PAWS 2024: LOCAL FIELDS
PROBLEM SET 3

JACKSYN BAKEBERG, THOMAS BROWNING, ANNA DIETRICH, SIDNEY WASHBURN

The goal for the exercises in Problem Set 3 is to give you a chance to practice using Hensel's lemma as well as explore other related ideas that were not introduced in the lecture. The problems are divided into three parts: beginner, intermediate, and advanced. Some of the advanced problems require prior knowledge of Galois theory, but all other problems should be entirely self-contained. There are many different ideas introduced in this set, so have fun trying some new things out!

Beginner

Problem 1. Prove that $\mathbb{Q}_p \not\cong \mathbb{Q}_q$ as fields for any $p \neq q$. Also prove $\mathbb{Q}_p \not\cong \mathbb{R}$.

Hint: Roots of unity

Problem 2. Prove that $(x^2-2)(x^2-17)(x^2-34)$ has a root in $\mathbb{Z}_p$ for every prime p.

Problem 3. Show that the equation $3x^3+4y^3+5z^3=0$ has nonzero solutions in $\mathbb{R}$ and in $\mathbb{Q}_p$ for every prime p (however, it has no nonzero solution in $\mathbb{Q}$, but this is much harder to prove).

Problem 4. The congruence $x^3+6 \equiv 0 \pmod{131}$ has a root at $x \equiv 5 \pmod{131}$. Use Hensel's lemma to find roots of $x^3+6 \equiv 0 \ (131^2)$ and $x^3+6 \equiv 0 \ (131^3)$.

Hint: Use the explicit lifting formula given in problem 5.

Intermediate

Problem 5. Let $f(x)$ be a polynomial with integer coefficients. Suppose that a is a root of $f(x) \equiv 0 \pmod{p}$ and that $f'(a) \not\equiv 0 \pmod{p}$. Let $f'(a)^{-1}$ denote the multiplicative inverse of $f'(a)$ mod p. Show that if a_n is a lift of a to a root of $f(x) \equiv 0 \pmod{p^n}$, then

$$a_{n+1} = a_n + p^n\left(-f'(a)^{-1}\frac{f(a)}{p^n}\right)$$

is a lift of a to a root of $f(x) \equiv 0 \pmod{p^{n+1}}$.

Problem 6.

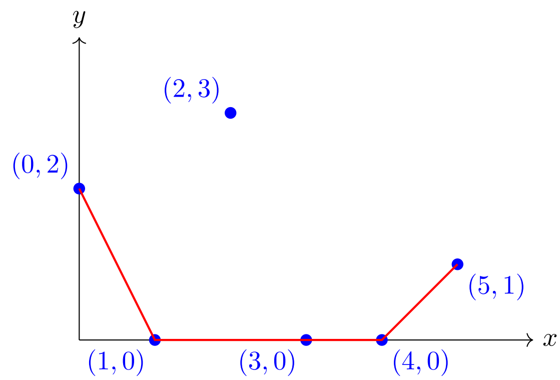
(1) Let p be an odd prime, and let $f\colon \mathbb{Q}_p \to \mathbb{Q}_p$ be a field automorphism.
  - (a) Let $x \in \mathbb{Q}_p$. Show that $x \in \mathbb{Z}_p$ if and only if $1+px^2$ is a square in $\mathbb{Q}_p$.
  - (b) Show that $f(\mathbb{Z}_p) = \mathbb{Z}_p$ and more generally $f(p^k\mathbb{Z}_p) = p^k\mathbb{Z}_p$.
  - (c) Show that f is continuous.
  - (d) Show that f is the identity map.

(2) Let $f\colon \mathbb{Q}_2 \to \mathbb{Q}_2$ be a field automorphism.
  - (a) Let $x \in \mathbb{Q}_2$. Show that $x \in \mathbb{Z}_2$ if and only if $1+8x^2$ is a square in $\mathbb{Q}_2$.
  - (b) Show that f is the identity map.

(3) Let $f\colon \mathbb{R} \to \mathbb{R}$ be a field automorphism.
  - (a) Show that $f(\mathbb{R}_{\geq 0}) = \mathbb{R}_{\geq 0}$.
  - (b) Show that f is the identity map.

Problem 7. Let $f(x) = a_n x^n + \ldots + a_0$ be a polynomial over a valued field K with a non-archimedean valuation v. The *Newton polygon* of f is defined as the *lower convex hull* of the points $(i, v(a_i))$.

For example, suppose that $f(x) = 5x^5 + x^3 + 125x^2 + 3x + 25 \in \mathbb{Q}[x]$. Then, the Newton polygon with respect to 5-adic valuation is the following:



(1) Draw the Newton polygon for $f(x) = x^5 + 12x^4 + 5x^3 + 27x^2 + 8x + 3$ with respect to 2-adic, 3-adic, and 5-adic valuations.

Newton polygons are useful when trying to determine whether a polynomial is irreducible or not. In fact, the valuations of the roots of a polynomial are entirely determined by the behavior of the Newton polygon. Suppose that m_i are the slopes of each of the lines in the Newton polygon, and p_i is the length of the projection of that line to the x-axis. Then, f has p_i roots of valuation $-m_i$ in an algebraic closure of K.

(2) Find two monic polynomials of degree 3 in $\mathbb{Q}_5[x]$ with the same Newton polygon, but where one is irreducible and the other not.

(3) A polynomial $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}_p[x]$ is an *Eisenstein polynomial* if $v(a_n) = 0$, $v(a_i) > 0$ for $i = 1, \ldots, n-1$, and $v(a_0) = 1$. Show that an Eisenstein polynomial is irreducible over $\mathbb{Q}_p$ using Newton polygons.

A *quadratic form* in n variables over a ring R is a function $f : R^n \to R$ that can be written as $f(x) = x^T Ax$ for some symmetric matrix $A \in M_{n\times n}(R)$. A is called the Gram matrix of f. We say that two quadratic forms f and g are *equivalent* over R if there exists an invertible matrix $U \in \mathrm{GL}_n(R)$ so that $f(x) = g(Ux)$. A quadratic form f is called *isotropic* if f represents 0 non-trivially (i.e. there exists $x \neq 0$ so that $f(x) = 0$).

Problem 8. Prove the "Weak Hasse Principle" for binary quadratic forms: If f is a rational binary (2 variable) quadratic form which is isotropic in $\mathbb{Q}_p$ for all p (including $p = \infty$ [i.e. $\mathbb{R}$]), then f is isotropic over $\mathbb{Q}$.

Problem 9. Let p be an odd prime. Let f and g be quadratic forms with coefficients in $\mathbb{Z}_p$. Show that if the coefficients of f and g are sufficiently close, then f and g are equivalent over $\mathbb{Z}_p$. Follow the steps below:

(1) Let F and G be the Gram matrices of f and g respectively. We are looking for invertible U so that $U^T FU = G$. Let $d = \nu_p(\det(F))$. Consider $(I + S)^T F(I + S)$ with $S = \frac{1}{2}F^{-1}(G - F)$. Prove that if $G = F \bmod p^\mu$, where $\mu \geq d + 1$, then $S = 0 \bmod p^{\mu-d}$.

(2) Put $F_1 = (I + S)^T F(I + S)$ and conclude $G - F_1 = 0 \bmod p^{2\mu-d}$. Now induct to construct U.

(3) Extra: Adapt the proof above to $p = 2$.

Problem 10. Prove the strong version of Hensel's Lemma in $\mathbb{Z}_p$: Let $f \in \mathbb{Z}_p[x]$ and $a_0 \in \mathbb{Z}_p$ so that $|f(a_0)| < |f'(a_0)|^2$. Then the sequence $a_{n+1} = a_n - f(a_n)/f'(a_n)$ converges to a root $\alpha \in \mathbb{Z}_p$ of f. Furthermore, $|\alpha - a_0| \leq |f(a_0)/f'(a_0)^2| < 1$.

Hints:

(1) Put $c = |f(a_0)/f'(a_0)^2| < 1$. Prove that $|a_n| \leq 1$, $|a_n - a_0| \leq c$ using induction, and that $|f(a_n)/f'(a_n)^2| \leq c^{2^n}$.

(2) For the third claim, apply the order 2 Taylor expansion to a_{n+1}. Also consider the Taylor expansion on $f'(a_{n+1})$.

Problem 11.

(1) Show there exists a non-trivial map $\lambda : \mathbb{Q}_p \to \mathbb{R}/\mathbb{Z}$ such that
   (i) $\lambda(x)$ is a rational number with only a p-power in its denominator;
   (ii) $\lambda(x) - x$ is a p-adic integer; and
   (iii) $\lambda(x + y) = \lambda(x) + \lambda(y)$.
(2) Define $\Lambda : \mathbb{Q}_p \to \mathbb{C}^\times$ by $\Lambda(x) = e^{2\pi i \lambda(x)}$. This is a homomorphism on the additive group of $\mathbb{Q}_p$. What is the kernel of Λ?
(3) We can define a measure μ on $\mathbb{Q}_p$ such that
   (i) $\mu(\mathbb{Z}_p) = 1$ and
   (ii) for every measurable set A and $x \in \mathbb{Q}_p$, we have $\mu(x + A) = \mu(A)$ (i.e. the measure is translation-invariant).

   Using these properties, compute $\mu(p^n\mathbb{Z}_p)$. More generally, compute $\mu(\alpha\mathbb{Z}_p)$ for any $\alpha \in \mathbb{Q}_p$.
(4) For a function $f : \mathbb{Q}_p \to \mathbb{C}$, define the Fourier transform of f to be

$$\widehat{f}(y) = \int_{\mathbb{Q}_p} f(x)\Lambda(xy)d\mu(x).$$

   Compute the Fourier transform of the indicator function

$$f(x) = \mathbb{I}_{p^n\mathbb{Z}_p}(x) = \begin{cases} 1 & x \in p^n\mathbb{Z}_p, \\ 0 & \text{else.} \end{cases}$$

   Hint: you will need to show the following very useful trick: on a compact group endowed with a translation-invariant measure, if $\Lambda : K \to \mathbb{C}^\times$ is a homomorphism, then

$$\int_K \Lambda(x)d\mu(x) = \begin{cases} \mu(K) & \Lambda \text{ trivial;} \\ 0 & \text{else.} \end{cases}$$

   First try to show this when K is a finite group endowed with the counting measure.

Advanced

Problem 12. Fix a prime number p.

(1) Let $X_0, X_1, \dots$ be an indeterminates, and let $W_n = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n$, $n \geq 0$. Show that there exist polynomials $S_0, S_1, \dots$ and $P_0, P_1, \dots$ in $\mathbb{Z}[X_0, X_1, \dots; Y_0, Y_1, \dots]$ such that

$$W_n(S_0, S_1, \dots) = W_n(X_0, X_1, \dots) + W_n(Y_0, Y_1, \dots),$$
$$W_n(P_0, P_1, \dots) = W_n(X_0, X_1, \dots) \cdot W_n(Y_0, Y_1, \dots).$$

(2) Let R be a commutative ring. For $a = (a_0, a_1, \dots)$ and $b = (b_0, b_1, \dots)$ where $a_i, b_i \in R$, define

$$a + b = (S_0(a, b), S_1(a, b), \dots), \quad a \cdot b = (P_0(a, b), P_1(a, b), \dots).$$

   Show that with these operations the sequences $a = (a_0, a_1, \dots)$ form a commutative ring with unit $W(R)$. This is called the **ring of Witt vectors** over R.
(3) Assume $pR = 0$ (for example, $R = \mathbb{F}_p$). For every Witt vector $a = (a_0, a_1, \dots) \in W(R)$, consider the "ghost components"

$$a^{(n)} = W_n(a) = a_0^{p^n} + pa_1^{p^{n-1}} + \cdots + p^n a_n$$

   as well as the two mappings $V, F : W(R) \to W(R)$ defined by

$$Va = (0, a_0, a_1, \dots) \quad \text{and} \quad Fa = (a_0^p, a_1^p, \dots)$$

   (these are called Verschiebung and Frobenius). Show that

$$(Va)^{(n)} = pa^{n-1} \quad \text{and} \quad a^{(n)} = (Fa)^{(n)} + p^n a_n.$$

(4) Let k be a field of characteristic p. Show that V is a homomorphism on the additive group of $W(k)$ and F is a ring homomorphism, and that

$$VFa = FVa = pa.$$

(5) If k is a perfect field of characteristic p, show that $W(k)$ is a complete discrete valuation ring with residue field k. What is the characteristic of $W(k)$?
(6) Describe $W(\mathbb{F}_p)$.

Problem 13. In this problem, we will prove Krasner's lemma and look at an application.

(1) Let K be a complete non-archimedean field and let K^{sep} be the separable closure of K. Given $x \in K^{\mathrm{sep}}$, let $x_2, \ldots, x_n \in K^{\mathrm{sep}}$ be the Galois conjugates of x over K.
  (a) Show that for all $\alpha \in K^{\mathrm{sep}}$ and $\sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$, $|\sigma(\alpha)| = |\alpha|$.
  (b) Let $y \in K^{\mathrm{sep}}$. Show that if $|y - x| < |y - x_i|$ for all $i = 2, \ldots, n$, then $K(x) \subseteq K(y)$.
  Hint: Consider the extension $K(x, y)/K(y)$. Apply Part (a) to $y - x$.

(2) Prove that the following are equivalent for a valued field (K, v):
  (a) Hensel's Lemma
  (b) Krasner's Lemma
  (c) Every monic polynomial $f(x) = x^n + \ldots + c_1 x + c_0 \in \mathcal{O}_K[x]$ with $\bar{c}_{n-1} \neq 0$ and $\bar{c}_i = 0$ for all $i \neq n-1$ has a linear factor $x + c$ in $\mathcal{O}_K$ with $\bar{c} = \bar{c}_{n-1}$.

(3) Use Krasner's lemma to prove that $\mathbb{C}_p$, the completion of the algebraic closure of $\mathbb{Q}_p$, is algebraically closed.

Hint: The roots of a separable, monic polynomial are a continuous function of the coefficients. You may use that the algebraic closure of $\mathbb{Q}_p$ is dense in $\mathbb{C}_p$.