Weakly ramified extensions

Bence Forrás

June 2022

Galois module structure seminar, talks 10–11

This pair of talks is based on Henri Johnston's paper [Joh15]. These notes were produced in preparation for the talks; apart from the typos, mistakes, and errors, nothing here is my intellectual product. Questions, comments, and suggestions for improvement are welcome. Thanks go out to Andreas Nickel for answering my many questions.

Warning. To me, 'local field' means a complete discretely valued field with finite residue field. Note that this differs from the terminology of the main reference [Joh15], which is why I have tried to avoid using this expression as much as possible. Most statements will be formulated for field extensions more general than just local fields (e.g. extensions of complete discretely valued fields with separable residue field extension). The reader may mentally replace these with local fields or even p-adic fields without missing out on much. I don't know whether one can generalise this theory by relaxing the completeness assumption to henselianity.

0 Introduction

Recall that for L/K finite Galois extension of complete discretely valued fields with separable residue field extension (e.g. with finite residue fields), then we have the ramification filtration on the Galois group $G = \mathrm{Gal}(L/K)$:

$$G_i = \{\sigma \in G : \sigma(\pi_L) \equiv \pi_L \bmod \mathfrak{P}_L^{i+1}\}$$

where π_L is some fixed uniformiser of $\mathcal{O}_L$. Recall that G_0 is the inertia subgroup of G, and G_1 is its p-part, called the wild inertia subgroup.

Definition 0.1. An extension L/K as above is *weakly ramified* if $G_2 = 1$.

In Guillermo's 1st talk, we have seen that unramified extensions as well as tamely and totally ramified extensions admit a NIB, that is, $\mathcal{O}_L$ is a free $\mathcal{O}_K[G]$-module. Conversely, in Riccardo's 1st talk we have seen that any extension of fields as above has to be tamely ramified if it has a NIB. Consequently, we cannot expect weakly ramified extensions (which may be wild) to admit a NIB. However, we can still ask whether $\mathcal{O}_L$ admits a free generator over some larger $\mathcal{O}_K$-order Γ in $K[G]$. We have seen that the only possible candidate for Γ is the associated order $\mathcal{A}_{L/K}$, see [Joh11, Proposition 3.15]. Indeed, we will see in my first talk that $\mathcal{O}_L$ is free (of rank 1) over the associated order (Theorem 2.1).

We can also ask for an explicit description of the generator, which will lead us to study the structure of the maximal ideal $\mathfrak{P}_L$ over $\mathcal{O}_K[G]$. It will turn out that $\mathfrak{P}_L$ (and certain powers of it) admits a free $\mathcal{O}_K[G]$-generator, which we will be able to describe explicitly (Theorem 3.4). One may consider this to be another weakening of the concept of a NIB: instead of enlarging

the order over which we study the Galois module structure (as in the previous paragraph), we shrink the module to be studied from $\mathcal{O}_L$ to $\mathfrak{P}_L$.

1 Examples of weakly ramified extensions

As a start, we will give an example of a wildly ramified extension. This will require some background from the theory of complete discretely valued fields.

We shall make use of Hilbert's formula. First recall that for an extension L/K of discretely valued fields, the different is defined to be the following fractional ideal:

$$\mathfrak{D}_{L/K} := \left\{x \in L : \forall y \in \mathcal{O}_L \ \mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_K\right\} \subset L$$

It follows directly from the definition that if $\mathfrak{a}$ resp. $\mathfrak{b}$ are fractional ideals of $\mathcal{O}_K$ resp. $\mathcal{O}_L$ then $\mathrm{Tr}_{L/K}(\mathfrak{b}) \subseteq \mathfrak{a}$ iff $\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{D}_{L/K}^{-1}$.

Proposition 1.1 (Hilbert's formula, [Ser68, IV§1, Prop. 4]). *Let L/K be a finite Galois extension of complete discretely valued fields with separable residue field extension. Then*

$$v_L(\mathfrak{D}_{L/K}) = \sum_{i=0}^{\infty}(\#G_i - 1)$$

Note that the sum on the right hand side is in fact finite, because $G_i = 1$ for $i \gg 0$.

Proof. We know from Riccardo's 2nd talk that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ for some $\alpha \in \mathcal{O}_L$, that is, x gives rise to a PIB. Let f denote the minimal polynomial of x over K. It is a well-known property of the different that $\mathfrak{D}_{L/K}$ is generated by $f'(x)$ [Ser68, III§6, Cor. 2 of Prop. 11]. Since

$$f(X) = \prod_{\sigma \in \mathrm{Gal}(L/K)} (X - \sigma(x)),$$

the formal derivative at x is

$$f'(x) = \prod_{1 \neq \sigma \in \mathrm{Gal}(L/K)} (x - \sigma(x)),$$

which allows one to compute the valuation of the different:

$$v_L(\mathfrak{D}_{L/K}) = v_L(f'(x)) = \sum_{1 \neq \sigma \in \mathrm{Gal}(L/K)} v_L(\sigma(x) - x)$$

It is easily seen (and was essentially shown in Riccardo's 2nd talk) that $v_L(\sigma(x) - x) \geqslant i + 1$ iff $\sigma \in G_i$. The claim follows. □

Remark 1.2. If the extension is totally ramified, Hilbert's formula gives a convenient tool for checking whether the extension is weakly ramified. Indeed, in this case $\#G_0$ is the degree and $\#G_1$ is the p-part of the degree, wherefore

$$\text{total ramification is weak} \quad \Leftrightarrow \quad v_L(\mathfrak{D}_{L/K}) = (L : K) + (L : K)_p - 2$$

We will use this repeatedly in the sequel. ○

Proposition 1.3 (Local cyclotomic extensions, [Ser68, IV§4, Prop. 17+18]). *Let ζ_{p^n} be a primitive p^nth root of unity. The extension $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ has the following properties.*

1) It is Galois with Galois group isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

2) It is totally ramified, and $\zeta_{p^n} - 1$ *is a uniformiser.*

3) The ramification groups are as follows:

$$\begin{aligned} G_0 &\simeq (\mathbb{Z}/p^n\mathbb{Z})^\times, \\ G_1 = \ldots = G_{p-1} &\simeq \{a \in (\mathbb{Z}/p^n\mathbb{Z})^\times : a \equiv 1 \bmod p\}, \\ G_p = \ldots = G_{p^2-1} &\simeq \{a \in (\mathbb{Z}/p^n\mathbb{Z})^\times : a \equiv 1 \bmod p^2\}, \\ &\vdots \\ G_{p^{n-2}} = \ldots = G_{p^{n-1}-1} &\simeq \{a \in (\mathbb{Z}/p^n\mathbb{Z})^\times : a \equiv 1 \bmod p^{n-1}\}, \\ G_{p^{n-1}} = \ldots &\simeq \{a \in (\mathbb{Z}/p^n\mathbb{Z})^\times : a \equiv 1 \bmod p^n\} = 1 \end{aligned}$$

Proof. The first assertion is easy. The second one is standard, using that totally ramified extensions are given by an Eisenstein polynomial, and the element in question has Eisenstein minimal polynomial. The third assertion then follows by computing the valuation of $\sigma(\zeta_{p^n}) - \zeta_{p^n}$. I suppose these could also be proven by exploiting the local-global property of ramification invariants and using our knowledge of global cyclotomic extensions. □

Example 1.4 ([Joh15, Example 5.4]). Let K be a finite unramified extension of $\mathbb{Q}_p$. By the theory of finite fields, any such K is obtained by adjoining a $(p^r - 1)$st root of 1 to $\mathbb{Q}_p$. In particular, K may contain no pth root of unity. Therefore $\mathrm{Gal}(K(\zeta_{p^2}/K) \simeq \mathbb{Z}/p \times (\mathbb{Z}/p)^\times$. Let L be the unique extension of K of degree p inside $K(\zeta_{p^2})$. We claim that L/K is totally, wildly and weakly ramified.

The claim that the ramification is total follows directly from the facts on local cyclotomic extensions; the unramified extension K is just a base change, and does not change ramification behaviour. As the degree is p, total ramification implies wildness. Finally, weakness can be verified by applying Hilbert's formula and the following property of the different in towers: $\mathfrak{D}_{K(\zeta_{p^2})/K} = \mathfrak{D}_{K(\zeta_{p^2})/L}\mathfrak{D}_{L/K}$. Indeed, Hilbert's formula yields

$$\begin{aligned} v_{K(\zeta_{p^2})}(\mathfrak{D}_{K(\zeta_{p^2})/K}) &= (\#G_0 - 1) + (\#G_1 - 1) + \ldots + (\#G_{p-1} - 1) \\ &= p(p-1) - 1 + (p-1)(p-1) = 2p^2 - 3p \end{aligned}$$

We can also apply Hilbert's formula to the tamely and totally ramified extension $K(\zeta_{p^2})/L$:

$$v_{K(\zeta_{p^2})}(\mathfrak{D}_{K(\zeta_{p^2})/L}) = (p-1) - 1 = p - 2$$

It follows that

$$\begin{aligned} v_L(\mathfrak{D}_{L/K}) &= \frac{1}{p-1}\left(v_{K(\zeta_{p^2})}(\mathfrak{D}_{L/K})\right) \\ &= \frac{1}{p-1}\left(v_{K(\zeta_{p^2})}(\mathfrak{D}_{K(\zeta_{p^2})/K}) - v_{K(\zeta_{p^2})}(\mathfrak{D}_{K(\zeta_{p^2})/L})\right) \\ &= \frac{2p^2 - 3p - p + 2}{p-1} = 2p - 2 \end{aligned}$$

Applying Hilbert's formula (or rather Remark 1.2) to L/K, we see that $G_2(L/K)$ must be trivial. So L/K is indeed weakly ramified.

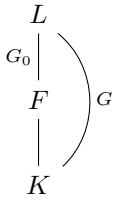
In the same way, it can be shown that $\mathbb{Q}_p(\zeta_{p^2})/\mathbb{Q}_p$ is not weakly ramified, but $\mathbb{Q}_p(\zeta_{p^2})/\mathbb{Q}_p(\zeta_p)$ is. ○

2 Wildly and weakly ramified extensions over $\mathcal{A}_{L/K}$

Theorem 2.1 ([Joh15, Theorem 1.2])**.** *Let L/K be a wildly and weakly ramified finite Galois extension of complete discretely valued fields with finite residue fields. Let $G = \mathrm{Gal}(L/K)$ and fix an arbitrary uniformiser π_K of $\mathcal{O}_K$. Then the associated order is $\mathfrak{A}_{L/K} = \mathcal{O}_K[G][\pi_K^{-1}\operatorname{Tr}_{G_0}]$, and any free generator of $\mathfrak{P}_L$ over $\mathcal{O}_K[G]$ is also a free generator of $\mathcal{O}_L$ over $\mathfrak{A}_{L/K}$.*

Remark 2.2. We will later see that any wildly and weakly ramified extension admits a free $\mathcal{O}_K[G]$-generator of $\mathfrak{P}_L$, so the theorem is always applicable. It shows that while we know that a NIB – that is, a free generator over $\mathcal{O}_K[G]$ – for wildly ramified extensions is out of the question, we have the next best thing: a free generator over the slightly larger associated order. ○

Proof. Let $F := L^{G_0}$ be the inertia subfield, that is, F/K is the maximal unramified subextension of L/K. Since L/K is wild, so is L/F, whence $\operatorname{Tr}_{L/F}(\mathcal{O}_L) \neq \mathcal{O}_F$ by [Joh11, Corollary 7.3], wherefore $\operatorname{Tr}_{L/F}(\mathcal{O}_L) \subseteq \mathfrak{P}_F$.



Since F/K is unramified, the uniformiser π_K of $\mathcal{O}_K$ is also a uniformiser of $\mathcal{O}_F$. Therefore

$$\pi_K^{-1}\operatorname{Tr}_{G_0}(\mathcal{O}_L) = \pi_K^{-1}\operatorname{Tr}_{L/F}(\mathcal{O}_L) \subseteq \pi_K^{-1}\mathfrak{P}_F = \pi_K^{-1}\pi_K\mathfrak{P}_F = \mathcal{O}_F \subseteq \mathcal{O}_L$$

Recalling that $\mathfrak{A}_{L/K} = \{x \in K[G] : x\mathcal{O}_L \subseteq \mathcal{O}_L\}$, we find that $\mathcal{O}_K[G][\pi_K^{-1}\operatorname{Tr}_{G_0}] \subseteq \mathfrak{A}_{L/K}$. Moreover, if ε is a free generator of $\mathfrak{P}_L$ over $\mathcal{O}_K[G]$ then $\mathcal{O}_K[G][\pi_K^{-1}\operatorname{Tr}_{G_0}]\cdot\varepsilon \subseteq \mathfrak{A}_{L/K}\cdot\varepsilon \subseteq \mathcal{O}_L$.

These give one half of each of the two assertions of the theorem; it remains to show that these containments are in fact equalities. We will show that the second containment is an equality through the use of generalised module indices. The first equality will follow directly from this.

The following will be one step in the aforementioned index computation. Let $S \subseteq G$ be a set of coset representatives for G/G_0, and let $T := \{\pi_K^{-1}s\operatorname{Tr}_{G_0} : s \in S\}$. We now make a series of claims about this:

- •) $\pi_K^{-1}\operatorname{Tr}_{G_0}$ *is a central nilpotent element if* $\operatorname{char} K = p$.
  Indeed,
  $$\left(\pi_K^{-1}\operatorname{Tr}_{G_0}\right)^2 = \pi_K^{-2}\sum_{\sigma\in G_0}\sum_{\sigma'\in G_0}\sigma\sigma' = \pi_K^{-2}\cdot\#G_0\cdot\operatorname{Tr}_{G_0} = 0$$
  since $p \mid \#G_0$. It is also central because G_0 is normal in G, hence multiplication by any element of G just permutes the summands of the trace around.

- •) $\pi_K^{-1}\operatorname{Tr}_{G_0}$ *is an $\mathcal{O}_K$-multiple of a central idempotent if* $\operatorname{char} K = 0$.
  Indeed, $\pi_K^{-1}\operatorname{Tr}_{G_0} = \#G_0\cdot\pi_K^{-1}\cdot\left((\#G_0)^{-1}\cdot\operatorname{Tr}_{G_0}\right)$, and
  $$\left(\frac{1}{\#G_0}\cdot\operatorname{Tr}_{G_0}\right)^2 = \frac{1}{(\#G_0)^2}\cdot\#G_0\cdot\operatorname{Tr}_{G_0} = \frac{\operatorname{Tr}_{G_0}}{\#G_0}$$
  is an idempotent. Centrality is as above.

- •) *$T \cup G \cup \{0\}$ is a multiplicatively closed subset of $\mathcal{O}_K[G]$.*
  This is obvious.
- •) *$T \cup G$ spans $\mathcal{O}_K[G]\left[\pi_K^{-1}\operatorname{Tr}_{G_0}\right]$ over $\mathcal{O}_K$.*
  This is obvious.
- •) *The elements of T are linearly independent over $\mathcal{O}_K$.*
  This is because S is a set of coset representatives.

Consider the generalised module index

$$\left[\mathcal{O}_K[G]\left[\pi_K^{-1}\operatorname{Tr}_{G_0}\right] : \mathcal{O}_K[G]\right]_{\mathcal{O}_K}$$

Recall that for a local ring $\mathcal{O}$, a $\operatorname{Frac}(\mathcal{O})$-vector space V, and $\mathcal{O}$-lattices L, M in V, the index $[L : M]_{\mathcal{O}}$ is the fractional ideal of $\mathcal{O}$ generated by the determinant of any automorphism of V that maps L to M. (We have also seen generalised module indices in the global case, that is, for modules over Dedekind domains, but we will only need the local version in this proof.)

In our setup, by our deliberations above, we have an $\mathcal{O}_K$-linear map given by $\pi_K^{-1} s \operatorname{Tr}_{G_0} \mapsto s \operatorname{Tr}_{G_0}$ for all $s \in S$ and $g \mapsto g$ for all $g \in G$. Its determinant is $\pi_K^{\#S}$, whence the generalised module index is

$$\left[\mathcal{O}_K[G]\left[\pi_K^{-1}\operatorname{Tr}_{G_0}\right] : \mathcal{O}_K[G]\right]_{\mathcal{O}_K} = \mathfrak{P}_K^{\#S}$$

We are now ready to prove that $\mathcal{O}_K[G][\pi_K^{-1}\operatorname{Tr}_{G_0}] \cdot \varepsilon = \mathfrak{A}_{L/K} \cdot \varepsilon = \mathcal{O}_L$:

$$\begin{aligned}
[\mathcal{O}_L : \mathfrak{P}_L]_{\mathcal{O}_K} &= [\mathcal{O}_F : \mathfrak{P}_F]_{\mathcal{O}_K} && \text{by Lemma 2.3}\\
&= \mathfrak{P}_K^{[F:K]} && \text{see below}\\
&= \mathfrak{P}_K^{\#S} && (F:K) = \#(G/G_0)\\
&= \left[\mathcal{O}_K[G]\left[\pi_K^{-1}\operatorname{Tr}_{G_0}\right] : \mathcal{O}_K[G]\right]_{\mathcal{O}_K} && \text{see above}\\
&= \left[\mathcal{O}_K[G]\left[\pi_K^{-1}\operatorname{Tr}_{G_0}\right]\cdot\varepsilon : \mathcal{O}_K[G]\cdot\varepsilon\right]_{\mathcal{O}_K} && \text{see below}\\
&= \left[\mathcal{O}_K[G]\left[\pi_K^{-1}\operatorname{Tr}_{G_0}\right]\cdot\varepsilon : \mathfrak{P}_L\right]_{\mathcal{O}_K} && \varepsilon \text{ is an } \mathcal{O}_K[G]\text{-generator of } \mathfrak{P}_L
\end{aligned}$$

The first equation is a direct application of Lemma 2.3: indeed, since L/F is totally ramified, the residue fields $\mathcal{O}_L/\mathfrak{P}_L$ and $\mathcal{O}_F/\mathfrak{P}_F$ agree, so the respective group indices $\#(\mathcal{O}_L/\mathfrak{P}_L)$ and $\#(\mathcal{O}_F/\mathfrak{P}_F)$ also agree, wherefore the module indices over $\mathcal{O}_K$ agree as well.

The second equation follows from the fact that $\mathcal{O}_F$ is a free $\mathcal{O}_K$-module of dimension $(F : K)$ because F/K is unramified, hence in particular tame; an appropriate linear map multiplies each generator by π_K, and has determinant $\pi_K^{(F:K)}$, which generates $\mathfrak{P}_K^{(F:K)}$.

To justify the penultimate step, consider the $K[G]$-module homomorphism $\vartheta : K[G] \to L, x \mapsto x\varepsilon$. By definition, ε is a free generator of $\mathfrak{P}_L$ over $\mathcal{O}_K[G]$. It follows that $\vartheta|_{\mathcal{O}_K[G]}$ is injective. Extending scalars from $\mathcal{O}_K$ to K, we see that ϑ itself is also injective. It follows that for any two $\mathcal{O}_K$-lattices M, N in $K[G]$, the indices $[M : N]_{\mathcal{O}_K} = [M \cdot \varepsilon : N \cdot \varepsilon]_{\mathcal{O}_K}$ agree. Apply this with $M := \mathcal{O}_K[G]\left[\pi_K^{-1}\operatorname{Tr}_{G_0}\right]$ and $N := \mathcal{O}_K[G]$.

From the index calculation above, we get that

$$\mathcal{O}_K[G][\pi_K^{-1}\operatorname{Tr}_{G_0}] \cdot \varepsilon \overset{*}{=} \mathfrak{A}_{L/K} \cdot \varepsilon \overset{**}{=} \mathcal{O}_L$$

$(**)$ implies that ε is a free generator of $\mathcal{O}_L$ over $\mathfrak{A}_{L/K}$: indeed, injectivity comes from ϑ being injective, hence all its restrictions being injective. Moreover, $(*)$ and $(**)$ together imply that $\mathcal{O}_K[G][\pi_K^{-1}\operatorname{Tr}_{G_0}]$ also has image $\mathcal{O}_L$ under ϑ, and from injectivity it follows that $\mathfrak{A}_{L/K} = \mathcal{O}_K[G][\pi_K^{-1}\operatorname{Tr}_{G_0}]$. □

Lemma 2.3 ([Joh11, Remark 4.2]). *Let $(\mathcal{O}, \mathfrak{p})$ be a local ring and let $N \subseteq M$ be $\mathcal{O}$-lattices in a vector space V over the field of fractions of $\mathcal{O}$ (in particular, M and N are free $\mathcal{O}$-modules of the same rank). Then $[M : N]_{\mathcal{O}} = \#(M/N)\mathcal{O}$. In words, the local generalised module index is determined by the group index.*

This may have been mentioned in Riya's talk, but I think it was not proven then.

Proof. First note that since the ring $\mathcal{O}$ is local, the ideal generated by an element $x \in \mathcal{O}$ is uniquely determined by the norm $\#(\mathcal{O} : x\mathcal{O})$ of said element.

Using the structure theorem of finitely generated modules over PIDs, we have that there are bases $m_1, \dots, m_k$ resp. $n_1, \dots, n_k$ of M resp. N such that $m_i = \alpha_i n_i$ for some $\alpha_i \in \mathcal{O}$ for all $i = 1, \dots, k$. Therefore an automorphism of V mapping M to N is given by the diagonal matrix

$$\begin{pmatrix} \alpha_1 & & & \\ & \alpha_2 & & \\ & & \ddots & \\ & & & \alpha_k \end{pmatrix}$$

The generalised module index is by definition $[M : N]_{\mathcal{O}} = \prod_{i=1}^{k} \alpha_i \mathcal{O} = \mathfrak{p}^{\sum_{i=1}^{k} v(\alpha_i)}$ where v is the valuation on $\mathcal{O}$. The norm is $p^{\sum_{i=1}^{k} v(\alpha_i) \cdot f}$ where $f = (\mathcal{O}/\mathfrak{p} : \mathbb{F}_p)$ is the inertia degree.

On the other hand, the group index is $\#(M/N) = \#(\mathcal{O}/\det(\alpha)) = \prod_{i=1}^{k} \#(\mathcal{O}/\alpha_i))$, which again has norm $p^{\sum_{i=1}^{k} v(\alpha_i) \cdot f}$. □

3 Arbitrary weakly ramified extensions over $\mathcal{O}_K[G]$

We are interested in free generators of Galois modules such as $\mathcal{O}_L$ or $\mathfrak{P}_L^n$ over $\mathcal{O}_K[G]$ where $G = \mathrm{Gal}(L/K)$. Time and again we will use the following lemma: it is a combination of elementary observations and Nakayama's lemma, and its argument has essentially been used by Guillermo in his proof of Proposition 9.1 of the notes.

Lemma 3.1 ([Joh15, Lemma 2.1]). *Let L/K be a finite Galois extension of complete discretely valued fields with residue fields ℓ/k. Let $\mathcal{I} \neq 0$ be a fractional ideal of $\mathcal{O}_L$, and $\overline{\mathcal{I}} := \mathcal{I}/\mathfrak{P}_K\mathcal{I}$. Let $\bar{\delta} \in \overline{\mathcal{I}}$ with lift $\delta \in \mathcal{I}$. The following are equivalent:*

1) *$\overline{\mathcal{I}} = k[G] \cdot \bar{\delta}$*
2) *$\mathcal{I} = \mathcal{O}_K[G] \cdot \delta$*
3) *$\bar{\delta}$ is a free $k[G]$-generator of $\overline{\mathcal{I}}$*
4) *δ is a free $\mathcal{O}_K[G]$-generator of $\mathcal{I}$*

Proof. 2) ⇒ 1) is obvious.

1) ⇒ 2) is a Nakayama style argument. Recall that (one instance of) Nakayama's lemma states that

Lemma 3.2 (Nakayama, [CR81, (5.7)]). *For A a ring with A and M a left A-module and $L \subseteq M$ a submodule, if $L + \mathrm{rad}(A)M = M$ then $L = M$, where $\mathrm{rad}(A)$ denotes the Jacobson radical, that is, the intersection of all maximal left ideals of A.*

By definition and 1),

$$\mathcal{I} = \overline{\mathcal{I}} + \mathfrak{P}_K\mathcal{I} = k[G]\bar{\delta} + \mathfrak{P}_K\mathcal{I} = \mathcal{O}_K[G]\delta + \mathfrak{P}_K\mathcal{I}$$

Next, note that $\mathrm{rad}(\mathcal{O}_K[G]) \supseteq \mathfrak{P}_K \cdot \mathcal{O}_K[G]$. Indeed, it is true in general that

Lemma 3.3. *If $(R, \mathfrak{m})$ is a commutative local ring and A an R-algebra that is finitely generated as an R-module, then* $\operatorname{rad}(A) \supseteq \mathfrak{m}A$.

Proof (Proof of Lemma 3.3). We show that $\mathfrak{m}A \cdot M = 0$ for all simple left A-modules M. This is enough, since an alternative characterisation of the Jacobson radical is $\operatorname{rad}(A) = \bigcap_M \operatorname{ann} M$. Any such M is finitely generated: indeed, $M = Am$ for any $m \in M \notin \{0\}$ by simplicity. Therefore Nakayama's lemma is applicable, and we have that $\mathfrak{m}M \neq M$ (unless $M = 0$). Since $\mathfrak{m}M \subset M$ and M is simple, this means $\mathfrak{m}M = 0$, so $\mathfrak{m}A \cdot M = 0$. □

From Lemma 3.3 it follows that

$$\mathcal{I} = \mathcal{O}_K[G]\delta + \mathfrak{P}_K\mathcal{I} = \mathcal{O}_K[G]\delta + \operatorname{rad}(\mathcal{O}_K[G])\mathcal{I}$$

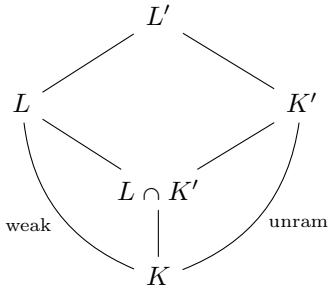
Now Nakayama's lemma finishes the proof.

2) ⇒ 4) Consider the map $\mathcal{O}_K[G] \to \mathcal{I}$, $x \mapsto x \cdot \delta$. Assumption 2) states that this map is surjective. On the other hand, both $\mathcal{O}_K[G]$ and $\mathcal{I}$ are rank 1 $\mathcal{O}_K[G]$-modules, hence the map is also injective.

4) ⇒ 2) is obvious.

The implications 1) ⇒ 3) and 3) ⇒ 1) can be proved in an analogous fashion, replacing everything by its mod $\mathfrak{P}_K$ reduction. □

Theorem 3.4 ([Joh15, Theorem 4.2])**.** *Let L/K be a weakly ramified finite Galois extension of complete discretely valued fields with finite residue fields. Let $G = \operatorname{Gal}(L/K)$ and let $n \in \mathbb{Z}$ such that $n \equiv 1 \bmod \#G_1$. Let d be any positive integer divisible by the exponent of G. Let K'/K be the unique unramified extension of degree d and let $L' = LK'$. Then L'/K is Galois, weakly ramified, and doubly split. Let $\varepsilon' \in L'$ be any free generator of $\mathfrak{P}_{L'}^n$ over $\mathcal{O}_K[\operatorname{Gal}(L'/K)]$. Then $\varepsilon := \operatorname{Tr}_{L'/L}(\varepsilon')$ is a free generator of $\mathfrak{P}_L^n$ over $\mathcal{O}_K[G]$.*



Remark. The assertion that L'/K is Galois and doubly split has been shown in Riccardo's 2nd talk (keywords: Schur–Zassenhaus theorem, Frattini argument). What remains to be shown is that L'/K is weakly ramified and the assertion that the weakly ramified extension L/K inherits any free generator of the weakly ramified extension L'/K. ○

Remark. Note that the theorem does not make any statement on where this generator ε' comes from, but it reduces the study of weakly ramified extensions to the study of weakly ramified *and doubly split* extensions. We will see an explicit construction of a free generator for the latter, which will then, by virtue of this theorem, settle the general case as well. (For now, recalling what doubly split even means is not necessary: the point is that it is a more specific class of extensions. The precise definition will be recalled later.) ○

In the proof, we will need a general fact on the behaviour of ramification groups in a tower of extensions.

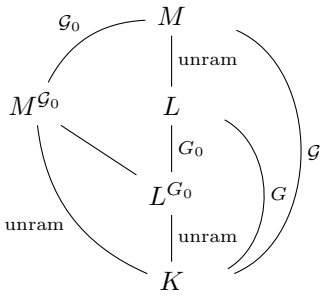
Proposition 3.5 ([Byo99, Prop. 4.4]). *If K is a complete discretely valued field with finite residue field, and $L \subseteq M$ are finite Galois extensions of K with M/L unramified, then the natural map*

$$\mathcal{G} := \mathrm{Gal}(M/K) \twoheadrightarrow G := \mathrm{Gal}(L/K), g \mapsto \bar{g}$$

induces isomorphisms $\mathcal{G}_i \to G_i$ of ramification groups for all $i \geqslant 0$.
In particular, M/K is weakly ramified iff L/K is.

Remark. Byott only considers finite extensions of $\mathbb{Q}_p$ in his paper [Byo99], and therefore it is enough for him to assume that M/L is normal. Here we allow positive characteristic, which is why we must insist that M/L is also Galois. ○

Proof.



$\mathrm{Gal}(M/L) \cap \mathcal{G}_0 = 1$ since M/L is unramified. It follows that the canonical surjection induces an injection $\mathcal{G}_0 \hookrightarrow G_0$. But the orders of these two finite groups are the same: $\#\mathcal{G}_0 = e(M/K) = e(L/K) = \#G_0$ as M/L in unramified, whence $\mathcal{G}_0 \cong G_0$.

To show the assertion for $i \geqslant 1$, let $g \in \mathcal{G}_0$ with image $\bar{g} \in G_0$. Then

$$\bar{g} \in G_i \;\Leftrightarrow\; (\bar{g}-1)\pi_L \in \mathfrak{P}_L^{i+1} \;\Leftrightarrow\; (g-1)\pi_M \in \mathfrak{P}_M^{i+1} \;\Leftrightarrow\; g \in \mathcal{G}_i$$

where we use that $\pi_M = \pi_L$. □

Proof (Proof of Theorem 3.4). First notice that L'/L is unramified. Indeed, $L/L \cap K'$ is totally ramified and $K'/L \cap K'$ is unramified, so by looking at the fundamental equation we deduce that L'/L must be unramified. This allows us to apply Proposition 3.5 to deduce that L'/K is weakly ramified.

We have $\mathrm{Tr}_{L'/L}(\mathfrak{P}_{L'}^n) = \mathfrak{P}_L^n$. Indeed, we have seen that for tame (and in particular, unramified) extensions, $\mathrm{Tr}_{L'/L}(\mathcal{O}_{L'}) = \mathcal{O}_L$ [Joh11, Corollary 7.3]; since L' and L share the same uniformiser π_L, and the trace map is $\mathcal{O}_L$-linear, we have

$$\mathrm{Tr}_{L'/L}(\mathfrak{P}_{L'}^n) = \mathrm{Tr}_{L'/L}(\pi_L^n \mathcal{O}_{L'}) = \pi_L^n \,\mathrm{Tr}_{L'/L}(\mathcal{O}_{L'}) = \pi_L^n \mathcal{O}_L = \mathfrak{P}_L^n$$

as claimed. Using this,

$$\begin{aligned}
\mathfrak{P}_L^n &= \mathrm{Tr}_{L'/L}(\mathfrak{P}_{L'}^n) && \text{by previous paragraph} \\
&= \mathrm{Tr}_{L'/L}(\mathcal{O}_K[\mathrm{Gal}(L'/K)] \cdot \varepsilon') && \text{by assumption} \\
&= \mathcal{O}_K[\mathrm{Gal}(L'/K)] \cdot \mathrm{Tr}_{L'/L}(\varepsilon') \\
&= \mathcal{O}_K[\mathrm{Gal}(L/K)] \cdot \mathrm{Tr}_{L'/L}(\varepsilon') && \mathrm{Tr}_{L'/L}(\varepsilon') \in L
\end{aligned}$$

Apply Lemma 3.1 2) ⇒ 4) with $\mathcal{I} := \mathfrak{P}_L^n$. □

4 Doubly split weakly ramified extensions over $\mathcal{O}_K[G]$

Recall the notion of various splittings from Riccardo's second talk.

Definition 4.1. An extension L/K of complete discretely valued fields with finite residue fields and Galois group G, inertia group $G_0 = I$, and wild inertia $G_1 = W$ is

- •) *split wrt. inertia* if $G = I \rtimes U$
- •) *split wrt. wild inertia* if $G = W \rtimes T$
- •) *doubly split* if the above two hold, and $I = W \rtimes C$.

In particular, unramified extensions are always doubly split ($I = 1$). We have also seen that the Schur–Zassenhaus theorem implies that totally ramified extensions are always doubly split.

Recall that we have reduced the study of arbitrary weakly ramified extensions to studying weakly ramified and doubly split extensions. Our strategy for doing so is to break down the problem to even more special, and hence more manageable, extensions. We shall do this in the following steps, the first two of which have already been taken in Guillermo's first talk:

0. *Unramified extensions:* there is a NIB, and it is given by any lift of a generator of the residue field extension.
0. *Totally and tamely ramified extensions:* there is a NIB, and it is given by any $\alpha = \sum u_i \pi_L^i$ where $u_i \in \mathcal{O}_L^\times$.
1. *Totally and weakly ramified p-extensions:* using results from representation theory of finite p-groups.
2. *Totally and weakly ramified extensions of arbitrary degree:* using the previous two steps.
3. *Weakly ramified and doubly split:* break up into unramified and totally weakly ramified extensions. It will be the doubly split property that allows us to do this in a way that helps.

4.1 Totally and weakly ramified p-extensions

4.1.1 Representation-theoretic interlude

Proposition 4.2 ([Joh15, Proposition 5.1])**.** *Let p be a prime, F a field of characteristic p and G a finite p-group. Let M be a left $F[G]$-module such that $\dim_F M = \#G$ and let $\mathrm{Tr}_G := \sum_{g\in G} g$. Let $x \in M$. Then x is a free $F[G]$-generator of M iff $\mathrm{Tr}_G \cdot x \neq 0$, i.e. $\mathrm{Tr}_G \notin \mathrm{Ann}_{F[G]}(x)$.*

Proposition 4.2 is an easy consequence of the following:

Lemma 4.3 ([CO81, Corollary (a)])**.** *For F a (skew) field of characteristic p and G a finite p-group, the group algebra $F[G]$ has unique minimal left ideal $F[G] \cdot \mathrm{Tr}_G$.*

Proof (Proof of Proposition 4.2). Let $x \in M$, and consider the right-multiplication-by-x map

$$\begin{aligned} m_x : F[G] &\to M \\ y &\mapsto yx \end{aligned}$$

In these terms, x is a free $F[G]$-generator of M iff m_x is a bijection. By assumption, m_x has domain and codomain of the same F-dimension, hence it is a bijection iff $\mathrm{Ann}_{F[G]}(x) = 0$. Since $F[G]$ has minimal left ideal generated by Tr_G, this is equivalent to $\mathrm{Tr}_G \notin \mathrm{Ann}_{F[G]}(x) = 0$, or $\mathrm{Tr}_G \cdot x \neq 0$. □

Lemma is, in turn, a direct consequence of the following:

Proposition 4.4 ([CO81, Theorem 2]). *For F a (skew) field of characteristic p and G a finite p-group, any module M over the group algebra $F[G]$ has a nonzero element m such that for all $\sigma \in G$, $\sigma m = m$.*

Proof (Proof of Lemma 4.3). On the one hand, $F[G] \cdot \mathrm{Tr}_G \simeq F$, which is simple, hence the ideal is minimal. Conversely, let $0 \neq L \subseteq F[G]$ be a nonzero left ideal. Apply Proposition 4.4 to $M := L$: then L has a nonzero element $\sum_{\sigma \in G} a_\sigma \sigma$ fixed by all σ's. But the σ-action on G is transitive and free, i.e. it permutes the coefficients of the sum around, which means that it is fixed under the action iff all coefficients agree, that is, iff the element is $a \cdot \mathrm{Tr}_G$ for some $a \in F$. Since $a \cdot \mathrm{Tr}_G \neq 0$, and F is a (skew) field, this already generates the ideal $F[G] \cdot \mathrm{Tr}_G$. □

Proof (Proof of Proposition 4.4). Write $\#G = p^n$. Since G is a finite p-group, it admits a normal series

$$G = G_n \rhd G_{n-1} \rhd \ldots \rhd G_0 = 1$$

with factor groups $G_{r+1}/G_r \simeq C_p$, $r = 0, \ldots, n-1$. The proof will be done by finite induction on this series.

Let $M_r := \{m \in M : \forall \sigma \in G_r : \sigma m = m\}$. Obviously $M_0 = M \neq 0$. We want to show that $M_n \neq 0$. We will now prove that $M_r \neq 0$ implies $M_{r+1} \neq 0$ for all r. This is clearly enough to prove Proposition 4.4.

Let $x \in M_r - \{0\}$ and τG_r a generator of G_{r+1}/G_r. Since the factor group is C_p, we have that $\tau^p \in G_r$, whence $\tau^p x = x$. For all $k \geqslant 0$, define

$$x_k := \sum_{i=0}^{p-1} i^k \tau^i x$$

We have that $x_k \in M_r$ because $\tau G_r = G_r \tau$ (since $G_r \lhd G_{r+1}$) and $x \in M_r$. Since the factor group G_{r+1}/G_r has order p, we have

$$\tau x_0 \overset{\text{def}}{=} \tau \left(x + \tau x + \ldots + \tau^{p-1} x \right) = \tau x + \ldots + \tau^{p-1} x + x \overset{\text{def}}{=} x_0$$

This shows that $x_0 \in M_{r+1}$, which means that we are done unless $x_0 = 0$.

So assume that $x_0 = \ldots = x_{k-1} = 0$ for some $k \geqslant 1$. Then for x_k, we have that

$$\begin{aligned}
\tau x_k &= \tau \left(\sum_{i=0}^{p-1} i^k \tau^i x \right) \\
&= \sum_{i=0}^{p-1} i^k \tau^{i+1} x \\
&= \sum_{i=1}^{p} (i-1)^k \tau^i x \\
&= (p-1)^k \tau^p x + \sum_{i=1}^{p-1} (i-1)^k \tau^i x \\
&= \sum_{i=0}^{p-1} (i-1)^k \tau^i x && (p-1)^k = (-1)^k \text{ akd } \tau^p x = x \\
&= \sum_{i=0}^{p-1} i^k \tau^i x + \sum_{i=0}^{p-1} \left((i-1)^k - i^k \right) \tau^i x
\end{aligned}$$

$$= x_k + \sum_{j=0}^{k-1} \sum_{i=0}^{p-1} (-1)^{k-1-j} \binom{k}{j} i^j \tau^i x$$

The sum in the last line is an F-linear combination of $x_0, \ldots, x_{k-1}$: indeed, there are k of these, and the sum has k terms (over j). But by assumption, these are all zero, hence $x_k \in M_{r+1}$.

This shows that we are done unless $x_k = 0$ for all $k \geqslant 0$. We now show that this is impossible. More precisely, we will see that even $x_0 = \ldots = x_{p-1} = 0$ is impossible. $\lightning$ Assume that $x_0 = \ldots = x_{p-1} = 0$. Let $g(X) = \sum_{j=0}^{p-1} a_j X^j \in F[X]$ be any polynomial. Then

$$\sum_{i=0}^{p-1} g(i)\tau^i x = \sum_{j=0}^{p-1} a_j \sum_{i=0}^{p-1} i^j \tau^i x = \sum_{j=0}^{p-1} a_j x_j = 0$$

Now choose $g(X) := \frac{1}{(p-1)!} \prod_{r=1}^{p-1} (r - X)$; clearly $g(0) = 1$ and $g(1) = \ldots = g(p-1) = 0$. This means that the sum $\sum_{i=0}^{p-1} g(i)\tau^i x$ is on the one hand x, on the other hand zero by the general computation above. Therefore $x = 0$. $\lightning$

This finishes the proof. □

Remark 4.5. From the statements above it follows easily that for a field F of characteristic p, and a finite p-group G, the group algebra $F[G]$ is local, and its unique maximal ideal is the augmentation ideal. Note that this is complementary to Maschke's theorem, which states that the group algebra $F[G]$ is semisimple if the order of the finite group G is coprime to the characteristic of F. ○

4.1.2 Back to number theory

Recall that an elementary abelian p-group is an abelian group in which every element has order p. By the structure theorem of finite abelian groups, a finite elementary abelian p-group is isomorphic to a direct product of finitely many copies of $\mathbb{Z}/p\mathbb{Z}$.

Theorem 4.6 ([Joh15, Theorem 5.2]). *Let L/K be a totally and weakly ramified Galois p-extension of complete discretely valued fields with perfect residue fields of characteristic $p > 0$. Then*

1) *$G = \mathrm{Gal}(L/K)$ is an elementary abelian p-group.*
2) *$\mathfrak{P}_L^n$ is a free (rank one) $\mathcal{O}_K[G]$-module iff $n \equiv 1 \bmod \#G$.*
3) *Suppose there is a free generator, that is, $n \equiv 1 \bmod \#G$. Then $\delta \in L$ is a free generator of $\mathfrak{P}_L^n$ over $\mathcal{O}_K[G]$ iff $v_L(\delta) = n$.*

Proof. First we prove 1). For this, we need the following

Lemma 4.7 ([Ser68, IV§2. Cor. 3]). *Let L/K be a finite Galois extension of complete discretely valued fields with separable residue field extension ℓ/k. If ℓ has characteristic $p > 0$ then the quotient groups G_i/G_{i+1} are elementary abelian p-groups for all $i \geqslant 1$.*

Proof (Proof of Lemma 4.7.). As we have seen in Riccardo's 2nd talk, there is an injective homomorphism

$$G_i/G_{i+1} \hookrightarrow U_L^i/U_L^{i+1}, [\sigma] \mapsto \left[\frac{\sigma(\pi_L)}{\pi_L}\right]$$

Moreover, for $i \geqslant 1$, there is an isomorphism of abelian groups $U_L^i/U_L^{i+1} \simeq \ell$, so we may view G_i/G_{i+1} as a subgroup of ℓ. Subgroups of ℓ can be seen as vector spaces over the prime field $\mathbb{F}_p$.

As G_i/G_{i+1} is finite, this means that it is isomorphic (as an abelian group) to the direct sum of finitely many copies of $\mathbb{F}_p$, which is the definition of an elementary abelian p-group. □

Since $G_2 = 1$, in the weakly ramified case this means that G_1 itself is an elementary abelian p-group.

On the other hand, since ramification is total, $G = G_0$. We know that $U_L^0/U_L^1 \simeq \ell^\times$, which has order prime to p. Since G_0/G_1 injects into this, and G is a p-group by assumption, it follows that $G_0/G_1 = 1$. Hence $G = G_0 = G_1$ is an elementary abelian p-group. This proves 1).

Now we prove the 'only if' part of 2). Our strategy will be the following: we compute the trace of $\mathfrak{P}_L^i$; then reducing by $\mathfrak{P}_K$, we can apply Proposition 4.2; then we come back to the non-reduced case by using Lemma 3.1.

We use Hilbert's formula (Proposition 1.1):

$$v_L(\mathfrak{D}_{L/K}) = \sum_{i=0}^{\infty}(\#G_i - 1) = 2(\#G) - 2$$

Recall the definition of the different: $\mathfrak{D}_{L/K} := \left\{x \in L : \forall y \in \mathcal{O}_L \ \mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_K\right\}$. As we have noted before, it follows directly from the definition that if $\mathfrak{a}$ resp. $\mathfrak{b}$ are fractional ideals of $\mathcal{O}_K$ resp. $\mathcal{O}_L$ then $\mathrm{Tr}_{L/K}(\mathfrak{b}) \subseteq \mathfrak{a}$ iff $\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{D}_{L/K}^{-1}$. Therefore the equation above is equivalent to

$$\mathrm{Tr}_{L/K}(\mathfrak{P}_L^i) = \mathfrak{P}_K^{2+\left\lfloor\frac{i-2}{\#G}\right\rfloor}$$

Let

$$\overline{\mathfrak{P}}_L^i := \mathfrak{P}_L^i/\mathfrak{P}_K\mathfrak{P}_L^i = \mathfrak{P}_L^i/\mathfrak{P}_L^{\mathcal{G}+i}$$

where the last equation is due to total ramification. Its trace is

$$\mathrm{Tr}_G\,\overline{\mathfrak{P}}_L^i = \left(\mathrm{Tr}_G\,\mathfrak{P}_L^i + \mathfrak{P}_L^{\#G+i}\right)\Big/\mathfrak{P}_L^{\#G+i}$$

which is 0 unless $i \equiv 1 \bmod \#G$, in which case it is $\mathfrak{P}_L^{\#G+i-1}/\mathfrak{P}_L^{\#G+i}$. Consequently, for $i \not\equiv 1 \bmod \#G$, every $\bar{\delta} \in \overline{\mathfrak{P}}_L^n$ is killed by the trace, which Proposition 4.2 states is equivalent to $\overline{\mathfrak{P}}_L^i$ not being free. Apply Lemma 3.1 with $\mathcal{I} := \mathfrak{P}_L^i$ to finish.

It remains to show that any δ of valuation n is a free generator of $\mathfrak{P}_L^n$ in case $n \equiv 1 \bmod \#G$. Again we will use Proposition 4.2. Consider the map

$$\vartheta : \overline{\mathfrak{P}}_L^n \to \overline{\mathfrak{P}}_L^n, x \mapsto \mathrm{Tr}_G \cdot x$$

This is a k-linear map. Its image is 1-dimensional over k. The domain $\overline{\mathfrak{P}}_L^n = \mathfrak{P}_L^i/\mathfrak{P}_L^{\mathcal{G}+i}$ has dimension $\#G$. Hence $\dim_k \ker\vartheta = \dim_k \overline{\mathfrak{P}}_L^n - \dim_k \mathrm{im}\,\vartheta = \#G - 1$.

We claim that the kernel is $\mathfrak{P}_L^{n+1}/\mathfrak{P}_L^{n+\#G}$. This is clearly a k-submodule of $\mathfrak{P}_L^n$, and it has the correct dimension, so it is sufficient to show that $\mathfrak{P}_L^{n+1}/\mathfrak{P}_L^{n+\#G}$ is actually annihilated by ϑ. As above,

$$\mathrm{Tr}_G \cdot \left(\mathfrak{P}_L^{n+1}/\mathfrak{P}_L^{n+\#G}\right) = \left(\mathrm{Tr}_G\,\mathfrak{P}_L^{n+1} + \mathfrak{P}_L^{n+\#G}\right)\Big/\mathfrak{P}_L^{n+\#G} = \left(\mathfrak{P}_K^{2+\left\lfloor\frac{n-1}{\#G}\right\rfloor} + \mathfrak{P}_L^{n+\#G}\right)\Big/\mathfrak{P}_L^{n+\#G} = 0$$

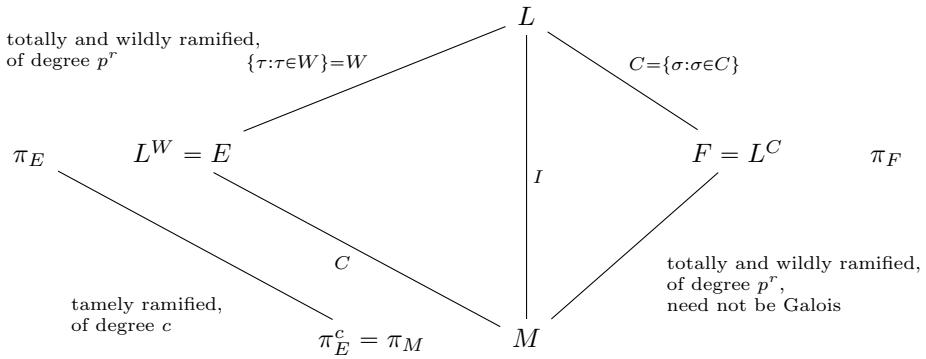
This shows that $\ker\vartheta = \mathfrak{P}_L^{n+1}/\mathfrak{P}_L^{n+\#G}$.

From Proposition 4.2 it follows that $\bar{\delta}$ is a free generator of $\overline{\mathfrak{P}}_L^n$ iff $\delta \in \mathfrak{P}_L^n/\mathfrak{P}_L^{n+\#G} - \mathfrak{P}_L^{n+1}/\mathfrak{P}_L^{n+\#G}$. Apply Lemma 3.1 with $\mathcal{I} := \mathfrak{P}_L^i$ to finish the proof. □

4.2 Totally and weakly ramified extensions

Remark. In this section, the extension under consideration will be denoted by L/M; while this may seem not to be coherent with the rest of these notes, this is because in the last step of the proof, when the extension L/K may not be totally ramified, L/M will be a totally ramified subextension to which we will apply the result of this section. ○

Let L/M be a totally and weakly ramified finite Galois extension of complete discrete valuation fields with finite residue fields of characteristic p. In particular, L/M is doubly split: $G = I = W \rtimes C$. Fix such a splitting (there is a choice of C here), and let $E := L^W$ and $F := L^C$ be the respective fixed fields. Then we have the following diagram:



Here we made the identification $C = \mathrm{Gal}(L/F) \xrightarrow{\sim} \mathrm{Gal}(E/M), \gamma \mapsto \gamma|_E$. Since E/M is totally and tamely ramified, we have seen in Guillermo's second talk that we may choose compatible uniformisers π_E and π_M, see [Joh11, Proposition 9.4] or [Joh15, p. 2.4]. The uniformiser π_F is chosen independently.

Since C and W have coprime orders, we may write $1 = ap^r + bc$ for some $a, b \in \mathbb{Z}$.

Proposition 4.8 ([Joh15, Proposition 6.1])**.** *In the above situation, let $n \equiv 1 \bmod \#W$, and choose $u_i \in \mathcal{O}_M^\times$ for $i = 0, 1, \ldots, c-1$. Let $\alpha := \sum_{i=0}^{c-1} u_i \pi_E^i$. Then $\pi_F^{nb} \pi_E^{na} \alpha$ is a free generator of $\mathfrak{P}_L^n$ over $\mathcal{O}_M[I]$.*

Proof. The point here is to break up L/M into the tamely and totally ramified extension E/M resp. the wildly and totally and weakly ramified extension L/E, then use the already known results for these extensions.

First note that L/E is weakly ramified, because $G_2(L/E) \leqslant G_2(L/M) = 1$. Therefore Theorem 4.6 applies, and we have that any $\delta \in L$ with $v_L(\delta) = n$ is a free $\mathcal{O}_E[W]$-generator of $\mathfrak{P}_L^n$. In particular, this is true for $\delta := \pi_F^{nb} \pi_E^{na}$:

$$v_L\left(\pi_F^{nb} \pi_E^{na}\right) = n v_L\left(\pi_F^b \pi_E^a\right) = n \cdot (bc + ap^r) = n$$

We also know that α is a free generator of $\mathcal{O}_E$ over $\mathcal{O}_M[C]$, and consequently $\pi_E^{na}\alpha$ is a free generator of $\pi_E^{na}\mathcal{O}_E$ over $\mathcal{O}_M[C]$. It remains to put these together:

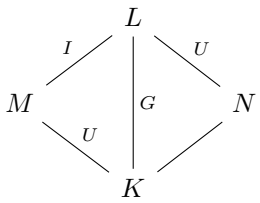
$$\begin{aligned}
\mathfrak{P}_L^n &= \mathcal{O}_E[W] \pi_F^{nb} \pi_E^{na} && \text{Theorem 4.6, see above} \\
&= \bigoplus_{\tau \in W} \tau\left(\pi_F^{nb} \pi_E^{na}\right) \mathcal{O}_E && \text{by definition} \\
&= \bigoplus_{\tau \in W} \tau\left(\pi_F^{nb}\right) \pi_E^{na} \mathcal{O}_E && \pi_E \in E = L^W
\end{aligned}$$

$$
\begin{aligned}
&= \bigoplus_{\tau\in W} \tau\left(\pi_F^{nb}\right)\pi_E^{na}\alpha\mathcal{O}_M[C] && E/M \text{ total tame, see above}\\
&= \bigoplus_{\tau\in W} \tau\left(\pi_F^{nb}\right)\bigoplus_{\sigma\in C}\sigma\left(\pi_E^{na}\alpha\right)\mathcal{O}_M && \text{by definition}\\
&= \bigoplus_{\tau\in W}\bigoplus_{\sigma\in C} \tau\left(\pi_F^{nb}\right)\sigma\left(\pi_E^{na}\alpha\right)\mathcal{O}_M && \text{reorganise}\\
&= \bigoplus_{\tau\in W}\bigoplus_{\sigma\in C} \tau\sigma\left(\pi_F^{nb}\right)\sigma\left(\pi_E^{na}\alpha\right)\mathcal{O}_M && \pi_F\in F=L^C\\
&= \bigoplus_{\tau\in W}\bigoplus_{\sigma\in C} \tau\sigma\left(\pi_F^{nb}\right)\tau\sigma\left(\pi_E^{na}\alpha\right)\mathcal{O}_M && \sigma\left(\pi_E^{na}\alpha\right)\in L^W \text{ by restriction iso above}\\
&= \bigoplus_{\tau\in W}\bigoplus_{\sigma\in C} \tau\sigma\left(\pi_F^{nb}\pi_E^{na}\alpha\right)\mathcal{O}_M && \text{reorganise}\\
&= \pi_F^{nb}\pi_E^{na}\alpha\mathcal{O}_M[I] && \text{by definition}
\end{aligned}
$$

Now apply Lemma 3.1 with $\mathcal{I} := \mathfrak{P}_L^n$. □

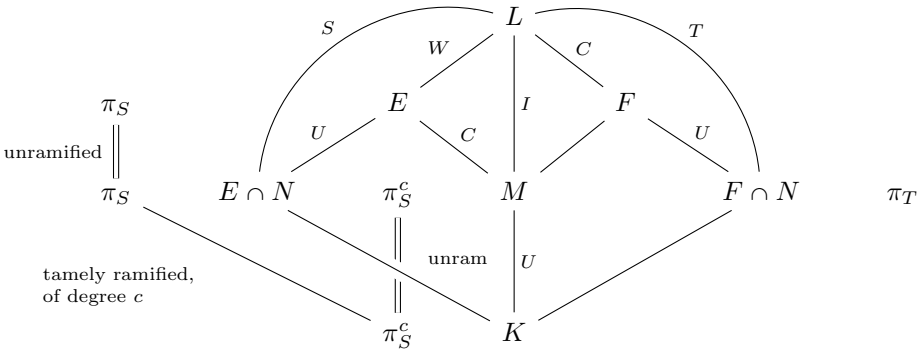
4.3 Doubly split weakly ramified extensions

Let L/K be a weakly ramified and doubly split finite Galois extension of complete discretely valued fields with finite residue fields of characteristic p. In particular, we have $G := \mathrm{Gal}(L/K) = W \rtimes T = W \rtimes C \rtimes U = I \rtimes U$ for the Galois group, with U non-canonical. Let $M := L^I$ be the inertia subfield, and $N := L^U$. That is, we have the following diagram:



Here we identified $U = \mathrm{Gal}(L/N)$ with $\mathrm{Gal}(M/K)$ via the restriction map $\gamma \mapsto \gamma|_M$.

The extension L/M is totally ramified by construction, and also weakly ramified because $G_2(L/M) \subseteq G_2(L/K) = 1$, hence L/M satisfies the conditions of the previous section. Let $S := WU \subseteq G$; S is in fact a subgroup because $W \lhd G$. This allows us to draw the following diagram of field extensions (not necessarily Galois):



Here we used the following facts:

- •) $W \lhd S$
- •) $I \lhd G$
- •) $C \lhd T$
- •) $E \cap N = L^W \cap L^U = L^{WU} = L^S$
- •) $F \cap N = L^C \cap L^U = L^{CU} = L^T$

As in the previous section, we write $\#W = p^r$, $\#C = c$, and choose $a, b \in \mathbb{Z}$ such that $ap^r + bc = 1$.

Since M/K is unramified, it has a NIB, that is, there is a $\beta \in \mathcal{O}_M$ such that $\mathcal{O}_M = \mathcal{O}_K[U] \cdot \beta$.

Proposition 4.9 ([Joh15, Proposition 7.1]). *In the setup above, let $n \equiv 1 \bmod \#W$, and choose $u_i \in \mathcal{O}_K^\times$ for $i = 0, 1, \ldots, c-1$. Let $\alpha := \sum_{i=0}^{c-1} u_i \pi_S^i$. Then $\pi_T^{nb} \pi_S^{na} \alpha\beta$ is a free generator of $\mathfrak{P}_L^n$ over $\mathcal{O}_K[G]$.*

Proof. Write $\gamma := \pi_T^{nb} \pi_S^{na} \alpha$. Then Proposition 4.8 states that $\mathfrak{P}_L^n = \mathcal{O}_M[I] \cdot \gamma$. Notice that γ is in N: indeed, $\pi_T \in F \cap N \subseteq N$, $\pi_S \in E \cap N \subseteq N$, wherefore also $\alpha \in N$. This is crucial.

Now it only remains to put everything together:

$$
\begin{aligned}
\mathfrak{P}_L^n &= \mathcal{O}_M[I] \cdot \gamma && \text{Proposition 4.8} \\
&= \bigoplus_{\tau \in I} \tau(\gamma) \mathcal{O}_M && \text{by definition} \\
&= \bigoplus_{\tau \in I} \tau(\gamma) \mathcal{O}_K[U] \cdot \beta && \beta \text{ gives a NIB for } M/K \text{ (unramified)} \\
&= \bigoplus_{\tau \in I} \tau(\gamma) \bigoplus_{\sigma \in U} \sigma(\beta) \mathcal{O}_K && \text{by definition} \\
&= \bigoplus_{\tau \in I} \bigoplus_{\sigma \in U} \tau(\gamma) \sigma(\beta) \mathcal{O}_K && \text{reorganise} \\
&= \bigoplus_{\tau \in I} \bigoplus_{\sigma \in U} \tau\sigma(\gamma) \sigma(\beta) \mathcal{O}_K && \gamma \in N = L^U \\
&= \bigoplus_{\tau \in I} \bigoplus_{\sigma \in U} \tau\sigma(\gamma) \tau\sigma(\beta) \mathcal{O}_K && \sigma(\beta) \in L^I \text{ since } \beta \in M \\
&= \bigoplus_{\tau \in I} \bigoplus_{\sigma \in U} \tau\sigma(\gamma\beta) \mathcal{O}_K && \text{reorganise} \\
&= \mathcal{O}_K[G] \cdot \gamma\beta && \text{by definition}
\end{aligned}
$$

Apply Lemma 3.1 to finish the proof. □

References

[Byo99] Nigel P. Byott. "Integral Galois module structure of some Lubin-Tate extensions". In: *J. Number Theory* 77.2 (1999), pp. 252–273. URL: https://mathscinet.ams.org/mathscinet-getitem?mr=1702149.

[CO81] Lindsay N. Childs and Morris Orzech. "On modular group rings, normal bases, and fixed points". In: *Amer. Math. Monthly* 88.2 (1981), pp. 142–145. URL: https://mathscinet.ams.org/mathscinet-getitem?mr=606253.

[CR81] Charles W. Curtis and Irving Reiner. *Methods of Representation Theory*. John Wiley & Sons, 1981. ISBN: 0-471-18994-4.

[Joh11] Henri Johnston. "Notes on Galois modules". In: (2011).

[Joh15] Henri Johnston. "Explicit integral Galois module structure of weakly ramified extensions of local fields". In: *Proc. Amer. Math. Soc.* 143 (2015), pp. 5059–5071. URL: https://www.ams.org/journals/proc/2015-143-12/S0002-9939-2015-12634-2/.

[Ser68] J.P. Serre. *Corps Locaux*. 1968, p. 245.