Solutions 22

Tame and Wild Extensions, Ramification Filtration

1. Let K be a non-archimedean local field of characteristic $p > 0$. Show that for any integer $n \geqslant 0$, up to isomorphism there exists a unique totally inseparable extension of K of degree p^n.

   Solution By induction it suffices to prove the statement for $n = 1$. So let L/K be purely inseparable of degree p. Set $\varphi(x) := x^p$ for any $x \in L$. Then $\varphi(L)$ is contained in K and contains the subfield $\varphi(K)$. Thus $\varphi(L)$ is an intermediate field of the extension $K/\varphi(K)$. To understand this extension, using Proposition 11.1.4 of the lecture we may without loss of generality assume that $K = k((u))$ for a finite field k of characteristic p. Thus $\varphi(K) = k((v))$ for $v := u^p$. Since $u \in K$ is a root of the polynomial $X^p - v \in \varphi(K)[X]$, which is irreducible by the Eisenstein criterion for the maximal ideal $(v) \subset k[[v]]$, we see that $K/\varphi(K)$ has degree p. Since $\varphi(L) \subset K$ is itself of degree p over $\varphi(K)$, we must therefore have $\varphi(L) = K$. But this now means that $L = k((\sqrt[p]{u}))$ is uniquely determined up to isomorphism over K. Conversely, since $K/\varphi(K)$ is purely inseparable of degree p, the same holds for the extension $k((\sqrt[p]{u}))/K$. This proves the existence, and we are done.

2. Let K be a non-archimedean local field. Show that the maximal tame abelian extension K^{atr} of K is finite over the maximal unramified extension K^{nr} of K.

   Solution By Proposition 11.3.6 of the lecture the maximal tame extension K^{tr}/K is Galois over K and contains K^{nr}. By the Galois correspondence the subfield K^{atr} corresponds to the maximal closed normal subgroup Δ of $\Gamma := \mathrm{Gal}(K^{\mathrm{tr}}/K)$ whose factor group is abelian. Thus Δ is the closure of the commutator subgroup of Γ. As K^{nr} is abelian over K, we have $K^{\mathrm{nr}} \subset K^{\mathrm{atr}}$ and therefore $\Delta < \Gamma' := \mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{nr}})$.

   Now recall from Proposition 11.3.7 that $\Gamma \cong \hat{\mathbb{Z}} \ltimes \Gamma'$ and

$$\Gamma' \;\cong\; \hat{\mathbb{Z}}^{(p)}(1) \;:=\; \varprojlim_{p \nmid n} \mu_n(\bar{k}),$$

   on which $1 \in \hat{\mathbb{Z}}$ acts by the map $x \mapsto x^q$ for $q := |k|$. Taking the commutator of $1 \in \hat{\mathbb{Z}}$ with an element of Γ' thus corresponds to the map $x \mapsto x^{q-1}$. Under the (non-canonical) isomorphism

$$\Gamma' \;\cong\; \hat{\mathbb{Z}}^{(p)}(1) \;\cong\; \hat{\mathbb{Z}}^{(p)} \;\cong\; \prod_{\ell \neq p} \mathbb{Z}_p$$

this map corresponds to the map $y \mapsto (q-1) \cdot y$. Thus the commutator subgroup Δ corresponds to the subgroup $(q-1)\hat{\mathbb{Z}}^{(p)}$ of $\hat{\mathbb{Z}}^{(p)}$. Since $q-1$ is already coprime to p, the group $\hat{\mathbb{Z}}^{(p)}/(q-1)\hat{\mathbb{Z}}^{(p)} \cong \mathbb{Z}/(q-1)\mathbb{Z}$ is finite of order $q-1$. Thus Γ'/Δ is finite of order $q-1$, and hence $K^{\mathrm{atr}}/K^{\mathrm{nr}}$ is finite (and cyclic) of degree $q-1$.

3. Let K be a non-archimedean local field of characteristic $p > 0$. Show that for every integer $s \geqslant 0$ that is not divisible by p there exists a cyclic extensions L/K with Galois group $\Gamma \cong \mathbb{F}_p$, for which $\Gamma_s = \Gamma$ and $\Gamma_{s+1} = 0$.

   (*Hint:* Study polynomials of the form $X^p - X - a$ with $v(a) < 0$.)

   Solution First we recall Artin-Schreier theory, for instance from exercise 3 of series 22 of Algebra II in Spring 2023: Consider a polynomial of the form $f(X) = X^p - X - a$ for some $a \in K$. Then if f does not have a zero on K, any root $b \in \bar{K}$ of f generates a cyclic extension of K and $\mathrm{Gal}(L/K) \cong \mathbb{F}_p$ acts by $b \mapsto b + \alpha$ for all $\alpha \in \mathbb{F}_p$. (In fact, every cyclic extension of degree p of any field of characteristic p can be constructed in this way.)

   Returning to our situation, we choose an isomorphism $K \cong k((u))$ with a finite field k of characteristic p. Let v denote the extension to $\bar{K}$ of the normalized valuation on K. Let $b \in \bar{K}$ be a root of the polynomial $X^p - X - u^{-s}$. Since the Newton polygon of this polynomial is a straight line segment of slope $\frac{s}{p}$, we then have $v(b) = -\frac{s}{p}$. As this is not an integer, we conclude that $b \notin K$. Thus $L := K(b)$ is a cyclic Galois extension of K with Galois group $\Gamma \cong \mathbb{F}_p$.

   Now choose integers i and j such that $ip - js = 1$. After replacing (i, j) by $(i + ms, j + mp)$ for $m \gg 0$ we may assume that $j > 0$. Consider the element $\pi = u^i b^j \in L$. Then $v(u^i b^j) = i \cdot 1 - j\frac{s}{p} = \frac{1}{p}$; hence π is a uniformizer of L. Also any non-trivial element $\gamma \in \mathrm{Gal}(L/K)$ acts by

$$\begin{aligned} \pi = u^i b^j \mapsto {}^\gamma\pi = u^i(b+\alpha)^j &= (1+\alpha b^{-1})^j u^i b^j \\ &= \Big(\textstyle\sum_{\nu=0}^{j} \binom{j}{\nu} \alpha^\nu b^{-\nu}\Big)\pi \\ &\equiv \pi + j\alpha b^{-1}\pi \bmod (b^{-2}\pi) \end{aligned}$$

   for some $\alpha \in \mathbb{F}_p^\times$. Here $ip - js = 1$ implies that $p \nmid j$ and hence

$$v(j\alpha b^{-1}\pi) = -v(b) + v(\pi) = \tfrac{s+1}{p} < \tfrac{2s+1}{p} = v(b^{-2}\pi).$$

   Therefore $v({}^\gamma\pi - \pi) = \frac{s+1}{p}$. For the normalized valuation v_L on L this means that $v_L({}^\gamma\pi - \pi) = s+1$. By the definition of the lower numbering subgroups this shows that $\gamma \notin \Gamma_{s+1}$; hence $\Gamma_{s+1} = \{0\}$. On the other hand, since L/K is totally ramified and π is a uniformizer of L, the valuation ring of L is $k[[\pi]]$. Moreover $v_L({}^\gamma\pi - \pi) = s+1$ implies that $v_L({}^\gamma c - c) \geqslant s+1$ for all elements $c \in k[[\pi]]$. By the definition of the lower numbering subgroups we therefore have $\gamma \in \Gamma_s$; hence $\Gamma_s = \Gamma$.

4. In the situation of the preceding exercise, what happens with polynomials of the form $X^p - X - a$ with $v(a) \geqslant 0$?

   Solution In this case the polynomial has coefficients in the valuation ring and its reduction modulo the maximal polynomial is separable. Therefore the extension generated by a root of this polynomial is unramified.

5. Show that a local field of characteristic zero possesses only finitely many extensions of any fixed degree, up to isomorphism.

   Solution This is clear for $K \cong \mathbb{R}, \mathbb{C}$, because its algebraic closure is finite over it. So let K be a finite extension of $\mathbb{Q}_p$ for $p > 0$.

   Let L/K be an extension of degree n. Then its normal closure $\tilde{L}/K$ has degree $\leqslant n!$. Also $\mathrm{char}(K) = 0$ implies that $\tilde{L}/K$ is separable; so it possesses only finitely many intermediate fields. Thus it suffices to prove the desired statement for Galois extensions.

   If L/K is Galois, its Galois group is solvable. Thus there exist intermediate fields $L = K_d/\ldots/K_1/K_0 = K$ such that each K_i/K_{i-1} is Galois of prime degree. By induction it therefore suffices to prove the desired statement for cyclic extensions of prime degree.

   So let L/K be cyclic of prime degree ℓ. Set $K' := K(\mu_\ell)$ and $L' := LK'$. Since $[K'/K] \leqslant \ell - 1$, by Galois theory the extension L'/K' is then again cyclic of degree ℓ. Since L'/K possesses only finitely many intermediate fields, it thus suffices to prove the statement for L'/K' instead of L/K. In other words we may suppose that $\mu_\ell \subset K$.

   Then by Kummer theory we have $L = K(\sqrt[\ell]{a})$ for some $a \in K^\times$. Moreover, we have $K(\sqrt[\ell]{a}) = K(\sqrt[\ell]{b})$ for any $b \in K^\times$ for which b/a is an ℓ-th power. Thus the isomorphism class of L/K is determined by the residue class of a in the group $K^\times/(K^\times)^\ell$. But by Proposition 11.1.6 we have $K^\times \;\cong\; \mathbb{Z} \times \mu_K \times \mathbb{Z}_p^n$ with μ_K finite. Thus
   $$K^\times/(K^\times)^\ell \;\cong\; \mathbb{Z}/\ell\mathbb{Z} \times \mu_K/\mu_K^\ell \times \mathbb{Z}_p^n/\ell\mathbb{Z}_p^n.$$
   As each factor on the right hand side is finite, it follows that $K^\times/(K^\times)^\ell$ is finite. Thus there are only finitely many possibilities for L/K up to isomorphism, as desired.

   (*Aliter:* One can treat unramified and tame extensions separately, for instance using the explicit description of $\mathrm{Gal}(K^{\mathrm{tr}}/K)$ from Proposition 11.3.7. But for ramified cyclic extensions of degree p one still needs to use the Kummer theory argument above.)

   (*Aliter:* See [Lang: Algebraic Number Theory, Ch.II §5 Proposition 14].)