Math 676. Tame ramification and composite fields

1. Review of tameness

Let F be the fraction field of a complete discrete valuation ring A with residue field k. Recall that a finite separable extension F'/F (with valuation ring A' and residue field k' that are necessarily finite free modules over A and k respectively) is *tamely ramified* if k'/k is separable and $\mathrm{char}(k) \nmid e(F'|F)$. If moreover $k' = k$ then we say that F'/F is *totally tamely ramified*; that is, F'/F is totally tamely ramified if $e(F'|F) = [F' : F]$ and $\mathrm{char}(k) \nmid e(F'|F)$.

If $\pi \in A$ is a uniformizer and $e > 0$ is a positive integer not divisible by $\mathrm{char}(F)$ then $X^e - \pi \in A[X]$ is separable and moreover irreducible over F (by Gauss' Lemma and Eisenstein's criterion). Thus, $F' = F[X]/(X^e - \pi)$ is a field, typically denoted $F(\pi^{1/e})$ (with $\pi^{1/e}$ denoting the residue class of X), and F'/F is separable of degree e with $\pi^{1/e}$ in the valuation ring contributing a factor of $e = [F' : F]$ in $e(F'|F)$. This forces F'/F to be totally ramified with $\pi^{1/e}$ as a uniformizer, so via $\pi^{1/e}$-adic expansions we see that the valuation ring of F' is exactly $A' = A[\pi^{1/e}] = A[X]/(X^e - \pi)$. This is a special case of the proof in class that adjoining the root to any Eisenstein polynomial gives a uniformizer for a totally ramified extension.

If $\mathrm{char}(k) \nmid e$ then $F(\pi^{1/e})$ is a totally tamely ramified extension, and we have seen in an earlier lecture that every totally tamely ramified extension of F arises by this construction for a suitable π. That is, whereas we proved in general that every totally ramified extension of F is obtained by adjoining a root to an Eisenstein polynomial over A, in the totally tame case we saw (via Hensel's Lemma) that this Eisenstein polynomial could be chosen to be of an especially simple form, namely $X^e - \pi$ for *some* choice of uniformizer π in A.

Beware that for a general tame extension F'/F (with valuation ring A' and residue k', but possibly $[k' : k] > 1$), it is *not* usually the case that there is a uniformizer of F' whose $e(F'|F)$th power lies in F. The best we can say is that if F_{u}/F is the maximal unramified subextension then this has residue field k' (here we use that k'/k is separable!) and F'/F_{u} is totally tamely ramified (why?). Hence, $F' = F_{\mathrm{u}}(\pi_{\mathrm{u}}^{1/e})$ with $e = e(F'|F_{\mathrm{u}}) = e(F'|F_{\mathrm{u}})e(F_{\mathrm{u}}|F) = e(F'|F)$ and $\pi_{\mathrm{u}} \in F_{\mathrm{u}}$ some uniformizer, but usually π_{u} cannot be found inside of F. In Homework 11 there is given an explicit example of such impossibility for $F = \mathbf{Q}_5$ and $[F' : F] = 4$ with $e(F'|F) = 2$.

To summarize, there is a reasonably "concrete" description of tamely ramified extensions F' of F, especially when F is a local field (in which case the maximal unramified subextension F_{u} in F'/F is a cyclotomic extension $F(\zeta_{q^f-1})$ with $q = \#k$ and $f = f(F'|F) = [k' : k]$). We would like to show that the property of tameness is reasonably well-behaved in the sense that it is preserved under formation of composite fields.

Due to lack of technical typing skills by the author, there are no field diagrams in this handout. The reader is strongly encouraged to draw field diagrams in order to more easily understand some of the arguments with various field extensions in what follows.

2. Composite fields

Let F'/F be a finite extension that is a compositum of two subextensions F_1' and F_2' over F. We shall express this condition by writing $F' = F_1'F_2'$, but this is slightly abusive notation because one must always remember that the concept of a composite of two finite extensions over a base field is generally *not* intrinsic to the abstract fields unless there is a condition of linear disjointness (which is to say that $F_1' \otimes_F F_2'$ is local, or equivalently is a field in the case that at least one of the F_i''s is separable over F). That is, the notation $F_1'F_2'$ only has meaning insofar as we have given ourselves a pair of F-embeddings of the F_i''s into a common extension of F.

Let A', A_1', and A_2' be the respective valuation rings of F', F_1', and F_2'. Although F' is a quotient of $F_1' \otimes_F F_2'$ by elementary field theory, it is *very rare* that A' is a quotient of $A_1' \otimes_A A_2'$. In general all one can say is that the A-subalgebra of A' generated by A_1' and A_2' is an order in A' (why is it at least an order?). For this reason, it is difficult to see "by hand" how properties of the A_i''s over A translate into properties of A' over A, or how properties of A_1' over A translate into properties of A' over A_2'. To make progress we

have to make fuller use of the structure theory of the fraction fields (such as multiplicativity properties of e's and f's, and so forth).

We have seen in class that unramifiedness is a rather well-behaved condition in the sense that if F_1'/F is unramified then F'/F_2' is unramified, and that consequently if F_1' and F_2' are unramified over F then $F' = F_1'F_2'$ is unramified over F. Our goal is to show the same holds for the property of tameness. The main result of this handout is:

Theorem 2.1. *Let F'/F be a compositum of subfields F_1' and F_2' of finite degree over F, with F_1'/F tamely ramified. The extension F'/F_2' is tamely ramified. In particular, if F_1' and F_2' are both tame over F then F'/F is tamely ramified.*

The final part of the theorem follows from the rest because of the trivial fact (from the definitions) that if $K''/K'/K$ is a tower of finite extensions of the fraction field K of a complete discrete valuation ring then K''/K is tame if and only if K''/K' and K'/K are each tame. Thus the real problem is to show that F'/F_2' is tame when F_1'/F is tame.

Example 2.2. Beware that the theorem becomes false if we try to replace "tame" with "totally tame" or even "totally ramified". Indeed, it can often happen that each F_i'/F is totally ramified (both tame, or even both wild) yet F'/F_1' and F'/F_2' are each unramified! (This does not contradict Theorem 2.1 because unramified extensions are obviously tamely ramified.)

For counterexamples in the tame and wild cases, we consider $F = \mathbf{Q}_p$ and non-isomorphic ramified quadratic extensions F_1' and F_2' of $\mathbf{Q}_p$. Such a pair of fields are linearly disjoint over F, so $F' = F_1' \otimes_F F_2'$ is a quartic extension. For odd p, there are exactly two quadratic ramified extensions, namely $F_1' = \mathbf{Q}_p(\sqrt{p})$ and $F_2' = \mathbf{Q}_p(\sqrt{up})$ for $u \in \mathbf{Z}_p^\times$ with non-square reduction $\overline{u} \in \mathbf{F}_p^\times$. Hence, $F = \mathbf{Q}_p(\sqrt{p}, \sqrt{u})$. The residue field k' of F' contains a square root of the non-square $\overline{u}$ in $\mathbf{F}_p$, so k' contains a quadratic extension of $\mathbf{F}_p$. Hence, $2|f(F'|F)$. However, the ramified quadratic subfields F_i' contribute a factor $2 = e(F_i'|F)$ in $e(F'|F)$. Since $e(F'|F)f(F'|F) = [F' : F] = 4$, we conclude $e(F'|F) = 2$ and $f(F'|F) = 2$. Since $e(F_i'|F) = 2$ and $e(F'|F_i')e(F_i'|F) = e(F'|F) = 2$, this forces $e(F'|F_i') = 1$; similarly, $f(F_i'|F) = 1$ forces $f(F'|F_i') = 2$. To summarize, for odd p the totally tame extensions F_1' and F_2' have compositum F' that is quadratic *unramified* over each F_i' and in particular F'/F is *not* totally ramified even though each F_i'/F is totally ramified.

Taking $p = 2$, let $F_1' = \mathbf{Q}_2(\sqrt{2})$ and $F_2' = \mathbf{Q}_2(\sqrt{-6})$, so $F = \mathbf{Q}_2(\sqrt{2}, \sqrt{-3})$. Since $(-1 + \sqrt{-3})/2 = \zeta_3$ is a primitive cube root of unity, the residue field of F must contain $\mathbf{F}_4$. Arguing as above with the e's and f's, we again conclude that F/F_i' is an unramified quadratic extension for each i even though each F_i'/F is a totally (wildly) ramified extension.

The moral is that $e(F'|F_2')$ cannot be easily predicted from knowledge of $e(F_1'|F)$ and $e(F_2'|F)$, and even if F_1'/F is wildly ramified it can happen that F'/F_2' is not wildly ramified and in fact F'/F_2' may have no non-trivial ramification whatsoever (that is, F'/F_2' can be unramified). Roughly speaking, F_2'/F can "eat up" all of the ramification in F'/F that comes from F_1'/F. The impossibility of formally computing $e(F'|F_2')$ in terms of e's and f's for F_1'/F and F_2'/F is what makes the proof of Theorem 2.1 require a bit of thought.

3. Proof of Theorem 2.1

We first wish to reduce to the case when F_1'/F is totally tamely ramified (so that it admits a simple description as extraction of an eth root of some uniformizer of F for some e not divisible by $\mathrm{char}(k)$). Since F_1'/F is tame, if we let $L \subseteq F_1'$ be the maximal unramified subextension over F then separability for k_1'/k implies that L has residue field k_1' and hence F_1'/L is totally tamely ramified. If we let L_2' denote the composite field LF_2' over F then $L_2' = LF_2'$ is unramified over F_2' because L is unramified over F (this is the "unramified" variant on Theorem 2.1 that was proved in class). Hence, by viewing the extension F'/F_2' as the tower $F'/L_2'/F_2'$ with L_2'/F_2' unramified we see that F'/F_2' is tame if and only if F'/L_2' is tame. Since $F' = F_1'F_2' = F_1'LF_2' = F_1'L_2'$ we may therefore rename L_2' as F_2' and L as F without loss of generality so as to reduce to the case when F_1'/F is totally tamely ramified.

With F_1'/F now totally tamely ramified, we may write $F_1' = F(\alpha)$ with $\alpha^e = \pi$ for some uniformizer $\pi \in F$ and some $e = e(F_1'|F)$ not divisible by $\mathrm{char}(k)$. Hence, $F' = F_1'F_2' = F_2'(\alpha)$ with $\alpha^e = \pi$ a nonzero

element in the maximal ideal of A_2' (even in the maximal ideal of A). Note that $\pi \in A_2'$ can fail to be a uniformizer (when F_2'/F is not unramified), and this is why it is hard to detect how much ramification is introduced on top of F_2' in F' by adjoining an eth root of π to F_2'. Beware also that the irreducible polynomial $X^e - \pi \in F[X]$ may be reducible in $F_2'[X]$ with factors of varying degrees, in which case $[F' : F_2']$ cannot be predicted without further information concerning the specific irreducible factor of $X^e - \pi$ in $F_2'[X]$ having α is a root. That is, if $\mathrm{ord}_{F_2'}(\pi) > 1$ then $X^e - \pi \in F_2'[X]$ may be reducible and hence the notation $F_2'(\pi^{1/e})$ is not well-defined and so can be very dangerous!

It now suffices to prove the following general claim concerning tameness:

Lemma 3.1. *Let K be the fraction field of a complete discrete valuation ring R with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. Choose $c \in \mathfrak{m} - \{0\}$, and let K'/K be a finite extension satisfying $K' = K(\alpha)$ with $\alpha^e = c$ for a positive integer e not divisible by* $\mathrm{char}(k)$*. Any such extension K'/K is tamely ramified with $e(K'|K) = e/\gcd(e, \mathrm{ord}_R(c))$.*

Remark 3.2. The formula for $e(K'|K)$ forces $e(K'|K)$ to not be divisible by the residue characteristic (due to the assumptions on e), but we emphasize (for those who wish to allow possibly imperfect residue fields to be considered in the general theory) that there is an auxiliary assertion in the lemma, namely that the residue field extension k'/k is separable. Do not forget to observe that all assertions of tameness throughout the proof must keep track of this property as well.

Before we prove the lemma, we note that $e(K'|K)$ can fail to equal e, and in fact $e(K'|K)$ may even equal 1 (that is, K'/K may be unramified). This is exactly the source of possibilities such as in Example 2.2. What is going on is that we have not specified $\mathrm{ord}_R(c)$, and if we do not know this value then we cannot rule out the possibility that $c = \pi^e u$ for a uniformizer $\pi \in R$ and a unit $u \in R^\times$. In such cases $K' = K(u')$ with $u' = \alpha/\pi$ satisfying $u'^e = u \in R^\times$, and such extensions (with e not divisible by the residue characteristic) are necessarily unramified!

To see why unramifiedness is automatic in such cases, first note that $X^e - u \in R[X]$ has *separable* reduction (here we use the fact that e is not divisible by the residue characteristic and that u has nonzero reduction), and so the unique irreducible monic factor $h \in R[X]$ of the K-separable $X^e - u$ with $h(u') = 0$ has separable reduction $\overline{h}$ in $k[X]$. Thus, the order $R' = R[X]/(h)$ in $K' \simeq K[X]/(h)$ satisfies $\mathrm{disc}(R'/R) = \mathrm{disc}(h)R = R$, and hence R' is finite étale over R. This in turn forces R' to be a discrete valuation ring (by the handout on finite étale algebras) that is unramified over R; explicitly, by the definition of R' we see $R'/\pi R' = k[X]/(\overline{h}) = k'$ is a field, so $\pi R'$ is visibly the maximal ideal.

Remark 3.3. The preceding discussion shows that extracting an eth root of a unit gives an unramified extension whenever e is not divisible by the residue characteristic. The example of the unramified quadratic extension $\mathbf{Q}_2(\sqrt{-3})/\mathbf{Q}_2$ shows that in some cases one can get unramified extensions by adjoining an eth root of a unit even when e is divisible by the residue characteristic, but this is very rare. More typical is that one gets ramification, such as in the extensions $\mathbf{Q}_2(\sqrt{-1})/\mathbf{Q}_2$ and $\mathbf{Q}_2(\sqrt{3})/\mathbf{Q}_2$. Explicitly, the identities

$$(1 + \sqrt{-1})^2 = 2\sqrt{-1}, \quad (1 + \sqrt{3})^2 = 2(2 + \sqrt{3})$$

in the valuation rings of $\mathbf{Q}_2(\sqrt{-1})$ and $\mathbf{Q}_2(\sqrt{3})$ shows that 2 is a *unit* multiple of a square in each case and hence the nonzero nonunit 2 cannot be a uniformizer in these valuation rings. (Where does this sort of calculation break down if we try it for $\mathbf{Q}_2(\sqrt{-3}) \simeq \mathbf{Q}_2(\sqrt{5})$?)

Now we turn to the proof of Lemma 3.1. The idea of the proof is to make a series of successive modifications to a concrete description of K'/K (or some auxiliary fields obtained via the harmless operation of forming composites against the unramified extensions of the base field) to eventually get to the case where we are extracting an e'th root of a *uniformizer* for $e' = e/\gcd(e, \mathrm{ord}_R(c))$, an extension that is totally tame *by inspection*. (Since there will be interemediate reduction steps that require replacing the base field with an unramified extension, we will lose touch with the initial residue field and so we certainly will not be able to prove the generally false statement that K'/K is totally ramified.)

Proof. Since c is a nonzero nonunit in R, we may write $c = \pi^i u$ for a unique integer $i > 0$ and $u \in R^\times$; clearly $i = \mathrm{ord}_R(c)$. The factor u is a bit of an annoyance when studying an eth root of c, so we want to get

rid of it. Let $L = K(u')$ with $u'^e = u$ and let L' be a compositum of L and K' over K. The discussion above Remark 3.3 shows that L/K is *unramified*, so L'/K' is unramified. Hence, K'/K is tame if and only if L'/K is tame. Consideration of the tower $L'/L/K$ with L/K unramified shows that L'/K is tame if and only if L'/L is tame. Since $L' = LK' = L(\alpha)$ with $\alpha^e = c = \pi^i u = \pi^i u'^e$ for a unit u' in L and a uniformizer π of L (as L/K is unramified!), we may replace K'/K with L'/L and replace α and c with α/u' and $c/u = c/u'^e$ respectively to get to the case when $c = \pi^i$ for some $i > 0$ and some uniformizer π in the base field. Since the cyclotomic extension $K(\zeta_e)/K$ is unramified (as e is not divisible by the residue characteristic!), we may pass through the same reduction steps to get to the case when K contains a primitive eth root of unity.

To sumarize, we have reduced to the case $K' = K(\alpha)$ with $\alpha^e = \pi^i$ for some $i > 0$ and some uniformizer π of K, and with K containing a primitive eth root of unity. It may happen that $d = \gcd(e, i)$ exceeds 1. In general, we write $e = de'$ and $i = di'$ with $\gcd(e', i') = 1$ and $(\alpha^{e'})^d = (\pi^{i'})^d$, so $\alpha^{e'} = \zeta\pi^{i'}$ with $\zeta^d = 1$. Note that e' is not divisible by $\mathrm{char}(k)$ since $e'|e$. Since $d|e$ and K contains a primitive eth root of unity, the dth root of unity ζ in K admits an (e/d)th root in K. Since $e/d = e'$, we can write $\zeta = \zeta'^{e'}$ in $K^\times$ for some eth root of unity ζ'. Thus, $K' = K(\alpha) = K(\alpha/\zeta')$ with $(\alpha/\zeta')^{e'} = \pi^{i'}$. We may therefore replace α with α/ζ' and e and i with e' and i' respectively (recall that e' is not divisible by $\mathrm{char}(k)$, so this step does not ruin any basic assumptions on the exponent of root extraction). We have brought ourselves to the case $\alpha^e = \pi^i$ with $\gcd(e, i) = 1$.

Since $\gcd(e, i) = 1$, there exist $a, b \in \mathbf{Z}$ such that $ae + bi = 1$. Thus,

$$(\alpha^b\pi^a)^e = \alpha^{eb}\pi^{ae} = \alpha^{eb}\pi^{1-bi} = \pi(\alpha^e/\pi^i)^b = \pi.$$

The extension $K' = K(\alpha)$ generated by a root of $X^e - \pi^i \in R[X]$ has degree at most e, yet it contains an eth root $\alpha' = \alpha^b/\pi^a$ of a uniformizer π. The subfield $K(\alpha')$ is totally tamely ramified of degree e over K, so degree considerations over K force the inclusion $K(\alpha') \subseteq K'$ to be an equality and thereby gives the result that $K' = K(\alpha')$ is a totally tamely ramified extension of K with ramification degree e. In particular, K'/K is tame with $e(K'|K) = e$. Unwinding the reduction steps and returning to the notation at the start, we have shown that the original extension is tamely ramified with ramification degree $e/\gcd(e, \mathrm{ord}_R(c))$ dividing e. ■