Math 676. Some examples of extension fields

The purpose of this handout is to probe the hypotheses of some of our results in class concerning the structure of finite extensions of local fields, or more generally of fraction fields of complete discrete valuation rings.

1. Number of extensions of a local field

In class we saw that if K is a local field and n is a positive integer not divisible by $\mathrm{char}(K)$ then the set of K-isomorphism classes of degree-n extensions of K is a finite set. Recall that the condition $\mathrm{char}(K) \nmid n$ is crucial in the proof, as otherwise the compact space of Eisenstein polynomials over K with degree n/f (for a fixed $f|n$) contains some inseparable polynomials (if $\mathrm{char}(K)|(n/f)$) and so the locus of separable Eisenstein polynomials of degree n/f would appear to be probably non-compact (as it is the complement of a "hypersurface" in a compact space, the "hypersurface" being the zero-locus of the universal discriminant for monic polynomials of degree n/f).

Let us show that this apparent non-compactness for $\mathrm{char}(K)|n$ is genuine and in fact leads to counterexamples to the desired finiteness statement in such cases. More specifically, we fix a local field K with characteristic $p > 0$ and we seek to show that there are infinitely many totally ramified separable p-extensions of K (up to K-isomorphism). Iterating such a construction would give infinitely many totally ramified separable p^r-extensions (up to K-isomorphism) for any $r > 0$, and then forming (linearly disjoint) composites with a totally tame extension $K(\pi^{1/e'})$ for any $e' > 0$ not divisible by p (and for a fixed choice of uniformizer $\pi \in K$) would give rise to infinitely many totally ramified separable extensions of K (up to K-isomorphism) with any desired degree n divisible by p.

To carry out the construction of the infinitely many non-isomorphic totally ramified separable p-extensions of K, note that we do not really need to keep track of ramification: a separable p-extension K'/K either has $e(K'|K) = p$ or $e(K'|K) = 1$. In the first case K'/K is totally ramified, and in the second case it is an unramified p-extension. There is only one unramified extension of each degree (due to the Galois theory of finite fields), and removing one element from an infinite list still yields an infinite set. Thus, we focus on the following problem: construct infinitely many separable p-extensions K'/K that are pairwise non-isomorphic over K. (Note that it is crucial to emphasize the K-isomorphism aspect, since if we ignore the K-structure and consider mere abstract topological field isomorphism then everything will have to collapse: any local field is abstractly topologically isomorphic to a formal Laurent series field over its residue field and so is determined up to abstract (topological) field isomorphism by its residue field alone.)

We will make examples that are even Galois (cyclic) of degree p, via Artin–Schreier theory. Recall the main result of Artin–Schreier theory: for any field F with characteristic $p > 0$, the set of F-isomorphism classes of cyclic p-extensions of F is identified with the set of non-zero elements in the additive quotient group of F modulo the additive subgroup $\wp(F)$ of elements of the form $\wp(b) = b^p - b$ for $b \in F$. (Explicitly, for every $c \in F$ the separable polynomial $T^p - T - c \in F[T]$ is either irreducible or totally split, so reducibility is equivalent to $c = b^p - b$ for some $b \in F$, and in the irreducible case a Galois splitting field F_c/F is of degree p and $F_c \simeq F_{c'}$ over F if and only if $c - c' = b^p - b$ for some $b \in F$. Moreover, all cyclic p-extensions F'/F are F-isomorphic to F_c for some $c \in F$ not of the form $b^p - b$ with $b \in F$.)

If k is the finite residue field of K, then $\mathrm{char}(k) = p$ and $K \simeq k((t))$ as discretely-valued fields (using the t-adic absolute value on $k((t))$). Thus, by Artin-Schreier theory, our task is to prove that the quotient group $K/\wp(K)$ is infinite when $K = k((t))$ for a finite field k of characteristic p. In fact, we claim that the same holds for *any* field k of characteristic p. Consider elements $1/t^n$ for $n > 0$ and $p \nmid n$. If $1/t^n - 1/t^{n'} \in \wp(K)$ with $n \neq n'$ and $p \nmid nn'$ then $1/t^n - 1/t^{n'} = f^p - f$ for some $f \in k((t))$ that is necessarily *not* in $k[\![t]\!]$ (since $n, n' > 0$ are distinct). Thus, f has a leading polar term with degree $-r < 0$, so f^p has a pole with degree $-rp < -r$. This forces $f^p - f$ to have a pole of order rp that is divisible by p, yet the difference $1/t^n - 1/t^{n'}$ does not have this property since n and n' are distinct and not divisible by p.

In the more positive direction, let us see that in a *very special case* we can explicitly "see" the finiteness aspect of the theorem on isomorphism classes of extensions of local fields: let us take K to be any local field (arbitrary characteristic) and pick a positive integer n not divisible by $\mathrm{char}(K)$ such that K contains

a full subgroup μ_n of nth roots of unity (that is, μ_n has order n). In this case, we will exhibit all degree-n Galois extensions K'/K such that $\mathrm{Gal}(K'/K)$ is *abelian*. In fact, we will do better: we will show by explicit construction that there are only finitely many Galois extensions K'/K such that $\mathrm{Gal}(K'/K)$ is abelian and killed by n (note that these hypotheses do not specify $[K' : K]$, nor that it is even finite!). The point is that since K contains a full set of nth roots of unity, by Kummer theory the set of such extensions (up to K-isomorphism) is in bijective correspondence with the set of subgroup of $K^\times/(K^\times)^n$ (explicitly, if B is such a subgroup then to B we associate the field K_B/K generated by adjoining nth roots to elements of B). Hence, to get the finiteness result in this aspect it suffices to show that the group $K^\times/(K^\times)^n$ is a *finite* group. (Contrast this with the group $\mathbf{Q}^\times/(\mathbf{Q}^\times)^n$ that is infinite.) In general, without any condition on roots of unity in K, we have:

Theorem 1.1. *Let K be a local field and n a positive integer not divisible by* $\mathrm{char}(K)$*. The quotient group $K^\times/(K^\times)^n$ is finite.*

Note that if $n = p = \mathrm{char}(K)$ then this finiteness result is always *false*: for $K = k(\!(t)\!)$ with a perfect (*e.g.*, finite) field k of characteristic p, $(K^\times)^p = k(\!(t^p)\!)^\times$, so $K^\times/(K^\times)^p$ is infinite because the elements $1 - t^i$ (for $i > 0$, $p \nmid i$) represent distinct residue class (why?). Such infinitude has no link with separable p-extensions of K!

Proof. As an abstract group we have $K^\times = \pi^{\mathbf{Z}} \times \mathscr{O}_K^\times \simeq \mathbf{Z} \times k^\times \times U_K$ with $U_K = 1 + \mathfrak{m}$ the subgroup of 1-units. (Slightly more canonically, $K^\times/\mathscr{O}_K^\times \simeq \mathbf{Z}$ via the normalized order function, and $\mathscr{O}_K^\times \simeq k^\times \times U_K$.) Since $\mathbf{Z}/n\mathbf{Z}$ and $k^\times/(k^\times)^n$ are finite, the finiteness of $K^\times/(K^\times)^n$ reduces to the finiteness of U_K/U_K^n. If $\mathrm{char}(K) = p > 0$ then $\mathrm{char}(k) = p$, and so for any $u \in \mathscr{O}_K^\times$ the polynomial $X^n - u \in \mathscr{O}_K[X]$ has separable reduction over k. For a 1-unit u, this reduction is $X^n - 1 \in k[X]$, and so by Hensel's lemma there is a unique nth root of u that is also a 1-unit. That is, the nth power map on U_K is an automorphism for local function fields K, and so U_K/U_K^n is trivial in this case.

Now suppose $\mathrm{char}(K) = 0$ and $\mathrm{char}(k) = p$. If n is not divisible by p, then the same argument as above shows that U_K is uniquely n-divisible, and so U_K/U_K^n is trivial. However, if $p|n$ then we need a different approach (as in fact U_K/U_K^n is non-trivial; its exact order is $\#U_K[n]/\|n\|_K$, as you will see when you begin your study of class field theory). In characteristic 0 there is another tool available, namely the p-adic logarithm! For sufficiently large N depending on p and the size of $e(K|\mathbf{Q}_p)$, on the open neighborhood $U_{K,N} = 1 + \mathfrak{m}^N \subseteq U_K$ around 1 the p-adic logarithm is convergent and sets up a group isomorphism (with p-adic exponential inverse) onto the additive group $\mathfrak{m}^N$ in $\mathscr{O}_K$. Thus, by the isometric properties of the p-adic log and exponential functions, $U_{K,N}^n = 1 + n\mathfrak{m}^N$ (since additively, n-fold addition on $\mathfrak{m}^N$ has image $n\mathfrak{m}^N$). We conclude that $U_{K,N}/U_{K,N}^n \simeq \mathfrak{m}^N/n\mathfrak{m}^N$ is visibly finite. Since $U_K/U_{K,N}^n$ is finite, $U_K/U_{K,N}^n$ is finite and hence so its quotient U_K/U_K^n. ∎

2. Imperfect residue field

Let F be the fraction field of a complete discrete valuation ring A with residue field k. Suppose k is imperfect with characteristic $p > 0$. We wish to exhibit non-trivial finite *separable* extensions F'/F (with residue field denoted k') such that $e(F'|F) = 1$ but k'/k is a non-trivial purely inseparable extension. In some cases the construction will even be Galois. Such extensions are *not* unramified: unramifiedness requires $e = 1$ and *separability* of the residue field extension. Recall that this separability aspect of the residual extension is crucial in the use of Hensel's lemma (or étale algebras) to prove that $\mathrm{Hom}_F(F_1, F_2) \to \mathrm{Hom}_k(k_1, k_2)$ is injective (even bijective) for finite extensions F_i/F with F_1/F unramified. Of course, if F'/F is a finite Galois extension with degree > 1 and with residual extension k'/k that is purely inseparable, then the reduction map $\mathrm{Gal}(F'/F) \to \mathrm{Aut}(k'/k)$ is non-injective because the source is non-trivial but the target is trivial.

We now proceed to give the desired constructions. Let $a \in k$ be an element that is not a pth power. Thus, $X^p - a \in k[X]$ is irreducible. Any monic $f \in A[X]$ with reduction $X^p - a$ in $k[X]$ must be irreducible in $F[X]$, by Gauss' lemma. Consider $f = X^p - \theta X - \widetilde{a}$ with $\theta \in \mathfrak{m}$, requiring $\theta \neq p^p(\widetilde{a}/(1-p))^{p-1}$ in K. (The case $\theta = 0$ is the one of most interest in characteristic 0.) In all cases, it is easy to check that f is separable, and clearly it has reduction $X^p - a$ in $k[X]$. Thus, $F' = F[X]/(f)$ is a degree-p separable extension of F and

its subring $A' \stackrel{\text{def}}{=} A[X]/(f)$ is a domain that is A-finite and $A'/\pi A' = k[X]/(X^p - a) = k'$ is a field, where $\pi \in A$ denotes a uniformizer. (We do not yet know that A' is a discrete valuation ring, or equivalently that it is the integral closure of A in F.) Hence, $\mathfrak{m}' = \pi A'$ is a principal maximal ideal in A'. This is the only maximal ideal of A' because any nonzero prime ideal of A' intersects A in its unique nonzero prime ideal πA and so contains $\pi A'$. It therefore follows from the axiomatic charactertization of discrete valuation rings as in the beginning of Serre's *Local Fields* that A' must be a discrete valuation ring, so A' is the integral closure of A in F. We conclude that $k' = A'/\mathfrak{m}'$ is the residue field associated to F' and $e(F'|F) = 1$ because a uniformizer of A is a uniformizer of A'. Thus, F'/F is a degree-p separable extension that has ramification degree 1 and residual extension k'/k that is purely inseparable of degree p. If F has characteristic 0 and contains a primitive pth root of unity then for $\theta = 0$ the extension $F' = F(\widetilde{a}^{1/p})$ is even Galois over F. As we noted above, in such Galois cases we cannot distinguish distinct F-automorphisms of F' by tracking their actions on k', since k' has no non-trivial k-automorphisms.

3. Trivial tame subextensions

Let F be the fraction field of a complete discrete valuation ring A. Assume that the residue field k has positive characteristic p. Recall that in our general study of finite separable extensions F' of F, say with maximal tamely ramified subextension F'_{t} and maximal unramified subextension F'_{un}, $[F'_{\mathrm{t}} : F'_{\mathrm{un}}]$ divides the prime-to-p part of $e = e(F'|F)$ (proof: $[F' : F'_{\mathrm{un}}] = [k' : k]_{\mathrm{i}} e$) and this divisibility is an equality when F'/F is Galois. (The proof of this uses Galois theory in an essential way: one forms the fixed field for a p-Sylow subgroup of $\mathrm{Gal}(F'/F'_{\mathrm{un}})$.) In particular, if F'/F is Galois and e is *not* a p-power then F'_{un} admits non-trivial totally tame extensions inside of F'.

We would like to determine if the Galois hypothesis is necessary for the equality of $[F'_{\mathrm{t}} : F'_{\mathrm{un}}]$ and the prime-to-p part of e. More specifically, we wish to determine if there exist examples of totally ramified separable extensions F'/F with degree $n = p^r n'$ for $r \geq 0$ and $p \nmid n'$ such that there exists no intermediate field with degree n' over F (which is to say, the necessary divisibility $[F'_{\mathrm{t}} : F] | n'$ is not an equality). Put another way, if F'/F is a finite separable extension then is $[F'_{\mathrm{t}} : F'_{\mathrm{un}}]$ necessarily as large as possible (that is, equal to the prime-to-p part of $e(F'|F)$)? For example, without a Galois condition, does non-triviality of the prime-to-p part of e "predict" the existence of non-trivial tame intermediate fields above F'_{un}? Indeed, the Galois hypothesis is unnecessary:

Theorem 3.1. *Let F be the fraction field of an arbitrary complete discrete valuation ring with residue characteristic $p > 0$. If F'/F is an arbitrary finite extension then $[F'_{\mathrm{t}} : F'_{\mathrm{un}}]$ is equal to the prime-to-p part of $e(F'|F)$.*

Proof. We will deduce the result from the Galois case. We can replace F' with the separable closure of F in F' without loss of generality, so we can assume F'/F is separable. We may also replace F with F'_{un} so that there are no nontrivial intermediate unramified extensions over F. Let $\widetilde{F}'$ be a finite extension of F' that is Galois over F. Let $\widetilde{F}'_{\mathrm{t}}$ and $\widetilde{F}'_{\mathrm{un}}$ be the maximal tamely ramified and maximal unramified subextensions for $\widetilde{F}'/F$. These are both Galois over F. Since $\widetilde{F}'_{\mathrm{un}}/F$ is finite Galois and F'/F is finite separable and their intersection (inside of $\widetilde{F}'$) is F (as F'/F has no non-trivial subextensions that are unramified over F), we conclude that these extensions are linearly disjoint. Thus, the compositum $F'\widetilde{F}'_{\mathrm{un}}$ is identified with $E = F' \otimes_F \widetilde{F}'_{\mathrm{un}}$. This latter extension has valuation ring $\mathscr{O}_{F'} \otimes_{\mathscr{O}_F} \mathscr{O}_{\widetilde{F}'_{\mathrm{un}}}$ (see the handout on finite étale algebras), so its ramification degree over $\widetilde{F}'_{\mathrm{un}}$ is equal to $e(F'|F)$.

If we can solve the problem for $E/\widetilde{F}'_{\mathrm{un}}$, which is to say that there exists a subextension whose degree over $\widetilde{F}'_{\mathrm{un}}$ is the prime-to-p part of the ramification degree $e(E|\widetilde{F}'_{\mathrm{un}}) = e(F'|F)$, then this is the maximal tamely ramified subextension E_{t} (as the residual degree for E over $\widetilde{F}'_{\mathrm{un}}$ is clearly a p-power) and so it is invariant under the action of $\mathrm{Gal}(\widetilde{F}'_{\mathrm{un}}/F)$ on $E = F' \otimes_F \widetilde{F}'_{\mathrm{un}}$. Thus, by Galois theory the fixed field K for this action is a subfield of F'/F such that $K\widetilde{F}'_{\mathrm{un}} = E_{\mathrm{t}}$, so $[K : F]$ is the prime-to-p part of $e(F'|F)$, as desired. Hence, we may replace F with $\widetilde{F}'_{\mathrm{un}}$ and F' with E to reduce to the case when $\widetilde{F}'/F$ has no non-trivial subextension unramified over F. Thus, $\widetilde{F}'_{\mathrm{t}}$ is the fixed field for the necessarily unique p-Sylow subgroup of $G = \mathrm{Gal}(\widetilde{F}'/F)$.

Let $L = F' \cap \widetilde{F}'_{\mathrm{t}}$. Since $\widetilde{F}'_{\mathrm{t}}/L$ is Galois and F'/L is finite separable, so these two extensions of L are linearly disjoint, $[F' : L]$ divides the integer $[\widetilde{F}' : \widetilde{F}'_{\mathrm{t}}]$ that is a p-power. However, L/F is a subextension of the tame extension $\widetilde{F}'_{\mathrm{t}}/F$, and this latter extension is totally tame because there are no non-trivial unramified subextensions in $\widetilde{F}'/F$. Thus, $[\widetilde{F}'_{\mathrm{t}} : F] = e(\widetilde{F}'_{\mathrm{t}}|F)$ is not divisible by p. Its factor $[L : F]$ is therefore also not divisible by p, so we conclude that L is an intermediate extension for F'/F with $[L : F]$ equal to the prime-to-p part of $[F' : F]$, which in turn is the prime-to-p part of $e(F'|F)$ (since F'/F has no non-trivial unramified subextensions). ■