

Math 538: Problem Set 5 (due 24/3/2017)

Do a good amount of problems; choose problems based on what you already know and what you need to practice. I recommend at least problems 2,4,7 and some of 5.

More on the multiplicative structure

- (Diversion on exp and log) Let F be a field of characteristic zero, complete with respect to a discrete valuation. Let R be the valuation ring, P the maximal ideal.
 - Show that the domain of convergence of the series $\log x = -\sum_{m=1}^{\infty} \frac{(1-x)^m}{m}$ is $U_1 = \{x \in R \mid x \equiv 1 \pmod{P}\}$.
 - Show that the domain of convergence of the series $\exp x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$ is $\left\{x \mid v(x) > \frac{v(p)}{p-1}\right\}$ where v is the valuation, and p is the rational prime such that $v(p) > 0$.
 - Show that $\exp(x+y) = (\exp x)(\exp y)$ and $\log(xy) = \log x + \log y$ in the domains of convergence.
 - Show that $\log(\exp x) = x$ if $|x|$ is small enough and that $\exp(\log x) = x$ if $|1-x|$ is small enough.
- Let K be a finite extension of \mathbb{Q}_p with ring of integers \mathcal{O}_K , maximal ideal \mathfrak{p} and residue field $\kappa \simeq \mathbb{F}_q$.
 - Show that the group of roots of unity in K of order dividing $q-1$ is the full group of units of that order, that is a cyclic group μ_{q-1} of order $q-1$.
 - Show that $K^\times \simeq \mathbb{Z} \times \mu_{q-1} \times U_1$, each isomorphism corresponding to a choice of uniformizing element.
 - Show that \log defined on U_1 in 1(a) can be extended to K^\times so that it satisfies $\log(xy) = (\log x)(\log y)$ there.
- (the unexpected \mathbb{Z}_p module) Let F be a field complete with respect to a non-archimedean absolute value with valuation ring R , and maximal ideal P such that $p \in P$ (for example, F might be of characteristic p). Let $U = R^\times$ be the group of units, $U_1 = \text{Ker}(R^\times \rightarrow (R/P)^\times)$.
 - Show that a product $\prod_{i=0}^{\infty} a_i$ converges in F iff $\lim_{i \rightarrow \infty} a_i = 1$.
 - Show that the map $\mathbb{Z} \times U_1 \rightarrow U_1$ given by $(a, x) \mapsto x^a$ extends to a unique continuous map $\mathbb{Z}_p \times U_1 \rightarrow U_1$.
 - Interpret (b) as showing that the topological commutative group U_1 has the structure of a \mathbb{Z}_p -module.
- (Quadratic extensions) Using 2(b), classify the quadratic extensions of the following fields. In each case determine which extensions are unramified.
 - \mathbb{Q}_p , p odd.
 - \mathbb{Q}_2 .
 - A finite extension K of \mathbb{Q}_p , p odd.

Unramified extensions

5. (Finite extensions) Let K be complete with respect to a non-archimedean absolute value, with residue field κ .
 - (a) Let L_1, L_2 be finite unramified extensions of K . Show that any κ -homomorphism $\lambda_1 \rightarrow \lambda_2$ is induced by a K -homomorphism $L_1 \rightarrow L_2$.
 - (b) Conclude from (a) that L_1/K and L_2/K isomorphic extensions iff λ_1/κ and λ_2/κ are isomorphic extensions.
 - (c) Conclude from (a) that the natural map $\text{Aut}_K(L) \rightarrow \text{Aut}_\kappa(\lambda)$ is an isomorphism when L/K is unramified. In particular, L/K is a Galois extension iff λ/κ is a Galois extension, and in that case they have isomorphic Galois groups.
 - (d) Let λ be a finite separable extension of κ . Show that there is an unramified extension L/K with residue field λ .

6. (Infinite extensions) Let K be complete with respect to a non-archimedean absolute value.
 - (a) Let $L/M/K$ be a tower of algebraic extensions of K . Show that L/K is unramified iff $L/M, M/K$ are so, extending Lemma 105 which handles the case of $[L : K]$ finite.
 - (b) Show that the results of problem 5 hold for infinite extensions of L and κ .
 - (f) Recall that the maximal unramified extension K^{nr} of K is the compositum of all finite unramified extensions contained in a fixed algebraic closure. Show that the maximal unramified extension is a Galois extension, and that any isomorphism of algebraic closures restricts to an isomorphism of the maximal unramified extensions (justifying the definite article in “the maximal unramified extension”).
 - (g) Show that the residue field of K^{nr} is the separable closure $\bar{\kappa}^{\text{sep}}$ of the residue field of K .

6. Let K be a p -adic field, that is a finite extension of \mathbb{Q}_p .
 - (a) Show that for any n , K has a unique (up to isomorphism) unramified extension of degree n .
 - (b) Show that the Galois group of any unramified extension of K is cyclic. Its generator is called a *Frobenius element*.

7. (Cyclotomic extensions) Let K be a p -adic field and let ζ_r be a primitive root of unity of order r .
 - (a) Suppose first that r is prime to p . Show that $K(\zeta_r)$ is an unramified extension of K .
 - (b) Suppose now that $r = p^e$ for some e and that $K = \mathbb{Q}_p$. Show that the minimal polynomial of $\Pi = \zeta - 1$ is an Eisenstein polynomial, and conclude that $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ is totally ramified.
 - (c) Now let $r = p^e s$ where $p \nmid s$. Show that the maximal unramified subextension of $\mathbb{Q}_p(\zeta_r)/\mathbb{Q}_p$ is $\mathbb{Q}_p(\zeta_s)/\mathbb{Q}_p$ and that $\mathbb{Q}_p(\zeta_r)/\mathbb{Q}_p(\zeta_s)$ is totally ramified.

Hint for 1a: Hensel's Lemma.

Hint for 3a: Use problem 1 to convert this to a question about an infinite sum.

Hint for 3b: Writing $(1+a)^p = 1+b$ bound $|b|$ in terms of $|a|$ and show that if $|a| < 1$ then $(1+a)^{p^n} \rightarrow 1$ as $n \rightarrow \infty$.

Hint for 7a: Use 2a, and later that the polynomial $x^r - 1$ is separable over the residue field.

Hint for 7b: This happened in the very first lecture.