Math 676. Global extensions approximating local extensions

1. Motivation

A very useful tool in number theory is the ability to construct global extensions with specified local behavior. This problem can arise in several different forms. For example, if F is a global field and $v_1, \dots, v_n$ is a finite set of distinct places of F equipped with finite separable extensions K_i'/F_{v_i}, and if S is an auxiliary finite set of non-archimedean places of F, does there exist a finite separable extension F'/F unramified at S such that the completion of F' at some place v_i' over v_i is F_{v_i}-isomorphic to K_i'? Moreover, if all extensions K_i'/F_{v_i} have degree d then can we arrange that $[F' : F]$ has degree d? If so, are there infinitely many such F' (up to F-isomorphism)?

An alternative problem is the following: if the extensions K_i'/F_{v_i} are Galois (and so have solvable Galois group, which is obvious when v_i is archimedean and which we saw in class in the non-archimedean case via the cyclicity of the Galois theory of the finite fields), then can we arrange for F'/F as above to also be Galois with solvable Galois group? If the extensions K_i'/F_{v_i} are abelian (resp. cyclic) then can we arrange for F'/F is have abelian (resp. cyclic) Galois group?

A typical example of much importance in practice is this: construct a totally real solvable extension $L/\mathbf{Q}$ that is unramified over a specified finite set of primes S of $\mathbf{Q}$ and induces a specified extension of $\mathbf{Q}_p$ for p in another disjoint finite set of primes. Here we are prescribing the local behavior of L at a finite set of primes p and also at the infinite place while insisting that L also be unramified at the auxiliary finite set S. In this handout we provide an affirmative answer to all such construction problems, though we must note at the outset that whereas the answer to the first problem (construction of F'/F with prescribed local behavior but no Galois conditions) will only require the weak approximation theorem (as in §9 of the handout on absolute values), the solution of the problems involving Galois groups will reduce to the abelian case whose solution requires class field theory (and so we will give suitable references in the book of Artin–Tate).

To indicate the subtle nature of such construction problems, consider the cyclic case of the preceding questions: if K_i'/F_{v_i} is cyclic with degree n_i for all i, can we find a cyclic extension F'/F inducing K_i'/F_{v_i} for each i? If such a construction can be done, then the cyclic group $\mathrm{Gal}(K_i'/F_{v_i})$ is the decomposition group at v_i in the cyclic group $\mathrm{Gal}(F'/F)$, and so $[F' : F]$ must be divisible by the least common multiple n of the n_i's. Can one always construct such a cyclic extensions F'/F with this minimal possible degree? It turns out that this is a subtle problem and in very special circumstances it has a negative answer, and then the best that can be done is $[F' : F] = 2n$. These special circumstances are exhaustively studied in Chapter X of Artin–Tate, and they only arise when F is a number field and some of the v_i's are non-archimedean with residue characteristic 2. We simply give an explicit counterexample here: $F = \mathbf{Q}$, $\{v_i\} = \{v_1\} = \{2\}$, and $K_1'/\mathbf{Q}_2$ the unramified extension of degree 8. There does *not* exist a cyclic extension $F'/\mathbf{Q}$ of degree 8 in which 2 is inert (which is to say that F' induces the degree-8 unramified extension of $\mathbf{Q}_2$). The proof of such non-existence can be given using class field theory, via the product formula for the norm residue symbol in cyclic extensions (see the discussion following Theorem 1 in §1, Chapter X in Artin–Tate). It can also be given in an elementary way as a consequence of the determination of $(2|p)$ for odd primes p; we leave this latter approach to non-existence as an exercise.

2. Approximation with one local field

Before we attack the problem of finding global extensions that induce given local extensions, we address an issue that we should have considered some time ago: is every local field K realized as a completion of a global field F? The archimedean case is obvious, and in the non-archimedean cases we treat characteristic 0 and positive characteristic separately, as follows. If K has positive characteristic then $K \simeq k(\!(t)\!)$ for a finite field k, and so we may take $F = k(t)$ and v to be the t-adic place of F. If K has characteristic 0 and residue characteristic p then K is a finite (separable) extension of $\mathbf{Q}_p$, and since $\mathbf{Q}$ is the p-adic completion of $\mathbf{Q}$ we may simply invoke the following theorem with $F = \mathbf{Q}$ and v the p-adic place. (Note that for this application to p-adic fields we only need the separable aspect of the theorem below, and this aspect is handled near the end of the proof by a simple self-contained application of Krasner's lemma.)

Theorem 2.1. *Let F be a global field and let v be a non-trivial non-archimedean place on F. Let K' be a finite extension of the local field $K = F_v$, say with degree d. There exists a finite extension F'/F with degree d and a place v' on F' over v such that $F'_{v'}$ is isomorphic to K' over the identification $F_v = K$. If K'/K is separable then F'/F must be separable.*

If K'/K is Galois, then there exists a finite Galois extension F'/F with a place v' over v and an intermediate field F_0 whose completion under v' is identified with $F_v = K$ such that $\mathrm{Gal}(F'/F_0)$ *is identified with* $\mathrm{Gal}(K'/K)$.

Note in particular that if K'/K is abelian then we can realize it as a completion of an abelian extension of global fields with the same Galois group. However, this comes at a serious cost: we have to replace the initial F with some unknown extension F_0. In the next section we will give a better solution to a generalization of the refined problem with Galois groups, avoiding the interference of the auxiliary F_0, by using the full power of class field theory.

Historically, the ability to realize an abelian extension of local fields as the completion of an abelian extension of global fields (with the same Galois group, but with weak control on the global base field) was important in the first approach to local class field theory via global class field theory. This is the approach followed in Lang's *Algebraic Number Theory*, but such an approach forces one to confront questions concerning dependence of the resulting theory on the choice of "global model" for a given local abelian extension. The approach to local class field theory via Galois cohomology (as in Serre's *Local fields*) is intrinsic to the local case and so avoids such hassles.

The reader will check that in the separable case, the proof below has nothing to do with global fields and so the result in the separable case is really a theorem about fraction fields of arbitrary discrete valuation rings.

Proof. Suppose we have such an F'. Let us show first that F'/F must be separable with v' the unique place on F' over v if K'/K is separable, in which case when F'/F is Galois then $\mathrm{Gal}(F'/F) = D(v'|v)$ obviously maps isomorphically to $\mathrm{Gal}(K'/K)$. Since $F'_{v'} = F'F_v = F'K$, the natural map $F' \otimes_F F_v \to F'_{v'}$ over F_v is surjective. Consideration of F_v-dimensions shows that this must be an isomorphism, and hence if $F'_{v'}/F_v$ is separable then the discriminant of the F_v-algebra $F' \otimes_F F_v$ is nonzero. Since the formation of the discriminant is compatible with extension of the base field, it follows that the discriminant of the F-algebra F' must be nonzero, and from the handout on étale algebras we know that this latter non-vanishing is equivalent to separability of the field extension F'/F. Since F'/F is separable, $F' \otimes_F F_v$ is F_v-isomorphic to the product of the completions of F' at the places over v on F', so since this tensor product is identified with $F'_{v'}$ we conclude that v' is indeed the unique place on F' over v.

Now we turn to the existence problem. By working in towers, we may separately treat the cases when K'/K is separable and (in characteristic $p > 0$) purely inseparable. We first dispose of the purely inseparable case, say with characteristic $p > 0$. We may assume K'/K has degree p, so $K' \subseteq K^{1/p}$. Since $K \simeq k(\!(t)\!)$ with k perfect (even finite) of characteristic p, it is clear that $K^{1/p} = k(\!(t^{1/p})\!) = K(t^{1/p})$ has degree p over K, so $K' \simeq K^{1/p}$ over K. In other words, K'/K is unique up to isomorphism. Let κ be the constant field of F and use Riemann–Roch to exhibit F as a finite separable extension of the field $F_0 = \kappa(t)$ such that v lies over the t-adic place of F_0. Note that t is not a pth power in F (as it is not a pth power in the subfield F_0 and F/F_0 is separable). Hence, $F' = F(t^{1/p})$ is a purely inseparable extension of degree p. There is a unique place v' on F' over v (why?) and $F'_{v'}$ contains a pth root of t. If we can show that t is not a pth power in F_v then it follows that the extension $F'_{v'} = F_v(t^{1/p})$ is purely inseparable of degree p and so realizes K'/K. Since v lies over the t-adic place on the subextension $F_0 = \kappa(t)$ over which F is finite separable, F_v is finite separable over the t-adic completion $\kappa(\!(t)\!)$ of F_0. Hence, t is a pth power in F_v if and only if it is a pth power in $\kappa(\!(t)\!)$, and so the obvious falsehood of this latter possibility shows that indeed t is not a pth power in F_v, as desired. This takes care of inseparability aspects. (Using stronger methods in commutative algebra, it can be proved that for any global function field F with characteristic p and any non-trivial place v on F, the non-algebraic extension of fields F_v/F is always separable in the sense of field theory, and so in particular an element of F that is not a pth power cannot become a pth power in F_v. This is best understood via Grothendieck's theory of excellent rings. The point of mentioning it here is to clarify that the preceding *ad*

hoc trick with Riemann–Roch is not really necessary if we grant ourselves better foundations in commutative algebra.)

It remains to study the more interesting (and more important) case when K'/F_v is a finite separable extension. By the primitive element theorem, we may write $K' \simeq F_v(\alpha)$ where α is a root of an irreducible separable monic polynomial $h \in F_v[T]$ with degree d. By Krasner's lemma, if $h_1 \in F_v[T]$ is a monic polynomial of degree d whose coefficients are sufficiently close to those of h, then h_1 is separable and irreducible with the field $F_v[T]/(h_1)$ isomorphic to $F_v[T]/(h) \simeq F_v(\alpha)$ over F_v. In other words, slightly moving h as a monic polynomial of degree d does not affect its usefulness as a way to describe K' over F_v. Hence, by denseness of F in F_v we may assume $h \in F[T]$. Irreducibility and separability of h over F_v forces the same over the subfield F, and thus $F' = F[T]/(h)$ is a finite separable extension of F with degree $\deg h = d$. Moreover, we have an F_v-algebra isomorphism $F_v \otimes_F F' \simeq F_v[T]/(h) \simeq K'$, yet since F'/F is a finite separable extension we have $F_v \otimes_F F' \simeq \prod_{v'|v} F'_{v'}$. Hence, it follows that v admits a unique extension to a place v' on F', and that $F'_{v'}$ is F_v-isomorphic to K'.

Finally, assume that K'/K is Galois. The finite separable extension F'/F as above is generally not Galois, so let F''/F' be a Galois closure of F' over F. Since F''/F is a splitting field for h, upon choosing a place v'' on F'' over v' we see that $F''_{v''} = F''F_v$ is a splitting field over $F_v = K$ for h. However, the subfield $K' = F'_{v'}$ is such a splitting field since K'/K is Galois and is generated by a root of h, so $F''_{v''} = F'_{v'}$. Taking F_0 to be the decomposition field for v'' over F, and v_0 to be the place on F_0 under v'', the general theory of the decomposition field shows that v'' is the unique place on F'' over v_0 and $D(v''|v) = D(v''|v_0)$, with $F''_{v''} = (F_0)_{v_0} \otimes_{F_0} F''$, and the resulting natural map

$$\mathrm{Gal}(K'/K) = \mathrm{Gal}(F''_{v''}/F_v) = \mathrm{Gal}(F''_{v''}/(F_0)_{v_0}) \to \mathrm{Gal}(F''/F_0) = D(v''|v_0) = D(v''|v)$$

an isomorphism. Hence, by completing F''/F_0 at v'' and v_0 we recover K'/K without changing the Galois group. ■

3. Approximation with several local fields

Having shown that any local field may be obtained by completing a global field at a suitable place, we can now turn to our main questions considered at the outset: can we simultaneously approximate extensions of finitely many completions of a fixed global field F with completions of a single finite extension of F? In other words, can we construct global extensions with prescribed local behavior? And how about refinements concerning the structure of local and global Galois groups? It is this simultaneous local approximation that will make use of weak approximation, as well as class field theory for the Galois aspects.

Let $v_1, \dots, v_n$ be distinct places of F and let K'_i/F_{v_i} be a finite extension. Can we find a finite extension F'/F and a place v'_i on F' over v_i such that $F'_{v'_i} \simeq K'_i$ over F_{v_i} for every i, with F'/F even separable (resp. Galois) when all K'_i/F_{v_i} are separable (resp. Galois)? This is a refinement of Theorem 2.1 in several respects: we permit several valuations at once, we allow archimedean places, and we insist on a *fixed* global base field F. If K'_i/F_{v_i} is separable for some i but inseparable for others then F'/F cannot be separable, so in such cases the simultaneous approximation is impossible: it can be proved that non-trivial inseparability in an extension of global function fields *cannot* be lost under passage to any completions. Likewise, if the inseparability degrees of K'_i/F_{v_i} are not all the same, the construction cannot be done. Hence, it is only reasonable to consider the cases when all K'_i/F_{v_i} are separable or all K'_i/F_{v_i} are inseparable with the same nontrivial degree of inseparability. Since local fields K of characteristic $p > 0$ admit exactly one purely inseparable extension of degree p^n for each $n > 0$ (namely, K^{1/p^n}), simultaneous approximation of inseparable local extensions with a common inseparability degree (which never comes up in practice, as far as I am aware) is easily reduced to the separable case. It is the separable case that is of fundamental importance, and so only this case will be considered in what follows.

Theorem 3.1. *Let F be a global field and let $v_1, \dots, v_n$ be inequivalent places on F. Let $K_i = F_{v_i}$, and let K'_i/K_i be finite separable extensions. There exists a finite separable extension F'/F and places v'_i on F' over v_i such that F'_{v_i} is K_i-isomorphic to K'_i for every i, and if $[K'_i : K_i] = d$ for all i then we can arrange*

that $[F' : F] = d$. If S is a finite set of non-archimedean places of F distinct from the v_i's then F'/F may be arranged to also be unramified over all places in S.

If moreover all K_i'/K_i are Galois then we can simultaneously arrange that F'/F is a solvable Galois extension. If in addition all K_i'/K_i are abelian then F'/F can be arranged to be abelian, and likewise for cyclic extensions.

Of course, in the Galois case it cannot be arranged that $[F' : F] = d$ if $[K_i' : K_i] = d$ for all i except for possibly if all of the Galois groups $\mathrm{Gal}(K_i'/K_i)$ are isomorphic (as each such decomposition group at v_i' must fill up the global group $\mathrm{Gal}(F'/F)$ for cardinality reasons). This is a very special situation that only seems to be tractable in the important cyclic case, in which case it has a negative answer in special situations; see Theorem 5 in §2, Chapter X in Artin–Tate for the full story concerning the degree aspects in the cyclic case. Our treatment of the Galois assertions in Theorem 3.1 will ultimately reduce to problems in class field theory that are solved in Chapter X of Artin–Tate.

Proof. Let $h_i \in F[T]$ be a monic irreducible separable polynomial such that $K_i' \simeq K_i[T]/(h_i)$ for each i; the existence of such h_i was shown via Kranser's lemma in the proof of Theorem 2.1 when v_i is non-archimedean, and it is trivial when v_i is archimedean (take $h_i = T$ if $K_i' = K_i$ and take $h_i = T^2+1$ if $K_i = \mathbf{R}$ and $K_i' \simeq \mathbf{C}$). Let $d = \max[K_i' : K_i]$, so by multiplying h_i against $d - \deg h_i$ distinct monic linears $T - \alpha_{ij}$ for $\alpha_{ij} \in F$ that are not roots of h_i, we get monic separable multiples $H_i \in F[T]$ of h_i with degree d such that K_i'/K_i is generated by a root of H_i, and in fact K_i'/K_i is a splitting field of H_i when K_i'/K_i is Galois.

Use weak approximation to find a monic polynomial $h \in F[T]$ that is v_i-close to H_i for every i, so in particular h is separable. Moreover, for some i we have $H_i = h_i$, and hence H_i is irreducible in $F_{v_i}[T]$ for such an i. Thus, by using sufficiently close approximation at this place we ensure that h is irreducible over F_{v_i} and so is irreducible over F. (Strictly speaking, this irreducibility step supposes that the distinguished place v_i is non-archimedean, but the archimedean analogue is trivial: the only non-linear monic irreducible polynomials in the archimedean case occur for monic quadratic polynomials in $\mathbf{R}[T]$ with negative discriminant, and in such cases a small perturbation of the lower-degree coefficients does not affect the sign of the discriminant and so does not affect irreducibility over $\mathbf{R}$.) Let $F' = F[T]/(h)$, so F'/F is finite separable with degree d.

For each i, we have

$$\prod_{v_i'|v_i} F'_{v_i} \simeq F_{v_i} \otimes_F F' \simeq F_{v_i}[T]/(h).$$

Since h and H_i are separable over F_{v_i}, by the theorem on continuity of roots (proved in the non-archimedean case in the handout on algebraic closedness of completions of algebraic closures in the non-archimedean case, and provable by elementary local compactness arguments in the archimedean case), it follows that the monic factorization type of h over F_{v_i} mirrors that of H_i in the sense that each monic irreducible factor of h is close to a unique monic irreducible factor of H_i with the same degree, with such closeness made as small as we please by taking h near enough to H_i in F_{v_i}. Hence, K_i' is a factor field of $F_{v_i}[T]/(h)$ and thus we can find a suitable $v_i'|v_i$ on F' for each i such that $F'_{v_i'}$ is F_{v_i}-isomorphic to K_i'. Moreover, if $[K_i' : K_i] = d$ for all i then our construction yields $[F' : F] = d$.

Now let S be a finite set of non-archimedean places away from the v_i's, and we ask if F'/F can be chosen to be unramified at all places in S. This is very easy: since $h \in F[T]$ is a monic polynomial of degree d that is merely constrained by approximation conditions on its lower-degree coefficients when viewed in F_{v_i} for each i, weak approximation permits us to arrange for h to also be simultaneously near any desired monic polynomial of degree d in $F_v[T]$ for each $v \in S$. There exists a monic irreducible polynomial $h_v \in \mathscr{O}_{F_v}[T]$ with degree d and $\mathrm{disc}(h_v) \in \mathscr{O}_{F_v}^\times$ for every $v \in S$, such as a monic lift of a separable irreducible polynomial of degree d over the finite residue field at each such v, and so we can arrange that $h \in F[T]$ is v-integral and separable irreducible over F_v with $\mathrm{disc}(h) \in F^\times$ a v-adic unit for all $v \in S$. It follows that $F_v \otimes_F F' \simeq F_v[T]/(h)$ is an unramified extension field of F_v for every $v \in S$, so each $v \in S$ is unramified (and even inert) in F'.

Assume that K_i'/K_i is Galois for each i. We seek to make F'/F such that F'/F is also Galois, with Galois group that is even solvable (and moreover abelian when all K_i'/K_i are abelian, and similarly in the cyclic case). Moreover, we wish to carry out such refined constructions while maintaining unramifiedness

conditions at a fixed finite set of non-archimedean places S disjoint from the v_i's. By the Galois theory of local fields (and the trivial archimedean case), the finite Galois extensions K_i'/K_i are *solvable*. Suppose we have solved the case when each K_i'/K_i is abelian. If the solvable extension K_1'/K_1 is not abelian then there exists a non-trivial intermediate field L, and by induction on field-degrees can find a solvable F'/F that "works" for the local extensions L/K_1 and K_i'/K_i for all $i > 1$. Now we use induction again, with this F' as the base field and with the local extensions K_1'/L and the trivial extensions K_i'/K_i' for $i > 1$ (and S replaced with the set of places over it in F') to get a further solvable extension F''/F'. The extension F''/F is finite separable but probably not Galois. However, it is clear (check!) that the Galois closure of F'' over F is solvable and does the job.

It remains to consider the case when all K_i'/K_i are abelian. By Theorem 4 in §2, Chapter X of Artin–Tate, there exists a finite abelian extension F'/F equipped with places v_i' over v_i such that F'_{v_i} is F_{v_i}-isomorphic to K_i' for all i and such that F' is unramified over each $v \in S$. By Theorem 5 in §2, Chapter X of Artin–Tate, the same holds in the cyclic case. ■

We conclude with two important classes of typical examples, one Galois and one not.

Example 3.2. Let F be global field and let $v_1, \dots, v_n$ be a set of distinct places on F. Let K_i'/F_{v_i} be a finite separable extension of degree $d > 1$. We claim that there exist infinitely many non-isomorphic finite separable extensions F'/F with degree d such that v_i is inert in F' with $F'_{v_i} \simeq K_i'$ over F_{v_i} for all i. By Theorem 3.1, we can use separable Eisenstein polynomials of degree d at non-archimedean places away from the v_i's to make separable extensions F'/F of degree d such that each v_i is inert in F' with $F'_{v_i} \simeq K_i'$ over F_{v_i} for every i and F'/F is totally ramified (resp. unramified) at any desired auxiliary finite set of non-archimedean places of F. Thus, by ramification reasons alone we infer that up to F-isomorphism there exist infinitely many F'/F that satisfy the requirements at the v_i's because a totally ramified extension of degree $d > 1$ cannot be unramified.

Example 3.3. Let F be a totally real number field (such as $F = \mathbf{Q}$), and let $\{v_1, \dots, v_n\}$ be a finite set of non-archimedean places of F. Let K_i'/F_{v_i} be a finite Galois extension. We claim that there exists a totally real solvable extension F'/F inducing K_i'/F_{v_i} as the local extension at v_i for each i, that such F'/F can be chosen to be unramified (resp. totally ramified) at any auxiliary finite set of places, and that if all K_i'/F_{v_i} are abelian (resp. cyclic) then F'/F can be taken to be abelian (resp. cyclic). Of course, as we vary the auxiliary finite set of ramification conditions, we would be getting necessarily non-isomorphic extensions of F.

Theorem 3.1 provides an affirmative answer to the preceding claim, as we merely insert the archimedean (all real) places of F into the collection of v_i's and at these places we impose the local condition that F'/F induces the extension $\mathbf{R}/\mathbf{R}$ at each of the real places of F. This ensures that F' is a totally real number field. Of course, we could similarly arrange that F' is totally complex.