Homework 6

Songyu Ye

October 10, 2025

1 Prove Krasner's Lemma ([S, p. 30, II.2 Exercise 1]) but only assuming that K is a non-Archimedean CVF.

Let E/K be a finite Galois extension of a complete field K¿ Prolong the valuation of K to E. Let $x \in E$ and let $\{x = x_1, x_2, \ldots, x_n\}$ be the Galois conjugates of x over K, with $x = x_1$. Let $y \in E$ so that $|y - x| < |y - x_i|$ for $i \geq 2$. Show that x belongs to the field $K(y)$. Note that if x_i is conjugate to x over $K(y)$, then $|y - x| = |y - x_i|$.

Note: We need not assume that the valuation is discrete since the unique extension of valuations (as covered in class; see [**?**, N, II.4.8] works without requiring discreteness.

Solution: Let E/K be a finite Galois extension of a complete non-Archimedean valued field K. Prolong the valuation of K to E. Let $x \in E$ have Galois conjugates $\{x_1 = x, x_2, \ldots, x_n\}$ over K. Suppose that $y \in E$ satisfies

$$|y - x| < |y - x_i| \quad \text{for all } i \geq 2.$$

We will show that $x \in K(y)$.

Let $f(T) = \prod_{i=1}^{n}(T - x_i) \in K[T]$ be the minimal polynomial of x over K. Then

$$f(y) = \prod_{i=1}^{n}(y - x_i) = (y - x) \cdot \prod_{i \geq 2}(y - x_i).$$

For each $i \geq 2$, since $|y - x| < |y - x_i| = |\alpha_i - \alpha|$, we have $|y - x_i| = |x_i - x|$ by the ultrametric inequality. Therefore

$$|f(y)| = |y - x| \cdot \prod_{i \geq 2} |x_i - x| = |y - x| \, |f'(x)|.$$

Because $|y - x| < |x_i - x|$ for all $i \geq 2$, it follows that

$$|f(y)| < |f'(x)|^2.$$

Lemma (Hensel's Lemma) Let A be a complete non-Archimedean valuation ring (for instance, a complete DVR), and let $f \in A[x]$. Suppose $a_0 \in A$ satisfies

$$|f(a_0)| < |f'(a_0)|^2.$$

Then the sequence defined by Newton iteration

$$a_{n+1} := a_n - \frac{f(a_n)}{f'(a_n)} \qquad (n \geq 0)$$

is well-defined and converges to a unique root $a \in A$ of f, satisfying

$$|a - a_0| \leq \frac{|f(a_0)|}{|f'(a_0)|^2}.$$

Moreover, this root is unique within the ball $\{z \in A : |z - a_0| < |f'(a_0)|\}$.

By Hensel's lemma (which does not require the valuation to be discrete), there exists a unique root $\tilde{x}$ of f such that

$$|\tilde{x} - y| \leq \frac{|f(y)|}{|f'(x)|} < |f'(x)|.$$

But the only conjugate of x that lies within this neighborhood of y is x itself, so $\tilde{x} = x$. Hence x is obtained from y by solving $f(T) = 0$ within $K(y)$, showing that $x \in K(y)$.

2

1. Do [S, p. 30, Exercise 2 in Section II.2] but only assuming that K is a non-Archimedean CVF (not necessarily discrete). Let K be a complete field, and let $f(X) \in K[X]$ be a separable irreducible polynomial of degree n. Let L/K be the extension of degree n defined by f. Show that for every polynomial $h(X)$ of degree n that is close enough to $f(X)$, $h(X)$ is irreducible and the extension L_h/K defined by h is isomorphic to L/K.

   - Two polynomials

     $$f(x) = \sum_{i=0}^{n} a_i x^i, \qquad g(x) = \sum_{i=0}^{n} b_i x^i$$

     are considered *close* if

     $$\sup_{0 \leq i \leq n} |a_i - b_i|$$

     is sufficiently small (i.e. less than some $\varepsilon > 0$ depending on the initial data of the problem).

2. Note that the p-adic valuation on $\mathbb{Q}_p$ extends uniquely to a valuation on $\overline{\mathbb{Q}}_p$. (We still refer to the latter as the p-adic valuation.) Let C denote the completion of $\overline{\mathbb{Q}}_p$ with respect to the p-adic valuation. Use (i) to prove that C is algebraically closed. (People often write $\mathbb{C}_p$ for this C.)

Solution:

1. Let $f \in K[X]$ be separable irreducible of degree n and let $L = K(\alpha)$ with $f(\alpha) = 0$. Write the distinct K-embeddings of L into a fixed algebraic closure as $\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_n$,

and set $\alpha_i := \sigma_i(\alpha)$. Since f is separable, $f'(\alpha) \neq 0$ and the finite set $\{\alpha_i\}_{i=1}^n$ has a positive mutual separation

$$\delta := \min_{i \geq 2} |\alpha - \alpha_i| > 0.$$

Let $h(X) = \sum_{i=0}^n b_i X^i$ be a polynomial of degree n with coefficients sufficiently close to those of $f(X) = \sum_{i=0}^n a_i X^i$ in the sense that $\sup_i |a_i - b_i| < \varepsilon$ for ε to be chosen below.

By continuity of evaluation, if ε is small then

$$|h(\alpha)| = \Big| \sum_{i=0}^n (b_i - a_i)\alpha^i \Big| \quad \text{is arbitrarily small,} \qquad \text{and} \qquad |h'(\alpha) - f'(\alpha)| \text{ is small,}$$

hence $|h'(\alpha)| = |f'(\alpha)| \neq 0$ for ε small enough. Choose ε so that

$$|h(\alpha)| < |h'(\alpha)|^2 \qquad \text{and} \qquad \frac{|h(\alpha)|}{|h'(\alpha)|} < \delta.$$

Applying Hensel's lemma (Newton form) in the complete non-Archimedean field K to the pair $(h, a_0 = \alpha)$, we obtain a unique root β of h with

$$|\beta - \alpha| \leq \frac{|h(\alpha)|}{|h'(\alpha)|} < \delta.$$

Therefore $|\beta - \alpha| < |\alpha - \alpha_i|$ for all $i \geq 2$. By Krasner's lemma, we conclude $K(\alpha) \subseteq K(\beta)$. But $[K(\beta) : K] \leq \deg h = n = [K(\alpha) : K]$, so necessarily $[K(\beta) : K] = n$ and $K(\beta) = K(\alpha)$. In particular h is irreducible over K and the extension $L_h := K(\beta)$ is K-isomorphic to L.

2. Let $K = \mathbb{Q}_p$, let $\overline{\mathbb{Q}}_p$ be its algebraic closure endowed with the unique extension of the p-adic valuation, and let C be the completion of $\overline{\mathbb{Q}}_p$ (often denoted $\mathbb{C}_p$). We prove C is algebraically closed.

   Take any nonconstant $h \in C[X]$ of degree n. Approximate its coefficients by elements of $\overline{\mathbb{Q}}_p$ to obtain $f \in \overline{\mathbb{Q}}_p[X]$ of the same degree n with coefficients sufficiently close so that the inequalities used in (i) hold for each simple root of f. Since characteristic is 0, we may (and do) choose f *separable* (discriminant nonzero is an open condition on the coefficients). Fix a root $\alpha \in \overline{\mathbb{Q}}_p \subset C$ of f. By the same Hensel argument as in (i), there exists $\beta \in C$ with $h(\beta) = 0$ and $|\beta - \alpha|$ arbitrarily small. Thus h has at least one root in C. Dividing h by $(X - \beta)$ and repeating by induction on the degree, we factor h completely over C. Hence C is algebraically closed.

3 Fix an integer $n \geq 2$ and an algebraic closure $\overline{\mathbb{Q}}_p$ of the field $\mathbb{Q}_p$ of p-adic numbers. Let L_n be a degree n extension of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}}_p$ such that $(p) \subset \mathbb{Z}_p$ is unramified in L_n. Write $\mu(L_n)$ for the (multiplicative) torsion subgroup of $L_n^\times$, namely the group of all roots of unity in L_n, and μ_N for the subgroup of N-th roots of unity in $\overline{\mathbb{Q}}_p^\times$.

(1) Show that

$$\mu(L_n) = \begin{cases} \mu_{p^n-1} & \text{if } p \text{ is odd,} \\ \mu_{2(p^n-1)} & \text{if } p \text{ is even (namely if } p = 2). \end{cases}$$

Hint: Hensel's lemma can help to show $\supseteq$.

(2) Prove that

$$L_n = \mathbb{Q}_p(\mu_{p^n-1}).$$

Note: This implies that there exists a *unique* degree n unramified extension of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}}_p$. It also follows that such an extension is Galois over $\mathbb{Q}_p$.

Solution:

1. Let $\mathcal{O}_{L_n}$ denote the valuation ring of L_n, with maximal ideal $\mathfrak{p}_{L_n}$ and residue field $k_{L_n} = \mathcal{O}_{L_n}/\mathfrak{p}_{L_n}$. Since $L_n/\mathbb{Q}_p$ is unramified of degree n, we have $k_{L_n} \cong \mathbb{F}_{p^n}$ and $\mathfrak{p}_{L_n} = p\mathcal{O}_{L_n}$. The reduction map

$$\mathcal{O}_{L_n}^\times \twoheadrightarrow k_{L_n}^\times = \mathbb{F}_{p^n}^\times$$

has kernel $1 + p\mathcal{O}_{L_n}$, which is a torsion-free. Therefore all torsion in $\mathcal{O}_{L_n}^\times$ comes from lifts of roots of unity in $\mathbb{F}_{p^n}^\times$. Since $\mathbb{F}_{p^n}^\times$ is cyclic of order $p^n - 1$, we expect $\mu(L_n)$ to have the same order.

Let $\bar{\zeta} \in \mathbb{F}_{p^n}^\times$ be a generator. It satisfies $\bar{\zeta}^{p^n-1} = 1$ and $(\bar{\zeta})^{p^n-1} - 1 = 0$ in $\mathbb{F}_{p^n}$. Consider the polynomial

$$f(X) = X^{p^n-1} - 1 \in \mathcal{O}_{L_n}[X].$$

Its derivative $f'(X) = (p^n - 1)X^{p^n-2}$ is nonzero mod p, since $p \nmid (p^n - 1)$. Thus all roots of f in the residue field are simple. By Hensel's lemma, each simple root in $\mathbb{F}_{p^n}$ lifts uniquely to a root in $\mathcal{O}_{L_n}$. Hence the reduction map induces an isomorphism

$$\mu_{p^n-1}(\mathcal{O}_{L_n}) \cong \mathbb{F}_{p^n}^\times,$$

and we conclude that $\mu(L_n) = \mu_{p^n-1}$ when p is odd. For $p = 2$, we also have $-1 \in L_n$ (of order 2), so

$$\mu(L_n) = \mu_{2(p^n-1)}.$$

2. We now show that $L_n = \mathbb{Q}_p(\mu_{p^n-1})$. The polynomial $X^{p^n-1} - 1$ splits completely over L_n since all $(p^n - 1)$-st roots of unity lie in L_n. Reducing mod p, $X^{p^n-1} - 1$ also splits completely over $\mathbb{F}_{p^n}$, and not over any smaller field, because $\mathbb{F}_{p^n}^\times$ is the unique cyclic group of order $p^n - 1$. Hence the minimal polynomial of a primitive $(p^n - 1)$-st root of unity over $\mathbb{Q}_p$ has degree n. Therefore

$$[\mathbb{Q}_p(\mu_{p^n-1}) : \mathbb{Q}_p] = n.$$

Since $p \nmid (p^n - 1)$, the extension $\mathbb{Q}_p(\mu_{p^n-1})/\mathbb{Q}_p$ is unramified. But there exists a *unique* unramified degree-n extension of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}}_p$, so we must have

$$L_n = \mathbb{Q}_p(\mu_{p^n-1}).$$

In summary, we have shown

$$\mu(L_n) = \begin{cases} \mu_{p^n-1}, & p \text{ odd}, \\ \mu_{2(p^n-1)}, & p = 2, \end{cases} \qquad \text{and} \qquad L_n = \mathbb{Q}_p(\mu_{p^n-1}).$$

4 Do [N, p. 134, Exercise 1 in Section II.4]: Show that an infinite *separable* algebraic extension L of a non-Archimedean complete valued field K is never complete. (The separability condition is missing in that exercise but it is needed. It is unnecessary, but feel free to assume that the valuation is discrete.)

Hint: A possible idea is to construct a well-designed Cauchy sequence in L that does not converge (so you get a contradiction if it converges). Krasner's lemma can help.

Examples: When $K = \mathbb{Q}_p$, examples of naturally occurring infinite extensions (which are thus incomplete) are:

- the algebraic closure $\overline{\mathbb{Q}}_p$,
- the *maximal unramified extension*

$$\mathbb{Q}_p^{\text{unr}} := \bigcup_{n \geq 1} L_n \quad \text{(where } L_n \text{ is as above)},$$

- the *infinite p-cyclotomic extension*

$$\mathbb{Q}_p(\mu_{p^\infty}) := \bigcup_{n \geq 1} \mathbb{Q}_p(\mu_{p^n}).$$

Note: The complete field C is an infinite but non-algebraic extension of $\mathbb{Q}_p$. So it does not contradict the conclusion of Problem 4 above.

Solution: Let K be a complete non-Archimedean valued field and let L/K be an infinite separable algebraic extension. Write $L = \bigcup_{n \geq 1} L_n$ where $L_1 \subset L_2 \subset \cdots$ is an ascending tower of finite separable extensions with $[L_n : K] < \infty$ and $\bigcup_n L_n = L$. Each L_n is complete because finite extensions of complete fields remain complete.

For each n, choose $\alpha_n \in L_{n+1} \setminus L_n$ and let $f_n(X) \in L_n[X]$ be its minimal polynomial. Since f_n is separable, its distinct conjugates $\sigma(\alpha_n)$ satisfy

$$\delta_n := \min_{\sigma \neq 1} |\alpha_n - \sigma(\alpha_n)| > 0.$$

By the density of L_n in L_{n+1}, we can choose $\beta_n \in L_{n+1}$ with $|\beta_n - \alpha_n| < \frac{1}{2}\delta_n$. By Krasner's lemma, $L_n(\alpha_n) = L_n(\beta_n)$, so replacing α_n by β_n does not change the field extension, but we may assume $|\alpha_n|$ is as small as we wish.

Now define

$$x_m := \alpha_1 + \alpha_2 + \cdots + \alpha_m \in L_m.$$

By choosing each α_n small enough so that $|\alpha_{n+1}| < |\alpha_n|^2$, the sequence (x_m) satisfies $|x_{m+1} - x_m| = |\alpha_{m+1}| \to 0$. Hence (x_m) is Cauchy in L. However, the limit of (x_m) cannot lie in any finite stage L_n since each $\alpha_{n+1} \notin L_n$; thus it has no limit in L. Therefore L is not complete.