PAWS 2024: LOCAL FIELDS
PROBLEM SET 5

JACKSYN BAKEBERG, THOMAS BROWNING, ANNA DIETRICH, SIDNEY WASHBURN

The goal for the exercises in Problem Set 5 is to study ramification of extensions of local fields and discover some cool applications of the things that we have learned throughout this course. Note that some of the problems require prior knowledge of Galois theory — if you are looking for what to study next, that is a great choice! The problems that use Galois theory are marked with a star.

Beginner

Problem 1. Let ζ be a p-th root of unity and let $L = \mathbb{Q}_p(\zeta)$. Use the identity

$$1 - \zeta^i = (1 - \zeta)(1 + \zeta + \cdots + \zeta^{i-1})$$

to show that

$$v_L(1 - \zeta^i) \leq v_L(1 - \zeta)$$

for $1 \leq i \leq p - 1$. By applying this inequality to different ζ and i, deduce the opposite inequality

$$v_L(1 - \zeta) \leq v_L(1 - \zeta^i).$$

Problem 2. Find all of the quadratic extensions of $\mathbb{Q}_2$, up to isomorphism.

Problem 3.

(1) Show that 16 is not an 8-th power in $\mathbb{Q}_2$, but is an 8-th power in $\mathbb{Q}_p$ for all odd primes p.
Hint: Factor the polynomial $x^8 - 16$.
(2) Show that 16 is not an 8-th power in $\mathbb{Q}(\sqrt{7})$ but is an 8-th power in $\mathbb{Q}_p(\sqrt{7})$ for all primes p.

Problem 4.

(1) Show that $\mathbb{Q}_3(\sqrt{-1})$ contains μ_8.
Hint: Use Proposition 3.3.1 from the lecture notes.
(2) Show that the minimal polynomial of ζ_8 over $\mathbb{Q}_3$ is $(X - \zeta_8)(X - \zeta_8^3)$.
Hint: Show that the minimal polynomial must be of the form $(X - \zeta_8)(X - \zeta_8^\ell)$ for some $\ell \in \{3, 5, 7\}$, and use the fact that the coefficients of the minimal polynomial must lie in $\mathbb{Q}_3$.

Problem 5. Prove the multiplicativity of the ramification index and residue field degree. That is, prove that for any extensions $M/L/K$, we have

$$e(M/K) = e(M/L)e(L/K) \text{ and } f(M/K) = f(M/L)f(L/K).$$

Problem 6. (Serre Local Fields #4 p. 72)
Let K be a local field with residue characteristic p. Let $\pi \in K$ be a uniformizer. Suppose that K contains a primitive p-th root of unity. Let $L = K(\alpha)$ where α is a root of the polynomial $X^p - \pi$. What is the ramification index of L/K?

Problem 7. Choose your favorite prime number p and use the LMFDB's database of p-adic fields to find a tower of fields

$$\mathbb{Q}_p \subsetneq M \subsetneq L \subsetneq K$$

where $M/\mathbb{Q}_p$ is unramified, L/M is totally ramified of degree prime to p, and K/L is totally ramified whose degree is a power of p. Give the defining polynomial for $K/\mathbb{Q}_p$, and the Eisenstein polynomial defining the extension K/M.
Access to LMFDB: `https://www.lmfdb.org/padicField/`
Remark: L is the maximal *tamely ramified* extension of K, which we will not define here.

Intermediate

Problem 8. Recall that a polynomial $f(x) = a_n x^n + \ldots + a_1 x + a_0$ over a complete non-archimedean local field K is called *Eisenstein* if $v_K(a_n) = 0$, $v_K(a_i) > 0$, and $v_K(a_0) = 1$ (see Problem Set 4 Exercise 7 for a problem about Eisenstein polynomials and Newton Polygons). Suppose that L/K is a finite extension.

(1) Suppose that $L = K[r]$, where r is a root of an Eisenstein polynomial.
  (a) Show that if v_L is the extension of v_K, then $v_L(r) = 1/n$.
  (b) Use part (a) to argue that L must be totally ramified over K.
  Hint: What is an upper and lower bound for the ramification index of L/K?

(2) Now, suppose that L is a totally ramified extension of K, and $[L : K] = n$.
  (a) Suppose that r is a generator of the maximal ideal in the ring of integers of L. Explain why $v_L(r) = 1/n$.
  (b) Show that if
$$a_{n-1} r^{n-1} + \ldots + a_1 r + a_0 = 0$$
  with $a_i \in K$, then $a_i = 0$ for all i. Conclude that $L = K[r]$.
  (c) Show that the set $\{1, r, r^2, \ldots r^n\}$ is linearly dependent over K. Prove that the resulting relation
$$b_0 + b_1 r + \ldots + b_n r^n = 0$$
  is given by an Eisenstein polynomial.

Problem 9. Use problem 8 and Krasner's lemma to prove that there are finitely many totally ramified extensions of degree n of a p-adic field K. Prove that there are finitely many unramified extensions of degree n. Conclude $\mathbb{Q}_p$ has only finitely many extensions of degree n.

Problem 10*. Prove that if $K/\mathbb{Q}_p$ is a finite unramified extension, then K is Galois over $\mathbb{Q}_p$.
Hint: The extension of residue fields is Galois. Apply Hensel's lemma to lift roots of a minimal polynomial.

Problem 11*. Let L/K be a Galois extension of local fields. There is a natural map
$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(\kappa_L/\kappa_K),$$
since the elements of $\mathrm{Gal}(L/K)$ fix the maximal ideal of $\mathcal{O}_K$. The kernel of this map is called the *inertia group* of L/K. Let K^{ur} be the maximal unramified extension of K. Show that the inertia subgroup $I(L/K)$ is equal to $\mathrm{Gal}(L/K^{\mathrm{ur}})$.

Problem 12. (Serre Local Fields #5 p. 72) Let $K/\mathbb{Q}_p$ be a finite extension of ramification index e and choose an element $y \in K$ of valuation -1. Show that the *Artin-Schreier polynomial*
$$f(X) = X^p - X - y$$
is irreducible over K, and defines an extension L/K of degree p.
Hint: If $L = K(x)$, use Hensel's lemma to show that the other roots of $f(X)$ lie in L and have the form $x + z_i$, $i = 0, \ldots, p-1$ where $z_i \in \mathcal{O}_L$ and $z_i \equiv i \mod \mathfrak{p}_L$.

Problem 13*. In this problem we will study the extension $\mathbb{Q}_3(\sqrt[8]{-9})/\mathbb{Q}_3$.

(1) Show that $\mathbb{Q}_3(\sqrt[8]{-9})$ contains $\mathbb{Q}_3(\sqrt{-1})$. Use problem 4 to conclude that $\mathbb{Q}_3(\sqrt[8]{-9})$ contains μ_8.
(2) Show that the extension $\mathbb{Q}_3(\sqrt[8]{-9})/\mathbb{Q}_3$ is Galois.
(3) In this part, we will show that the extension $\mathbb{Q}_3(\sqrt[8]{-9})$ has degree 8 by showing that the polynomial $f(X) = X^8 + 9$ is irreducible over $\mathbb{Q}_3$.
  (a) For $p \in \mathbb{Q}_3[X]$, let $p^*(X) = (-1)^{\deg p} p(-X)$. Verify that $(p^*)^* = p$, that $(pq)^* = p^* q^*$, and that
$$p^* \text{ is monic} \iff p \text{ is monic},$$
$$p^* \text{ is irreducible} \iff p \text{ is irreducible}.$$
  (b) Suppose that $p^* = p$. By considering the factorization of p into monic irreducible polynomials over $\mathbb{Q}_3$, show that we can factor $p = gg^* h_1 \cdots h_k$ where $g, h_1, \ldots, h_k \in \mathbb{Q}_3[X]$ are monic and where each h_i is irreducible and satisfies $h_i = h_i^*$.
  (c) Suppose that $p(X) = q(X^2)$ with q irreducible. Show that if p is not irreducible then we can factor $p = gg^*$ where $g \in \mathbb{Q}_3[X]$ is monic.

(d) Show that $X^2 + 9$ is irreducible over $\mathbb{Q}_3$.
(e) Use part (c) to show that $X^4 + 9$ is irreducible over $\mathbb{Q}_3$.
(f) Use part (c) to show that $X^8 + 9$ is irreducible over $\mathbb{Q}_3$.

(4) In this part, we will show that the Galois group $G = \mathrm{Gal}(\mathbb{Q}_3(\sqrt[8]{-9})/\mathbb{Q}_3)$ is isomorphic to the quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.
(a) Show that the elements of G are $\sigma_k(\sqrt[8]{-9}) = \zeta_8^k \sqrt[8]{-9}$ for $k \in \mathbb{Z}/8\mathbb{Z}$.
(b) By considering the action of σ_k on $\sqrt{-9} = \sqrt[8]{-9}^4$, show that if k is even, then σ_k acts trivially on $\mathbb{Q}_3(\mu_8)$, and if k is odd, then σ_k acts nontrivially on $\mathbb{Q}_3(\mu_8)$.
(c) Use problem 4 to deduce that

$$\sigma_k(\zeta_8) = \begin{cases} \zeta_8 & \text{if } k \text{ is even,} \\ \zeta_8^3 & \text{if } k \text{ is odd.} \end{cases}$$

(d) Show that $G \cong Q_8$.

(5) Determine the intermediate fields of the extension $\mathbb{Q}_3(\sqrt[8]{-9})/\mathbb{Q}_3$.
Hint: Use the Galois correspondence and our knowledge of quadratic extensions of $\mathbb{Q}_3$.
(6) Determine the ramification indices and inertia degrees in this lattice of intermediate fields.
(7) Determine the inertia subgroup of the extension $\mathbb{Q}_3(\sqrt[8]{-9})/\mathbb{Q}_3$.

Advanced

Problem 14*.

(1) Construct a tower of Galois extensions $\cdots/K_2/K_1/\mathbb{Q}$ with $\mathrm{Gal}(K_n/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$.
Hint: Look at subfields of $\mathbb{Q}(\zeta_{p^k})$.
In this case, we say that the compositum $K = \bigcup_n K_n$ is Galois over $\mathbb{Q}$ with Galois group $\mathbb{Z}_p$.
(2) If you know some infinite Galois theory, compute $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ and use infinite Galois theory to construct an extension $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_p$.