to \mathbb{C}^*$ (where $\mathbb{C}^*$ has the complex topology) is finite.

(e) The topology is really necessary in the infinite Galois correspondence. Give an example of a subgroup $H \subset G_{\mathbb{Q}}$ such that $\overline{\mathbb{Q}}^H = \mathbb{Q}$ but $H \neq G_{\mathbb{Q}}$.

(f) Define $\mathbb{Z}_p\{x\}$ to be the completion of $\mathbb{Z}[x]$ with respect to the ideal (p). Show that this is not equal to $\mathbb{Z}_p[\![x]\!]$. Characterize the elements of $\mathbb{Z}_p[\![x]\!]$ which lie in $\mathbb{Z}_p\{x\}$. Show that $\mathbb{Z}_p\{x\}$ is isomorphic to the completion of $\mathbb{Z}[x]$ with respect to the maximal ideal (p, x).

(g) Let $k \subset L \subset K$ be algebraic extensions and suppose that K is Galois over k. Show that $\mathrm{Aut}(K/L)$ is a closed subgroup of $\mathrm{Aut}(K/k)$.

(3) **Valuations and $\mathbb{Q}_p$.**

(a) Show that $z \in \mathbb{Q}_p$ has a periodic p-adic expansion if and only if it is rational.
(b) Show that $\mathbb{Q}_p$ has no continuous field automorphisms other than the identity. Does it have any non-continuous automorphisms?
(c) The boundary of $\mathbb{Z}_p$ (i.e. $\mathbb{Z}_p^*$) is clopen. (Dwork called $\mathbb{Z}_p^*$ the p-adic unit tire.)
(d) Classify all closed subgroups of $\mathbb{Z}_p$. (Modified Sept 9.)
(e) Show that $\mathbb{Z}_p$ is homeomorphic to the Cantor set; $\mathbb{Q}_p$ is homeomorphic to the Cantor set minus any single point.
(f) Let G be a topological group. A lattice is a discrete subgroup $\Lambda \subset G$ which is free (as an abelian group, so $\Lambda \cong \oplus\mathbb{Z}$ and which is discrete with respect to the induced topology. Show that $\mathbb{Q}_p$ contains no lattices.
(g) Let (K, v) be a valued field with v non-Archimedean, discrete, and non-trivial. Prove that $v = v_{\mathfrak{m}}$ for some ideal $\mathfrak{m}$ of $\mathcal{O}_v$.
(h) Show that two non-Archimedean norms $|\cdot|_1$ and $|\cdot|_2$ give the same topology on a field K if and only if $|\cdot|_1 = |\cdot|_2^\alpha$ for some $\alpha > 0$.

(4) **Hensel's lemma.**
(a) Use Newton iteration (i.e. the proof of Hensel's lemma) to compute the 3-adic expansion of $\sqrt{7}$.
(b) Show that $u \in \mathbb{Z}_2^*$ is a square (in $\mathbb{Q}_2$) if and only if u is congruent to 1 mod 8.
(c) Suppose $p \neq 2$. Show that $u \in \mathbb{Z}_p^*$ is a pth power (in $\mathbb{Q}_p$) if and only if u is congruent to a pth power mod p^2.
(d) Use the Banach fixed point theorem to give another proof of Hensel's lemma.
(e) Show that an infinite algebraic extension of a complete field K is never complete. Give an example of something in the completion of $\mathbb{Q}_p^{cyc}$ which is not in $\mathbb{Q}_p^{cyc}$.
(f) For a prime p, describe all quadratic extensions of $\mathbb{Q}_p$.
(g) Let K be a non-Archimedean local field with finite residue field of characteristic p. Use Hensel's lemma to prove that if n is a nonzero integer then $(K^\times)^n$ is open with finite index in $K^\times$ when $p \nmid n$. When $\mathrm{char}(K) = 0$ use the p-adic logarithm to prove that the same result is true for *any* nonzero integer n. Deduce that any subgroup of finite index in $K^\times$ is open when $\mathrm{char}(K) = 0$.
(h) Let $K = \mathbb{F}_p((t))$ Show that $(K^\times)^p$ is closed but not open in $K^\times$.
(i) For which $a \in \mathbb{Z}$ is $7X^2 = a$ solvable in $\mathbb{Z}_7$? For which $a \in \mathbb{Q}$ is it solvable in $\mathbb{Q}_7$?
(j) Find all quadratic extensions of $\mathbb{Q}_2$ (up to isomorphism).

(5) **Miscellaneous** Let K be complete with respect to a non-Archimedean discrete valuation. Let L be a purely inseparable algebraic extension. Show that the valuation extends uniquely to L.

(6) **Newton Polygons**
(a) Let $E_n(x) = 1 + x + \frac{x}{2} + \cdots + \frac{x^n}{n!}$. Show that f is irreducible.
(b) Find two monic polynomials of degree 3 in $\mathbb{Q}_5[x]$ with the same Newton polygon, but one irreducible and the other not.
(c) Let $f - 1 + a_1 x + \cdots + a_{2n} x^{2n}$ be a polynomial such that if α is a root of f then $p\alpha$ is also a root of f, with the same multiplicity. What does this imply about

the shape of the Newton polygon of f? Draw all possible such polygons for n in the range $n = 1, 2, 3, 4$.

(d) Let $f(t) \in \mathbb{Q}_p[t]$ and assume that $f'(t) \in \mathbb{Z}_p[t]$. Let m be the order of vanishing of $f'(t)$ mod p at 0. Prove that if $m < p - 2$, then f has at most $m + 1$ zeroes in $p\mathbb{Z}_p$.

(7) **Structure of units**

(a) Compute $\mathbb{Q}_5^*/\mathbb{Q}_5^{*3}$, $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$, $\mathbb{Q}_2^*/\mathbb{Q}_2^{*3}$, and $\mathbb{Q}_3(\sqrt{3})^*/\mathbb{Q}_2(\sqrt{3})^{*3}$.

(b) Let K be a finite extension of $\mathbb{Q}_p$. Find a formula for the index of $K^{*n} \subset K^*$.

(c) For $p > 2$, the isomorphism $\log\colon \mathbb{Z}_p^{(1)} \to \mathbb{Z}_p$ endows $\mathbb{Z}_p^{(1)}$ with the structure of a $\mathbb{Z}_p$ module. Given $1 + x \in \mathbb{Z}_p^{(1)}$ and $z \in \mathbb{Z}_p$, what is $(1 + x)^z$? (without reference to log.)

(d) Let K be a finite extension of $\mathbb{Q}_p$ with valuation ring $\mathcal{O}$. Let $n > e/(p - 1)$. What is the torsion subgroup of $\mathcal{O}^{*(1)}$? What is the structure of $\mathcal{O}^{*(1)}$ as a $\mathbb{Z}_p$ module?

(8) **Miscellaneous.**

(a) Show that $\overline{\mathbb{Q}}_p$ is not complete.

(b) Show that $\mathbb{C}_p := \widehat{\overline{\mathbb{Q}_p}}$ is not spherically complete. (A field K with an absolute value is called spherically complete if the intersection of every decreasing sequence of balls (in the sense of the metric induced by the absolute value) is nonempty.)

(c) Let p be a prime, K be a finite extension of $\mathbb{Q}$, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ the primes of $\mathcal{O}_K$ above p.

(i) Show that $K \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod K_{\mathfrak{p}_i}$.

(ii) Show that $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \prod (\mathcal{O}_K)_{\mathfrak{p}_i} \cong \prod \mathcal{O}_{K_{\mathfrak{p}_i}}$.

(d) Let K be a finite extension of $\mathbb{Q}_p$, with valuation ring $\mathcal{O}$. Analyze the zeroes of $\log(1 + x)$ on $\mathcal{O}$ using Newton polygons; show that there are only finitely many in $\mathcal{O}$, and try to say roughly how many zeroes there are. Let $L = \cup_{(n,p)=1} \mathbb{Q}_p(\zeta_n)$; how many zeroes does log have on L? (See Koblitz chapter 4 for a precise statement on how Newton polygons work for power series.)

(e) Argue via Newton Polygons that the series $\prod_{i=0}^{\infty} (1 - xp^i)$ has a unique root of every negative integer valuation.

(9) **Miscellaneous.**

(a) Show that the maximal tamely ramified **abelian** extension of $\mathbb{Q}_p$ is finite over the maximal unramified extension of $\mathbb{Q}_p$.

(b) List, with proof, all degree 4 extensions of $\mathbb{Q}_5$.

(c) Prove that the completion of an algebraically closed field is algebraically closed.

(d) Recall that $\mathbb{Q}_p^{\text{tame}} = \cup_{(n,p)=1} \mathbb{Q}_p(\zeta_n, p^{1/n})$. Give an explicit presentation (i.e. generators and relations) of $\mathrm{Gal}(\mathbb{Q}_p^{\text{tame}}/\mathbb{Q}_p)$.

(10) **Miscellaneous.**

(a) Compute the lower ramification filtration for $\mathbb{Q}_p(\zeta_{p^n})$ and for $\mathbb{Q}_p(p^{1/(p^n)})$.

(b) For what primes p does $\mathbb{Q}_p$ have an extension with Galois group S_4.

(11) **Different.**

Let L/K be a finite extension. Recall that the dual of a fractional ideal $\mathcal{U} \subset L$ is ${}^*\mathcal{U} := \{x : x \in L \,|\, \mathrm{Tr}(x\mathcal{U}) \subset \mathcal{O}_K\}$

(a) Show that ${}^*\mathcal{U}$ is a fractional ideal.
(b) Show that ${}^*\mathcal{U} \cong \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{U}, \mathcal{O}_K)$.
(c) Is ${}^{**}\mathcal{U} \cong \mathcal{U}$?

(12) **Local Artin Map.**

(a) Assume that a functorial local Artin map exists. Verify that proof from class that finite index subgroups of $K^\times$ are in bijection with finite abelian extensions of K.
(b) Compute all degree 3 extensions of $\mathbb{Q}_2$.
(c) Prove that a finite extension $K \subset L$ of local fields is totally ramified if and only if the image of $N_{L/K}$ contains a uniformizer.