Scuola Normale Superiore
Classe di Scienze
Pisa

Perfezionamento in Matematica
2009-2011

A constructive theory for extensions of p-adic fields

March 5, 2012

Thesis submitted for the degree of Doctor of Philosophy

Candidate
Maurizio Monge
Scuola Normale Superiore

Advisor
Prof. Roberto Dvornicich
University of Pisa

Abstract

The subject of this thesis in the study of finite extensions of p-adic fields, in different aspects. Via the study of the Galois module of p-th power classes $L^\times/(L^\times)^p$ of a general Galois extension L/K of degree p, it is possible to deduce and classify the extensions of degree p^2 of a p-adic field. We exhibit formulæ counting how many times a certain group appears as Galois group of the normal closure, generalizing previous results.

In general degree we give a synthetic formula counting isomorphism classes of extensions of fixed degree. The formula is obtained via Krasner formula and a simple group-theoretic Lemma allowing to reduce the problem to counting cyclic extensions, which can be done easily via local class field theory.

When K is an unramified extension of $\mathbb{Q}_p$ we study the problem of giving necessary and sufficient conditions on the coefficients of an Eisenstein polynomial for it to have a prescribed group as Galois group of the splitting field. The techniques introduced allow to recover very easily Lbekkouri's result on cyclic extensions of degree p^2, and to give a complete description of the Galois group, with its ramification filtration, for splitting fields of Eisenstein polynomials of degree p^2 which are a general p-extension. We then show how the same methods can be used to characterize Eisenstein polynomials defining a cyclic extension of degree p^3.

We then study Eisenstein polynomials in general, describing a family of special reduced polynomials which provide almost unique generators of totally ramified extensions, and a reduction algorithm. The number of special polynomials generating a fixed extension L/K is always smaller than the number of conjugates of L over K, so that each Galois extension is generated by exactly one special polynomial. We give an algorithm to recover all special polynomials generating one extension, and a criterion that allows to detect when the extension generated by an Eisenstein polynomial is different from a fixed extension whose special generators are all given, the criterion does not only depend only on the usual distance on the set of Eisenstein polynomials defined by Krasner and others. An algorithm to construct the special polynomial generating an abelian class field is given, provided a suitable description of a candidate norm subgroup of $K^\times$.

Contents

Chapter 1

Introduction

In this thesis we study extensions of p-adic fields, with the aim of providing efficient tools to make easy working concretely with finite extensions. The results obtained in this thesis concern different and unrelated aspects of this subject, while being all contributions to the general problem of giving an explicit characterization of finite extensions of p-adic fields. For this reason, and being each chapter essentially self-contained, it will be more convenient to describe the results obtained while illustrating the structure of the thesis.

Fields of p-adic numbers, and local fields in general, are a fundamental tool in number theory and arithmetic geometry, and often allow to study complicated problems in a simplified context. The study of the extensions and Galois theory over these fields is indeed much simpler than over number fields. For instance Galois extension of local fields are always solvable, and when K is an extension of $\mathbb{Q}_p$ the extensions of fixed degree are in a finite number.

An extension L/K can be decomposed in a simpler unramified subextension, which is cyclic and corresponds to an extension of the residue field, of degree f say (inertia degree), and a further totally ramified extension which corresponds to an extension of the group of valuations, and has degree e (ramification index). When $p \nmid e$ the extension is called tamely ramified, while if $p \mid e$ it is said to be wildly ramified.

As long as the extensions considered are tamely ramified the extensions of local field are very well understood, and the same can be said for what concerns general abelian extensions. General extensions where p divides exactly the ramification index e are also quite tractable. For instance various sets of generating equation are known in degree p for totally ramified extensions, such as Amano's polynomials and generalized Artin-Schreier equations, which provide sets of generators of isomorphism classes of extensions, one for each possible class.

However when considering extensions whose degree is divisible by a bigger power of p the complexity increases quickly. A celebrated result of Shafarevich [Sha47] says that the p-part of the absolute Galois group of a p-adic field K not containing a primitive p-th roots of the unity is the p-completion of a free group on $[K:\mathbb{Q}_p]+1$ generators, so in a certain sense the set of possible p-extensions is as complicated as possible. When a primitive p-th root of the unity is contained in K similar results describe the structure of the p-part of the Galois group as finitely presented group [Lab67], and a presentation is also known [Jak68, JW83] for the absolute Galois group when $p \neq 2$.

Describing concretely the set of possible extensions is indeed quite a hard problem also when the base field is the rational p-adic field $\mathbb{Q}_p$. A database collecting extensions of p-adic fields was created by Jones-Roberts [JR06], to make easy the study of the extensions of $\mathbb{Q}$ providing a systematic description of the local structure. However the database essentially only contains extensions of degree n of $\mathbb{Q}_p$ where $p^2 \nmid n$. In fact, the biggest n divisible by p^2 present in the database is for the extensions of degree 9 of $\mathbb{Q}_3$, and to describe the 795 extensions it was necessary a work on its own [JR04].

In this thesis we study in general the problem of describing totally ramified extensions of p-adic fields. A presentation of the absolute Galois group could be used to describe abstractly the possible extensions with their groups, but working with the finite quotient of finitely presented groups can be as hard as working directly with field extensions, and doing so we would also lose any connection with the extensions which are being considered. We will in particular give the preference to all instruments which could be used in practice to study the extensions of local fields, when possible.

Another aspect, on which we concentrate in last chapters, which is certainly less understood than Galois groups of local fields, is that of generating equations. Each totally ramified extension is generated by an Eisenstein polynomial, and we study the problem of characterizing the polynomials whose splitting field is an extension with a prescribed Galois group. We also consider a family of polynomials which in general provides a set of almost-canonical generators of extensions, and derive a few results on these families, such as a criterion to detect when different polynomials generate non-isomorphic extensions, and an algorithm to construct class fields.

Incidentally the algorithm to construct a class fields shows that there exists exactly one extension having a prescribed norm subgroup $N \subset K^\times$ corresponding to a totally ramified extension, having degree equal to the index $(K^\times : N)$. Such extension can be easily shown to be Galois. We obtain consequently an alternate and constructive proof of the Existence Theorem of local class field theory.

1.1 Description of the work

We describe here the structure of all chapters, giving an abstract of the original results obtained in each. The first two chapters contain essentially no new results. They are accounts of well known results that are however central to the thesis, and that appeared to be useful recalling though. Everything else is the author's work, except for Section 4.2, Chap. 4 which was obtained in collaboration with Ilaria Del Corso and Roberto Dvornicich. When a lemma appears in a similar form in some other paper (and the author is at knowledge) this is clearly stated, and a reference is given.

1.1.1 Preliminaries (Chap. 2 and 3)

In Chapter 2 we give a very short account of representation theory in characteristic p for finite groups having a normal cyclic p-Sylow. This theory is not very different from the theory for cyclic p-groups, and it is possible to give a classification of the indecomposable representations. In the same chapter we also give a very terse treatment of study of the normal closure of the tower formed by a cyclic extension of degree p over a cyclic extension of degree p^k. Every result is well known and can be found in [Wat94, MS05], our exposition attempts to be as synthetic as possible while making clear what is going on, and the reader may appreciate the point of view offered.

Chapter 3 is a quick account of the basic theory of local fields. No attempt to give a full exposition is done, and we are very sketchy. Our purpose is that of helping a reader already sufficiently expert in the field to recall easily the most important results. A notable exception is the exposition of non-Galois ramification theory, where we supply more details not being very well known, we will essentially follow the exposition of Helou [Hel91]. In this chapter we also give a reworked proof of the characterization of the ramification break of a radical extension obtained adding a p-th root in terms of the p-th power defect, which is a classical result [Wym69]. Our proof has the advantage of showing that the different cases can be treated in a unified way.

1.1.2 Extensions of degree p^2 (Chap. 4)

In Chapter 4, we present results allowing to derive easily and very explicitly a classification of extensions of degree p^2 of p-adic fields of characteristic 0 via Kummer theory, via the study of the Galois modules of power classes $F^\times/(F^\times)^p$ for a suitable extension F of the base field K.

The general idea is that under suitable hypotheses, and for an appropriate choice of F, we should have a one-to-one correspondence of the indecomposable submodules of dimension 2 of $F^\times/(F^\times)^p$ with the possible normal closures of extensions of p^2. We remark the extensions with more than one intermediate field are obtained as the compositum of extensions of degree p, so they are the trivial ones in a certain sense, and we can just consider extensions with one, or none, intermediate extension.

When restricting to extensions having no intermediate extension this idea works very well indeed, and for all extensions of p-th power degree, not just p^2. The extension F can be taken to be a suitable tamely ramified extension of K, and we have exactly one possible normal closure for each irreducible submodule, and each normal closure is coming from exactly one isomorphism class of extensions. We remark that these extension have a very simple ramification filtration, and the possible ramification data can be easily classified. This is a direct generalization of the methods used by Dvornicich-Del Corso [DCD07], where an effective parametrization isomorphism classes of extensions of degree p was obtained.

For extensions having exactly one intermediate extension we have a similar result, even though it is a bit more intricate. In this case for each isomorphism class of extensions E/K of degree p we can consider a suitable extension $E_F = EF$ obtained taking the compositum with the maximal abelian extension F/K of exponent $p-1$. The indecomposable submodules of $E_F^\times/(E_F^\times)^p$ will correspond to the possible normal closures of an extension of degree p^2 containing a subextension isomorphic to E/K. However, each normal closure will generally be obtained as normal closure of a big number of extensions of degree p^2, which we will characterize. It is possible that different isomorphism classes over E become isomorphic over K, and we will give a precise characterization of when this can happen. We add that in this case the ramification filtration of the normal closure can be very complicated, and the possible ramification breaks cannot be easily determined.

As an application of these parametrization results, we show how it is possible to deduce easily formulæ counting the isomorphism classes with specified Galois group of the normal closure, the possible normal closures, and the total number of extension of each type.

We conclude considering the transitive solvable subgroups of S_{p^2} that possess a suitable filtration, and describing which among them are realized as Galois groups. When creating the database of local fields, it was observed by Jones-Roberts [JR04] that "somewhat incidentally" all candidate subgroups of S_9 happen to be realized as Galois groups of $\mathbb{Q}_3$. We will show that this statement is always false over $\mathbb{Q}_p$ for $p \geq 5$, while it is true for all proper extensions of odd residual degree over $\mathbb{Q}_p$. For $p = 3$ it is indeed incidentally true, the ultimate reason being that 1 and $p-1$ are all possible divisors of $p-1$, for $p = 3$.

1.1.3 Enumeration of classes of extensions (Chap. 5)

In this chapter we solve the problem of giving a formula enumerating the isomorphism classes of extensions of degree n in general degree. A formula had been obtained in a special case by Hou-Keating [HK04] in a complicated paper, enumerating the classes of extensions with specified inertia degree f and ramification index e when $p^2 \nmid e$, and under additional hypotheses also when $p^2 \| e$.

We will give a complete solution to this problem, enumerating the isomorphism classes of extensions with arbitrary fixed values of f and e, or alternatively all extensions of fixed total degree. We illustrate how it is obtained.

A key result is a group theoretic lemma, which allows to count isomorphism classes of subgroups of a group G in terms of the number of chains of subgroups $H \lhd J \leq G$, where $(G : H) = n$ and J/H is a cyclic group of order d, for all possible d dividing n. This strategy had been already found and applied in a totally different context by Mednykh [Med08].

Let K be the base field. Via Galois theory this is equivalent to counting all possible towers $L/F/K$ in the algebraic closure, where L/F is cyclic Galois of degree d, and L has degree n over K. This can be done because the extensions F/K of degree n/d in the algebraic closure can be computed exactly via Krasner formula, while for fixed F the number of extensions L/F which are cyclic of degree d has little dependence on the particular F taken into account.

In particular, we have by local class field theory that the number of cyclic extensions of degree d only depends on the degree $[F : \mathbb{Q}_p]$, on the residual degree $f(F/\mathbb{Q}_p)$, and on the group of p-th power roots of the unity contained in F. Different cases have to be considered, but it is possible to write down a rather simple formula, showing in particular that the number of isomorphism classes of extensions, with fixed f and e, only depends on the ramification and inertia of the extensions $K/\mathbb{Q}_p$, and $K(\zeta_{p^m})/K$ obtained adding the p^m-th roots of 1, for all p^m dividing e.

1.1.4 Galois group of Eisenstein polynomials (Chap. 6)

In this section we assume that the base field is an unramified extension of $\mathbb{Q}_p$, and introduce general methods allowing to give necessary and sufficient conditions on the coefficients of an Eisenstein polynomial for its Galois group to be a prescribed group. We characterize in particular all polynomials of degree p^2 whose splitting field is a p-extensions, determining completely the Galois group with its ramification filtration, and the polynomials of degree p^3 generating a cyclic extension.

It is not hard describing exactly what is the Galois group of the splitting field of an Eisenstein polynomial of degree p. This had been already done in ancient times by Ore [Ore28] and later Amano [Ama71], which gave necessary and sufficient conditions for an Eisenstein polynomial to generate a cyclic Galois extensions of degree p. It is indeed easy to show that the splitting field of an Eisenstein polynomial $f(T)$ of degree p having a root π is obtained from $K(\pi)$ adding a root of $T^{p-1} - f'(\pi)$.

However the problem is much more complicated for degrees divisible by a bigger power of p, excluding the fortunate easy class of polynomials which generate an extension having only one ramification break (or equivalently, “whose ramification polygon has only one side”, as considered in [Gre10]). This case is quite similar to the case of polynomials of degree p, and we remark that in this case the p-Sylow is always an elementary abelian p-group, but the condition of having only one ramification break is even more restrictive.

A necessary and sufficient condition was given for a polynomial of degree p^2 to generate a cyclic Galois extension over $\mathbb{Q}_p$ by Lbekkouri [Lbe09]. However the characterization was obtained via a complicated computation, and is not very enlightening about what is going on.

We outline a new general approach for studying this kind of problems. Let $f(T)$ be an Eisenstein polynomial, π a root, and $L = K(\pi)$. The idea is that, for each $\theta \in K$ and $m \geq 1$, we can find an efficient expression of the norms of the element $1 + \theta\pi^m$, in terms of the coefficients of $f(T)$. By local class field theory the totally ramified extension L/K is Galois and abelian with group G if and only if $U_K/N_{L/K}(U_L)$ is isomorphic to G.

When the field K is not too complicated, and in particular when it is unramified over $\mathbb{Q}_p$, it is possible to determine easily the possible structures of the group $N_{L/K}(U_L)$, for the quotient $U_K/N_{L/K}(U_L)$ to be isomorphic to G. A condition on the possible values of $N_{L/K}(1 + \theta\pi^m)$ follows, and consequently on the coefficients of the polynomial $f(T)$, and the condition is satisfied if and only if the extension is Galois with the prescribed group.

With this strategy we can recover very easily Lbekkouri's characterization of cyclic extensions of degree p^2 over an arbitrary unramified extension of $\mathbb{Q}_p$, and give a substantial generalization.

Certain conditions on the coefficients are equivalent to requesting that the extension should be obtained as a two steps tower $L/F/K$ formed by cyclic extensions L/F and F/K of degree p, and that the ramification breaks have prescribed values. Assume these conditions are respected, then the normal closure $\tilde{L}$ over K is a p-extension, and the group $\mathrm{Gal}(\tilde{L}/F)$ will be an indecomposable module over $\mathrm{Gal}(F/K)$ of length $1 \leq \ell \leq p$ say.

When some of the remaining conditions is not respected, we prove that the first condition which fails will determine the length ℓ of the module $\mathrm{Gal}(\tilde{L}/F)$. The proof uses in a crucial way the functoriality properties of the reciprocity map of local class field theory. Since the ramification data force $\mathrm{Gal}(\tilde{L}/K)$ to always have exponent p^2, its isomorphism class is uniquely determined.

Taking into account the remaining extensions L/K of degree p^2 whose normal closure is a p-group we obtain full description of the Galois groups of Eisenstein polynomials of degree p^2, whose splitting field is a p-extension.

We conclude showing how the developed methods apply to give a necessary and sufficient condition on the coefficients of a polynomial of degree p^3 to generate a cyclic Galois extension. While the condition obtained is very complicated, it is derived quite easily, applying the same methods in a relatively straightforward way.

1.1.5 Special Eisenstein polynomials (Chap. 7)

In this Chapter we define a special class of Eisenstein polynomials which are reduced in a suitable sense, and provide a very restricted set of generating polynomials for each totally ramified extension over a local field K. A criterion to exclude distinct Eisenstein polynomials from generating isomorphic extensions is given. We then describe a procedure to recover a unique reduced polynomial generating a totally ramified class field, provided a suitable description of a norm subgroup.

Let $f(T)$ be an Eisenstein polynomial, and π a root generating the extension $L = K(\pi)$. We can consider an alternative uniformizer $\tilde{\pi} = \pi + \theta\pi^{m+1}$ for $\theta \in U_K$ and $m \geq 1$, and its minimal polynomial $\tilde{f}(T)$. Then $\tilde{f}(T)$ provides an alternative generating polynomial for L/K which is Eisenstein, and it is possible to relate the coefficients of $\tilde{f}(T)$ to those of $f(T)$.

We will call this operation which transform $f(T)$ into $\tilde{f}(T)$ *reduction step* relative to the substitution $\pi \to \pi+\theta\pi^{m+1}$. We will describe a simple algorithm that, iterating reduction steps for substitutions $\pi \to \pi+\theta\pi^{m+1}$ for increasing m, will output a generating polynomial for L, whose coefficients are in normal form in a suitable sense. The polynomials that can be obtained from this procedure can be easily described in terms of the coefficients.

The reduction procedure allows some choices, but we will bound the number of possible reduced polynomials generating a fixed extension L/K. The number of reduced polynomials generating the same extension L/K turns out to be equal to a ratio of a quantity that can be interpreted as a naive upper bound for $\#\operatorname{Aut}(L/K)$, and the actual value of $\#\operatorname{Aut}(L/K)$. In particular the number of reduced polynomials is always at most $[L : K]$. When the extension is Galois, or when it has a unique ramification break, then the upper bound is exact, and the extension is generated by exactly one reduced polynomial.

A special generating polynomial had already been considered by Krasner [Kra37], and it turns out to be one element of the set of special polynomials we consider. In general Krasner's representative cannot be easily identified in terms of the coefficients, though.

Then, we give a synthetic criterion which allows to exclude easily an Eisenstein polynomial from being a possible generator of a given extension. In particular we show that if a polynomial $f(T)$ is obtained from $g(T)$ via reduction steps relative to substitutions $\pi \to \pi + \theta\pi^{m+1}$ with $m \geq r$ for some r, then the coefficients of $f(T)$ and $g(T)$ should exhibit a quite strong similarity. The bigger is r, the stronger will be the similarity they should satisfy. We remark that this similarity is essentially the same type of continuity observed by Heiermann [Hei96] for power series.

When a reduced polynomial can be obtained from $f(T)$ applying the reduction algorithm for $m \geq r$ for some r, we obtain a criterion in the case we know the set of all reduced polynomials generating a fixed extension L/K, because one of them should be similar to $f(T)$ according to our definition. This observation turns out to be particularly effective when L/K is a Galois extension. We remark that the criterion we give is more stringent than what can be said considering the first order value of $f(\pi) - g(\pi)$ for a uniformizer π of L, and generalizes results based on the study of this value at the first order [Yos11].

At last, we consider the problem of determining the reduced polynomial generating a totally ramified class field. Assume a suitable description of a candidate norm subgroup $N \subset K^\times$, and in particular let's assume we are given for each $i > 0$ an isomorphism ν_i of $U_iN/U_{i+1}N$ into an abstract group which is either cyclic for $i = 0$, either a vector space over $\mathbb{F}_p$ for $i > 0$. We show a procedure allowing to convert inductively the knowledge of the ν_i into a p-adic expansion of the coefficients of a reduced polynomial.

This is obtained requesting via ν_i that $N_{L/K}(1+\theta\pi^m)$ should be in $U_{i+1}N$ for all $\theta \in U_K$ and $m, i \geq 0$, and translating this request to a condition on the coefficients of $f(T)$. When the coefficients are only partially determined, it is necessary to find a suitable pair m, i such that the evaluation of $\nu_i(N_{L/K}(1+\theta\pi^m))$, for all θ, will allow to determine a new term in the p-adic expansion of some coefficient.

The argument is quite intricate, but shows, for $(K^\times : N) = n$, that we can obtain exactly one reduced polynomial $f(T)$ of degree n, such that $N_{L/K}(L^\times) \subset N$. It is easy to observe that we actually have $N_{L/K}(L^\times) = N$, and that L/K is Galois (even if we do not have directly that the extension should be abelian, without assuming local class field theory). Consequently the construction also provides an alternative proof of the Existence Theorem of local class field theory.

1.2 Acknowledgements

There are many people I have to thank for valuable suggestions and discussions during my thesis work. Also, I'm indebted to other people for general advices about mathematics, and for sharing with me some research experience. In random order (except that women should come first!) and making no distinction, I thank Selena Marinelli, Sara Checcoli, Ilaria Del Corso, Valentina Disarlo, Dajano Tossici, Roberto Dvornicich, Manabu Yoshida, Vincenzo Mantova, Ján Mináč, Luca Caputo, Angelo Vistoli, Samuele Mongodi, Nevio Dubbini, Gabriele Dalla Torre, Philippe Cassou-Noguès, Federico Poloni, Boas Erez, Alessandro Cobbe, François Laubie.

I feel also grateful to the Scuola Normale Superiore of Pisa for welcoming me as student, and the Institut de Mathématiques de Bordeaux for hospitality while part of my thesis work was conceived.

Chapter 2

Preliminaries on relative Kummer theory

Let p be a fixed prime. We give here a short account on relative Kummer theory, and deduce a characterization of the normal closure of a general tower formed by two Galois extensions of degree p over a field containing a primitive p-th root of the unity, and some properties of the module of p-th power classes. This characterization is quite well known [Wat94, MS05], and consequently we will be very terse.

We start giving the classification of indecomposable representations of a finite group having a cyclic p-Sylow over a field of characteristic p. The classification is not very different from the very well known classification of indecomposable representations of a cyclic p-groups. We refer to [Alp93] for a systematic study of modular representation theory.

For $k \in \mathbb{Z}$ we denote as C_k the cyclic group of order k.

2.1 Modular representations of finite groups

In this section we quickly review the classification of indecomposable modules in characteristic p over a finite group G having a normal cyclic Sylow subgroup $S = \langle \sigma \rangle$ of order p^a. This material is standard and all proofs can be found for instance in [Alp93, Chap. 2, §5-§6].

Let κ be a fixed field a characteristic p, and A a finite dimensional unital algebra over κ. A finite dimensional module will be called *simple* (or *irreducible* over a group algebra) if it has no proper submodule, and *semisimple* (or *completely reducible* over a group algebra) if it is a direct sum of simple submodules, or (equivalently) if every submodule is a direct summand. The *radical* of A, denoted as $\operatorname{rad} A$, is defined as the set of elements annihilating every simple A-module, and can be proved to be equivalent to each of

- the smallest submodule of A whose quotient is semisimple,

- the intersection of all maximal submodules of A,
- the largest nilpotent ideal of A.

If X is an A-module we define $\operatorname{rad}(X) = (\operatorname{rad} A)X$, and it turns out to be equal to the intersection of all the maximal submodules of X, or equivalenty the smallest submodule of X with semisimple quotient. We define $\operatorname{rad}^n(X)$ inductively putting $\operatorname{rad}^0(X) = X$, and $\operatorname{rad}^n(X) = \operatorname{rad}(\operatorname{rad}^{n-1}(X))$. We will call *radical series* the sequence

$$X = \operatorname{rad}^0(X) \supseteq \operatorname{rad}^1(X) \supseteq \operatorname{rad}^2(X) \supseteq \dots .$$

We define the *socle*, and denote as $\operatorname{soc}(X)$, to be the set of elements which are annihilated by $\operatorname{rad} A$. It turns out to coincide with the module generated by all simple submodules. We put similarly $\operatorname{soc}^0(X) = 0$ and $\operatorname{soc}^n(X)$ to be the inverse image of $\operatorname{soc}(X/\operatorname{soc}^{n-1}(X))$ via the map $X \to X/\operatorname{soc}^{n-1}(X)$. They form the *socle series*

$$0 = \operatorname{soc}^0(X) \subseteq \operatorname{soc}^1(X) \subseteq \operatorname{soc}^2(X) \subseteq \dots .$$

For each module X we will call X^* the dual module $\operatorname{Hom}_\kappa(X, \kappa)$, we have that as usual $X \cong X^{**}$ canonically, and $X^*/\operatorname{rad}^i(X^*) = \operatorname{soc}^i(X)^*$ for each $i \geq 0$. For an A-module X the smallest indices after which the radical series and the socle series become constant are equal, and they are called *Loewy length.* We will call *composition length* the maximal length of a composition series, it is equal to the Loewy length precisely when the module has a unique composition series, and if this is the case the module will be called *uniserial.*

We say that X is *projective* (resp. *injective*) if every surjection $Y \twoheadrightarrow X$ (resp. injection $X \hookrightarrow Y$) is split.

Proposition 2.1.1. *A module over a group algebra $\kappa[G]$ is projective if and only if is injective, and furthermore this is satisfied if and only if X is a direct summand of a free module.*

Proof. See [Alp93, Chap. 2, §5, Theo. 2 and §6, Theo. 4] for a proof of the proposition. □

If $H \subseteq G$ is a subgroup and X an $\kappa[H]$-module, we will denote as $\operatorname{Ind}_H^G(X)$ the module $\kappa[G] \otimes_{\kappa[H]} X$, and call it the *induced* module from H to G.

2.1.1 Groups with cyclic normal p-Sylow

Let G be a group with normal cyclic Sylow subgroup S, generated by σ and of order p^n say. Assume the action by conjugation of G on S is described by $\tilde{\rho} : G/S \to \operatorname{Aut}(S)$. Since G/S has order prime with p the action on S is unequivocally described its action $\rho : G \to \operatorname{Aut}(T)$ on $T = S/S^p$. We can canonically identify $\operatorname{Aut}(T)$ with $\mathbb{F}_p^\times \subseteq \kappa^\times$, and view T as a one dimensional vector space over $\mathbb{F}_p$. Let's put also $T_\kappa = T \otimes_{\mathbb{F}_p} \kappa$.

Let $A = \kappa[G]$, then $\mathrm{rad}(A)$ is equal to the kernel of the canonical projection $\eta : \kappa[G] \to \kappa[G/S]$. Indeed, the algebra $\kappa[G/S]$ is semisimple, so $\mathrm{rad}(A)$ is certainly contained in the kernel of η. Furthermore the kernel is the bilateral ideal generated by $\sigma - 1$, and it is readily verified to be a nilpotent ideal.

Consequently the irreducible modules are naturally irreducible $\kappa[G/S]$-modules. The indecomposable modules are classified by the following proposition.

Proposition 2.1.2. *Each indecomposable X module of $\kappa[G]$ is uniserial with composition length at most p^n. It is uniquely determined by its composition length, and either the module $\mathrm{soc}(X)$ or $X/\mathrm{rad}(X)$ as $\kappa[G/S]$-modules. If X has length ℓ and composition series*

$$X = X_0 \supsetneq X_1 \supsetneq \cdots \supsetneq X_\ell = 0,$$

then $X_i/X_{i+1} \cong X_{i-1}/X_i \otimes_\kappa T_\kappa$ as $\kappa[G/S]$-modules, for $0 < i < \ell$.

Proof. See [Alp93, Chap. 2, §5-§6] for a proof of the proposition. □

In particular X is indecomposable if and only if $X/\mathrm{rad}(X)$ or $\mathrm{soc}(X)$ are simple modules, and the action on the quotients X_i/X_{i+1} is uniquely determined taking the twists with the character ρ. We expand on this last observation, describing explicitly the map $X_{i-1}/X_i \to X_i/X_{i+1}$.

If $x \in X_{i-1} \setminus X_i$, then $(\sigma - 1)x \in X_i \setminus X_{i+1}$, and furthermore we can deduce the action of a $\gamma \in G$ on the next quotient as

$$\begin{aligned} \gamma \cdot (\sigma - 1)x &= (\gamma\sigma\gamma^{-1} - 1)\gamma x \\ &= (\sigma^{\tilde{\rho}(\gamma)} - 1)\gamma x \\ &= (\sigma^{\tilde{\rho}(\gamma)-1} + \cdots + \sigma + 1)(\sigma - 1)\gamma x \\ &\equiv \rho(\gamma) \cdot (\sigma - 1)\gamma x \pmod{X_{i+1}}, \end{aligned}$$

with the small abuse of notation of identifying $\tilde{\rho}(\gamma)$ with a positive integer such that $\gamma\sigma\gamma^{-1} = \sigma^{\tilde{\rho}(\gamma)}$. The particular map $X_{i-1}/X_i \to X_i/X_{i+1}$ considered (which is not in general $\kappa[G/S]$-equivariant, unless $\rho = 1$) depends on the class modulo S^p of the chosen generator σ.

2.2 Relative Kummer theory

If F is a field let's denote as $[\ \cdot\ ]_F$ the map of reduction modulo p-th power classes, in the style of [MS05]. Thus we have $[X]_F = {}^{X(F^\times)^p}/{}_{(F^\times)^p}$ for $X \subseteq F^\times$, and $[\alpha]_F = {}^{\alpha(F^\times)^p}/{}_{(F^\times)^p}$ for $\alpha \in F^\times$.

In this section we study the Kummer theory for p-extensions over a field F containing the p-th roots of the unity, which is itself a Galois extension over another field K, with $H = \mathrm{Gal}(F/K)$ say. We refer to [Lan02, Chap. 6, §8] for a basic exposition of Kummer theory.

Let's denote by $F^{(p)}$ the maximal extension of F with exponent p. Kummer theory over F tells us that we have a canonical perfect pairing of topological groups

$$\langle\cdot,\cdot\rangle_F : [F^\times]_F \times \mathrm{Gal}(F^{(p)}/F) \longrightarrow \mu_p, \qquad (x,\sigma) \mapsto \left(x^{1/p}\right)^{\sigma-1},$$

denoting as usual as μ_p the group of p-th roots of 1. The group $[F^\times]_F$ is equipped with the discrete topology, and the Galois group with the usual Krull topology.

Now H acts on both $[F^\times]_F$ and $\mathrm{Gal}(F^{(p)}/F)$, and the above pairing has to be *a fortiori* H-equivariant, being canonical. If Δ is any subset of $[F^\times]_F$ then the Galois closure of $F(\Delta^{1/p})/K$ will correspond to the biggest $\mathbb{F}_p[H]$-submodule of $\mathrm{Gal}(F^{(p)}/F)$ which is orthogonal to Δ in the above pairing. It is equal to the subgroup orthogonal to the submodule $\Xi = \langle\Delta\rangle_{\mathbb{F}_p[H]}$ generated by Δ over $\mathbb{F}_p[H]$, and the Galois closure $F(\Delta^{1/p})/K$ will be exactly $F(\Xi^{1/p})$.

If Δ is a subspace of $[F^\times]_F$ the Kummer pairing can also be interpreted as a canonical isomorphism

$$\mathrm{Gal}(F(\Delta^{1/p})/F) \xrightarrow{\sim} \mathrm{Hom}(\Delta,\mu_p) \cong \Delta^* \otimes \mu_p, \tag{2.1}$$

which is an isomorphism of $\mathbb{F}_p[H]$-modules when Δ is $\mathbb{F}_p[H]$-invariant. If Δ is $\mathbb{F}_p[H]$-invariant, but H is subgroup of a bigger group of automorphisms G of F, then the module $\langle\Delta\rangle_{\mathbb{F}_p[G]}$ is a quotient of the induced module $\mathbb{F}_p[G] \otimes_{\mathbb{F}_p[H]} \Delta$, and is obtained from it as the image of the map induced by $g \otimes x \mapsto gx$.

2.2.1 Normal closure over a cyclic p-extension

Suppose now K is a field containing the p-th roots of the unity, and F/K a cyclic p-extension with group $S = \langle\sigma\rangle$ of order p^n. Let $L = F(\gamma^{1/p})$ be a cyclic extension of degree p over F for some class $\gamma \in [F^\times]_F$. A condition on γ for the extension L/K to be cyclic Galois where already given by Albert [Alb35], and more generally a classification of the possibilities for the Galois closure can be found in [Wat94] and [MS05]. We will now review those results in a modern and concise way.

As observed above, the Galois closure $\tilde{L}$ of L over K is given by $F(\Delta^{1/p})$, where $\Delta = \langle\gamma\rangle_{\mathbb{F}_p[S]} \subseteq [F^\times]_F$ is the $\mathbb{F}_p[S]$-module generated by the image γ in $[F^\times]_F$. It is indecomposable of length $\ell \leq p^n$ by Prop. 2.1.2. A basis as vector space is given by the elements $\gamma, \gamma^{\sigma-1}, \gamma^{(\sigma-1)^2}, \dots, \gamma^{(\sigma-1)^{\ell-1}}$.

The action of a p-group on the group μ_p of p-th roots of the unity is always trivial, being $\mathrm{Aut}(\mu_p)$ cyclic of order $p-1$. Thus we have by equation (2.1) that $X = \mathrm{Gal}(\tilde{L}/F)$ is isomorphic to Δ^*, and as $\mathbb{F}_p[S]$-module it is again indecomposable of length ℓ, and isomorphic to ${}^{\mathbb{F}_p[\sigma]}/_{(\sigma-1)^\ell}$. Hence the full group $G = \mathrm{Gal}(\tilde{L}/K)$ fits in the exact sequence

$$1 \to X \to G \to S \to 1,$$

with the natural action of the quotient on the kernel.

We give now a characterization of such p-groups.

Proposition 2.2.1. *Let G be an extension of the cyclic group $S = \langle\sigma\rangle$ of order p^n by an indecomposable $\mathbb{F}_p[S]$-module X, whose length is assumed $\ell \leq p^n$.*

Then if $\ell < p^n$ the group G is in one of two possible isomorphism classes, one being the semidirect product $X \rtimes S$, which has exponent p^n, and one being a non-split extension $X \bullet S$ of exponent p^{n+1}.

If $\ell = p^n$ then there is only one possible isomorphism class, which is the semidirect product $X \rtimes S$ and has exponent p^{n+1}.

Furthermore every quotient of G by a non-trivial normal subgroup has exponent at most p^n.

Proof. Take a lift of $\sigma \in S$ to some $\tilde{\sigma} \in G$. Then $\tilde{\sigma}^{p^n} \in X$ is clearly invariant under the action of the quotient, and hence should be in the socle $\mathrm{soc}(X)$ which is a cyclic group of order p, generated by x_0 say.

Let's use the additive notation for X, and denote with an exponent the action of S. The group G is obtained from X adding one generator $\tilde{\sigma}$ and the relations

$$\tilde{\sigma}x\tilde{\sigma}^{-1} = x^{\sigma} \quad \text{for all } x \in X, \qquad \tilde{\sigma}^{p^n} = ax_0,$$

for some $a \in \mathbb{F}_p$. Each choice for $a \in \mathbb{F}_p$ allows to construct a group. For $a \neq 0$ we can replace every $x \in X$ by $a^{-1}x$ reducing to the case $a = 1$, so we can just consider the groups obtained with $a = 0, 1$.

Any alternative representative for σ can be written as $\tilde{\sigma} \cdot x$ for some $x \in X$, and we have that

$$\begin{aligned}(\tilde{\sigma} \cdot x)^{p^n} &= \tilde{\sigma}^{p^n} \cdot \sum_{i=0}^{p^n-1} x^{\sigma^i} \\ &= \tilde{\sigma}^{p^n} \cdot x^{(\sigma-1)^{p^n-1}}.\end{aligned}$$

Indeed, $(\sigma-1)^{p^n-1}$ is equal to $\sum_{i=0}^{p^n-1} \sigma^i$ in the polynomial ring $\mathbb{F}_p[\sigma]$, and hence also in the group algebra $\mathbb{F}_p[S]$ which is a quotient. The map $X \to X$ defined by $x \mapsto x^{(\sigma-1)^{p^n-1}}$ is a surjection to the socle when $\ell = p^n$, and is the zero map if $\ell < p^n$.

Consequently when $\ell < p^n$ the group obtained setting $a = 0$ has exponent p^n, so it is certainly different from the group obtained setting $a = 1$ which has exponent p^{n+1}. On the other hand by when $\ell = p^n$ we can replace $\tilde{\sigma}$ with a suitable $\tilde{\sigma} \cdot x$ to satisfy $\tilde{\sigma}^{p^n} = 0$, the group obtained is always the semidirect product, and has exponent p^{n+1}.

To prove the last claim, observe that when G is non-abelian its center is exactly $\mathrm{soc}(X)$. If N is a normal subgroup then it has non-trivial intersection with the center, by the formula of classes applied to the conjugacy classes contained in N. Consequently $\mathrm{soc}(X) \subseteq N$, but as we proved above all p^{n+1}-th powers are contained in $\mathrm{soc}(X)$. □

When considering the normal closure of L/K we have $X = \mathrm{Gal}(\tilde{L}/F) \cong \Delta^*$, and let $\tilde{\sigma}$ be an extension to $\tilde{L}$ of the generator $\sigma \in \mathrm{Gal}(F/K)$. If X has length

$\ell = p^n$ the isomorphism class of the group $\mathrm{Gal}(\tilde{L}/K)$ is uniquely determined by Prop. 2.2.1, so let's consider the case of length $\ell < p^n$.

We have that $\tilde{\sigma}^{p^n}$ is one element of $\mathrm{soc}(X) \xrightarrow{\sim} \mathrm{soc}(\Delta^*)$ via the Kummer pairing, and $\mathrm{soc}(\Delta^*)$ is also canonically isomorphic to $[\Delta/\operatorname{rad}(\Delta)]^*$. On the other hand the quotient $\Delta/\operatorname{rad}(\Delta)$ is generated by γ. Consequently for an extension $\tilde{\sigma}$ of σ to $\tilde{L}$ we can detect if $\tilde{\sigma}^{p^n} = 1$ testing the Kummer pairing $\langle \gamma, \tilde{\sigma}^{p^n} \rangle_F$ over F.

Now what is remarkable, while requiring just a trivial verification, is that the test with the Kummer pairing can be done in K. More precisely let K_1 be the unique extension of degree p over K contained in F, and let $\bar{\sigma} = \sigma|_{K_1}$. We have that

$$\langle \gamma, \tilde{\sigma}^{p^n} \rangle_F = \langle \bar{N}_{F/K}(\gamma), \bar{\sigma} \rangle_K,$$

where $\bar{N}_{F/K}$ denotes the reduced norm map $[F^\times]_F \to [K^\times]_K$. Being $\ell < p^n$, the independence of the left hand side from the choice of $\tilde{\sigma}$, and hence the equality, can be proved considering the effect of replacing $\tilde{\sigma}$ with a $\tilde{\sigma} \cdot x$ for $x \in \mathrm{Gal}(\tilde{L}/F)$, and observing that $(\tilde{\sigma} \cdot x)^{p^n} = \tilde{\sigma}^{p^n}$ like in Prop. 2.2.1.

Proposition 2.2.2. *Assume* $\mathrm{Gal}(F/K)$ *is cyclic of order* p^n *and generated by* σ*, and let* $L = F(\gamma^{1/p})$*. Assume* $[\tilde{L} : F] < p^n$*, then the full group* $\mathrm{Gal}(\tilde{L}/K)$ *has exponent* p^{n+1} *if and only if* $\langle \bar{N}_{F/K}(\gamma), \bar{\sigma} \rangle_K \neq 1$*.*

If σ is fixed let's denote

$$\varepsilon(\gamma) = \langle \bar{N}_{F/K}(\gamma), \bar{\sigma} \rangle_K. \tag{2.2}$$

This is basically what is being considered in slightly different forms in [Wat94] and [MS05], where a primitive p-th root of the unity ζ_p is fixed, and the integer e_γ such that $\zeta_p^{e_\gamma} = \varepsilon(\gamma)$ is called *index* of γ.

Let's consider the smallest i such that there exist a $\gamma \in \mathrm{soc}^i([F^\times]_F)$ with $\varepsilon(\gamma) \neq 1$. We will show that the value of i depends on whether $\zeta_p \in N_{F/K}(F^\times)$ or not, and this condition is also controlling structure of the socle of $[F^\times]_F$. In particular we have the

Proposition 2.2.3. *Let* F/K *be a cyclic extension of degree* p^n*, with group generated by* σ*. Then the function* ε *is identically* 1 *on* $\operatorname{rad}^1([F^\times]_F)$*, and distinguishing two different cases we have*

$\zeta_p \in N_{F/K}(F^\times)$ – *then* $\mathrm{soc}([F^\times]_F) = [K^\times]_F \oplus \langle \delta \rangle$ *for a class* $\delta \in \mathrm{soc}([F^\times]_F)$ *such that* $\varepsilon(\delta) \neq 1$*,*

$\zeta_p \notin N_{F/K}(F^\times)$ – *then* $\mathrm{soc}([F^\times]_F) = [K^\times]_F$*, and we can find a class* $\eta \in \mathrm{soc}^{p^{n-1}+1}([F^\times]_F)$ *such that* $\varepsilon(\eta) \neq 1$*.*

Being quite well known we give a very terse sketch of proof, see [MS03, Lemma 2, §2] for more details. It has to be remarked that the $p^{n-1}+1$ is not best possible in general, but since we will work with $n = 1$ we need no more accurate results, see [MSS06] and [MSS11] for further investigations.

Proof. Indeed for each $\gamma \in [F^\times]_F$ we have $\bar{N}_{F/K}(\gamma^{\sigma-1}) = 1$, and consequently $\varepsilon(\gamma^{\sigma-1}) = 1$. All extensions obtained from elements in $\operatorname{soc}([F^\times]_F)$ are p-elementary abelian over K precisely when they are from elements in $[K^\times]_F$, so the map induced on the quotient

$$\bar{\varepsilon} : {}^{\operatorname{soc}([F^\times]_F)}\!/_{[K^\times]_F} \longrightarrow \mu_p$$

has to be injective. Now if $[\theta]_F \in \operatorname{soc}([F^\times]_F)$ we can verify that

$$\varepsilon([\theta]_F) = N_{F/K}\left((\theta^{\sigma-1})^{1/p}\right)$$

(independently of the particular p-th root taken). Consequently if ζ_p is not a norm then the image of the above map $\bar{\varepsilon}$ is identically 1, and being injective we obtain $\operatorname{soc}([F^\times]_F) = [K^\times]_F$.

On the other hand if $N_{F/K}(\lambda) = \zeta_p$ for some $\lambda \in F^\times$, then $N_{F/K}(\lambda^p) = 1$, and $\lambda^p = \delta^{\sigma-1}$ for some $\delta \in F^\times$ by “Hilbert 90” Theorem. It follows that

$$\varepsilon([\delta]_F) = N_{F/K}\left((\delta^{\sigma-1})^{1/p}\right) = N_{F/K}(\lambda) = \zeta_p.$$

We still need to prove the existence of a suitable η when ζ_p is not a norm. Let F' be the field fixed by $\sigma^{p^{n-1}}$, and suppose $F = F'(\alpha^{1/p})$ for some class $\alpha \in [F'^\times]_{F'}$. Then $\langle \alpha, \sigma^{p^{n-1}} \rangle_{F'} \neq 1$, and we have

$$\langle \alpha, \sigma^{p^{n-1}} \rangle_{F'} = \langle \bar{N}_{F'/K}(\alpha), \bar{\sigma} \rangle_K = \varepsilon(\alpha^{1/p}).$$

Let’s take $\eta = \alpha^{1/p}$, then $\eta \in \operatorname{soc}^{p^{n-1}+1}([F^\times]_F)$ being killed by $(\sigma-1)^{p^{n-1}+1}$. □

Chapter 3

Preliminaries on local fields

In this chapter we introduce the general notation and give a short account on the basic theory of local fields. Since we are not attempting to give a complete account we will generally be very terse and provide very schematic proofs, or no proof at all. The aim of the sketched proofs will be helping a reader already acquainted with the subject to easily recall the general theory, we refer to the standard books [FV02, Ser79] for a systematic exposition of this topic.

We will make a notable exception for ramification theory, because the theory for non-Galois extension is not very well known and scattered in various papers. We give also an improved proof for the characterization of the ramification breaks of extensions obtained adding a p-th root of the unity, it has the advantage of treating the different cases in a unified way, and clarifying that the result also holds for fields not containing a p-th root of 1.

Notation

For $k \in \mathbb{Z}$ we denote as C_k the cyclic group of order k.

For $a, b \in \mathbb{Z}$, and for a prime p implicit in the context, we will indicate with $[\![a, b]\!]$ the set of integers $a \leq i \leq b$ such that $p \nmid i$.

If F is a field we denote as $[\,\cdot\,]_F$ the reduction modulo power classes, so $[X]_F = {}^{X(F^\times)^p}/_{(F^\times)^p}$ for $X \subseteq F^\times$ and $[\alpha]_F = {}^{\alpha(F^\times)^p}/_{(F^\times)^p}$ for $\alpha \in F^\times$.

3.1 Valued fields

Let F be a field, and assume Γ is a totally ordered abelian group. We define *valuation* to be a map $v : F \to \Gamma \cup \{\infty\}$ satisfying the properties

- $v(\alpha) = \infty \;\Leftrightarrow\; \alpha = 0$,
- $v(\alpha\beta) = v(\alpha) + v(\beta)$,
- $v(\alpha + \beta) \geq \min\{v(\alpha), v(\beta)\}$,

note that if $v(\alpha) \neq v(\beta)$ then $v(\alpha+\beta)$ is always equal to $\min\{v(\alpha), v(\beta)\}$.

If F is equipped with such a function it will be said to be a *valued field*. The map v describes a homomorphism of $F^\times$ to Γ, and its group value $v(F^\times)$ is a totally ordered subgroup of Γ. If $v(F^\times) = \{0\}$ we will call v the *trivial valuation*, and when $v(F^\times)$ is isomorphic to $\mathbb{Z}$ with the natural order it will be said to be a *discrete valuation*.

If F is a valued field, we define $\mathcal{O}_F = \{\alpha \in F : v(\alpha) \geq 0\}$ and $\mathfrak{p}_F = \{\alpha \in F : v(\alpha) \geq 0\}$. Then $\mathfrak{p}_F$ is the unique maximal ideal of $\mathcal{O}_F$, formed by the set of non-invertible elements of $\mathcal{O}_F$. We will denote by κ_F the field $\mathcal{O}_F/\mathfrak{p}_F$, which is called the *residue field*, and for $\alpha \in \mathcal{O}_F$ its image in κ_F will be denoted by $\bar{\alpha}$. The set of invertible elements $U_F = \mathcal{O}_F \setminus \mathfrak{p}_F$ is a multiplicative group, and is called the *group of units*.

If F is a discretely valued field, we will denote by v_F the *normalized* valuation, that is the valuation which makes $v(F^\times)$ coincide with $\mathbb{Z}$. It is obtained as $v_F = \iota \circ v$ where $\iota : v(F^\times) \xrightarrow{\sim} \mathbb{Z}$ is the unique possible isomorphism of $v(F^\times)$ with $\mathbb{Z}$ as ordered groups. Any element π in $\mathfrak{p}_F \setminus \mathfrak{p}_F^2$ has valuation exactly 1 and generates $\mathfrak{p}_F = \pi\mathcal{O}_F$ as $\mathcal{O}_F$-module. Such a π will be called *uniformizer* or *uniformizing element*, and we will often denote by π_F a fixed choice of a uniformizing element.

Definition 3.1.1 ("big-Oh" and "Dots" notations)**.** In an expression we will denote as $\mathcal{O}(\alpha)$ any element with valuation at least as big as that of α.

The dots ... in an expression will have a precise and well defined meaning, they stand for "a term whose valuation is bigger than the smallest possible valuation of each term appearing in the expression". So if $a, b, c \geq 0$ and $\alpha, \beta \in \mathcal{O}_F$, in the expression $1 + \alpha\pi_F^a + \beta\pi_F^b + \pi_F^c + \dots$ the dots stand for a $\mathcal{O}(\pi_F^{\max\{a,b,c\}+1})$ in the "big-Oh" notation. In particular we ignore that $v_F(\alpha)$, $v_F(\beta)$ may happen to be > 0, being α, β general elements of $\mathcal{O}_F$. In any case this notation will only be used where no confusion may arise, but its usage would rather make a computation or a statement less cumbersome.

3.1.1 Complete fields

A sequence $(\alpha_n)_{n\geq 0}$ of elements of F is called a *Cauchy sequence* if for each $c \in \mathbb{R}$ there exists an $n_0 \geq 0$ such that $v_F(\alpha_n - \alpha_m) \geq c$ for $m, n \leq n_0$. It coincides with the usual definition in a metric space when F is equipped with the distance induced by the norm defined as $|\alpha| = \varepsilon^{-v_F(\alpha)}$, for some fixed $\varepsilon \in (0,1)$. Such a norm is called *non-archimedean*, and the associated distance *ultrametric*, because additionally to the common axioms we have the strengthened inequality $|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$

The valuation induces a topology on F, making it a topological field. A system of neighborhood of 0 is given by the powers of the maximal ideal $\mathfrak{p}_F^i$, for $i \geq 1$.

Lemma 3.1.2. *The topologies on F defined by two normalized discrete valuations v_1, v_2 coincide if and only if $v_1 = v_2$.*

Proof. The proof is obtained by absurd, considering a suitable combination of elements where v_1 and v_2 differ, and considering the limit of its powers with respect to the topology. We refer to [FV02, Chap. 1, Lemma 3.5] for the full proof. $\square$

We say that F is a *complete discrete valued field* if every Cauchy sequence is convergent.

Proposition 3.1.3. *For any discrete valuation field there exists a completion, which is unique up to isomorphism.*

Proof. The completion is obtained considering the ring of all Cauchy sequences up to equivalence, and characterizing the elements in a completion as the set of all possible limits. The argument is very standard and we refer to [FV02, Chap. 1, Prop. 4.2] and [Ser79, Chap. 2, §1]. $\square$

A completion of the discretely valued field F will be denoted as $\hat{F}$. A complete discretely valued field with perfect residue field is often referred to as a *local field* [FV02, Chap. 4]. However, sometimes also the fields complete with respect to an archimedean absolute value $\mathbb{R}$ and $\mathbb{C}$ are considered local fields, and often a local field is assumed to be locally compact.

It's easy to prove that F is locally compact if and only if it is complete and the residue field κ_F is a finite field. We will always assume a local field is a complete discretely valued field which is locally compact, and having a fixed prime p as the characteristic of the residue field.

We will denote by f_F the absolute residual degree $[\kappa_F : \mathbb{F}_p]$, which will be called *absolute inertia degree.* We will set $e_F = v_F(p)$, which will be called *absolute ramification index.* When F has itself characteristic p we will be fine with $e_F = +\infty$, unless differently specified.

We denote by $\mathbb{Q}_p$ the p-adic field, that is the completion of $\mathbb{Q}$ with respect to the p-adic valuation defined as $v_p(p^k \frac{a}{b}) = k$, where a rational is written as $p^k \frac{a}{b}$ with a and b are prime with p. The ring of p-adic integers is denoted as $\mathbb{Z}_p$.

For some $q = p^m$ we denote by $\mathbb{F}_q[[Y]]$ the ring of formal power series with coefficients in $\mathbb{F}_q$, and by $\mathbb{F}_q((Y))$ its quotient field. It is complete with respect to the valuation induced by the order at Y, with ring of integers exactly equal to $\mathbb{F}_q[[Y]]$.

3.1.2 Multiplicative group

Let F be a local field. Then we have the exact sequence

$$1 \longrightarrow U_F \longrightarrow F^\times \xrightarrow{v_F} \mathbb{Z} \longrightarrow 1,$$

and each choice of a uniformizer π_F provides a splitting of the above exact sequence. Such a splitting $\mathbb{Z} \to F^\times$ is obtained as $1 \mapsto \pi_F$. So in particular we have $F^\times = U_F \oplus \langle \pi_F \rangle$.

We define the *higher unit groups* as $U_{0,F} = U_F$, and $U_{i,F} = 1 + \mathfrak{p}_F^i$ for $i \geq 1$. For $i \geq 1$, an element of the quotient $U_{i,F}/U_{i+1,F}$ can we written as $1+\alpha\pi_F^i+\dots$, and the map $(1+\alpha\pi_F^i+\dots) \mapsto \bar{\alpha}$ can be easily verified to induce a (non canonical because it depends on π_F) isomorphism of groups $U_{i,F}/U_{i+1,F} \to \kappa_F$. Similarly we have a canonical isomorphism $U_{0,F}/U_{1,F} \to \kappa_F^\times$ induced by the reduction modulo $\mathfrak{p}_F$.

The properties of the p-th power maps on the higher unit groups are resumed in the following proposition (see also [FV02, Chap. 1, Prop 5.7]).

Proposition 3.1.4. *Assume $i \geq 1$ and $\alpha \in U_F$. Then we have*

$$(1+\alpha\pi_F^i+\dots)^p = \begin{cases} 1+\alpha^p\pi_F^{pi}+\dots & \text{if } i < {}^{e_F}/_{(p-1)}, \\ 1+(\alpha^p+\theta_0\alpha)\pi_F^{pi}+\dots & \text{if } i = {}^{e_F}/_{(p-1)}, \\ 1+\theta_0\alpha\pi_F^{i+e_F}+\dots & \text{if } i > {}^{e_F}/_{(p-1)}, \end{cases}$$

where θ_0 is such that $p = \theta_0\pi_F^{e_F}+\dots$.

Proof. This is an immediate consequence of the binomial expansion

$$(1+\alpha\pi_F^i)^p = \sum_{j=0}^{p}\binom{p}{j}(\alpha\pi_F^i)^j = 1+\alpha^p\pi_F^{pi}+p\alpha\pi_F^i+\mathcal{O}(\pi^{2i+e_F}). \qquad \square$$

Generators of $U_{1,F}$ as $\mathbb{Z}_p$-module. Since $U_{i,F}^p \subseteq U_{i+1,F}$ we have that $\alpha^{p^i} \to 1$ for each $\alpha \in U_{i,F}$, and in particular we can put a natural structure of $\mathbb{Z}_p$-module on the multiplicative group $U_{1,F}$. Thanks to the proposition we can take as generators of $U_{1,F}/U_{1,F}^p$ the a union of the elements in $U_{i,F}$ generating $U_{i,F}/U_{i+1,F}$ for all $0 < i < {}^{pe_F}/_{(p-1)}$ and $(i,p)=1$, and an additional element in $U_{pe_F/(p-1)}$ when the map $\bar{\alpha} \mapsto \bar{\alpha}^p + \bar{\theta}_0\bar{\alpha}$ is not surjective. When κ_F is finite, it is not hard to show that this condition is verified if and only if $F^\times$ contains a primitive p-th root of the unity ζ_p (see [FV02, Chap. 1, Prop 5.7]).

In particular, putting $I_F = {}^{pe_F}/_{(p-1)}$ for convenience, we can take the basis

$$\Big\{1+\beta_j\pi^i\Big\}_{\substack{1\leq j\leq k \\ i\in[\![1,I_F]\!]}} \cup \Big\{1+\eta\pi^{I_F}\Big\},$$

where $[\![a,b]\!]$ denotes the integers in $[a,b]$ which are prime with p, and the reductions of $\beta_1,\dots,\beta_k$ are a basis of κ_F as vector space over $\mathbb{F}_p$. The second term is present only when $\zeta_p \in F^\times$ (and consequently I_F is an integers), and in this case $\bar{\eta}$ should be a generator of the cokernel of the map $\bar{\alpha} \mapsto \bar{\alpha}^p + \bar{\theta}_0\bar{\alpha}$.

We remark that, when F is a finite extension of degree n of the p-adic field $\mathbb{Q}_p$, then $U_{1,F}$ has finite rank as $\mathbb{Z}_p$-module, and is isomorphic to $\mathbb{Z}_p^n \oplus \mathbb{Z}/p^r\mathbb{Z}$, where r is the biggest integer such that $F^\times$ contains a primitive p^r-th root of the unity.

Multiplicative representatives. For each $\bar{\alpha} \in \kappa_F$ and $i \geq 0$ we can define $A_i = \{\beta : \overline{\beta^{p^i}} = \bar{\alpha}\}$. Each sets $A_i^{p^i}$ is nonempty being κ_F perfect, is formed by element whose reduction is $\bar{\alpha}$ and is contained in $A_{i-1}^{p^{i-1}}$ for $i \geq 1$, and the ratio of two elements in $A_i^{p^i}$ is $\in U_{i+1,F}$. Consequently the intersection of all the $A_i^{p^i}$ is formed by precisely one element $T(\bar{\alpha})$, called *multiplicative representative* of $\bar{\alpha}$. Indeed it easy to verify that $T(\bar{\alpha}\bar{\beta}) = T(\bar{\alpha})T(\bar{\beta})$, so in particular T gives a canonical map $\kappa_F^\times \to U_{0,F}$ which splits the exact sequence

$$1 \longrightarrow U_{1,F} \longrightarrow U_{0,F} \longrightarrow \kappa_F^\times \longrightarrow 1.$$

When F has characteristic p, the map T extends to an embedding $\kappa_F \to F$ which is also additive, and in this case it is easy to prove that a uniformizer is transcendental over the image of the embedding. In particular when F has finite residue field we have the following proposition.

Proposition 3.1.5. *If F is a local field with finite residue field then F is either isomorphic to $\mathbb{F}_q((Y))$ for some $q = p^m$, either it is a finite extension of the p-adic field $\mathbb{Q}_p$.*

Proof. We omit the proof, see [Neu99, Chap. 2, §5, Prop. 5.2]. □

3.2 Extensions of local fields

Let F be a local field, then there exists precisely one extension of the valuation v_F to the separable closure F^{sep}. This is a consequence of Lemma 3.1.2, because the unique topology on L as vector space is induced by that of F, see [FV02, Chap. 2, Theorem 2.5] for more details. The extension is *a fortiori* Galois invariant, so if α and β are conjugated we have $v_F(\alpha) = v_F(\beta)$, denoting again the extension of the valuation with v_F.

Let L/F be a finite extension of degree n. We denote by $f = f(L/F)$, and call *inertia degree*, the degree of the residue extension $[\kappa_L : \kappa_F]$. We denote by $e = e(L/F)$, and call *ramification index*, the index of $v_L(F^\times)$ as subgroup of $v_L(L^\times)$.

Proposition 3.2.1. *We have that $ef = n$, and if the reductions of $\beta_1, \dots, \beta_f \in \mathcal{O}_L$ are a basis of κ_L as vector space over κ_F then the elements $\left\{\beta_i \pi^j\right\}$ for $1 \le i \le k$ and $0 \le j < e$ are a basis of $\mathcal{O}_L$ as $\mathcal{O}_F$-module, and also a basis of L as F-vector space.*

Proof. See [FV02, Chap. 2, Prop. 2.4]. □

Assume now $L = F(\alpha)$, for some $\alpha \in F^{\mathrm{sep}}$.

Lemma 3.2.2 (Krasner Lemma)**.** *Let $\beta \in F^{\mathrm{sep}}$, and let $\alpha = \alpha_1, \alpha_2, \dots, \alpha_k$ be the conjugates of α in F^{sep}. Assume that*

$$v_F(\beta - \alpha) > v_F(\alpha - \alpha_i)$$

for each $2 \le i \le k$. Then we have $F(\alpha) \subseteq F(\beta)$.

Proof. Arguing by contradiction, let σ be an element of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ moving α but fixing β. Then $\beta - \sigma(\alpha)$ would have the same valuation as $\beta - \alpha$, but their difference $\alpha - \sigma(\alpha)$ should have strictly smaller valuation. This is absurd. □

3.2.1 Norm map.

We recall here very briefly a description of the norm map on $U_{1,L}$, for a totally ramified Galois extension L/F of degree p. If $\sigma \in \mathrm{Gal}(L/F)$ is a non-trivial automorphism, we have that

$$\frac{\sigma^i(\pi_L)}{\pi_L} = 1 + i\eta\pi_L^s + \dots$$

for some unit η and integers s, so the residue class $\bar{\eta}$ is characterized up to multiplication by elements in the prime field $\mathbb{F}_p^\times$, and $\bar{\eta}^{p-1}$ is uniquely determined.

Proposition 3.2.3. *Assume $i \geq 1$ and $\alpha \in U_F$. The map $N_{L/F}$ satisfies*

$$N_{L/F}(1+\alpha\pi^i+\dots) = \begin{cases} 1 + \alpha^p\pi^i + \dots & \text{if } 1 \leq i < s, \\ 1 + (\alpha^p - \eta^{p-1}\alpha)\pi^s + \dots & \text{if } i = s, \\ 1 + (-\eta^{p-1}\alpha)\pi^{j+s} + \dots & \text{if } i = s + pj \text{ for some } j \in \mathbb{N}, \end{cases}$$

and furthermore if $j > 0$, $(j, p) = 1$ we have $N_{L/F}(U_{s+j,L}) = N_{L/F}(U_{s+j+1,L})$.

Proof. See [FV02, Chap. 3, §1, Prop. 1.5]. □

3.3 Ramification theory

We give here a short exposition on ramification theory, considering in particular the case of non-Galois extensions. This material is certainly not new, and it can be found for instance in [Yam68, Lub81, Del84, Hel91]. However being less well known we will be less terse and give a more detailed account.

We assume F is a local field, and L/F a finite separable extension. We will denote as $\Gamma = \Gamma(L/F)$ the set of embeddings $L \to F^{\mathrm{sep}}$ fixing F. We will identify L with one subfield of F^{sep}, then Γ contains a distinguished element which is the identity embedding, and a distinguished subset which is $\mathrm{Aut}(L/F)$. If L/F is not normal then Γ is not a group, but can be identified with the quotient space G/H where G is the Galois group $\mathrm{Gal}(M/F)$ of a Galois extension M containing L, and L is fixed by the subgroup H. The identity embedding corresponds clearly to the class H/H, and $\mathrm{Aut}(L/F)$ to $N_G(H)/H$.

We define the index function i_L on Γ as

$$i_L = \min\left\{v_L(\sigma(x) - x),\ \forall x \in \mathcal{O}_L\right\},$$

we remark that if $\sigma, \tau \in \Gamma(L/K)$ then we have

$$i_L(\sigma\tau) \geq \min\left\{i_L(\sigma), i_L(\tau)\right\}. \tag{3.1}$$

If α is generator of $\mathcal{O}_L$ over $\mathcal{O}_K$ (such a generator always exists by [Ser79, Chap. 3, §6, Prop. 12]) then $i_L(\sigma) = v_L(\sigma(\alpha) - \alpha)$, this expression can also be taken as definition. Up to a shift by one, i_L is the index function of the filtration of the *ramification subsets* which are defined as

$$\Gamma_t = \{\sigma \in \Gamma : i_L(\sigma) \geq t+1\}\,, \qquad \Gamma_{t^+} = \{\sigma \in \Gamma : i_L(\sigma) > t+1\}\,.$$

We will say that the real number t is an *(lower) ramification break* (or *jump*) of the extension L/F if $\Gamma_t \supsetneq \Gamma_{t^+}$.

The conjugates of the generator α form a homogeneous space under the action of G which is isomorphic to $\Gamma = G/H$, the correspondence being given by $\sigma \mapsto \sigma(\alpha)$. Let $f(T)$ be the minimal monic polynomials of α. Then the elements $\sigma(\alpha) - \alpha$, for $\sigma \in \Gamma$, are exactly the roots of $f(Y + \alpha)$, and their valuations can be obtained via the Newton polygon. In particular in this way we recover the cardinality of Γ_t (resp. Γ_{t^+}) as the number of roots of $f(T+\alpha)$ having valuation $\geq t+1$ (resp. $> t+1$).

We point out that the reductions $\overline{\sigma(\alpha)}$ over the residue field generate κ_L as vector space over κ_F, so all the conjugates of $\bar{\alpha}$ over κ_F appear, and each is repeated $\#\Gamma_0$ times. Consequently $f(L/K) = {}^{\#\Gamma}/_{\#\Gamma_0}$, and $e(L/K) = \#\Gamma_0$. Clearly $\#\Gamma_0$ fixes the set of multiplicative representatives, so the field they generate over K is unramified of degree $f(L/K)$. In this way we obtain the field fixed by $\#\Gamma_0$, and it is the maximal unramified subextension of L/F.

The cornerstone of the theory of Hasse-Herbrand is the following proposition, which is a generalization of [Ser79, Chap. 4, §1, Prop. 3].

Proposition 3.3.1. *Let $M \subseteq F^{\mathrm{sep}}$ be a finite separable extensions of L. Then for each $\sigma \in \Gamma(L/F)$ we have*

$$i_L(\sigma) = \frac{1}{e(M/L)} \sum_{\tilde{\sigma} \to \sigma} i_M(\tilde{\sigma}),$$

where sum is over all the $\tilde{\sigma} \in \Gamma(M/F)$ extending σ.

Proof. Let α,β be elements such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, and $\mathcal{O}_M = \mathcal{O}_K[\beta]$. Assume the minimal polynomial of β over $\mathcal{O}_L$ is $g(T)$. Then the polynomial $g^\sigma(T)$ obtained acting with σ on the coefficients is

$$g^\sigma(T) = \prod_{\tilde{\sigma} \to \sigma} (T - \tilde{\sigma}(\beta)),$$

and

$$\sum_{\tilde{\sigma} \to \sigma} v_M(\tilde{\sigma}(\beta) - \beta) = v_M(g^\sigma(\beta)) = v_M((g^\sigma - g)(\beta)) \geq v_M(\sigma(\alpha) - \alpha),$$

because the coefficients of $(g^\sigma - g)(T)$ are of the form $\sigma(g_i) - g_i$ for $g \in \mathcal{O}_L$, and $v_M(\sigma(g_i) - g_i) \geq v_M(\sigma(\alpha) - \alpha)$.

Let now $\alpha = f(\beta)$ for a polynomial $f(T) \in \mathcal{O}_F[T]$. Then $g(T) \mid f(T) - \alpha$, so applying σ to the coefficients and evaluating in α we have the reversed inequality

$$v_M(g^\sigma(\beta)) \leq v_M(f(\beta) - \sigma(\alpha)) = v_M(\alpha - \sigma(\alpha)). \qquad \square$$

The Hasse-Herbrand *transition function* is defined as

$$\phi_{L/F}(u) = \frac{1}{e(L/F)} \int_0^u (\#\Gamma_t)\, dt.$$

The inverse function $\phi_{L/K}^{-1}$ will be denoted as $\psi_{L/F}$.

Proposition 3.3.2. *For each $u \geq 0$ we have*

$$\phi_{L/F}(t) = \frac{1}{e(L/F)} \sum_{\sigma \in \Gamma} \min\{t,\ i_L(\sigma) - 1\}.$$

Proof. Indeed, it is easy to see that the function is piecewise linear, and has slope equal to $1/e(L/F)$ times the number of $\sigma \in \Gamma$ such that the minimum is given by t, so $t \leq i_L(\sigma) - 1$. These σ being exactly those in Γ_t, we have the proposition. □

Proposition 3.3.3. *Let $M \subset F^{\text{sep}}$ be a finite separable extension of L, and let $\Gamma = \Gamma(L/F)$, $\Gamma' = \Gamma(M/F)$. For each $\sigma \in \Gamma$, if $\tilde{\sigma} \in \Gamma$ is an extension of σ with $i_M(\tilde{\sigma})$ is as big as possible, than we have*

$$i_L(\sigma) - 1 = \phi_{M/L}(i_M(\tilde{\sigma}) - 1).$$

Proof. Let σ' be an automorphism of F^{sep} extending $\tilde{\sigma}$. Then the elements of Γ' extending σ are exactly those in the set $\sigma'\Lambda$, for $\Lambda = \Gamma(M/L)$. By the choice of $\tilde{\sigma}$ and by the (3.1) we have

$$i_M(\sigma'\tau) = \min\{i_M(\tilde{\sigma}), i_M(\tau)\}$$

for each $\tau \in \Lambda$, and the thesis follow by the Prop. 3.3.1 and 3.3.2. □

Assume M, Γ, Γ' be like in the proposition. The set Γ' has a natural equivalence relation with respect to L, where the elements σ, τ are equivalent if $\sigma|_L = \tau|_L$. Let $\Lambda = \Gamma(M/L)$, then the equivalence classes induced on Γ'_u are the sets $\sigma'\Lambda_u$, for some $\sigma \in \Gamma'_u$ and an automorphism σ' of F^{sep} extending it. The quotient by the equivalence relation may thus be denoted by Γ'_u/Λ_u. The function $\phi_{M/L}$ of an extension describes the images of the ramification subsets under the restriction map.

Proposition 3.3.4. *For $u \geq 0$ we have a natural bijection*

$$\Gamma'_u/\Lambda_u \to \Gamma_{\phi_{M/L}(u)},$$

associating to every class $\sigma'\Lambda$ the restriction $\sigma|_L$.

Proof. The map is clearly injective, and if $\sigma \in \Gamma_{\phi_{M/L}(u)}$ then it is the restriction of some $\tilde{\sigma} \in \Gamma'_u$ by Prop. 3.3.3. □

Corollary 3.3.5. *The breaks of M/F are the union of those of M/L and images by $\psi_{M/L}$ of the breaks of L/F*

Proof. Indeed, $\Gamma'_u \supsetneq \Gamma'_{u^+}$ if and only if at least one of

$$\Lambda_u \supsetneq \Lambda_{u^+}, \qquad \Gamma_{\phi_{M/L}(u)} \supsetneq \Gamma'_{\phi_{M/L}(u)^+}$$

is verified. □

For each $X \subset \Gamma'$, lets denote by $X\Lambda/\Lambda \subseteq \Gamma/\Lambda$ the image of X modulo the equivalence induced by Λ.

Proposition 3.3.6. *The image of* $\Gamma'_u\Lambda/\Lambda$ *via the map* $\Gamma'/\Lambda \to \Gamma$ *is* $\Gamma_{\phi_{M/L}(u)}$.

Proof. Indeed, the representative of a class of $\Gamma'_u\Lambda/\Lambda$ with biggest index is certainly mapped into $\Gamma_{\phi_{M/L}(u)}$, the map is clearly injective, and each $\sigma \in \Gamma_{\phi_{M/L}(u)}$ is restriction of some $\tilde{\sigma} \in \Gamma'_u$ by Prop. 3.3.3. □

The following transitivity property of $\phi_{L/F}$ is fundamental. It can be used to define the $\phi_{L/F}$ for non-Galois extensions from the Galois case, by reduction to the Galois case, as done in [FV02] for instance.

Proposition 3.3.7. *Assume* M *is a finite separable extension of* L*. Then we have*

$$\phi_{M/K} = \phi_{L/K} \circ \phi_{M/L}.$$

Proof. Let Γ, Γ' and Λ be defined as in Prop. 3.3.4. The derivative of the right had side is $\phi'_{L/K}(\phi_{M/L}(u)) \circ \phi'_{M/L}(u)$, which is also equal to

$$\frac{1}{e(L/K)}\left(\#\Gamma_{\phi_{M/L}(u)}\right) \cdot \frac{1}{e(M/L)}(\#\Lambda_u).$$

By Prop. 3.3.4 the expression can be rewritten as

$$\frac{1}{e(M/K)}(\#\Gamma'_u) = \phi'_{M/K}(u). \qquad \square$$

Proposition 3.3.8. *For* $u \geq 0$*, let* $L_u \subseteq L$ *be the field fixed by the ramification subset* $\Gamma_u \subseteq \Gamma(L/F)$*. Then*

$$\Gamma(L/L_u) = \Gamma_u.$$

Proof. Indeed, let M is a bigger extension which is Galois over F with $G = \mathrm{Gal}(M/F)$ and where the subgroup fixing L is $H = \mathrm{Gal}(M/L)$. Then by Prop. 3.3.6 putting $v = \psi_{M/L}(u)$ we have the bijection

$$(G_vH)/H \to \Gamma_u.$$

Since G_v is defined in a Galois-invariant way, it is certainly a normal subgroup of G. Consequently the set of products G_vH is a group, and we can consider the fixed field L_u. Then L/L_u has degree exactly equal to $(G_vH : H)$, and $\Gamma(L/L_u) = \Gamma_u$. □

We will in general call L_u (resp. L_{u^+}) the field fixed by Γ_u (resp. Γ_{u^+}). In general it is convenient defining an alternative numbering which has better properties with respect to the quotient, and this is achieved putting $\Gamma^{\phi_{L/F}(u)}$ equal to Γ_u. This new *upper numbering* is preserved when passing to the quotient, as we can easily verify thanks to Prop. 3.3.6 and 3.3.7.

Like for lower numbering we define Γ^{v^+} to be $\Gamma_{\psi_{L/K}(v)^+}$, it is also equal to the union of the Γ^t for $t > v$. We will say that the real number v is an *upper ramification break* (or *jump*) of the extension L/F if $\Gamma^v \supsetneq \Gamma^{v^+}$, where $\Gamma = \Gamma(L/F)$. When we do not specify *lower* or *upper* we will always intend *lower* ramification break. When there is only one ramification break, then the upper break and the lower break coincide, so in this case the distinction is not even necessary.

3.3.1 Arithmetically disjoint extensions

We say that two extensions L/F and E/F are *arithmetically disjoint* if the sets of upper ramification breaks for L/F and E/F have empty intersection.

Proposition 3.3.9. *Assume $u_1, \dots, u_k$ be the upper ramification break of L/F. If L/F and E/F are arithmetically disjoint then the ramification breaks of LE/E are $\psi_{E/F}(u_1), \dots, \psi_{E/F}(u_k)$, and the cardinality of the corresponding ramification subsets is preserved.*

Proof. Considering one intermediate extension in the tower of ramification subfield, we can reduce to the case of L/F and E/F having just one break u and v respectively, and that $u < v$ say. Then u, v are the upper breaks of LE/F and L/F is the ramification subfield. Consequently the lower breaks are $u = \psi_{LE/F}(u) = \psi_{E/F}(u)$ and $\psi_{LE/F}(v) = \psi_{L/F}(v)$, and they are the breaks of LE/L and LE/E. See [Yam68, Theorem 4] and [Mau67] for more details. □

3.3.2 Galois extensions

Assume now L/F is Galois. Then $G = \mathrm{Gal}(L/F)$ has a filtration formed by subgroups which are certainly normal, being defined in a canonical way. The quotient G/G_0 can be identified with the Galois group of the residue field extension $\mathrm{Gal}(\kappa_L/\kappa_K)$. We also have embeddings

$$G_i/G_{i+1} \to U_{i,L}/U_{i+1,L}, \qquad \text{for } i \geq 1,$$

induced by $\sigma \mapsto \frac{\sigma(\pi_L)}{\pi_L} + \mathcal{O}(\pi_L^{i_L(\sigma)})$. They are readily verified to be injective homomorphisms and independent of the choice of π_L.

In particular it follows that G/G_0 is cyclic, G_0/G_1 is cyclic with order prime with p, while each G_i/G_{i+1} is an elementary abelian p-group of rank $\leq f(L/F)$. See [Ser79, Chap. 4] for more properties.

3.3.3 Radical extensions

We now characterize the ramification number of the p-extension L/F obtained adding the p-th roots of some $\alpha \in F^\times$ which is not a p-th power, $L = F(\alpha^{1/p})$. Put $V_0 = F^\times$, and $V_i = U_{i,F}$ for $i \geq 1$. We define $\partial([\alpha]_F) = \partial_F(\alpha)$, and call it *defect*, to be the biggest integer i such that $\alpha \in V_i(F^\times)^p$. We have from Section 3.1.2 that $\partial(\alpha)$ can be 0, an integer in $[\![0, I_F]\!]$, or I_F when $\zeta_p \in F$.

The proposition which follows is well known and is contained for instance in [Has30, §9, §11] and [Wym69, §4]. We give here a very concise proof, treating the different cases in a unified way.

Proposition 3.3.10. *Assume $\alpha \in F^\times$ is not a p-th power, then $F(\alpha^{1/p})/F$ is unramified when $\partial(\alpha) = I_F$, and has unique ramification break equal to $I_F - \partial(\alpha)$ when $\partial(\alpha) \neq I_F$.*

Proof. Let $i = \partial(\alpha)$, and π_F an uniformizer for F.

Suppose $i = 0$, then $v_F(\alpha)$ is prime with p, replacing it with $\alpha^s \pi_F^{pt}$ where $v_F(\alpha)s + pt = 1$ we can assume that $v_F(\alpha) = 1$. Then $\pi_L = \alpha^{1/p}$ is a uniformizer for L, and for nontrivial $\sigma \in \Gamma(L/F)$ we have

$$v_L(\sigma(\pi_L) - \pi_L) = v_L((\zeta_p - 1)\pi_L) = pe_F/(p-1) + 1,$$

and consequently $i_L(\sigma) - 1 = {}^{pe_F}/_{(p-1)} = I_F$.

Suppose $p \nmid i$. We can assume $v_F(\alpha - 1) = i$ changing α by an element of $(F^\times)^p$ if necessary. If $\beta = \alpha^{1/p}$ then $v_L(\beta - 1)$ should be an integer and hence $e(F(\beta)/F) = p$, and $\beta = 1 + \lambda\pi_L^i$ for a uniformizer π_L and some $\lambda \in F$. Applying a non-trivial $\sigma \in \Gamma(L/F)$ with $s = i_L(\sigma) - 1$ we have that

$$\sigma(\beta) = 1 + \lambda\pi_L^i + \lambda\eta i \pi_L^{i+s} + \dots,$$

assuming that $\sigma(\pi_L) = \pi_L + \eta\pi_L^{s+1} + \dots$. Since $v_L(\sigma(\beta) - \beta) = {}^{e_L}/_{(p-1)}$, we obtain that $i + s$ is equal to ${}^{e_L}/_{(p-1)} = I_F$, that is $s = I_F - i$.

Suppose $i = I_F$, and assume $v_F(\alpha - 1) = i$ changing α by an element of $(F^\times)^p$ if necessary. We have $\beta = 1 + \lambda\pi_F^{i/p} + \dots$ with for some $\lambda \in U_L$. Since $v_F(\sigma(\beta) - \beta) = {}^{i}/_{p}$ for all $\sigma \in \Gamma(L/F)$, we have that every σ acts non-trivially on κ_L, and consequently L/F is unramified. □

3.4 Local Class Field Theory

We give here a short resume, with no proof, of the most important results of local class field theory. We give references to the standard literature for the proofs.

We recall the definition of the *transfer map* in group theory. If G is a group, let's denote by G^{ab} the *abelianized*, that is G/G' where G' is the commutator subgroup (or derived subgroup). Let H be a subgroup of finite index, and assume $G = \bigcup_i H\rho_i$ be a decomposition as disjoint union of right cosets.

We define the transfer map Ver as

$$\mathrm{Ver} : G^{\mathrm{ab}} \to H^{\mathrm{ab}}, \qquad (\sigma \bmod G') \mapsto \prod_i \left(\rho_i \sigma \rho_{\sigma(i)}^{-1} \bmod H'\right),$$

where σ_i is defined as the index such that $\rho_i \sigma \in H\rho_{\sigma(i)}$. We refer to [FV02, Chap. 4, §3.6] for a proof that Ver is well defined and a homomorphism.

Theorem 3.4.1 ("Local class field theory")**.** *Let F be a local field with finite residue field. Denote by F^{ab} and L^{ab} the maximal abelian extension. Then we have a canonical homomorphism*

$$\Psi_F : F^\times \longrightarrow \mathrm{Gal}(F^{\mathrm{ab}}/F)$$

which is injective and has dense image.

Let L/F be a finite Galois extension. For $\alpha \in F^\times$, $\Psi_F(\alpha)$ acts trivially on $L \cap F^{\mathrm{ab}}$ if and only if $\alpha \in N_{L/F}(L^\times)$.

The restriction of $\Psi_F(\alpha)$ to the maximal unramified extension F^{ur} coincides with $\phi_F^{v_F(\alpha)}$, where $\phi_F \in \mathrm{Gal}(F^{\mathrm{ur}}/F)$ is induced by the q-th power Frobenius.

Let L/F be a finite separable extension, and σ and automorphism in $\mathrm{Gal}(F^{\mathrm{sep}}/F)$. Then the diagrams

$$\begin{tikzcd}
L^\times \arrow[r, "\Psi_L"] \arrow[d, "\sigma"'] & \mathrm{Gal}(L^{\mathrm{ab}}/L) \arrow[d, "\tau\mapsto\sigma\tau\sigma^{-1}"] \\
\sigma L^\times \arrow[r, "\Psi_{\sigma L}"] & \mathrm{Gal}((\sigma L)^{\mathrm{ab}}/\sigma L)
\end{tikzcd}$$

$$\begin{tikzcd}
L^\times \arrow[r, "\Psi_L"] \arrow[d, "N_{L/F}"'] & \mathrm{Gal}(L^{\mathrm{ab}}/L) \arrow[d, "\tau\mapsto\tau|_F"] \\
F^\times \arrow[r, "\Psi_F"] & \mathrm{Gal}(F^{\mathrm{ab}}/F)
\end{tikzcd} \qquad (3.2)$$

$$\begin{tikzcd}
F^\times \arrow[r, "\Psi_F"] \arrow[d] & \mathrm{Gal}(F^{\mathrm{ab}}/F) \arrow[d, "\mathrm{Ver}"] \\
L^\times \arrow[r, "\Psi_L"] & \mathrm{Gal}(L^{\mathrm{ab}}/L)
\end{tikzcd}$$

are commutative.

We refer to [FV02, Chap. 4, §4] for the proof. Alternative proofs can be found in [Ser79] and in Milne's notes.

Theorem 3.4.2 ("Existence Theorem")**.** *There is a one to one correspondence between open subgroups of finite index of $F^\times$ and finite abelian extensions of F, where each subgroup N of $F^\times$ as above is the subgroup of norms $N_{L/F}(L^\times)$ of exactly one finite abelian extension. This correspondence is inclusion reversing, and the intersection of two objects on one side corresponds to the composite of the corresponding objects on the other side.*

The proof can be found in [FV02, Chap. 4, §6]. We will show a very constructive proof for totally ramified extension, using Eisenstein polynomials.

Chapter 4

Classification of extensions of degree p^2

In this chapter we give a synthetic parametrization of all separable extensions of degree p^2 of a $\mathfrak{p}$-adic field, that is a finite extension of $\mathbb{Q}_p$.

A database of the extensions of $\mathbb{Q}_p$ has been created Jones-Roberts [JR06], with the purpose of facilitating the study extensions of $\mathbb{Q}$ by providing in a unique place a complete description of the local structure. However the complexity of the extensions of degree n grows very quickly with the power of p dividing n, to the point that the database essentially contains only extensions for n with $p^2 \nmid n$. The biggest degree n divisible by p^2 present the database is for extensions of degree 9 of $\mathbb{Q}_3$, and to handle this case a work on its own was required [JR04]. In that work it was observed that all transitive subgroups of S_9 that may fit into the ramification filtration are actually appearing as normal closures of extensions of degree p^2, hence raising the question of determining whether the same happens for general p over $\mathbb{Q}_p$. It turns out that this false for $p \geq 5$ over $\mathbb{Q}_p$, but it is true whenever the base field is a proper extension $K \supsetneq \mathbb{Q}_p$ whose residual degree $f(K/\mathbb{Q}_p)$ is odd.

We will show a synthetic way to parametrize the extensions of degree p^2 of a p-adic field, which can be viewed as a generalization of the methods of [DCD07], and up to some extent also of [Cap07]. The abstract idea is that the possible extensions $\tilde{L}/K$, appearing as normal closure of an isomorphism class of extensions L/K, will correspond to the indecomposable representations of a certain group G acting naturally on a suitable module X.

While we concentrate on fields of characteristic 0, we point out the same strategy can be applied to fields of characteristic p, replacing Kummer theory with Artin-Schreier theory. Another possible approach would be via local class field theory, but the field considered will always contain the required roots of the unity so we lose nothing by just using Kummer theory, which gives an interpretation of elementary abelian p-extensions in terms of subgroups of $[K^\times]_K$ rather than its quotients.

We remark that the p-part of the absolute Galois group of a p-adic field K not containing a primitive p-th root of the unity ζ_p is equal to the p-completion of the free group on $[K : \mathbb{Q}_p] + 1$ generators as proved in [Sha47], so it is "as complicated as possible" within groups of a fixed number of generators. When $\zeta_p \in K$ the p-part of the Galois group is a Demuškin group, and can be characterized by generators and relation of group with exactly one relation [Lab67]. This characterization can be used to classify the Galois p-extensions having a fixed group via character theory, as done in [Yam95] where in particular explicit formulæ for Galois extensions of degree p^3 where obtained.

When $p \neq 2$ a presentation of the full absolute Galois group of a p-adic field is also known [Jak68, JW83, NSW08], and while the relations are not very easy to manage the presentation could be used to study abstractly the extensions. The classification we give is however very explicit, and makes explicit all the isomorphism classes of extensions considered.

The general strategy

We illustrate this idea in the case of isomorphism classes of extensions L/K of degree p, as done in [DCD07, Dal10]. Such an extension L/K is either unramified and hence cyclic, either the group of the normal closure $\mathrm{Gal}(\tilde{L}/K)$ has a normal p-Sylow $S \cong C_p$, while L is fixed by a subgroup H of index p. The intersection of the conjugates of H is trivial, or it would fix $\tilde{L}$, so H has no element acting trivially on S by conjugacy, and the induced map $H \to \mathrm{Aut}(S) \cong \mathbb{Z}/p\mathbb{Z}^\times$ is injective. Consequently H is cyclic of order d dividing $p-1$, and the group $\mathrm{Gal}(\tilde{L}/K)$ is isomorphic to $S \rtimes H$.

Each subgroup of index p in $S \rtimes H$ is generated by one element of order d, and these elements are exactly the generators of the conjugates of H. Consequently $\tilde{L}$ can only be obtained as normal closure of extensions of degree p that are in the same isomorphism class.

Let F be the compositum of all extensions of exponent diving $p-1$. If L/K is an arbitrary extension of degree p then the composite extension $L_F = FL$ is clearly Galois over K. Its p-Sylow is normal and cyclic $\hat{S} = \mathrm{Gal}(L_F/F)$, and $\hat{H} = \mathrm{Gal}(L_F/L) \cong \mathrm{Gal}(F/K)$ is a complement acting on $\hat{S}$, whose image in $\mathrm{Aut}(\hat{S})$ is equal to the image of H. The elements of $\hat{H}$ acting trivially on $\hat{S}$ are exactly those fixing $\tilde{L}$, so from L_F there exists a way to recover unequivocally $\tilde{L}$ as field fixed by the central elements of $\mathrm{Gal}(L_F/K)$ of order prime with p.

The L_F obtained in this way for some L are all the extensions of degree p of F that are Galois extensions over K: indeed, L_F is aways Galois over K as already observed, and assume that M is such an extension. Then $\mathrm{Gal}(M/K)$ contains a complement H' of the p-Sylow $S' = \mathrm{Gal}(M/F)$ say, so we can take as L the field fixed by H, and clearly $M = L_F$.

The field F always contains the p-th roots of the unity, and by Kummer theory the M with this property correspond to subgroups of order p of $[F^\times]_F = {}^{F^\times}\!/_{(F^\times)^p}$ that are invariant when applying an automorphism $\sigma \in \mathrm{Gal}(F/K)$. Consequently they are exactly the irreducible representations contained in $[F^\times]_F$ as representation of $\mathrm{Gal}(F/K)$, and the strategy outlined in the introduction can be applied taking $G = Gal(F/K)$ and $X = [F^\times]_F$.

Theorem 4.0.3. *Let K be a p-adic field, and F be the compositum of all cyclic extensions of exponent $p-1$. Then we have a natural one-to-one correspondence of isomorphism classes of extensions of degree p of K with the irreducible subspaces of $[F^\times]_F$ as $\mathrm{Gal}(F/K)$-module.*

We remark that the correspondence is very explicit, and makes it possible to recover easily additional invariants of the extensions, such as the Galois group of the normal closure and the ramification data.

In higher degree unluckily it is not possible to make the same philosophy work in a straightforward way. We will see that a similar correspondence can be established for the extensions of p-th power degree having no intermediate extension.

Concentrating on the case of extensions of degree p^2, the most complicated case is however the case of extensions having exactly one intermediate extension. Indeed, extensions with ≥ 2 intermediate extensions are obtained as the compositum of two distinct extensions of degree p, and can be viewed as the trivial case.

In the case of a unique intermediate extension we can still parametrize the extensions fixing the intermediate extension E/K of degree p, and considering the extensions L/E of degree p and such that L/K has indeed a unique intermediate extension. This is not enough yet, because different isomorphism classes over E may correspond to extensions in the same isomorphism class over K. But once this issue is taken into account it becomes possible to enumerate the isomorphism classes.

Let $E_F = EF$, in this case the indecomposable submodules of $X = [E_F^\times]_{E_F}$ under the action of $G = \mathrm{Gal}(E_F/K)$ will correspond to the possible normal closures of extensions containing E. In general however the same extensions can be obtained as the normal closure of a big number of different isomorphism classes, and we will characterize the extensions sharing the same normal closure.

4.1 Parametrization of isomorphism classes

In this section we will state and prove the key results allowing to classify easily the extensions of degree p^2 of a p-adic field. The first one is a direct generalization of Theorem 4.0.3, and describes the isomorphism classes of extensions of degree p^k having no intermediate extension, for $k \geq 2$. The second one gives a more involved description of extensions of degree p^2 having exactly one intermediate extension.

We will denote as $[E/K]$ an isomorphism class of extensions represented by the extension E/K.

Theorem 4.1.1. *Assume $k \geq 2$. Let K be a local field, and let F/K be a finite and tamely ramified extension containing all tame extensions whose Galois group is a subgroup of $GL(k, \mathbb{F}_p)$, and let $H = \mathrm{Gal}(F/K)$.*

Then there exists a natural one-to-one correspondence of isomorphism classes of extensions $[L/K]$ of degree p^k having no intermediate extension, with the irreducible $\mathbb{F}_p[H]$-submodules $\Xi \subset [F^\times]_F$ of dimension k of the Galois module $[F^\times]_F$. The isomorphism class $[L/K]$ corresponds to Ξ when $LF = F(\Xi^{1/p})$, and $\mathrm{Gal}(LF/K)$ is always a split extension of $\mathrm{Gal}(F/K)$.

It turns out that this case is very similar to the case of extensions of degree p. It follows easily that the Galois group of the normal closure connected to Ξ is the semidirect product of Ξ by smallest quotient of H acting on it.

For general k it seams hard giving a unified description of the irreducible representations of fixed degree k of H, but we will give a characterization of their structure allowing to derive a few possible special cases in which they may fall, for small k.

We give now a result allowing to parametrize extension of degree p^2 having proper subextensions. In this context we will denote by F the compositum of the cyclic extensions of K having degree dividing $p-1$, and for each extension E/K we denote by E_F the compositum EF.

Theorem 4.1.2. *Let K be a local field, E/K be an extension of degree p, and let F be the compositum of the cyclic extensions of K having degree dividing $p-1$. Denote $E_F = EF$, which is always Galois over K, let $G = \mathrm{Gal}(E_F/K)$ and H be its subgroup $\mathrm{Gal}(E_F/E)$.*

Then there is a one-to-one correspondence of the indecomposable $\mathbb{F}_p[G]$-submodules of $[E_F^\times]_{E_F}$ and the possible normal closures $\tilde{L}$ of the extensions L/K of degree p^2 containing E. Let $\tilde{L}_F = \tilde{L}F$, then the indecomposable submodule $\Xi \subseteq [E_F^\times]_{E_F}$ corresponds to the normal closure $\tilde{L}$ if and only if $E_F(\Xi^{1/p}) = \tilde{L}_F$.

For fixed $\tilde{L}$, we have a one-to-one correspondence of the $\mathbb{F}_p[H]$-submodules $\Delta \subset \Xi$ generating Ξ as $\mathbb{F}_p[G]$-module, and the isomorphism classes of extensions $[L/E]$ such that the normal closure of L over K is exactly $\tilde{L}$. These possible L have E as unique intermediate extension if and only if Ξ is not contained in the submodule $[F^\times]_{E_F}$ of $[E_F^\times]_{E_F}$.

The irreducible $\mathbb{F}_p[H]$-submodules Δ of $[E_F^\times]_{E_F}$ parametrize isomorphism classes $[L/K]$ of extensions of degree p^2 containing an extension in the class $[E/K]$. The parametrization is one-to-one except when E/K is Galois and Δ generates a module of length ≥ 2 over $\mathbb{F}_p[G]$. In that case the parametrization is p-to-one, the submodules $\sigma\Delta$ for all $\sigma \in \mathrm{Gal}(E_F/F)$ are all distinct, and they correspond to the same class over K.

The p-Sylow subgroup of $\mathrm{Gal}(\tilde{L}/K)$ is normal, and it is complemented by Schur-Zassenhaus. Consequently once we know the p-Sylow and the action of the quotient on it, we have that the structure of $\mathrm{Gal}(\tilde{L}/K)$ is uniquely determined.

As recalled in Prop. 2.2.1 such a p-group is uniquely determined by the exponent and the length of the kernel. The action of $H = \mathrm{Gal}(F/K)$ on $\mathrm{Gal}(\tilde{L}_F/F)$ is described by its action on $\mathrm{Gal}(E_F/F)$, and by the action of $\mathrm{Gal}(E_F/K)$ on Ξ as $\mathbb{F}_p[G]$-module.

The theorems, which will now be proved, provide a quite effective way to enumerate the isomorphism classes of extension of degree p^2, obtaining formulæ for the number of isomorphism classes of extensions with prescribed Galois group of the normal closure.

Lemma 4.1.3. *Let G be finite group, and H a normal subgroup such that $|H|$ is prime with p and G/H a p-group. Let V be a finite dimensional irreducible representation of G over $\mathbb{F}_p$ having dimension ≥ 2. Then any extension of G by V with the given action is isomorphic to the split extension $V \rtimes G$, and the possible complements to V in $V \rtimes G$ are exactly the conjugates of G.*

Proof. This is essentially the same argument used in the proof of [BD11, Theo. 6.1]. Since $|V|$ and $|H|$ are relatively prime we have $H^q(H, V) = 0$ for all $q \geq 1$ (see [Ser79, Cor. 1, §2, Chap. VIII]). Consequently we have [Ser79, Prop. 5, §6, Chap. VII] the exactness of the sequence

$$0 \to H^2(G/H, V^H) \to H^2(G, V) \to H^2(H, V) = 0,$$

so in particular $H^2(G/H, V^H) \cong H^2(G, V)$. We will now show that the module V^H of H-invariants has to be trivial. Suppose it is not the case: G/H is a p-group, and its action on V^H would have a non-trivial invariant subspace, which would imply that V is not irreducible. Consequently $V^H = 0$ implying $0 = H^2(G/H, V^H) = H^2(G, V)$, so that all extensions of G by V are split (see [Ser79, §3, Chap. VII] for the interpretation of $H^2(G, V)$).

In the same way we obtain that $H^1(G, V) = 0$. But $H^1(G, V)$ classifies the possible splittings $G \to V \rtimes G$ of the canonical projection up to conjugacy (see [Bro82, Prop. 2.3, §2, Chap. IV]), so the only possible complements of V are the conjugates of G. □

We can now give the proof of Theorem 4.1.1.

Proof of Theorem 4.1.1. We will show that F is such that, taking the compositum $L_F = LF$ with an extension L/K of degree p^k having no intermediate extension, we obtain a field L_F which is an abelian elementary p-extension of degree p^k of F. By Kummer theory L_F will be of form $F(\Xi^{1/p})$ for some $\Xi \subset [F^\times]_F$ that is an irreducible $\mathbb{F}_p[T]$-module, L_F will be Galois over K, and it will uniquely determine the isomorphism class of L/K.

The extension L/K has to be totally ramified, or it would have an unramified subextension that is cyclic Galois over K, and would contain an unramified subextension of degree p. Let $G = \mathrm{Gal}(\tilde{L}/K)$ be the Galois group of the normal closure $\tilde{L}$ of L/K, and let

$$G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \dots$$

be its lower numbering ramification filtration. We have that G_i is normal in G, and that for $i \geq 1$ the quotient ${}^{G_i}\!/_{G_{i+1}}$ is an elementary abelian group.

Let $\tilde{H} \subseteq G$ be the subgroup fixing L, and let t be the unique index such that $G_{t+1} \subseteq \tilde{H}$ but $G_t\tilde{H} = G$, we clearly have $t \geq 1$ being L/K a totally ramified wild extension.

Now the core $\mathrm{Core}_G(\tilde{H})$ of $\tilde{H}$, that is the intersection of all conjugates $\bigcap_{\sigma \in G} \sigma \tilde{H} \sigma^{-1}$, is trivial, or it would correspond to a normal extension containing L and strictly smaller than $\tilde{L}$. In particular G_{t+1} has to be trivial being normal in G and contained in $\tilde{H}$, and the centralizer $C_{\tilde{H}}(G_t)$ of G_t in $\tilde{H}$ has to be trivial too or it would be contained in all the conjugates of $\tilde{H}$.

Hence G_t is a faithful $\mathbb{F}_p[\tilde{H}]$-module, and it should also be irreducible, or a proper submodule A would be normal in G, and we would have intermediate group $A\tilde{H}$ between $\tilde{H}$ and G, corresponding to an intermediate extension in L/K.

We will now show that the p-core $O_p(\tilde{H})$, i.e. the intersection of all p-Sylow subgroups of $\tilde{H}$, is trivial. Suppose $O_p(\tilde{H}) \neq 1$, then the subgroup $G_t \rtimes O_p(\tilde{H})$ is normal in G, because quotienting by G_t we obtain $O_p(\tilde{H}) \lhd \tilde{H}$. Furthermore $O_p(\tilde{H})$ is a p-group and has a non-trivial invariant subspace in G_t, which is not the whole G_t being the action faithful. This is also a representation of $\tilde{H}$ being $O_p(\tilde{H}) \lhd \tilde{H}$, but it is impossible because G_t is irreducible.

We obtain that the field L_1 fixed by G_t is such that $\mathrm{Gal}(L_1/K) \cong \tilde{H}$, so it is a tame extension being the p-Sylow of $\tilde{H}$ trivial. Its Galois group embeds into $\mathrm{Aut}(G_t)$, so we have $L_1 \subseteq F$ and $\tilde{L} \subseteq L_F$.

Since $\tilde{L}/L_1$ is an abelian elementary extension then L_F/F will also be, $L_F = F(\Xi^{1/p})$ for $\Xi \subseteq [F^\times]_F$ say. The module Ξ has clearly also to be an irreducible as $\mathbb{F}_p[H]$-module of dimension k, where $H = \mathrm{Gal}(F/K)$.

We show now that each irreducible Ξ of dimension k corresponds to one isomorphism class $[L/K]$. Let $M = F(\Xi^{1/p})$, then $S = \mathrm{Gal}(M/F)$ is an irreducible H-module. Let $G = \mathrm{Gal}(M/K)$, then it is an extension of H by S. We observe that any such extension with no intermediate extension should be fixed by a subgroup B that complements S, or SB would correspond to a proper intermediate extension.

We show that we can get rid of the p-core $O_p(H)$ of H. Indeed, $O_p(H)$ should act trivially on S or it would have an invariant subspace that is hence H invariant. Furthermore $O_p(H)$ is cyclic, and hence its preimage Q in G is abelian. Each p-Sylow of H is cyclic and complemented by a normal subgroup, hence $O_p(H)$ is contained in the center of H.

Consequently $Q \lhd G$ and $G/Q \cong H/O_p(H)$ acts on Q by conjugacy. Reasoning like in the proof of Lemma 4.1.3 we have that the maximal subgroup with order prime with p in $H/O_p(H)$ should act without fixed points on S, while it acts trivially on $Q/S \cong O_p(H)$. Consequently its action determines the existence of a unique H-invariant complement to S in $Q = S \oplus R$, being a group of order prime with p acting on an abelian p-group (see for instance [Gor80, Theorem 2.3, Chap. 5]).

Quotienting out by the unique possible R we reduce to the case of H having a trivial p-core. Then H satisfies the hypothesis of Lemma 4.1.3, because it has a subgroup fixing the maximal unramified subextension of p-th power degree, which is normal and has order prime with p.

Consequently $S \subseteq \mathrm{Gal}(N/K)$ has a complement in G, which is unique up to conjugacy. The fixed field of a complement is an extension L/K of degree p^k

with no intermediate extension. □

As byproduct of the proof, we can assume that $\operatorname{Gal}(F/K)$ has trivial p-core, that is, if F/K is as requested by the Theorem, than the field fixed by the p-core will also satisfy the hypotheses. Requiring $k \geq 2$ is necessary, as can be shown with a simple counterexample, taking an F containing the unramified extension of degree p, and two totally ramified extensions of degree p such that the compositum with the unramified extension of degree p is the same, so that the correspondence is no longer unique in this case.

We give now the proof of Theorem 4.1.2. We remark that the Galois group of the maximal abelian extension of exponent $p-1$ of a local field is always isomorphic to $C_{p-1} \times C_{p-1}$, as it follows immediately by the structure of $K^\times/(K^\times)^{p-1}$, applying Kummer theory (the $(p-1)$-th roots of the unity are always in K) or class field theory.

Proof of Theorem 4.1.2. Let E/K be fixed, and $E_F = EF$. Let L/K be an extension of degree p^2 containing E, and $L_F = LF$. Then E_F/E is also the maximal abelian extension of exponent $p-1$, and L_F/E_F is cyclic Galois. Furthermore F certainly contains the p-roots of the unity, and $L_F = E_F(\Delta^{1/p})$ for some $\Delta \in [E_F^\times]_{E_F}$ that is an irreducible $\mathbb{F}_p[H]$-submodule. Each such irreducible $\mathbb{F}_p[H]$-submodule of $[E_F^\times]_{E_F}$ comes from an extension L/E of degree p.

Let $S = \operatorname{Gal}(E_F/F)$ be the p-Sylow of G, so that $G = S \rtimes H$. Let Ξ be the $\mathbb{F}_p[G]$-module generated by Δ, then Δ generates $\Xi/\operatorname{rad}(\Xi)$, which is consequently irreducible as $\mathbb{F}_p[G/S]$-module, and Ξ is indecomposable by Prop. 2.1.2, Chap. 2.

The normal closure of L_F over K should certainly contain $\tilde{L}$ and F, so it is equal to $\tilde{L}_F$ being this extension normal. Furthermore we have $\tilde{L}_F = E_F(\Xi^{1/p})$, as observed in Chap. 2, §2.2.

We now show that it is possible to recover uniquely $\tilde{L}$ from $\tilde{L}_F$. Let $G = \operatorname{Gal}(\tilde{L}_F/K)$, and P its p-Sylow $\operatorname{Gal}(\tilde{L}_F/F)$. Let $\tilde{H}$ be a complement of the normal p-Sylow of $\operatorname{Gal}(\tilde{L}/L)$ by Schur-Zassenhaus, and $\hat{H}$ be its preimage in $\operatorname{Gal}(\tilde{L}_F/L)$. Then $\hat{H}$ is also a complement for P in G and we have $G = P \rtimes \hat{H}$. Since $\hat{H}$ fixes L, the intersection of the conjugates $\operatorname{Core}_G(\hat{H})$ is certainly fixing $\tilde{L}$, and the subgroup fixing $\tilde{L}$ cannot be bigger, being normal and contained in $\hat{H}$. It's immediate to see that $\operatorname{Core}_G(\hat{H})$ is also characterized in $G = P \rtimes \hat{H}$ as the group of elements that are central and have order prime with p.

Let's show that each indecomposable submodule Ξ of $[E_F^\times]_{E_F}$ is obtained in this way from a possible normal closure. Its submodule $\operatorname{rad}(\Xi)$ is complemented as $\mathbb{F}_p[H]$-submodule, and each complement Δ corresponds with to an isomorphism class of extensions $[L/E]$ of degree p satisfying $L_F = E_F(\Delta^{1/p})$. Thus $E_F(\Xi^{1/p})$ is the normal closure of L_F/K, and the choice of Δ corresponds to isomorphism class of extensions $[L/E]$ from which is can be obtained.

It remains to determine when different isomorphism classes of extensions over E may actually be in the same class over K. This indeed happens only when E/K has some nontrivial automorphism σ, which maps an isomorphism class $[L/E]$ of extensions over E to a conjugated class $[L/E]^\sigma$. The classes are different if and only if the Δ such that $L_F = E_F(\Delta^{1/p})$ is different from $\sigma\Delta$, and if this is the case then we have p possible distinct Δ, considering that E/K has to be Galois of order p.

Clearly the Ξ contained in $[F^\times]_{E_F}$ give by Kummer theory extension that are Galois and with group isomorphic $C_p \times C_p$ over F, so of the form $F(\Theta^{1/p})$ for some submodule Θ of dimension 2 in $[F^\times]_F$, and Θ has clearly multiple subspaces that are invariant under $\mathrm{Gal}(F/K)$. The field L is fixed by a complement of the p-Sylow of $\mathrm{Gal}(F(\Theta^{1/p})/K)$, and each proper invariant subspace of Θ gives an intermediate extension. This argument can clearly be reversed. □

4.2 No intermediate extension

Here we classify the extensions with no intermediate extension, via Theorem 4.1.1. On a suitable tamely ramified Galois extension F/K, we will describe the irreducible representations of $\mathrm{Gal}(F/K)$, and determine the Galois module structure of $[F^\times]_F$. It is worth observing that it will not even be necessary to identify the exact extension F, provided that it is "sufficiently big".

In this section we observe that we can always assume that $G = \mathrm{Gal}(F/K)$ is such that the inertia subgroup G_0 is complemented, and the group is a semidirect product. We will then study its representations over $\mathbb{F}_p$, first on the algebraic closure, and then over $\mathbb{F}_p$. Later we determine the structure of $[F^\times]_F$ as Galois module. As application we enumerate irreducible sub-representations of degree 2, which correspond to isomorphism classes of extensions of degree p^2, and obtain formulæ counting the extensions whose normal closure has a prescribed group. We conclude with the characterization of the imprimitive solvable subgroups of S_{p^2} that are realized.

We recall the structure of the Galois group of a tamely ramified extension. Let F be a tamely ramified extension, let $G = \mathrm{Gal}(F/K)$ and let F^{ur} be the maximal unramified subextension, that is, the field fixed by G_0. Then G/G_0 is canonically $\mathrm{Gal}(\kappa_F/\kappa_K)$, while G_0 can be canonically embedded into $\kappa_F^\times$ via the map $\sigma \mapsto \overline{\sigma(\pi_F)/\pi_F}$, which is independent of the uniformizer π_F. Assume $q = |\kappa_K|$, then G/G_0 has a distinguished generator, the q-th power Frobenius ϕ_q, and $G/G_0 = \langle\phi_q\rangle$ acts on G_0 via $\phi_q\tau\phi_q^{-1} = \tau^q$. Iterating we obtain that it is necessary that $\tau^{q^f-1} = 1$ for $f = f(F/K)$, and f is also equal to the order of G/G_0.

While the normal subgroup G_0 may not have a complement, there exists an unramified extension of F whose Galois group G over K is such that the inertia subgroup has actually a complement, and G is a semidirect product of G_0 and a cyclic group with the q-th power action. If υ is a representative of ϕ_q in G and τ a generator of G_0, then $\upsilon^f = \tau^r$ for some r, and the order of τ^r should divide $q-1$ considering that it commutes with υ. Let $e = e(F/K)$, which is also the order of τ, then $e \mid r(q-1)$. In particular the Galois group of a finite tame extension is of the form

$$\left\langle \upsilon, \tau \mid \upsilon\tau\upsilon^{-1} = \tau^{q},\ \tau^{e} = 1,\ \upsilon^{f} = \tau^{r} \right\rangle,$$

for some e dividing $\big(q^{f} - 1, r(q-1)\big)$.

If we consider the unramified extension M/F with degree $s = {}^{e}/_{(e,r)}$ equal to the order of τ^{r}, we have that M/K is Galois, while M^{ur} and F are linearly disjoint over F^{ur}. We will still denote as τ,υ liftings to $\mathrm{Gal}(M/K)$. Then τ generates the inertia subgroup, and υ will satisfy $\upsilon^{fs} = 1$, considering that υ^{fs} fixes both F and M^{ur}. In particular $\mathrm{Gal}(M/K)$ is generated by υ, τ with relations $\upsilon\tau\upsilon^{-1} = \tau^{q}$, $\tau^{e} = \upsilon^{fs} = 1$, and its inertia subgroup is generated by τ. We remark that $\mathrm{Gal}(M/K)$ still has a trivial p-core if this was true for $\mathrm{Gal}(F/K)$.

The Galois group of the maximal tame extension of K is isomorphic to the full profinite completion of the group generated by two elements a, b with the relation $bab^{-1} = a^{q}$, as was first proved by Iwasawa [Iwa55].

4.2.1 Irreducible representations of a tame Galois group

In this section we recover the structure of irreducible representations over $\mathbb{F}_p$ of certain semidirect products of cyclic groups. We will consider products of the form $T \rtimes U$, for cyclic groups $T = \langle\tau\rangle$ and $U = \langle\upsilon\rangle$ of orders respectively t and u with $(t, p) = 1$ and $t \mid q^{u} - 1$, the action of υ being described as $x \mapsto x^{q}$ for each $x \in T$, where as usual $q = |\kappa_K| = p^{f_K}$. The characterization we obtain is quite similar to that of [CMR10].

Quotienting out the elements acting trivially and contained in T, which form a normal subgroup, we can assume that the representation is faithful on T. Furthermore the p-core is certainly acting trivially or the representation would have an invariant subspace, so we can also quotient out the p-core.

Let $\tilde{U}$ be the kernel of $U \to \mathrm{Aut}(T)$, we don't assume that u is prime with p, but $\tilde{U}$ shall have order prime with p or $T \rtimes U$ would have a non-trivial p-core. Let $r = \mathrm{ord}_t^{\times}(p)$, this is the smallest power of p such that $t \mid p^{r} - 1$. Let $s = {}^{r}/_{(r, f_K)}$, then q^{s} is the smallest power of q such that $t \mid q^{s} - 1$, and $\tilde{U}$ is generated by υ^{s}, that we will denote as $\tilde{\upsilon}$.

Let X be an irreducible representation over $\bar{\mathbb{F}}_p$. Since $T \times \tilde{U}$ is an abelian group with order prime with p, there exists an invariant subspace of dimension 1, X_χ say, where the action is described by the character $\chi : T \rtimes \tilde{U} \to \bar{\mathbb{F}}_p^{\times}$. Let $\alpha = \chi(\tau)$ and $\beta = \chi(\tilde{\upsilon})$, then υ^{i} maps X_χ to a space where τ acts via a conjugate $\alpha^{q^{i}}$ of α, and the orbit under υ generates the whole X. Consequently α should have order t, because the representation was assumed to be faithful on T. Hence for $0 \leq i < s$ the $\upsilon^{i} X_\chi$ are all distinct, and X contains a copy of $\mathrm{Ind}_{T\rtimes\tilde{U}}^{T\rtimes U}(X_\chi)$.

If $x \in X_\chi$ is a generator, then the elements $x, \upsilon x, \ldots, \upsilon^{s-1}x$ generate a representation on which τ and υ act as the matrices:

$$\mathcal{T} = \begin{pmatrix} \alpha & & & & \\ & \alpha^q & & & \\ & & \alpha^{q^2} & & \\ & & & \ddots & \\ & & & & \alpha^{q^{s-1}} \end{pmatrix}, \qquad \mathcal{U} = \begin{pmatrix} & & & & \beta \\ 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \end{pmatrix}.$$

The representations obtained in this way starting from X_χ or $\upsilon^i X_\chi$ are equal for all i, and on $\upsilon^i X_\chi$ the action is described via the character χ^{υ^i} defined composing with conjugation by υ^i, that is, as $g \mapsto \chi(\upsilon^{-i} g \upsilon^i)$ for all $g \in T \rtimes U$.

Proposition 4.2.1. *All irreducible representation of $T \rtimes U$ over $\bar{\mathbb{F}}_p$ that are faithful on T are obtained as $\mathrm{Ind}_{T \rtimes \tilde{U}}^{T \rtimes U}(V_\chi)$, where the character $\chi : T \rtimes \tilde{U} \to \bar{\mathbb{F}}_p^\times$ is faithful on T, and V_χ a representation of dimension 1 where the action is described by χ. Two different characters induce the same representation if and only if they are conjugated. If $T \times U$ has a non-trivial p-core, then it is contained in the kernel of the representation.*

The rationality of a representation can be studied via the following criterion: let $\rho : G \to GL(V)$ be a representation of a group over $V = K^n$ in some field K, and let $\sigma \in \mathrm{Aut}(K)$ be an automorphism. If $\sigma\rho\sigma^{-1}$ is isomorphic to ρ, then ρ is defined over the field fixed by σ. Indeed, if this is the case $\sigma : V \to V$ defines an isomorphism and by Schur lemma must be a multiplication by a constant, which has to be 1 testing the representation over the identity. Hence the σ-invariant subspace V^σ is preserved by ρ, or equivalently the representation ρ has coefficients in the field fixed by σ. In other words, an element of the Galois group fixing the isomorphism class of a representation (which may be a subrepresentation of some bigger representation) fixes the representation itself.

Consequently we can compute the field of definition as the field fixed by the elements of the absolute Galois group fixing the isomorphism class of a representation. The orbit of the action of the Galois group over the base field will correspond to a rational representation.

In our case, let's consider $\mathrm{Ind}_{T \rtimes \tilde{U}}^{T \rtimes U}(V_\chi)$, and set $\alpha = \chi(\tau)$ and $\beta = \chi(\tilde{\upsilon})$ as above. Clearly $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p(\alpha, \beta))$ stabilizes the representation, and it is also stabilized by the powers of the Frobenius ϕ_q fixing β, because χ and χ^{υ^i} correspond to the same representation. In $\mathrm{Gal}(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$ the group generated by ϕ_q is equal to the group generated by $\phi_{p^{(r,f_K)}}$. Putting $w = [\mathbb{F}_p(\beta) : \mathbb{F}_p]$, we obtain that the smallest power fixing $\mathbb{F}_p(\beta)$ is $\phi_{p^{\mathrm{lcm}(w,(r,f_K))}}$, which generates also the stabilizer of the representation. Consequently the cardinality of the Galois orbit is $\mathrm{lcm}(w, (r, f_K))$.

Proposition 4.2.2. *Let X be an irreducible representation of $T \rtimes U$ over $\mathbb{F}_p$ that is faithful on T. Assume that, over the algebraic closure, $T \rtimes \tilde{U}$ has an invariant subspace of dimension 1 where it acts via the character χ. Then*

$$\dim_{\mathbb{F}_p} X = \mathrm{lcm}({}^{rw}\!/\!{}_{(r,f_K)}, r)$$

where $r = \operatorname{ord}_t^{\times}(p)$, and $w = [\mathbb{F}_p(\beta) : \mathbb{F}_p]$ where $\beta = \chi(\tilde{\upsilon})$.

Proof. Indeed $\operatorname{Ind}_{T \rtimes \tilde{U}}^{T \rtimes U}(V_\chi)$ has dimension s so we obtain

$$\dim_{\mathbb{F}_p} X = s \cdot \operatorname{lcm}(w, (r, f_K)),$$

and the proposition follows because $s = {}^{r}/_{(r,f_K)}$. □

4.2.2 Structure of $[F^\times]_F$

We describe now the structure of $U_{i,F}$ as $\mathbb{F}_p[H]$-module, for $H = \operatorname{Gal}(F/K)$. We can assume that H_0 is complemented, so let $H_0 = T = \langle \tau \rangle$, and υ be a lifting of the Frobenius ϕ_q generating a complement U, so that $H = T \rtimes U$. Let F' be field fixed by U, then F/F' is unramified, and a uniformizer for F' is also a uniformizer for F. Let π be such an element, that we take to be an e-th root of a uniformizer of K, for $e = e(K/F)$. For $i \geq 1$, the action of τ and υ on $U_{i,F}/U_{i+1,F}$ is described as

$$\tau(1 + \alpha\pi^i) = 1 + \zeta^i \alpha \pi^i + \dots, \qquad \upsilon(1 + \alpha\pi^i) = 1 + \alpha^q \pi^i + \dots,$$

for each $\alpha \in U_F$, where ζ is the fixed primitive e-th root of 1 defined as $\tau(\pi)/\pi$.

The choice of π establishes an identification of $U_{i,F}/U_{i+1,F}$ with κ_F, as

$$(1 + \alpha\pi^i + \dots) \mapsto \bar{\alpha}.$$

Transferring the action on κ_F, we have that the action is

$$\tau(\bar{\alpha}) = \bar{\zeta}^i \bar{\alpha}, \qquad \upsilon(\bar{\alpha}) = \bar{\alpha}^q.$$

Proposition 4.2.3. *For $i \geq 0$, let M_i be the $\kappa_K[H]$-module formed by κ_F as set, and with the above action. Then M_i is projective.*

Proof. Consider the sum $M = \oplus_{i=0}^{e-1} M_i$, we claim that if $\bar{\eta}$ generates a normal basis for κ_F over κ_K, then the vector $(\bar{\eta})_{0 \leq i < e}$ with all components equal to $\bar{\eta}$ is a generator for M. Indeed via υ we obtain any element of the form $(\bar{\alpha})_{0 \leq i < e}$ (that is with equal components), and we obtain as

$$\frac{1}{e} \sum_{j=0}^{e-1} \tau^j \left((\bar{\zeta}^{-jk} \bar{\alpha})_{0 \leq i < e} \right)$$

the vector whose k-th component is $\bar{\alpha}$ (recall that $(e, p) = 1$), and the other components are 0. Consequently $M = \kappa_F[H]w$ is a quotient of the free module $\kappa_F[H]$, and is equal because they have the same dimension. Hence M_i is projective, being a direct summand of a free module. □

It follows that $[U_{i+1,F}]_F$ is complemented in $[U_{i,F}]_F$ as $\mathbb{F}_p[H]$-module, and

$$[F^\times]_F \cong \left({}^{[F^\times]_F}/_{[U_{1,F}]_F} \right) \oplus \bigoplus_{i=1}^{\infty} \left({}^{[U_{i,F}]_F}/_{[U_{i+1,F}]_F} \right).$$

We recovered essentially [Iwa55, Lemma 1], where the same result is obtained via a computation. The i such that the term appearing in the summand is possibly nontrivial are $0, I_F = {}^{pe_F}\!/_{(p-1)}$, and the $0 < i < I_F$ that are prime with p. We remark that we did not require H to have order prime with p, not even a trivial p-core.

We now study the M_i changing the scalars to the algebraic closure $\bar{\mathbb{F}}_p$.

Proposition 4.2.4. *Let V_i be the $\bar{\mathbb{F}}_p[T]$ module of dimension 1 where τ acts as multiplication by $\bar{\zeta}^i$. Then*

$$M_i \otimes_{\kappa_K} \bar{\mathbb{F}}_p \cong \operatorname{Ind}_T^H(V_i),$$

as $\bar{\mathbb{F}}_p[H]$-modules.

Proof. By definition M_i is a $\kappa_K[H]$-module, but it also has a natural structure of $\kappa_F[T]$-module. We have the map

$$\begin{aligned} M_i \otimes_{\kappa_K} \kappa_F &\xrightarrow{\sim} \kappa_F[H] \otimes_{\kappa_F[T]} M_i = \operatorname{Ind}_T^H(M_i), \\ \alpha \otimes \beta &\mapsto \sum_{i=0}^{f-1} \upsilon^{-i} \otimes \upsilon^i(\alpha)\beta, \end{aligned}$$

which is readily verified to be an isomorphism of $\kappa_F[H]$-modules. Extending further the scalars from κ_F to $\bar{\mathbb{F}}_p$ we have the proposition. □

Since H acts trivially on the coefficients κ_K we have that $M_i \otimes_{\mathbb{F}_p} \kappa_K \cong (M_i)^{f_K}$ as $\kappa_K[H]$-modules, and consequently

$$M_i \otimes_{\mathbb{F}_p} \bar{\mathbb{F}}_p = \left(\operatorname{Ind}_T^H(V_i)\right)^{f_K}.$$

Being induced from a simple module the module obtained is projective [Alp93, Chap. 3, §8, Lemma 5], and together with the fact that this equivalent to M_i itself being projective this implies an alternate proof of Prop. 4.2.3.

4.2.3 Irreducible submodules

Let $H = T \rtimes U$ be the group of the tame extension F/K, with inertia equal to T. For $i \geq 1$ let M_i be the Galois module defined above, formed by the set κ_F with action defined as

$$\tau(\alpha) = \zeta^i \alpha, \qquad \upsilon(\alpha) = \alpha^q,$$

where ζ is a fixed e-th root of the unity.

Assume that F contains the p-th roots of the unity, and let V_ω be the $\mathbb{F}_p[H]$-module dimension 1 corresponding to the cyclotomic character ω. Then we have that

$$[F^\times]_F \cong [F^\times]_F/[U_{1,F}]_F \oplus \bigoplus_{i \in [\![0, I_F]\!]} \left({}^{[U_{i,F}]_F}\!/_{[U_{i+1,F}]_F}\right) \oplus [U_{I_F,F}]_F$$

$$\cong \mathbb{F}_p \oplus \left(\bigoplus_{i \in [\![0, I_F]\!]} M_i \right) \oplus V_\omega,$$

where $I_F = {}^{pe_F}/_{(p-1)}$, and $[\![0, I_F]\!]$ is the set of integers prime with p in the interval $[0, I_F]$. Indeed, $[U_{I_F,F}]_F$ corresponds via Kummer theory to the unramified extension of degree p, which is Galois, so the action on the module is twisted via ω and $[U_{I_F,F}]_F \cong V_\omega$, while the action on $[F^\times]_F/[U_{1,F}]_F \cong \mathbb{F}_p$ is clearly trivial.

When considering the irreducible sub-representations of dimension 2 we can clearly reduce to consider the M_i. Consequently fix $i \in [\![0, I_F]\!]$, and consider the extension to the algebraic closure $\bar{M}_i = M_i \otimes_{\mathbb{F}_p} \bar{\mathbb{F}}_p$. To study the representation we can assume that T acts faithfully, quotienting out the elements in T that act trivially.

Putting $\alpha = \zeta^i$ we have that its order is equal to t, and let V_α be representation of dimension 1 where τ acts as multiplication by α. By Prop. 4.2.4 we have $\bar{M}_i \cong \left(\operatorname{Ind}_T^H(V_\alpha)\right)^{f_K}$.

Let $\tilde{U}$ be the centralizer of T in U, and consider first

$$\operatorname{Ind}_T^{T\times\tilde{U}}(V_\alpha) = \bar{\mathbb{F}}_p[\tilde{U}] \otimes V_\alpha.$$

Assume that $\tilde{U}$ is generated by $\tilde{v}$ of order $\tilde{u}$, and consider the structure of $\bar{\mathbb{F}}_p[\tilde{U}]$. Then the above representation can be written as

$$\bigoplus_{\beta:\beta^{\tilde{u}}=1} V_{(\alpha,\beta)},$$

where $V_{(\alpha,\beta)}$ is the representation of dimension 1 such that τ, $\tilde{v}$ act by multiplication by α and β. Consequently we have

$$\operatorname{Ind}_T^H(V_\alpha) = \bigoplus_{\beta|\beta^{\tilde{u}}=1} \operatorname{Ind}_{T\rtimes\tilde{U}}^H(V_{(\alpha,\beta)}).$$

Denote $\operatorname{Ind}_{T\rtimes\tilde{U}}^H(V_{(\alpha,\beta)})$ as $J_{(\alpha,\beta)}$, and let $Y = \sum_{i\in[\![0,I_F]\!]} \bar{M}_i$. We compute now the multiplicity of $J_{(\alpha,\beta)}$ in Y. The i such that $\zeta^i = \alpha$, and $\bar{M}_i$ appears in the sum, have equal remainder modulo e. Those in $[0, I_F]$ having fixed remainder are $I_F/e = {}^{pe_K}/_{(p-1)}$, and being $(e,p) = 1$ those prime with p are exactly e_K. Consequently the representation appears $e_K f_K = [K : \mathbb{Q}_p]$ times as $J_{(\alpha,\beta)}$, and this multiplicity should be multiplied by $s = (U : \tilde{U})$, when taking into account the conjugate pairs (α^{q^i}, β) that yield the same representation.

Lemma 4.2.5. *Assume $\alpha^e = 1$ for $e = e(F/K)$, and the order of α to be exactly t. Let $s = \operatorname{ord}_q^\times(t)$, and put $u = f = f(F/K)$, and $\tilde{u} = u/s$. Assume $\beta^{\tilde{u}} = 1$. Then the multiplicity of $J_{(\alpha,\beta)}$ in Y is equal to $s \cdot [K : \mathbb{Q}_p]$.*

As obtained proving Prop. 4.2.2, the representation $J_{(\alpha,\beta)}$ has $\operatorname{lcm}(w, (r, f_K))$ conjugates over $\mathbb{F}_p$, where $r = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$, and $w = [\mathbb{F}_p(\beta) : \mathbb{F}_p]$. Let D be the field of definition of $J_{(\alpha,\beta)}$, its degree over $\mathbb{F}_p$ is also equal to $d = \operatorname{lcm}(w, (r, f_K))$.

Let X be an irreducible sub-representation of Y that is defined over $\mathbb{F}_p$, and containing a unique copy of $J_{(\alpha,\beta)}$, necessarily defined over D. Then it contains the full Galois orbit, and from each copy of $J_{(\alpha,\beta)}$ contained in Y and defined over D we obtain a representation isomorphic to X.

Consequently to count the sub-representations isomorphic to X and defined over $\mathbb{F}_p$, we are reduced to count the sub-representations that are isomorphic to $J_{(\alpha,\beta)}$, and defined over D. Let $J_{(\alpha,\beta)}$ have multiplicity m in Y, we can equivalently consider the sub-representations contained in $(J_{(\alpha,\beta)})^m$, working over D.

Let's consider the immersions

$$J_{(\alpha,\beta)} \to (J_{(\alpha,\beta)})^m,$$

which are defined over D. By Schur lemma each component is multiplication by a constant $\in D$, and two immersions have the same image if and only if they differ by multiplication by a constant. The total number of immersions is consequently $|D|^m - 1$, while the possible constants are $|D| - 1$.

Lemma 4.2.6. *Assume that the irreducible representation $J_{(\alpha,\beta)}$ has multiplicity m in Y. Assume that $J_{(\alpha,\beta)}$ is defined over D, and let $d = [D : \mathbb{F}_p]$. Then the number of representations defined over $\mathbb{F}_p$ and containing a representation isomorphic to $J_{(\alpha,\beta)}$ is $(p^{dm} - 1)/(p^d - 1)$.*

4.2.4 Extensions with prescribed Galois group

We give now a specialization of the characterization of the previous section to irreducible representations of degree 2, obtaining the classification of extensions of degree p^2 with no intermediate extension.

Let $\alpha, \beta \in \bar{\mathbb{F}}_p$, let t be the order of α and $r = \mathrm{ord}_t^\times(p)$, which is also equal to $[\mathbb{F}_p(\alpha) : \mathbb{F}_p]$. Let $s = \mathrm{ord}_t^\times(q)$ and $w = [\mathbb{F}_p(\beta) : \mathbb{F}_p]$.

Let F/K be a tamely ramified extension with group $H = T \rtimes U$, where $T = \langle \tau \rangle$ is the inertia subgroup H_0 whose order is assumed divisible by t, and let $U = \langle \upsilon \rangle$. Let $\tilde{U} = \langle \tilde{\upsilon} \rangle$, for $\tilde{\upsilon} = \upsilon^s$, be the set of elements of U acting trivially on T/T^t, and assume that F/K is big enough so that $|\tilde{U}|$ is divisible by the order of β, and $|T|$ is divisible by the order t of α.

Let $V_{(\alpha,\beta)}$ be the $\bar{\mathbb{F}}_p[T \rtimes \tilde{U}]$-representation of dimension 1 where τ, $\tilde{u}$ act by multiplication by α, β. The representation

$$J_{(\alpha,\beta)} = \mathrm{Ind}_{T \rtimes \tilde{U}}^{H}(V_{(\alpha,\beta)})$$

has dimension s, and by Lemma 4.2.5 its multiplicity in $[F^\times]_F \otimes_{\mathbb{F}_p} \bar{\mathbb{F}}_p$ is $s \cdot [K : \mathbb{Q}_p]$, when α, β are not both in $\mathbb{F}_p^\times$ (so the representation cannot be trivial or $\cong \mu_p$). Its Galois orbit is formed by $d = \mathrm{lcm}(w, (r, f_K))$ elements, and this is also the degree of the field of definition over $\mathbb{F}_p$. The irreducible representation over $\mathbb{F}_p$ obtained forming the orbit has degree $\mathrm{lcm}({}^{rw}/_{(r,f_K)}, r)$. It is clear that we can chose once and for all an extension F/K satisfying the above requirements for all α and β corresponding to a representation of bounded degree. Indeed, F

can be taken as in Theorem 4.1.1, ensuring additionally that its Galois group is a direct product of the inertia and a complement.

Let $Y = [F^\times]_F$. By Theorem 4.1.1 an irreducible submodule $X \subset Y$ corresponds to an isomorphism class of extensions whose group of the normal closure is

$$(X^* \otimes \mu_p) \rtimes (H/\ker(\hat{\rho})), \qquad \text{for } \hat{\rho} : H \to \mathrm{Aut}(X^* \rtimes \mu_p).$$

Considering rather the submodules X of $Y^* \otimes \mu_p$, which is $\cong Y$, we can assume that the Galois group is

$$X \rtimes (H/\ker(\rho)), \qquad \text{for } \rho : H \to \mathrm{Aut}(X).$$

We remark that the subgroup of $GL(2, \mathbb{F}_{p^2})$ generated by all matrices of the form $\begin{pmatrix}\alpha & \\ & \alpha^p\end{pmatrix}$ for $\alpha \in \mathbb{F}_{p^2}^\times$, and the matrix $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$, is isomorphic to $\mathbb{F}_{p^2}^\times \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$. Its action is exactly the natural action induced on the left component of $\mathbb{F}_{p^2} \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$, where $\alpha \otimes \beta$ is identified with $(\alpha\beta, \sigma(\alpha)\beta)$. The group obtained making it act on the $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$-invariant elements, that is the representation over $\mathbb{F}_p$, is consequently isomorphic to the extension of $\mathbb{F}_{p^2}^\times \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ acting naturally on $\mathbb{F}_{p^2}^+ \cong (\mathbb{F}_p)^2$. Equivalently we have that the action described by the matrices is obtained extending scalars to $\mathbb{F}_{p^2}$. All groups we are considering act like a subgroup of this group of matrices, and the isomorphism class of the subgroup will identify it uniquely as a subgroup of $\mathbb{F}_{p^2}^\times \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$.

Let's defined for convenience the function $\psi(a, b)$, that for natural a, b counts the number of elements with order a in the group $C_a \times C_b$. It can be expressed as

$$\psi(a, b) = a \cdot (a, b) \cdot \prod_{\substack{\ell \text{ prime} \\ \ell | a/(a,b)}} \left(1 - \frac{1}{\ell}\right) \cdot \prod_{\substack{\ell \text{ prime} \\ \ell | a,\ \ell \nmid a/(a,b)}} \left(1 - \frac{1}{\ell^2}\right). \tag{4.1}$$

Case $(2 \mid f_K)$**.** In this case for the dimension to be 2 we need $r, w \leq 2$, and at least one to be equal to 2, and we always have $s = 1$. The group acting in the representation is cyclic of order equal to the order of (α, β) in $\mathbb{F}_{p^2}^\times \times \mathbb{F}_{p^2}^\times$, and acts as the unique subgroup of $\mathbb{F}_{p^2}^\times$ of that order on a space isomorphic to $\mathbb{F}_{p^2}^+$ itself.

Let $c \mid p^2 - 1$ but $c \nmid p - 1$, then the number of elements in $\mathbb{F}_{p^2}^\times \times \mathbb{F}_{p^2}^\times$ having order c is equal to $\psi(c, p^2 - 1)$. In the other hand $J_{(\alpha,\beta)} = V_{(\alpha,\beta)}$ has multiplicity $n = [K : \mathbb{Q}_p]$, and by Lemma 4.2.6 the number of sub-representations is $(p^{2n} - 1)/(p^2 - 1)$ being the representation defined over $\mathbb{F}_{p^2}$. Since the we need to count together (α, β) and (α^p, β^p), we need to divide by 2.

Let C be the cyclic group of order c in $\mathbb{F}_{p^2}^\times$, we obtain that the number of classes of extensions whose normal closure has Galois group isomorphic to $\mathbb{F}_{p^2}^+ \rtimes C$ is exactly

$$\frac{p^{2n} - 1}{p^2 - 1} \cdot \frac{1}{2} \psi(c, p^2 - 1).$$

Computing the full number of pairs (α, β) in $\mathbb{F}_{p^2}^\times \times \mathbb{F}_{p^2}^\times$ but not in $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$ we obtain the full number of classes of extensions with degree p^2 having no intermediate extensions

$$\frac{p^{2n}-1}{p^2-1} \cdot \frac{1}{2}\left[(p^2-1)^2 - (p-1)^2\right] = \frac{p(p^2+p-2)(p^{2n}-1)}{2(p+1)}.$$

Case $(2 \nmid f_K)$**.** In this case the representations of dimension 2 over are obtained when one of r, w is 1 and the other 2.

For $r = 1$, $w = 2$ we need to consider the pairs (α, β) in $\mathbb{F}_p^\times \times \mathbb{F}_{p^2}^\times$ but not in $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$. Let $c \mid p^2-1$ but $c \nmid p-1$, the possible pairs (α, β) of order c are $\psi(c, p-1)$. Similarly to above the number of extensions with Galois group $\mathbb{F}_{p^2}^+ \rtimes C$ is

$$\frac{p^{2n}-1}{p^2-1} \cdot \frac{1}{2}\psi(c, p-1),$$

and the full number of extensions obtained in this way is

$$\frac{p^{2n}-1}{p^2-1} \cdot \frac{1}{2}\left[(p-1)(p^2-1) - (p-1)^2\right] = \frac{p(p-1)(p^{2n}-1)}{2(p+1)}.$$

Assume now $r = 2$, $w = 1$. In this case the group acting in the representation is non-abelian, $s = 2$, and the action on $J_{(\alpha,\beta)}$ is described by the matrices

$$\mathcal{T} = \begin{pmatrix} \alpha & \\ & \alpha^p \end{pmatrix}, \qquad \mathcal{U} = \begin{pmatrix} & \beta \\ 1 & \end{pmatrix},$$

which generate the subgroup H of $GL(2, \mathbb{F}_{p^2})$ say. The multiplicity of the representation is equal to $2n$, but the pairs (α, β) and (α^p, β) in $\mathbb{F}_{p^2}^\times \times \mathbb{F}_p^\times$ induce the same representation. Being $J_{(\alpha,\beta)}$ defined over $\mathbb{F}_p$, the representations coming from $J_{(\alpha,\beta)}$ are exactly $(p^{2n}-1)/(p-1)$, by Lemma 4.2.6.

We identify the isomorphism class of groups generated by $\mathcal{T}$ and $\mathcal{U}$. The matrix $\mathcal{T}$ and $\mathcal{U}^2$ generate a cyclic group C of diagonal matrices, which taking the first entry on the diagonal can be identified to the subgroup of $\mathbb{F}_{p^2}^\times$ generated by α, β. Multiplying $\mathcal{U}$ by a diagonal matrix in the group, we obtain

$$\begin{pmatrix} \gamma & \\ & \gamma^p \end{pmatrix} \cdot \begin{pmatrix} & \beta \\ 1 & \end{pmatrix} = \begin{pmatrix} & \gamma\beta \\ \gamma^p & \end{pmatrix},$$

which scaling the second vector of the basis by γ^p becomes

$$\begin{pmatrix} & \gamma\gamma^p\beta \\ 1 & \end{pmatrix} = \begin{pmatrix} & \gamma^{p+1}\beta \\ 1 & \end{pmatrix}.$$

In particular β is defined up to elements of C^{p+1}, and clearly different classes correspond to non-isomorphic groups, considering the invariant obtained squaring a the non-diagonal matrix. Consequently the generated group is identified by the order of the cyclic group $C \subseteq \mathbb{F}_{p^2}^\times$, and the class of β in $(C \cap \mathbb{F}_p^\times) \bmod C^{p+1}$.

Being $(\mathbb{F}_{p^2}^\times)^{p+1}$ the whole $\mathbb{F}_p^\times$, we remark that each group of matrices considered above is contained in the group obtained taking a primitive root for α and $\beta = 1$, which turns out to be isomorphic to $\mathbb{F}_{p^2}^\times \rtimes \operatorname{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ with the natural action on $\mathbb{F}_{p^2}^+$. On the other hand each subgroup is obtained from a suitable pair (α, β).

Let c be the order of C. Since $(p-1, p+1) = 2$ (or 1 for $p = 2$) we have that $(C \cap \mathbb{F}_p^\times)/C^{p+1}$ has order 1 or 2, and the order is 2 exactly when $v_2(c) > 0$, but $v_2(c) < v_2(p^2-1)$. Let's consider this case, and let (α, β) generate C, and 2^k be the biggest power of 2 dividing c. Then $\beta \in C^{p+1}$ if and only if its order is not divisible by a power of 2 bigger than $2^k/(2^k, p+1)$. Since β can be changed by an element of C^{p+1} obtaining an isomorphism group H, we have that $\beta \in C^{p+1}$ if and only if $C \to H$ splits.

Let's decompose $\mathbb{F}_{p^2}^\times \times \mathbb{F}_p^\times$ as direct sum of ℓ-groups for each prime ℓ, and chose the components of (α, β) in this sum, which can be taken to be any element with the correct order. For $\ell \neq 2$, the choices have no effect on the condition that $\beta \in C^{p+1}$.

For $\ell = 2$ the group is $C_{2^{w+z}} \times C_{2^z}$, where $2^w \| (p+1)$ and $2^z \| (p-1)$. Assume $2^k \| c$ for some $1 \leq k < w + z$. If $z = 1$, then $\beta \in C^{p+1}$ precisely when we are selecting the 2-component as $(x, 1)$, and this amounts to 1/2 of the cases for $k > 1$, and 1/3 of the possible cases for $k = 1$. If $w = 1$, then $\beta \in C^{p+1}$ precisely when the 2-component (x, y) is such that x has bigger order than y, and since $k \leq z$ this happen 1/3 of the times.

Consequently let

$$\lambda(c, p) = \begin{cases} 1 & \text{if } v_2(c) = 0 \text{ or } v_2(c) = v_2(p^2-1), \\ 1/2 & \text{if } v_2(p-1) < v_2(c) < v_2(p^2-1), \\ 1/3 & \text{if } 0 < v_2(c) \leq v_2(p-1). \end{cases}$$

Then $\lambda(c, p-1)\psi(c, p-1)$ is the number of pairs (α, β) such that the group C generated by α, β has order c, and $\beta \in C^{p+1}$, while $(1 - \lambda(c, p-1))\psi(c, p-1)$ is the number of pairs such that $\beta \notin C^{p+1}$. Multiplying by $\frac{1}{2}(p^{2n}-1)/(p-1)$ we obtain the number of isomorphism classes of extensions having a particular group.

The total number of classes of extensions for $r = 2$, $w = 1$ is obtained as

$$\frac{p^{2n}-1}{p-1}\frac{1}{2}\left[(p-1)(p^2-1) - (p-1)^2\right] = \frac{1}{2}p(p-1)(p^{2n}-1),$$

and the total number of classes of extension having no intermediate extension is again

$$\frac{1}{2}p(p-1)(p^{2n}-1) + \frac{p(p-1)(p^{2n}-1)}{2(p+1)} = \frac{p(p^2+p-2)(p^{2n}-1)}{2(p+1)}.$$

We collect all the results obtained in the following theorem.

Theorem 4.2.7. *Let K be an extension of $\mathbb{Q}_p$ of degree n. Let c be an integer dividing (p^2-1) but not $(p-1)$, and let C be the cyclic subgroup of $\mathbb{F}_{p^2}^{\times}$ of order c. Let $\mathcal{G}(C)$ be the number of isomorphism classes of extensions of degree p^2 such that the normal closure has group isomorphic to $\mathbb{F}_{p^2}^{+} \rtimes C$. Then*

$$\mathcal{G}(C) = \frac{p^{2n}-1}{p^2-1} \cdot \frac{1}{2}\psi(c, p^{(f_k,2)} - 1).$$

Let H be a non-abelian subgroup of $\mathbb{F}_{p^2}^{\times} \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ not contained in $\mathbb{F}_{p^2}^{\times}$. Let $\mathcal{G}(H)$ be the number of isomorphism classes of extensions of degree p^2 such that the normal closure has group isomorphic to $\mathbb{F}_{p^2}^{+} \rtimes H$. Put $C = H \cap \mathbb{F}_{p^2}^{\times}$ and $c = |C|$. If $2 \mid f_K$ then $\mathcal{G}(H) = 0$, while if $2 \nmid f_K$ we have

$$\mathcal{G}(H) = \begin{cases} \lambda(c, p-1) \cdot \frac{p^{2n}-1}{2(p-1)} \cdot \psi(c, p-1) & \textit{if } C \to H \textit{ splits,} \\ (1 - \lambda(c, p-1)) \cdot \frac{p^{2n}-1}{2(p-1)} \cdot \psi(c, p-1) & \textit{if } C \to H \textit{ does not split.} \end{cases}$$

The above groups exhaust the groups of normal closures of isomorphism classes of extensions of degree p^2 having no intermediate extension. The total number $\mathcal{K}_K$ of isomorphism classes of extensions of degree p^2 with no intermediate extension is

$$\mathcal{K}_K = \frac{p(p^2+p-2)(p^{2n}-1)}{2(p+1)}.$$

We obtain 4 classes of extensions of degree 4 over $\mathbb{Q}_2$ with no intermediate extension, and 30 of degree 9 over $\mathbb{Q}_3$, as can be verified in the database of local fields.

4.2.5 Solvable subgroups of S_{p^2} which are realized

We characterize here the transitive solvable subgroups of S_{p^2} that possess a filtration that could fit into the ramification filtration, and describe which of them are Galois groups of a $\mathfrak{p}$-adic field.

Let G be a Galois group of the normal closure of an extension L/K, if W is the subgroup fixing L/K then we have a natural G-set formed by the lateral classes G/W. A set of laterals containing W forms a block for the action if and only if their union is a subgroup. Consequently the action is imprimitive if and only if there exists an intermediate group between W and G, or equivalently if and only if L/K has a proper subextension, E say.

Let's restrict to primitive subgroups, so let G be a solvable transitive subgroup of S_{p^2} that we assume primitive. In a solvable group a minimal normal subgroup is always abelian elementary, or it could be replaced with an ℓ-Sylow of the last non-zero term of its derived series, which is characteristic in the subgroup and consequently normal in the full group. Let A be a minimal normal subgroup of G.

Now if X is an orbit for A, then gX is an orbit for $gAg^{-1} = A$. Thus G can only permute pairwise disjoint orbits of A, and its orbits form blocks for the action of G. In our case the action is imprimitive, so A should be an ℓ-group acting transitively on p^2 elements, so $A \cong C_p \times C_p$ and we will consider it as a vector space over $\mathbb{F}_p$.

The stabilizer of one point H is a complement for A, so $G \cong A \rtimes H$. Now H cannot have a non-trivial p-core, or it would imply the existence of a non-trivial invariant subspace B of A, and the G-set G/H would have a quotient G/BH, implying that the action was not primitive. Furthermore the elements of H commuting with A are contained in all conjugates of H, which are exactly the stabilizers of the points, so $C_H(A)$ is trivial because each element in it fixes all p^2 elements of the action, and hence H embeds into $\mathrm{Aut}(A) \cong GL(2, \mathbb{F}_p)$.

Since H has trivial p-core, it follows that if G is the Galois group of a local field then we must have $G_1 \subseteq A$. In particular we should have $G_1 = A$ because G_1 cannot be trivial or a p-Sylow should be cyclic, neither it can be a proper subspace of A, which cannot be normal in G.

In particular H is the Galois group of the tame subextension, and has a cyclic subgroup H_0 of order prime with p, such that H/H_0 is also cyclic with a generator ϕ_q acting on H_0 by $x \mapsto x^q$. It is consequently a quotient of a group of a tame extension that was considered in Section 4.2.1, and we already showed that the action on an irreducible representation of dimension 2 over $\mathbb{F}_p$, in a suitable basis over $\bar{\mathbb{F}}_p$, is always generated by a matrix $\begin{pmatrix} \alpha & \\ & \alpha^p \end{pmatrix}$ for some $\alpha \in \mathbb{F}_{p^2}^\times$, plus possibly a matrix $\begin{pmatrix} & \beta \\ 1 & \end{pmatrix}$ for $\beta \in \mathbb{F}_p^\times$.

Proposition 4.2.8. *Each Galois group of the normal closure of an extension of degree p^2 with no intermediate extension is an extension by $\mathbb{F}_{p^2}^+$ of a subgroup $H \subseteq \mathbb{F}_{p^2}^\times \rtimes \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ that is not an abelian group of exponent $p-1$. If $2 \nmid f_K$ all possible $\mathbb{F}_{p^2}^+ \rtimes H$ are realized over K, and if $2 \mid f_K$ those realized are all $\mathbb{F}_{p^2}^+ \rtimes H$ for H abelian.*

4.3 One intermediate extension

In this section we apply Theorem 4.1.2 to classify the isomorphism classes of extensions of degree p^2 of a p-adic field K having exactly one intermediate extension. When the isomorphism class of the intermediate extension $[E/K]$ is fixed, we will obtain formulæ giving the exact number of classes that have E as unique intermediate extension, and as Galois group of the normal closure a group with prescribed p-Sylow and prescribed action of $\mathrm{Gal}(F/K)$ on it. A slightly less explicit formula counts the number of classes of extensions whose Galois group is in a fixed isomorphism class. We then determine which solvable subgroups of S_{p^2} can be realized, and in particular we will see that each transitive subgroup with a suitable ramification filtration occurs as Galois group over a proper extension of $\mathbb{Q}_p$, while this is false for $\mathbb{Q}_p$ itself for $p \geq 5$. We end with a formula for the total number of classes of extensions with one intermediate extension.

Let as above F be the maximal abelian extension of exponent $p-1$, and $H = \mathrm{Gal}(F/K)$. We will fix a class $[E/K]$ of extensions of degree p of K, with $E_F = EF$. Then E_F/K is Galois with group G, whose unique normal p-Sylow is $S = \mathrm{Gal}(E_F/F)$. Assume $E_F = F(\Gamma^{1/p})$ for the submodule Γ of dimension 1 of $[F^\times]_F$.

The groups S, Γ and the group of p-th roots of the unity $\mu_p \in F$ are cyclic groups of order p, and their automorphism group can be canonically identified with $\mathbb{F}_p^\times$. The action of H on them can consequently be described by characters. Let

$$\omega : H \to \mathrm{Aut}(\mu_p) \cong \mathbb{F}_p^\times, \qquad \rho : H \to \mathrm{Aut}(\Gamma) \cong \mathbb{F}_p^\times$$

be the character describing the action on μ_p and Γ. Then being canonically $S \cong \Gamma^* \otimes \mu_p$ the action on S is described by $\hat{\rho} = \rho^{-1}\omega$.

Let

$$H^* = \left\{ \phi : H \to \mathbb{F}_p^\times \right\}$$

be the set of all characters. For $\phi \in H^*$ will put $\hat{\phi} = \phi^{-1}\omega$, and call it *twisted inverse* of ϕ. We clearly have $\hat{\hat{\phi}} = \phi$.

If we fix the extension E in the class $[E/K]$, then H can be identified with $\mathrm{Gal}(E_F/E)$, which is a complement of S in G, and then $G \cong S \rtimes_{\hat{\rho}} H$. We remark that if $\tilde{E}$ is the normal closure of E/K then $\mathrm{Gal}(\tilde{E}/K)$ is isomorphic to $S \rtimes_{\hat{\rho}} ({}^{H}/_{\ker(\tilde{\rho})})$.

When the action $\hat{\rho}$ of H on the p-Sylow is fixed, we will see that the $\mathbb{F}_p[G]$-module structure of $[E_F^\times]_{E_F}$ is essentially independent on the particular field E_F considered. In particular the only other information required will be whether ζ_p is in $N_{E_F/F}(E_F^\times)$ or not.

Once this structure is described, it is possible to consider the indecomposable $\mathbb{F}_p[G]$-submodules of $[E_F^\times]_{E_F}$, and enumerate such submodules Ξ having fixed length, and a fixed action of H on $\Xi/\operatorname{rad}(\Xi)$.

Let $M = E_F(\Xi^{1/p})$, and let $T = \mathrm{Gal}(M/E)$. Then $T \cong \Xi^* \otimes \mu_p$ as $\mathbb{F}_p[G]$-module, and the group of M/K fits into the exact sequence

$$1 \longrightarrow T \longrightarrow \mathrm{Gal}(M/K) \longrightarrow G \longrightarrow 1.$$

Being $G \cong S \rtimes_{\hat{\rho}} H$ it is easy to see that the isomorphism class of $\mathrm{Gal}(M/K)$ is uniquely determined by its p-Sylow $P = \mathrm{Gal}(M/F)$. Indeed, the p-Sylow is normal and hence it has a complement, that we will still identify with H up to a choice. The action on the p-Sylow is uniquely determined by the action on T and $S = P/T$: if it was not the case, there would exist an non trivial action of H on P fixing T and S. Any such action would map a generator σ of S to an element $\sigma\tau$ for $\tau \in T$, and consequently it would have order p, and this is impossible considering that $|H|$ is prime with p.

If Δ is an $\mathbb{F}_p[H]$-module generating Ξ, and the action of H is described by χ, then this is also the action on $\Xi/\operatorname{rad}(\Xi)$, and the action on $\mathrm{soc}(T)$ will rather be given by $\hat{\chi} = \chi^{-1}\omega$. The group of a normal closure $\tilde{L}$ of the corresponding class $[L/K]$ of extensions of degree p^2 such that $L_F = E_F(\Delta^{1/p})$ will be $P \rtimes {}^{H}/_{(\ker(\hat{\rho}) \cap \ker(\hat{\chi}))}$.

We have from Chap. 2, Prop. 2.2.2 and 2.2.3, that fixing a generator of S we can define a homomorphism $\varepsilon : [E_F^\times]_{E_F} \to \mu_p$, with the property that P has exponent p if and only if Ξ has length $< p$ and is contained in $\ker(\varepsilon)$. This additional data allows to determine uniquely the p-Sylow, and hence the full group.

4.3.1 The module of power classes

Let $M = [E_F^\times]_{E_F}$ for short. In this section we will completely describe its structure as $\mathbb{F}_p[G]$-module.

We have $G = S \rtimes H$ where $S = \mathrm{Gal}(E_F/F)$ is the normal p-Sylow, which is cyclic of order p, and H a complement. Assume $S = \langle\sigma\rangle$, then the radical of $\mathbb{F}_p[G]$ is generated by $(\sigma - 1)$. In particular the elements of the socle series and radical series of a module coincide if it is considered as $\mathbb{F}_p[G]$-module or as $\mathbb{F}_p[S]$-module.

Each indecomposable $\mathbb{F}_p[G]$-module X is uniserial of length $\ell \leq p$, so in particular $\mathrm{rad}^{\ell-1}(X) = \mathrm{soc}^1(X)$, and is uniquely determined by the length and by the $\mathbb{F}_p[H]$-module structure of $\mathrm{soc}^1(X)$. Let $N = \mathrm{rad}^{p-1}(M)$, then it detects the indecomposable factors of length exactly p, and M contains a direct factor, which is isomorphic to $\mathrm{Ind}_H^G(N)$. Since $(\sigma-1)^{p-1}$ is equal to $\sigma^{p-1} + \cdots + \sigma + 1$ in $\mathbb{F}_p[S]$, it follows that N is equal to $[N_{E_F/F}(E_F^\times)]_{E_F}$.

We will now describe the structure of N as $\mathbb{F}_p[H]$-module. If $\chi \in H^*$ is a character and X an $\mathbb{F}_p[H]$-module, we denote by X_χ the generalized eigenspace of X on which H acts via χ. Being $|H|$ prime with p, it follows that X can be decomposed as direct sum of the X_χ over all possible characters.

We will start from a description of $[F^\times]_F$ as $\mathbb{F}_p[H]$-module.

Proposition 4.3.1. *Assume $[K : \mathbb{Q}_p] = n$. Let $\chi \in H^*$, then we have*

$$\dim_{\mathbb{F}_p} [F^\times]_{F,\chi} = n + \delta_\chi^1 + \delta_\chi^\omega,$$

where ω is the cyclotomic character $H \to \mathrm{Aut}(\mu_p) \cong \mathbb{F}_p^\times$.

Proof. See for instance [DCD07]. □

Assume $E_F = F(\Gamma^{1/p})$ for a submodule $\Gamma \subseteq M$. Then Γ is the kernel of the reduction $[F^\times]_F \to [F^\times]_{E_F}$, indeed is represented by the elements in $F^\times \cap (E_F^\times)^p$ by Kummer theory. Furthermore Γ is contained in $[N_{E_F/F}(E_F^\times)]_F$, unless $p = 2$ and $-1 \notin N_{E_F/F}(E_F^\times)$. In this last case if the extension is obtained by the equation $x^2 - \alpha$, then α becomes a square and $-\alpha$ a norm, and α is a norm if and only if -1 is a norm too. We will assume that we are not in the case of $p = 2$ and $-1 \notin N_{E_F/F}(E_F^\times)$, which will be considered later.

Let's recall that the action of H on Γ is described by ρ. By local class field theory

$$F^\times/N_{E_F/F}(E_F^\times) \cong [F^\times]_F/[N_{E_F/F}(E_F^\times)]_F$$

is canonically isomorphic to $S = \mathrm{Gal}(E_F/F)$, and is also isomorphic to $[F^\times]_{E_F}/N$ being $\Gamma \subseteq [N_{E_F/F}(E_F^\times)]_F$. They are isomorphic as $\mathbb{F}_p[H]$-modules, and the action is described by the character $\hat{\rho} = \rho^{-1}\omega$.

Consequently removing one multiplicity for each of these characters we the following description.

Proposition 4.3.2. *Assume we are not in the case* $p = 2$ *and* $-1 \notin N_{E_F/F}(E_F^\times)$. *Then for each* $\chi \in H^*$ *we have*

$$\begin{aligned} \dim_{\mathbb{F}_p} [F^\times]_{E_F,\chi} &= n + \delta_\chi^1 + \delta_\chi^\omega - \delta_\chi^\rho, \\ \dim_{\mathbb{F}_p} N_\chi &= n + \delta_\chi^1 + \delta_\chi^\omega - \delta_\chi^\rho - \delta_\chi^{\hat{\rho}}. \end{aligned}$$

We remark that $\mathbb{F}_p[H] \otimes_{\mathbb{F}_p[H]} N$ has dimension $p(p-1)^2 n$, which is equal to $[E_F : \mathbb{Q}_p]$. By the description of the multiplicative group we obtain instead that M has dimension $p(p-1)^2 n + 2$, so what is left to determine is just a module of dimension 2. It will be determined thanks to the description of $\operatorname{soc}^1(M)$.

We recall that by Chap. 2, Prop. 2.2.3 the socle of M is equal to

$$\operatorname{soc}^1(M) = \begin{cases} [F^\times]_{E_F} \oplus \langle \delta \rangle & \text{if } \zeta_p \in N_{E_F/F}(E_F^\times), \\ \quad [F^\times]_{E_F} & \text{if } \zeta_p \notin N_{E_F/F}(E_F^\times), \end{cases} \tag{4.2}$$

in the first case $\delta \in M$ is such that $E_F(\delta^{1/p})$ is cyclic of order p^2 over F.

This is already enough to determine the remaining factor. When ζ_p is a norm, it has length one and is product of two submodules of dimension 1 where H acts via $\hat{\rho}$ and ρ. When ζ_p is not a norm, it is indecomposable of length 2, and H acts on the socle via $\hat{\rho}$. We remark that the second case can happen only when ζ_p generates $F^\times/N_{E_F/F}(E_F^\times)$, so the action on S and μ_p have to be equal and $\hat{\rho} = \omega$.

The function $\varepsilon : M \to \mu_p$ is surjective, and $\varepsilon(\delta) \neq 1$ when $\zeta_p \in N_{E_F/F}(E_F^\times)$, while $\varepsilon(\eta) \neq 1$ for some $\eta \in \operatorname{soc}^2(M)$ when $\zeta_p \notin N_{E_F/F}(E_F^\times)$. While ε depends on some choice, $\ker(\varepsilon)$ is defined in a canonical way so it is an $\mathbb{F}_p[G]$-submodule, let's denote it by Π.

Since we assume we are not in the case $p = 2$ and $-1 \notin N_{E_F/F}(E_F^\times)$, then $\operatorname{rad}^{p-1}(\Pi) = N$. Indeed either $p > 2$ and $\operatorname{soc}^2(M)\Pi = M$ so Π generates $M/\operatorname{soc}^{p-1}(M)$, either $p = 2$ and $\operatorname{soc}^1(M)\Pi = M$ being a complement generated by δ, and we also have that Π generates $M/\operatorname{soc}^{p-1}(M)$. Applying $(\sigma - 1)^{p-1}$ we obtain that $\operatorname{rad}^{p-1}(\Pi)$ is the whole $N = \operatorname{rad}^{p-1}(M)$.

Consequently Π is a direct sum of a module isomorphic to $\mathbb{F}_p[G] \otimes_{\mathbb{F}_p[H]} N$ and one isomorphic to $[F^\times]_{E_F}/N$.

Proposition 4.3.3. *Assume we are not in the case* $p = 2$ *and* $-1 \notin N_{E_F/F}(E_F^\times)$. *Then the module* Π *is isomorphic to*

$$(\mathbb{F}_p[G] \otimes_{\mathbb{F}_p[H]} N) \oplus ([F^\times]_{E_F}/N). \tag{4.3}$$

In any case we always have

$$\dim_{\mathbb{F}_p}(\operatorname{soc}^\ell(\Pi)_\chi) = \ell n + \delta_\chi^{\hat{\rho}} + \sum_{i=0}^{\ell-1} \left(\delta_{\hat{\rho}^i\chi}^1 + \delta_{\hat{\rho}^i\chi}^\omega - \delta_{\hat{\rho}^i\chi}^\rho - \delta_{\hat{\rho}^i\chi}^{\hat{\rho}} \right).$$

Proof. We only have to prove the second formula, which is immediate considering that the action on $[F^\times]_{E_F}/N$ is given by $\hat{\rho}$, and for each indecomposable module X of length p have

$$\dim_{\mathbb{F}_p}(\operatorname{soc}^{i+1}(X)/\operatorname{soc}^i(X))_\chi = \dim_{\mathbb{F}_p}\operatorname{soc}(X)_{\hat{\rho}^i\chi},$$

by the description of indecomposable modules of Chap. 2, Prop. 2.1.2.

For $p = 2$ and $-1 \notin N_{E_F/F}(E_F^\times)$ we have that all characters are trivial, and N is equal to $[F^\times]_{E_F}$, rather than being a subspace of codimension 1. However $\operatorname{soc}^1(M) \subseteq \Pi$ and $\Pi/\operatorname{soc}^1(M)$ has codimension 1 in $M/\operatorname{soc}^1(M)$, so $\operatorname{rad}^{p-1}(\Pi)$ has codimension 1 in N, and the formula is still verified being Π equal to the (4.3) with $\operatorname{rad}^1(\Pi)$ in the place of N. □

Let's set $h = h(E_F/F)$ to be

$$h(E_F/F) = \begin{cases} 1 & \text{if } \zeta_p \in N_{E_F/F}(E_F^\times), \\ 2 & \text{if } \zeta_p \notin N_{E_F/F}(E_F^\times). \end{cases}$$

The following proposition gives comfortable description of M.

Proposition 4.3.4. *As an $\mathbb{F}_p[H]$-submodule Π is complemented in M by a submodule $\Lambda = \langle\lambda\rangle$, on which the action of H is described by ρ. The smallest length of the $\mathbb{F}_p[G]$-module generated by λ is $h(E_F/F)$.*

Proof. Indeed, $\operatorname{soc}^h(\Pi)$ is strictly smaller that $\operatorname{soc}^h(M)$ for $h = h(E_F/F)$, and hence there exists an $\mathbb{F}_p[H]$ invariant complement. The action is either equal to the action on $\langle\delta\rangle$, that is ρ, either $h = 2$ and the action is $\hat{\rho}^{-1}\hat{\rho} = 1$, but this case is only possible when $\rho = 1$. □

4.3.2 Classification of extensions

We will now exploit the description of $M = [E_F^\times]_{E_F}$ to give formulæ counting the extension with a fixed group of the normal closure.

In particular the extensions having a fixed p-Sylow and action of H on it are described by the following proposition. We remark that when the p-Sylow P has exponent p^2 and is a non-split extension $T \bullet S$ for an indecomposable $\mathbb{F}_p[S]$-module T, then the action of H on S and $\operatorname{soc}^1(T)$ must be described by the same character. This is implied by Prop. 4.3.4 describing a complement of Π, but can also be observed directly, because the p-th power map induces a canonical isomorphism of $S = P/T$ with $\operatorname{soc}^1(T)$, so H should clearly act with the same character.

Proposition 4.3.5. *Let $[E/K]$ be a class of extensions of degree p, F the maximal abelian extension of exponent $p-1$ and $E_F = EF$. Put $H = \operatorname{Gal}(F/K)$ acting on $S = \operatorname{Gal}(E_F/F)$ via the character $\hat{\rho}$ so that $G = \operatorname{Gal}(E_F/K) \cong S \rtimes_{\hat{\rho}} H$. Let $1 \leq \ell < p$, $\hat{\chi} \in H^*$ a character, and let T be an indecomposable $\mathbb{F}_p[G]$-module of length ℓ and such that H acts on $\operatorname{soc}^1(T)$ via $\hat{\chi}$. Let $h = h(E_F/F)$ be 1 or 2 depending if $\zeta_p \in N_{E_F/F}(E_F^\times)$ or not, like in Prop. 4.3.4.*

Assume as usual $\hat\rho = \rho^{-1}\omega$, and $\hat\chi = \chi^{-1}\omega$. Consider the isomorphism classes $[L/E]$ such that the Galois group of the normal closure $\tilde L_F$ of $L_F = LF$ over K is isomorphic to the semidirect product $T \rtimes G$, with the action of H described by $\hat\rho$ and $\hat\chi$. Their number is

$$\mathcal{E}_S(h,\rho,\chi,\ell) = \frac{1}{p-1}\left(p^{s(\rho,\chi,\ell)} - p^{s(\rho,\chi,\ell-1)}\right),$$

where for each $1 \leq m \leq p$ we have put

$$s(\rho,\chi,m) = mn + \delta_\chi^{\hat\rho} + \sum_{i=0}^{m-1}\left(\delta^1_{\hat\rho^i\chi} + \delta^\omega_{\hat\rho^i\chi} - \delta^\rho_{\hat\rho^i\chi} - \delta^{\hat\rho}_{\hat\rho^i\chi}\right).$$

Assume $\chi = \rho$ and $\ell < p$, then the number of classes $[L/E]$ such that $\mathrm{Gal}(\tilde L_F/K)$ *is the non-split extension $T \bullet G$ with the given action of H is*

$$\mathcal{E}_N(h,\rho,\ell) = \begin{cases} p^{s(\rho,\rho,\ell)} - p^{s(\rho,\rho,\ell-1)} & \textit{if } \ell > h, \\ p^{s(\rho,\rho,\ell)} & \textit{if } \ell = h, \\ 0 & \textit{if } \ell < h. \end{cases}$$

In the case $\ell = p$, any extension of G by T is always the semidirect product $T \rtimes G$, and the number of such extensions is

$$\mathcal{E}_S(h,\rho,\chi,p) = \begin{cases} \frac{1}{p-1}\left(p^{s(\rho,\chi,p)} - p^{s(\rho,\chi,p-1)}\right) & \textit{if } \chi \neq \rho, \\ \frac{1}{p-1}\left(p^{s(\rho,\rho,p)+1} - p^{s(\rho,\rho,p-1)+1}\right) & \textit{if } \chi = \rho \textit{ and } p > h, \\ \frac{1}{p-1}\left(p^{s(\rho,\rho,p)+1} - p^{s(\rho,\rho,p-1)}\right) & \textit{if } (\chi = \rho \textit{ and}) \ p = h = 2. \end{cases}$$

Proof. It follows immediately by Prop. 4.3.3 and Prop. 4.3.4. Indeed, the we have one class to count in $\mathcal{E}_S(h,\rho,\chi,\ell)$ for each subspace of M generated by an element in $\mathrm{soc}^\ell(\Pi)_\chi \backslash \mathrm{soc}^{\ell-1}(\Pi)_\chi$. The number of generators is exactly $p^{s(\rho,\chi,\ell)} - p^{s(\rho,\chi,\ell-1)}$, and each subspace is generated by $p-1$ possible generators.

Similarly for $\mathcal{E}_N(h,\rho,\ell)$ the possible generators are of the form $\gamma + \alpha\lambda$ for $\alpha \in \mathbb{F}_p^\times$, and $\gamma \in \mathrm{soc}^\ell(\Pi)_\rho \setminus \mathrm{soc}^{\ell-1}(\Pi)_\rho$ when $\ell > h$, or $\gamma \in \mathrm{soc}^\ell(\Pi)_\rho$ when $\ell = h$, because λ generates a module of length h.

The last formula is obtained in the same way putting together the two cases, when $\rho = \chi$. Indeed for $\ell = p$ the p-Sylow is always the semidirect product, by Chap. 2, Prop. 2.2.1. □

It is also possible to pass easily to the enumeration of isomorphism classes over K, rather than the classes over L.

Proposition 4.3.6. *Keep the same notation as in Prop. 4.3.5, and let's denote as $\mathcal{K}_S(h,\rho,\chi,\ell)$ and $\mathcal{K}_N(h,\rho,\ell)$ the number of isomorphism classes over K of extensions containing an extension in the class $[E/K]$ and which are computed in $\mathcal{E}_S(h,\rho,\chi,\ell)$ and $\mathcal{E}_N(h,\rho,\ell)$. Then we have*

$$\mathcal{K}_S(h,\rho,\chi,\ell) = \begin{cases} \frac{1}{p}\mathcal{E}_S(h,\rho,\chi,\ell) & \textit{if } \hat\rho = 1 \textit{ and } \ell \geq 2, \\ \mathcal{E}_S(h,\rho,\chi,\ell) & \textit{in any other case,} \end{cases}$$

and similarly

$$\mathcal{K}_N(h,\rho,\ell) = \begin{cases} \frac{1}{p}\mathcal{E}_N(h,\rho,\ell) & \text{if } \hat\rho = 1 \text{ and } \ell \geq 2, \\ \mathcal{E}_N(h,\rho,\ell) & \text{in any other case,} \end{cases}$$

where as usual $\hat\rho$ is the twisted inverse $\rho^{-1}\omega$, where ω is the cyclotomic character.

Proof. Follows immediately from Prop. 4.3.5 and Theorem. 4.1.2. □

4.3.3 The possible Galois closures

We show how it is possible enumerating the extensions sharing the same normal closure. Let $[E/K]$ be a fixed class of extensions of degree p, F and E_F be like in the previous section, $M = [E_F^\times]_{E_F}$, and the same for $G = \operatorname{Gal}(E_F/K)$, which is isomorphic to $S \rtimes_{\hat\rho} H$.

For each indecomposable $\mathbb{F}_p[G]$-module $\Xi \subset M$ the isomorphism classes $[L/E]$ of extensions such that $L_F = LF$ has normal closure equal to $E_F(\Xi^{1/p})$ correspond to the $\mathbb{F}_p[H]$-submodules Δ that generate it. If we request the action on Δ to be given by the character χ and Ξ to have length ℓ, all possible Δ are enumerated in Prop. 4.3.5.

We can compute the number of Δ generating the same Ξ: each is generated by an element in $\Xi_\chi \setminus \operatorname{rad}^1(\Xi)_\chi$. Clearly the dimension of Ξ_χ is equal to the number of quotients $\operatorname{soc}^i(\Xi)/\operatorname{soc}^{i-1}(\Xi)$ in the socle series such that the action on the quotient is described by χ. By the description of indecomposable modules Chap. 2, Prop. 2.1.2 we have that Ξ_χ has dimension $\lceil \ell/o(\hat\rho)\rceil$ where $o(\hat\rho)$ is the order of $\hat\rho$, that is the smallest integer i such that $\hat\rho^i = 1$. The dimension of $\operatorname{rad}^1(\Xi)_\chi$ is smaller by 1.

Each Δ being generated by $p-1$ generators, the number of possible submodules is

$$\frac{1}{p-1}\left(p^{\lceil \ell/o(\hat\rho)\rceil} - p^{\lceil \ell/o(\hat\rho)\rceil - 1}\right) = p^{\lceil \ell/o(\hat\rho)\rceil - 1}.$$

From Prop. 4.3.5 we obtain the following enumeration of the possible Galois closures.

Proposition 4.3.7. *Keep the same notation as in Prop. 4.3.5, with $[E/K]$ fixed and $h = h(E_F/F)$. The number of the different Galois extensions obtained as normal closures of the classes of extensions computed in $\mathcal{E}_S(h,\rho,\chi,\ell)$ and $\mathcal{E}_N(h,\rho,\ell)$ are respectively*

$$\frac{\mathcal{E}_S(h,\rho,\chi,\ell)}{p^{\lceil \ell/o(\hat\rho)\rceil - 1}}, \qquad \frac{\mathcal{E}_N(h,\rho,\ell)}{p^{\lceil \ell/o(\hat\rho)\rceil - 1}}.$$

4.3.4 Extensions with prescribed Galois group

We give formulæ in terms of the $\mathcal{K}_N(h,\rho,\ell)$ and $\mathcal{K}_S(h,\rho,\chi,\ell)$ counting the total number of extensions of degree p^2 of K with prescribed p-Sylow, and prescribed action of $\operatorname{Gal}(F/K)$ on the groups $\operatorname{Gal}(E_F/F)$ and $\operatorname{Gal}(L_F/E_F)$. The actions on these groups will be described as usual by $\hat\rho = \rho^{-1}\omega$ and $\hat\chi = \chi^{-1}\omega$.

First, we need to know the number of classes $[E/K]$ of extensions of degree p such that, putting $E_F = EF$, the group $H = \mathrm{Gal}(F/K)$ acts on $\mathrm{Gal}(E_F/F)$ via the character $\hat{\rho}$. Let $\mathcal{B}(\rho)$ be such number, by Prop. 4.3.1 it can be computed as

$$\mathcal{B}(\rho) = \frac{1}{p-1}\left(p^{n+\delta^1_\rho+\delta^\omega_\rho} - 1\right). \tag{4.4-ρ}$$

However the values of $\mathcal{K}_S$ are different, depending whether the intermediate extension $[E/K]$ is such that $\zeta_p \in N_{E_F/F}(E_F^\times)$ or not. It may happen that $\zeta_p \notin N_{E_F/F}(E_F^\times)$ only for $\hat{\rho} = \omega$, which implies $\rho = 1$. We will denote the two possibilities for the E_F/F corresponding to $\rho = 1$ as $\mathcal{B}^{\zeta}(1)$ and $\mathcal{B}^{\not\zeta}(1)$, and compute these numbers.

If $\zeta_{p^2} \in F^\times$ we clearly have $\mathcal{B}^{\zeta}(1) = \mathcal{B}(1)$ and $\mathcal{B}^{\not\zeta}(1) = 0$, so assume $\zeta_{p^2} \notin F^\times$. Consider the intersection of all norm groups of the extensions E_F such that E_F/K is Galois, and the action of H on $\mathrm{Gal}(E_F/F)$ is described by $\hat{\rho}$. By local class field theory it is the biggest $\mathbb{F}_p[H]$-submodule G of $[F^\times]_F$ such that the action on the quotient is described by $\hat{\rho}$. By Prop. 4.3.1 it has dimension $n + 1 + \delta^\omega_1$.

The extensions such that $\zeta_p \in N_{E_F/F}(E_F^\times)$ correspond via local class field theory to the subspaces of codimension 1 containing the non-trivial subgroup $\langle[\zeta_p]_F\rangle \subseteq [F^\times]_F$. We can equivalently count the subspaces of codimension 1 in the quotient, which has dimension $n + \delta^\omega_1$. They are

$$\mathcal{B}^{\zeta}(1) = \frac{1}{p-1}\left(p^{n+\delta^\omega_1} - 1\right) \qquad (\text{if } \zeta_{p^2} \notin F^\times). \tag{4.4-ζ}$$

Computing the complement to $\mathcal{B}(1)$ we obtain also

$$\mathcal{B}^{\not\zeta}(1) = \frac{1}{p-1}\left(p^{n+1+\delta^\omega_1} - p^{n+\delta^\omega_1}\right) = p^{n+\delta^\omega_1} \qquad (\text{if } \zeta_{p^2} \notin F^\times). \tag{4.4-$\not\zeta$}$$

In conclusion since $\zeta_{p^2} \in F^\times$ if and only if $\zeta_{p^2} \in K^\times$ we have

$$\mathcal{B}^{\zeta}(1) = \begin{cases} \frac{1}{p-1}\left(p^{n+\delta^\omega_1} - 1\right) & \text{if } \zeta_{p^2} \notin F^\times, \\ \mathcal{B}(1) & \text{if } \zeta_{p^2} \in F^\times, \end{cases} \qquad \mathcal{B}^{\not\zeta}(1) = \begin{cases} p^{n+\delta^\omega_1} & \text{if } \zeta_{p^2} \notin F^\times, \\ 0 & \text{if } \zeta_{p^2} \in F^\times. \end{cases}$$

We deduce the following proposition, giving the exact number of extensions with prescribed group, where the group is identified by the p-Sylow and the action of H.

Proposition 4.3.8. *Denote by $\mathcal{A}_S(\rho, \chi, \ell)$ and $\mathcal{A}_N(\rho, \ell)$ the number of isomorphism classes $[L/K]$ having a unique intermediate extension $[E/K]$, where the group $H = \mathrm{Gal}(F/K)$ acts on $\mathrm{Gal}(E_F/F)$ and $\mathrm{Gal}(L_F/E_F)$ via $\hat{\rho} = \rho^{-1}\omega$ and $\hat{\chi} = \chi^{-1}\omega$ respectively (set $\chi = \rho$ for $\mathcal{G}_N$), and such that the p-Sylow is respectively a split or non-split extension of $\mathrm{Gal}(E_F/F)$ by a module of length ℓ. Then we have*

$$\mathcal{A}_S(\rho, \chi, \ell) = \begin{cases} \mathcal{B}(\rho) \cdot \mathcal{K}_S(1, \rho, \chi, \ell) & \text{if } \rho \neq 1, \\ \mathcal{B}^{\zeta}(1) \cdot \mathcal{K}_S(1, 1, \chi, \ell) + \mathcal{B}^{\not\zeta}(1) \cdot \mathcal{K}_S(2, 1, \chi, \ell) & \text{if } \rho = 1. \end{cases}$$

and similarly

$$\mathcal{A}_N(\rho,\ell) = \begin{cases} \mathcal{B}(\rho)\cdot\mathcal{K}_N(1,\rho,\ell) & \textit{if } \rho \neq 1, \\ \mathcal{B}^{\zeta}(1)\cdot\mathcal{K}_N(1,1,\ell) + \mathcal{B}^{\not\zeta}(1)\cdot\mathcal{K}_N(2,1,\ell) & \textit{if } \rho = 1. \end{cases}$$

We remark that fixing the action we are considering an equivalence on the Galois group of the normal closures that is finer than that of just the isomorphism class of the group. The number of extensions having group isomorphic to a prescribed group can be obtained as a sum over the possible ρ, ξ giving the isomorphism class.

We show now how to enumerate the extensions in the same isomorphism class. Assume that H acts via the characters $\hat{\rho}$ and $\hat{\chi}$ on $S = \mathrm{Gal}(E_F/F)$ and $\mathrm{Gal}(L_F/E_F)$, and let $T = \mathrm{Gal}(\tilde{L}_F/E_F)$, which as usual is assumed to be an indecomposable $\mathbb{F}_p[S]$-module of length ℓ. Let A be the image of the homomorphism

$$(\hat{\rho}, \hat{\rho}^{1-\ell}\hat{\chi}) : H \to (\mathbb{F}_p^\times \times \mathbb{F}_p^\times),$$

which is isomorphic to ${}^{H}/_{\ker(\hat{\rho},\hat{\chi})}$. As subgroup of $(\mathbb{F}_p^\times \times \mathbb{F}_p^\times)$ it carries the natural characters given by the projections π_1, π_2 on the coordinates. This characters are clearly equal to $\hat{\rho}$, $\hat{\rho}^{1-\ell}\hat{\chi}$ via the identification of A with ${}^{H}/_{\ker(\hat{\rho},\hat{\rho}^{1-\ell}\hat{\chi})}$. Note that if H acts on $\mathrm{soc}^1(T)$ via $\hat{\chi}$, then the action on $T/\mathrm{rad}^1(T)$ is given by $\hat{\rho}^{1-\ell}\hat{\chi}$, by Chap. 2, Prop. 2.1.2.

Consequently the group G of the normal closure over K is one of

$$(T \rtimes S) \rtimes A, \qquad (T \bullet S) \rtimes A,$$

where as usual T is an indecomposable $\mathbb{F}_p[S]$-module of length ℓ, and the action of A is uniquely determined by the actions on S and $T/\mathrm{rad}^1(T)$, which are given by π_1 and π_2.

Let

$$\Delta^i = \left\{(x, x^i) : x \in \mathbb{F}_p^\times\right\} \subseteq (\mathbb{F}_p^\times \times \mathbb{F}_p^\times),$$

and for each subgroup $B \subseteq (\mathbb{F}_p^\times \times \mathbb{F}_p^\times)$ let B^τ be the subgroup obtained flipping the coordinates.

Proposition 4.3.9. *In the case of the non-split extension, $A \subseteq \Delta^{2-\ell}$, and the isomorphism class is determined by A. If the extension is split, then the isomorphism class of group is determined by A when $\ell \geq 3$, and by $\{A, A^\tau\}$ when $\ell \leq 2$.*

Proof. When the extension is non-split, the p-th power map determines a canonical isomorphism $S \to \mathrm{soc}^1(T)$, and on these modules the action of $(x,y) \in A$ is given by multiplication by x and $x^{\ell-1}y$, which must therefore be equal. The particular group A is determined by its order, so clearly the group determines the isomorphism class.

Let the extension be split, then the Frattini subgroup of the p-Sylow is $\mathrm{rad}^1(T)$, being the corresponding quotient an abelian elementary p-group of rank 2. When $\ell \geq 3$, the elements of T are exactly those acting trivially by conjugacy on $\mathrm{rad}^1(T)$. Thus, given an action of A on $T \rtimes S$ we have that A is uniquely identified to a subgroup of $(\mathbb{F}_p^\times \times \mathbb{F}_p^\times)$. If $\ell \leq 2$ then each subgroup of index p in $T \rtimes S$ is an indecomposable split extension of the quotient, and it is A-invariant (and hence a normal subgroup of G) precisely if the image in ${}^{T}/_{\mathrm{rad}^1(T)} \times S$ is A-invariant. Each invariant subspace gives a possible splitting, and an element $(x, y) \in A$ acts on the quotient and the subspace by multiplication by x and y, or vice-versa. □

For a fixed A, we can now count the extensions with group isomorphic to a prescribed extension.

Theorem 4.3.10. *Let $A \subseteq (\mathbb{F}_p^\times \times \mathbb{F}_p^\times)$, and $1 \leq \ell \leq p$. Let S be a cyclic group of order p, and T an indecomposable $\mathbb{F}_p[S]$-module of length ℓ. Denote by $\mathcal{G}_S(A, \ell)$ and $\mathcal{G}_N(A, \ell)$ the number of isomorphism classes $[L/K]$ whose Galois group of the normal closure isomorphic to $(T \rtimes S) \rtimes A$ and $(T \bullet S) \rtimes A$ respectively, where (x, y) acts on S and $T/\mathrm{rad}^1(T)$ as multiplication by x and y respectively. Assume $A \subseteq \Delta^{2-\ell}$ in the case of the non split extension. Then we have*

$$\mathcal{G}_S(A,\ell) = \begin{cases} \displaystyle\sum_{\substack{\rho,\chi \in H^* \\ \mathrm{img}(\hat{\rho},\hat{\rho}^{1-\ell}\hat{\chi}) = A}} \mathcal{A}_S(\rho,\chi,\ell) & \text{if } \ell \geq 3, \\ \displaystyle\sum_{\substack{\rho,\chi \in H^* \\ \mathrm{img}(\hat{\rho},\hat{\rho}^{1-\ell}\hat{\chi}) = A \text{ or } A^\tau}} \mathcal{A}_S(\rho,\chi,\ell) & \text{if } \ell \leq 2, \end{cases}$$

and similarly for $\ell \leq p - 1$ we have

$$\mathcal{G}_N(A,\ell) = \sum_{\substack{\rho \in H^* \\ \mathrm{img}(\hat{\rho},\hat{\rho}^{2-\ell}) = A}} \mathcal{A}_N(\rho,\ell).$$

Proof. The proof is clear by Prop. 4.3.9, and observing that whenever the action on S and $\mathrm{soc}^1(T)$ are given by $\hat{\rho}$ and $\hat{\chi}$, then the action on $T/\mathrm{rad}^1(T)$ is given by $\hat{\rho}^{1-\ell}\hat{\chi}$. □

4.3.5 Solvable subgroups of S_{p^2} realized

Similarly to what done in the primitive case, we consider now the imprimitive solvable transitive subgroups of S_{p^2} having a suitable ramification filtration, which correspond to possible Galois group of the normal closure of an extensions with intermediate extensions. We characterize here the transitive solvable subgroups of S_{p^2} that possess a filtration that could fit into the ramification filtration, and describe those realized as Galois groups of a p-adic field.

Consider the elements acting trivially on the set of blocks, their action on each block is described by a solvable subgroup of S_p, which is a subgroup of the group F_p of functions $C_p \to C_p$ of the form $x \mapsto ax + b$ for $a \neq 0$. On the other hand such elements are exactly the kernel of the action on the blocks, which has image contained in F_p as well. In this way we obtain that G is contained in the semidirect product $(F_p)^p \rtimes F_p$, with the action of permutation of the coordinates. The second F_p acts on p^2 elements permuting the blocks, and preserving the orbits on each block.

Let's identify F_p with $C_p \rtimes C_p^*$, where $C_p^* = \mathrm{Aut}(C_p)$. Quotienting by the subgroup $(C_p)^p \cap G$ we obtain a subgroup $\bar{G}$ of $(C_p^*)^p \rtimes F_p$. Now the ramification filtration forces the subgroup $C_p \lhd F_p$ (which is non-trivial because the action is transitive) to act trivially on $\bar{G} \cap (C_p^*)^p$, or the derived subgroup would contain a non cyclic subgroup of order prime with p. Indeed, $\bar{G}'$ is smaller than the image of G', which is contained in G_0, and recall that G_1 is a p-group, while G_0/G_1 is cyclic.

Consequently $\bar{G} \cap (C_p^*)^p$ is formed by elements whose components are all equal so it can be identified to a subgroup of C_p^* itself, and its action on $(C_p)^p$ commute with the action of F_p. Thus G is a subgroup of

$$[(C_p)^p \rtimes C_p)] \rtimes (C_p^* \times C_p^*),$$

where one of the C_p^* acts diagonally on $M = (C_p)^p$ and trivially on C_p, and the other C_p^* acts by automorphisms on C_p and trivially on $M/\operatorname{rad}^1(M)$, where M is viewed as an $\mathbb{F}_p[C_p]$-module. In other words, G has to be one of the groups $(T \rtimes S) \rtimes A$ or $(T \bullet S) \rtimes A$ considered in Prop. 4.3.10.

Proposition 4.3.11. *Let $G = (T \rtimes S) \rtimes A$ or $G = (T \bullet S) \rtimes A$ be like in Prop. 4.3.10, for a subgroup A of $(\mathbb{F}_p^\times \times \mathbb{F}_p^\times)$ that we assume contained in $\Delta^{2-\ell}$ in the case of the non split extension.*

Then G is always realizable, unless the base field is $\mathbb{Q}_p$ and $A \subsetneq \Delta^1$ and non-trivial.

Proof. Let $H = \mathrm{Gal}(F/K)$ like in Prop. 4.3.5. For an arbitrary surjection $H \to A$ we have composing with π_1, π_2 two characters α, β, which are equal to $\hat{\rho}$ and $\hat{\rho}^{1-\ell}\hat{\chi}$ for some $\rho, \chi \in H^*$. As usual the characters $\hat{\rho}$ and $\hat{\chi}$ describe the actions on S and $\mathrm{soc}^1(T)$.

From Prop. 4.3.5, G with the fixed action of H is realizable when

$$s(\rho, \chi, \ell) - s(\rho, \chi, \ell - 1) = n + \delta^1_{\hat{\rho}^{\ell-1}\chi} + \delta^\omega_{\hat{\rho}^{\ell-1}\chi} - \delta^\rho_{\hat{\rho}^{\ell-1}\chi} - \delta^{\hat{\rho}}_{\hat{\rho}^{\ell-1}\chi}$$

is positive. If this condition is satisfied then we are done, because the intermediate extension E_F/F corresponding to ρ can always be taken to satisfy $\zeta_p \in N_{E_F/F}(E_F^\times)$ by equation 4.4-ζ, so $h = 1$ in Prop. 4.3.5.

Since $\hat{\rho}^{\ell-1}\chi = \hat{\beta}$ and $\rho = \hat{\alpha}$ it can we rewritten as

$$n + \delta^1_{\hat{\beta}} + \delta^\omega_{\hat{\beta}} - \delta^{\hat{\alpha}}_{\hat{\beta}} - \delta^\alpha_{\hat{\beta}}.$$

Now if A is not contained in Δ^1 the characters $\hat{\alpha}$ and $\hat{\beta}$ are always different. Assume $\omega \neq 1$, in the case $\alpha = \hat{\beta}$, or equivalently $\alpha = \beta\omega$, we can compose the map $H \to A$ with an automorphism of H not fixing ω, to obtain a new pair of α, β such that $\delta^\alpha_{\hat{\beta}} = 0$. If $n = 1$ and $\omega = 1$ then we are in the case $K = \mathbb{Q}_2$, so all the characters are trivial and the expression is still positive.

On the other hand $A \subset \Delta^1$ if and only if $\alpha = \beta$. If $n = 1$ the (4.3.5) can be positive if and only if we can have $\beta = 1$ or $\beta = \omega$, so A is either trivial, either the whole Δ^1. In this last case $\alpha = \omega$, and $\delta^{\alpha}_{\hat{\beta}} = 0$.

When $A \subset \Delta^1$ and $n = 2$, it may happen that $\delta^{\alpha}_{\hat{\beta}}$ is positive only when $\hat{\alpha} = \hat{\beta} = \alpha$, so $\alpha^2 = \omega$, but applying an automorphism of H we can always ensure that $\alpha^2 \neq \omega$. □

We observe that, in the imprimitive case, all the possible groups are realized over a proper extension of $\mathbb{Q}_p$. Over $\mathbb{Q}_p$ those not realized are those where A is cyclic of order d dividing $p-1$ but $\neq 1, p-1$, and with identical action on S and $T/\operatorname{rad}^1(T)$.

In the classification of the extensions of degree 9 of $\mathbb{Q}_3$ it was observed by Jones and Roberts [JR04] that somewhat coincidentally all the 23 transitive subgroups of S_9 having a proper ramification filtration have a normal 3-Sylow and are realized as extensions of $\mathbb{Q}_3$. This turns out to be true because for $p = 3$ the only divisors of $p-1$ are 1 and $p-1$, so this is indeed very incidental.

4.3.6 The total number of extensions

Theorem. 4.1.2 supplies a way to obtain the total number of extensions having exactly one intermediate extension, that is in the class $[E/K]$. The purpose of this section is to obtain an opaque formula giving just the number of such extensions, independently of the group of the normal closure.

To enumerate the isomorphism classes over E we are indeed reduced to consider the $\mathbb{F}_p[H]$-submodules of dimension 1 contained in $M = [E_F^{\times}]_{E_F}$, but not in $[F^{\times}]_{E_F}$. To have the isomorphism classes over L it will be enough remembering, when $\hat{\rho} = 1$, to divide by p the number of modules not contained in $\operatorname{soc}^1(M)$.

For each character χ we know the dimensions of the generalized eigenspaces

$$\dim_{\mathbb{F}_p}\left([E_F^{\times}]_{E_F}\right)_{\chi} = np + \delta^1_{\chi} + \delta^{\omega}_{\chi}, \qquad \dim_{\mathbb{F}_p}\left([F^{\times}]_{E_F}\right)_{\chi} = n + \delta^1_{\chi} + \delta^{\omega}_{\chi} - \delta^{\rho}_{\chi},$$

thanks Prop. 4.3.1 and Prop. 4.3.2. and we obtain that the number $\mathcal{E}(\rho, \chi)$ of isomorphism classes over E is

$$\mathcal{E}(\rho, \chi) = \frac{p^{\delta^1_{\chi} + \delta^{\omega}_{\chi}}}{p-1} \cdot \left(p^{pn} - p^{n - \delta^{\rho}_{\chi}}\right).$$

When $\hat{\rho} = 1$ (or equivalently $\rho = \omega$) the extensions coming from subspaces not contained in $\operatorname{soc}^1(M)$ are conjugated over K and belong to classes of order p. Consequently recalling the description of $\operatorname{soc}^1(M)$ of Prop. 4.2 we have

$$\mathcal{K}(\rho, \chi) = \begin{cases} \frac{p^{\delta^1_{\chi} + \delta^{\omega}_{\chi}}}{p-1} \cdot \left(p^{pn} - p^{n - \delta^{\rho}_{\chi}}\right) & \text{if } \rho \neq \omega, \\ \frac{1}{p} \cdot \frac{p^{\delta^1_{\chi} + \delta^{\omega}_{\chi}}}{p-1} \cdot \left(p^{pn} - p^{n - \delta^{\omega}_{\chi}}\right) & \text{if } \rho = \omega = 1 \text{ and } \zeta_p \notin N_{E_F/F}(E_F^{\times}), \\ \frac{p^{\delta^1_{\chi} + \delta^{\omega}_{\chi}}}{p-1} \cdot \left(\frac{1}{p}(p^{pn} - p^n) + (p^n - p^{n - \delta^{\omega}_{\chi}})\right) & \text{if } \rho = \omega \text{ and } \zeta_p \in N_{E_F/F}(E_F^{\times}). \end{cases}$$

We now compute the sum $\mathcal{K}(\rho) = \sum_{\chi\in H^*}\mathcal{K}(\rho,\chi)$ for all possible values of ρ, in order to obtain the full number of extension as a sum of the kind

$$\mathcal{K} = \sum_{\rho\in H^*}\mathcal{B}(\rho)\cdot\mathcal{K}(\rho).$$

We need to consider distinct cases depending if ω is trivial or not (or equivalently if $\zeta_p\in K$ or not). We recall that if $\zeta_p\notin N_{E_F/F}(E_F^\times)$ then we always have $\omega=\hat{\rho}$, so in the case $\hat{\rho}=1$ we also have $\omega=\rho=1$.

Case $\omega\neq 1$**.** Suppose first that $\omega\neq 1$. Recall that $|H| = (p-1)$. If $\rho=1\neq\omega$, the sum $\mathcal{K}(\rho)=\mathcal{K}(1)$ is obtained as

$$\begin{aligned}\mathcal{K}(1) &= \sum_{\chi\neq\omega,1}\mathcal{K}(1,\chi)+\mathcal{K}(1,\omega)+\mathcal{K}(1,1)\\ &= \left[p^2-2p-1\right]\cdot\frac{1}{p-1}\left(p^{pn}-p^n\right)\\ &+\frac{p}{p-1}\left(p^{pn}-p^n\right)+\frac{p}{p-1}\left(p^{pn}-p^{n-1}\right)\\ &= \frac{[p^2-2p-1+p+p]}{p-1}\cdot p^{pn}-\frac{[p^2-2p-1+p+1]}{p-1}p^n\\ &= (p+1)p^{pn}-p^{n+1}.\end{aligned} \tag{4.5-1}$$

If $\rho=\omega\neq 1$ (and necessarily $\zeta_p\in N_{E_F/F}(E_F^\times)$) we have

$$\begin{aligned}\mathcal{K}(\omega) &= \sum_{\chi\neq\omega,1}\mathcal{K}(\omega,\chi)+\mathcal{K}(\omega,\omega)+\mathcal{K}(\omega,1)\\ &= \left[p^2-2p-1\right]\cdot\frac{1}{p-1}\cdot\frac{1}{p}\left(p^{pn}-p^n\right)\\ &+\frac{p}{p-1}\left(\frac{1}{p}(p^{pn}-p^n)+(p^n-p^{n-1})\right)+\frac{p}{p-1}\cdot\frac{1}{p}(p^{pn}-p^n)\\ &= \frac{[p-2-1/p]+1+1}{p-1}\cdot p^{pn}-\frac{[p-2-1/p]+1-(p-1)+1}{p-1}p^n\\ &= (p+1)p^{pn-1}-p^{n-1}.\end{aligned} \tag{4.5-ω}$$

If ρ is different from both $1,\omega$, we can compute

$$\begin{aligned}\mathcal{K}(\rho) &= \sum_{\chi\neq\omega,1,\rho}\mathcal{K}(\rho,\chi)+\mathcal{K}(\rho,\omega)+\mathcal{K}(\rho,1)+\mathcal{K}(\rho,\rho)\\ &= \left[p^2-2p-2\right]\cdot\frac{1}{p-1}\left(p^{pn}-p^n\right)+\frac{p}{p-1}\left(p^{pn}-p^n\right)\\ &+\frac{p}{p-1}\left(p^{pn}-p^n\right)+\frac{1}{p-1}\left(p^{pn}-p^{n-1}\right)\\ &= \frac{[p^2-2p-2]+p+p+1}{p-1}\cdot p^{pn}-\frac{[p^2-2p-2]+p+p+1/p}{p-1}\cdot p^n\end{aligned}$$

$$= (p+1)p^{pn} - (p^2+p-1)p^{n-1}. \tag{4.5-ρ}$$

We can obtain the total number $\mathcal{K}$ of isomorphism classes of extensions of degree p^2 having precisely one intermediate extension as

$$\mathcal{K} = \sum_{\rho \neq 1, \omega} \mathcal{B}(\rho) \cdot \mathcal{K}(\rho) + \mathcal{B}(\omega) \cdot \mathcal{K}(\omega) + \mathcal{B}(1) \cdot \mathcal{K}(1)$$

and thanks to the computation of $\mathcal{B}(\rho)$ in (4.4-ρ) it is computed as

$$\begin{aligned}
&= [p^2-2p-1] \cdot \frac{p^n-1}{p-1} \cdot \left[(p+1)p^{pn} - (p^2+p-1)p^{n-1}\right] \\
&\quad + \frac{p^{n+1}-1}{p-1} \cdot \left[(p+1)p^{pn-1} - p^{n-1}\right] \\
&\quad \frac{p^{n+1}-1}{p-1} \cdot \left[(p+1)p^{pn} - p^{n+1}\right] \\
&= \frac{[p^2-2p-1]+1+p}{p-1} \cdot (p+1)p^{(p+1)n} \\
&\quad - \frac{[p^2-2p-1]+1+1}{p-1} \cdot (p+1)p^{pn} \\
&\quad - \frac{[p^2-2p-1](p^2+p-1)+p+p^3}{p-1} \cdot p^{2n-1} \\
&\quad + \frac{[p^2-2p-1](p^2+p-1)+1+p^2}{p-1} \cdot p^{n-1} \\
&= (p+1)p^{(p+1)n+1} - (p^3-2p-1)p^{pn-1} \\
&\quad -(p^3+p^2-3p-1)p^{2n-1} + (p^3-3p-2)p^{n-1}.
\end{aligned} \tag{4.6}$$

Case $\omega = 1$**.** In this case for $\rho = 1 = \omega$ we have a different number of extensions of $[E/K]$ depending whether $\zeta_p \in N_{E_F/F}(E_F^\times)$ or not. Let's disambiguate the values of the sum as $\mathcal{K}(1 \mid \zeta \in N)$ and $\mathcal{K}(1 \mid \zeta \notin N)$. For the extensions such that $\zeta_p \in N_{E_F/F}(E_F^\times)$ we obtain via the computation of $\mathcal{K}(\rho, \chi)$ at the beginning

$$\begin{aligned}
\mathcal{K}(1 \mid \zeta \in N) &= \sum_{\chi \neq 1} \mathcal{K}(1, \chi) + \mathcal{K}(1,1) \\
&= \left[p^2 - 2p\right] \cdot \frac{1}{p-1} \left(\frac{1}{p}(p^{pn} - p^n) \right) \\
&\quad + \frac{p^2}{p-1} \left(\frac{1}{p}(p^{pn} - p^n) + (p^n - p^{n-1}) \right) \\
&= \frac{[p-2]+p}{p-1} \cdot p^{pn} - \frac{[p-2]+p-(p^2-p)]}{p-1} p^n \\
&= 2p^{pn+1} + (p-2)p^n.
\end{aligned} \tag{4.7-ζ}$$

In the case of $\zeta_p \notin N_{E_F/F}(E_F^\times)$ we have

$$\begin{aligned}
\mathcal{K}(1 \mid \zeta \notin N) &= \sum_{\chi \neq 1} \mathcal{K}(1,\chi) + \mathcal{K}(1,1)\\
&= \left[p^2 - 2p\right] \cdot \frac{1}{p-1}\left(\frac{1}{p}(p^{pn} - p^n)\right)\\
&\quad + \frac{p^2}{p-1}\left(\frac{1}{p}(p^{pn} - p^{n-1})\right)\\
&= \frac{[p-2]+p}{p-1} \cdot p^{pn} - \frac{[p-2]+1]}{p-1} p^n\\
&= 2p^{pn+1} - p^n. \qquad (4.7\text{-}\not\zeta)
\end{aligned}$$

For general $\rho \neq 1 = \omega$ we have

$$\begin{aligned}
\mathcal{K}(\rho) &= \sum_{\chi \neq 1,\rho} \mathcal{K}(\rho,\chi) + \mathcal{K}(\rho,1) + \mathcal{K}(\rho,\rho)\\
&= \left[p^2 - 2p - 1\right] \cdot \frac{1}{p-1}\left(p^{pn} - p^n\right)\\
&\quad + \frac{p^2}{p-1}\left(p^{pn} - p^n\right)) + \frac{1}{p-1}\left(p^{pn} - p^{n-1}\right)\\
&= \frac{[p^2-2p-1]+p^2+1}{p-1} \cdot p^{pn} - \frac{[p^2-2p-1]+p^2+1/p]}{p-1} p^n\\
&= 2p^{pn+1} - (2p^2-1)p^{n-1}. \qquad (4.7\text{-}\rho)
\end{aligned}$$

We compute now the total number of extension, depending whether $\zeta_{p^2} \in K^\times$ or not.

Case $\zeta_{p^2} \notin K^\times$. In this case the total number of classes can be computed as

$$\mathcal{K} = \sum_{\rho \neq 1} \mathcal{B}(\rho) \cdot \mathcal{K}(\rho) + \mathcal{B}^{\zeta}(1) \cdot \mathcal{K}(1 \mid \zeta \in N) + \mathcal{B}^{\not\zeta}(1) \cdot \mathcal{K}(1 \mid \zeta \notin N)$$

and via equations (4.7-ζ), (4.7-$\not\zeta$) and (4.7-ρ) we obtain

$$\begin{aligned}
&= [p^2-2p] \cdot \frac{p^n-1}{p-1} \cdot \left[p^{pn+1} - (2p^2-1)p^{n-1}\right]\\
&\quad + \frac{p^{n+1}-1}{p-1} \cdot [2p^{pn} + (p-2)p^n]\\
&\quad + p^{n+1} \cdot [2p^{pn} - p^n]\\
&= \frac{[p^2-2p]p + 2p + 2p(p-1)}{p-1} \cdot p^{(p+1)n}\\
&\quad - \frac{[p^2-2p]p+2}{p-1} \cdot p^{pn}
\end{aligned}$$

$$
\begin{aligned}
&-\frac{[p-2](2p^2-1)-p(p-2)+p(p-1)}{p-1}\cdot p^{2n}\\
&\quad+\frac{[p-2](2p^2-1)-(p-2)}{p-1}\cdot p^{n}\\
&=\frac{1}{p-1}\left(p^{(p+1)n+3}-(p^3-2p^2+2)p^{pn}\right)\\
&\quad-2(p^2-p-1)p^{2n}+2(p^2-p-2)p^{n}
\end{aligned}
\tag{4.8}
$$

Case $\zeta_{p^2}\in K^\times$. If $\zeta_{p^2}\in K^\times$ then ζ_p is always a norm, and we have

$$
\begin{aligned}
\mathcal{K}&=\sum_{\rho\neq 1}\mathcal{B}(\rho)\cdot\mathcal{K}(\rho)+\mathcal{B}(1)\cdot\mathcal{K}(1\mid\zeta\in N)\\
&=[p^2-2p]\cdot\frac{p^n-1}{p-1}\cdot\left[p^{pn+1}-(2p^2-1)p^{n-1}\right]\\
&\quad+\frac{p^{n+2}-1}{p-1}\cdot[2p^{pn}+(p-2)p^n]\\
&\quad=\frac{[p^2-2p]p+2p}{p-1}\cdot p^{(p+1)n}\\
&\quad-\frac{[p^2-2p]p+2}{p-1}\cdot p^{pn}\\
&\quad-\frac{[p-2](2p^2-1)-p^2(p-2)}{p-1}\cdot p^{2n}\\
&\quad+\frac{[p-2](2p^2-1)-(p-2)}{p-1}\cdot p^{n}\\
&=\frac{1}{p-1}\left(p^{(p+1)n+3}-(p^3-2p^2+2)p^{pn}\right)\\
&\quad-(p^2-p-2)p^{2n}+2(p^2-p-2)p^{n}
\end{aligned}
\tag{4.9}
$$

We remark that $\omega=1$ if and only if $\zeta_p\in K^\times$. Consequently equations (4.6), (4.8) and (4.9) can be summarized in the following theorem.

Theorem 4.3.12. *Let $[K:\mathbb{Q}_p]=n$. Let $\mathcal{K}_K$ be the number of isomorphism classes of extensions of degree p^2 of K having precisely one intermediate extension. Then we have*

$$
\mathcal{K}_K=\begin{cases}
\begin{array}{c}(p+1)p^{(p+1)n+1}-(p^3-2p-1)p^{pn-1}\\ -(p^3+p^2-3p-1)p^{2n-1}+(p^3-3p-2)p^{n-1}\end{array} & \text{if } \zeta_p\notin K^\times,\\[2ex]
\begin{array}{c}\frac{1}{p-1}\left(p^{(p+1)n+3}-(p^3-2p^2+2)p^{pn}\right)\\ -2(p^2-p-1)p^{2n}+2(p^2-p-2)p^{n}\end{array} & \text{if } \zeta_p\in K^\times \text{ but } \zeta_{p^2}\notin K^\times,\\[2ex]
\begin{array}{c}\frac{1}{p-1}\left(p^{(p+1)n+3}-(p^3-2p^2+2)p^{pn}\right)\\ -(p^2-p-2)p^{2n}+2(p^2-p-2)p^{n}\end{array} & \text{if } \zeta_{p^2}\in K^\times.
\end{cases}
$$

Applying the above formula we obtain 48 extensions of degree 4 over $\mathbb{Q}_2$ with exactly one intermediate extension, and 730 of degree 9 over $\mathbb{Q}_3$. These numbers are correct, according to the online database of local fields, see [JR06].

4.4 More intermediate extensions

For reference, we give here a quick computation of the number of isomorphism classes of extensions of degree p^2 having more than one intermediate extension. Let F be the maximal abelian extension of K of exponent $p-1$, and $H = \mathrm{Gal}(F/K)$.

We are reduced to count the number of reducible $\mathbb{F}_p[H]$-submodules of dimension 2 contained in $[F^\times]_F$. Each such submodule X has exactly 2 or $p+1$ subspaces of dimension 1, depending whether X is the sum of two subspaces of dimension one corresponding to distinct characters of H, and in this case the decomposition is unique, or if the action on X is described by a unique character with multiplicity 2, and in this case each of the possible $p+1$ subspaces is invariant.

Each invariant subspace correspond to a proper subextension of degree p, so if L/K is an extension of degree p^2 with ≥ 1 intermediate extensions, then it has either 2, either $p+1$ intermediate extensions. We will now compute the number of isomorphism classes in each of the two sub-cases.

4.4.1 One character with multiplicity 2

As it is well known, and can be easily computed, the number of distinct subspaces of dimension k of a vector space of dimension m over a field of q elements is given by the q-binomial

$$\binom{m}{k}_q = \frac{(q^m-1)(q^{m-1}-1)\dots(q^{m-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)}.$$

By Prop. 4.3.1 we obtain that the number of invariant subspaces of $[F^\times]_F$ of dimension 2 of $[F^\times]_F$ contained in one generalized eigenspace is

$$\sum_{\chi\in\hat{H}} \binom{n+\delta_\chi^1+\delta_\chi^\omega}{2}_p.$$

To give an explicit formula let's consider first the case with $\omega = 1$, considering that $|\hat{H}| = (p-1)^2$ we have that the number of subspaces is

$$\begin{aligned}&\left[(p-1)^2-1\right]\binom{n}{2}_p + \binom{n+2}{2}_p \\ &= \frac{(p^2-2p)(p^n-1)(p^{n-1}-1)+(p^{n+2}-1)(p^{n+1}-1)}{(p^2-1)(p-1)} \\ &= \frac{[(p^2-2p)p^{2n-1}+p^{2n+3}]-(p^2-2p)(p^n+p^{n-1})}{(p^2-1)(p-1)}\end{aligned}$$

$$
\begin{aligned}
&+\frac{-(p^{n+2}+p^{n+1})+[p^2-2p+1]}{(p^2-1)(p-1)}\\
&=\frac{(p^3+p-2)p^{2n}-(2p^2-2)p^n+(p^2-2p+1)}{(p^2-1)(p-1)}\\
&=\frac{(p^2+p+2)p^{2n}-2(p+1)p^n+(p-1)}{(p^2-1)},
\end{aligned}
$$

while in the case $1 \neq \omega$ we have

$$
\begin{aligned}
&\big[(p-1)^2-2\big]\binom{n}{2}_p+2\binom{n+1}{2}_p\\
&=\frac{(p^2-2p-1)(p^n-1)(p^{n-1}-1)+2(p^{n+1}-1)(p^n-1)}{(p^2-1)(p-1)}\\
&=\frac{[(p^2-2p-1)p^{2n-1}+2p^{2n+1}]-(p^2-2p-1)(p^n+p^{n-1})}{(p^2-1)(p-1)}\\
&\quad+\frac{-2(p^{n+1}+p^n)+[p^2-2p+1]}{(p^2-1)(p-1)}\\
&=\frac{(3p^2-2p-1)p^{2n-1}-(p^3+p^2-p-1)p^{n-1}+(p^2-2p+1)}{(p^2-1)(p-1)}\\
&=\frac{(3p+1)p^{2n-1}-(p+1)^2p^{n-1}+(p-1)}{(p^2-1)},
\end{aligned}
$$

which gives 2 for $p=3$ and $n=1$, as required.

4.4.2 Two distinct characters

On the other hand, the number of invariant subspaces that factor in two distinct eigenspaces for $\omega = 1$ is

$$
\begin{aligned}
&[(p-1)^2-1]\cdot\binom{n+2}{1}_p\cdot\binom{n}{1}_p+\binom{(p-1)^2-1}{2}\cdot\binom{n}{1}_p^2\\
&=\frac{p^n-1}{p-1}\cdot\left[(p^2-2p)\frac{p^{n+2}-1}{p-1}+\frac{(p^2-2p)(p^2-2p-1)}{2}\frac{p^n-1}{p-1}\right]\\
&=p\frac{(p^n-1)(p-2)}{2(p-1)^2}\cdot\big[2p^{n+2}+(p^2-2p-1)p^n-[2+(p^2-2p-1)]\big]\\
&=p\frac{(p^n-1)(p-2)}{2(p-1)^2}\cdot[(3p^2-2p-1)p^n-(p^2-2p+1)]\\
&=p\frac{(p^n-1)(p-2)\big[(3p+1)p^n-(p-1)\big]}{2(p-1)},
\end{aligned}
$$

while when $\omega \neq 1$ we have

$$
\binom{n+1}{1}_p^2+2\cdot((p-1)^2-2)\cdot\binom{n+1}{1}_p\cdot\binom{n}{1}_p+\binom{(p-1)^2-2}{2}\cdot\binom{n}{1}_p^2
$$

$$
\begin{aligned}
&= \frac{2[p^{2n+2} - 2p^{n+1} + 1] + 4(p^2 - 2p - 1)(p^{2n+1} - p^{n+1} - p^n + 1)}{2(p-1)^2} \\
&\qquad + \frac{(p^2 - 2p - 1)(p^2 - 2p - 2)[p^{2n} - 2p^n + 1]}{2(p-1)^2} \\
&= \frac{(p^3 + p^2 - 4p - 2)p^{2n} - 2(p^2 - p - 2)p^{n+1} + (p^2 - 3p + 2)p}{2(p-1)},
\end{aligned}
$$

which gives 33 for $p = 3$ and $n = 1$.

4.4.3 Formulæ for the number of extensions

Considering that $\omega = 1$ if and only if $\zeta_p \in K$, the results of this section can be resumed in the following proposition.

Proposition 4.4.1. *Let $n = [K : \mathbb{Q}_p]$. Let $\mathcal{S}_K$ be the number of isomorphism classes of extension of degree p^2 of K corresponding to a submodule with a unique character, and having exactly $p+1$ intermediate subextension. Then*

$$
\mathcal{S}_K = \begin{cases} \frac{(p^2+p+2)p^{2n}-2(p+1)p^n+(p-1)}{(p^2-1)} & \text{if } \zeta_p \in K, \\ \frac{(3p+1)p^{2n-1}-(p+1)^2p^{n-1}+(p-1)}{(p^2-1)} & \text{if } \zeta_p \notin K. \end{cases}
$$

Let $\mathcal{D}_K$ be the number of isomorphism classes of extension of degree p^2 of K corresponding to a submodule with distinct characters, and having exactly 2 intermediate subextension. Then we have

$$
\mathcal{D}_K = \begin{cases} p\frac{(p^n-1)(p-2)(3p^{n+1}-p^n-p+1)}{2(p-1)} & \text{if } \zeta_p \in K, \\ \frac{(p^3+p^2-4p-2)p^{2n}-2(p^2-p-2)p^{n+1}+(p^2-3p+2)p}{2(p-1)} & \text{if } \zeta_p \notin K. \end{cases}
$$

Chapter 5

Enumeration of isomorphism classes of extensions

Let K be a finite extension of $\mathbb{Q}_p$ with residue field κ_K. Let $n_0 = [K : \mathbb{Q}_p]$, and let respectively $e_0 = e(K/\mathbb{Q}_p)$ and $f_0 = f(K/\mathbb{Q}_p)$ be the absolute ramification index and inertia degree. Formulæ for the total number of extensions with given degree in a fixed algebraic closure were computed by Krasner and Serre [Kra62, Ser78], as well as formulæ counting all totally ramified extensions and totally ramified extension with given valuation of the discriminant.

We will show how it is possible, with some help from class field theory, to modify such formulæ to enumerate the isomorphism classes of extensions with fixed ramification and inertia, and all extension with fixed degree.

The problem of enumerating isomorphism classes of $\mathfrak{p}$-adic field had been solved in a special case by Hou-Keating [HK04] for extensions with ramification e satisfying $p^2 \nmid e$, with a partial result when $p^2 \parallel e$.

5.1 Group theoretic preliminaries

For $k \geq 1$, let $C_k \cong \mathbb{Z}/k\mathbb{Z}$ denote the cyclic group of order k. Given a group G, let $\mathscr{F}$ be a family of subgroups of G which is closed under conjugation and contain a finite number of subgroups of fixed index in G. For each integer n, let $\mathcal{I}_n$ be the number of conjugacy classes of subgroups $H \in \mathscr{F}$ having index n in G. For a finite group Q, let $\mathcal{T}_n(Q)$ denote the number of two-steps chains of subgroups $H \lhd J \leq G$ such that $H \in \mathscr{F}$, $(G : H) = n$ and H is normal in J with $J/H \cong Q$.

Lemma 5.1.1. *For a group G and a family of subgroup $\mathscr{F}$ which is closed under conjugation and containing a finite number of subgroups of fixed index in G we* *have*

$$\mathcal{I}_n = \frac{1}{n} \sum_{d|n} \phi(d) \mathcal{T}_n(C_d), \tag{5.1}$$

for each n.

Proof. For fixed $H \in \mathscr{F}$ with $(G : H) = n$, let's compute the contribute of the chains of the form $H \lhd J \leq G$. All the admissible J are contained in the normalizer $N_G(H)$, and the number of subgroups in $N_G(H)/H$ isomorphic to C_d multiplied by $\phi(d)$ counts the number of elements of $N_G(H)/H$ with order precisely equal to d, because $\phi(d)$ is the number of possible generators of a group isomorphic to C_d. The contribute for all possible d is hence equal to $(N_G(H) : H)$, and having H precisely $(G : N_G(H))$ conjugates its conjugacy class contributes n to the sum, i.e. 1 to the full expression. □

We remark that this lemma had been found in essentially the same form by Mednykh [Med08], which however applied it in a different context, to count isomorphism classes of covering of surfaces. The author was not aware when the results contained in this chapter where first published [Mon11].

The absolute Galois group of a $\mathfrak{p}$-adic field has only a finite number of closed subgroups with fixed index and consequently the closed subgroups can be taken as family $\mathscr{F}$. By Galois theory the formula (5.1) can be interpreted denoting with $\mathcal{I}_n$ the number of isomorphism classes of extensions L/K of degree n over a fixed field K, and with $\mathcal{T}_n(Q)$ the number of all towers of extensions $L/F/K$ such that $[L : K] = n$, and L/F is Galois with group isomorphic to Q. Similarly, the above formula can be used to count, say, extensions with prescribed ramification and inertia, all the extensions of given degree, or totally ramified extensions with prescribed valuation of the different, restricting the computation via an appropriate choice of the family $\mathscr{F}$ of subgroups of G.

The above formula can be applied to local fields with great effectiveness because the number of cyclic extension with prescribed ramification and inertia (which will be carried over in the next section) has little dependence on the particular field taken into account, and only depends on the absolute degree over $\mathbb{Q}_p$, the absolute inertia, and the p-part of the group of the roots of the unity.

5.2 On the number of cyclic extensions

In this section we briefly deduce via class field theory the number $\mathcal{C}(F, e, f)$ of cyclic extensions of a $\mathfrak{p}$-adic field F with prescribed ramification e, inertia f and degree $d = ef$, and the number $\mathcal{C}(F, d)$ of all cyclic extension of degree d, for any d.

By class field theory (see §3.4, Chap. 3), the maximal abelian extension with exponent d has Galois group isomorphic to the biggest quotient of $F^\times$ which has exponent d, and consequently its Galois group is isomorphic to $F^\times/(F^\times)^d$.

Furthermore, the upper numbering ramification groups are the images of the principal units $U_0, U_1, \dots$ under this isomorphism.

The choice of a uniformizer π provides a factorization $F = \langle\pi\rangle \times U_0$ (see §3.1.2, Chap. 3), and U_0 is isomorphic to the direct product of the group of the roots of the unity μ_F and a free $\mathbb{Z}_p$ module with rank $m = [F : \mathbb{Q}_p]$. Consequently calling G the Galois group of the maximal abelian extension with exponent d we have

$$G \cong C_d \times C_z \times C_{p^r}^m \times C_{p^{\min\{\xi,r\}}}, \qquad G^0 \cong \{1\} \times C_z \times C_{p^r}^m \times C_{p^{\min\{\xi,r\}}}$$

where $d = p^r k$ with $(d,k) = 1$, z is the g.c.d. of k and the order $|\kappa_F^\times| = p^{f(F/\mathbb{Q}_p)} - 1$ of the group of the roots of the unity with order prime with p, and ξ is the integer such that p^ξ is the order of the group of the roots of the unity with p-power order.

The number of subgroups $H \subseteq G$ such that $G/H \cong C_d$ and $G/(HG^0) \cong C_f$ will be computed using the duality theory of finite abelian groups. Let $\hat{G} = Hom(G, \mathbb{Q}/\mathbb{Z})$, and for each subgroup H of G put $H^\perp = \{\phi \in \hat{G} : \phi(x) = 0, \text{ for } x \in H\} \cong \widehat{G/H}$.

The conditions on H amounts to having $H^\perp \cong C_d$, and $(HG^0)^\perp = H^\perp \cap (G^0)^\perp \cong C_f$. Since we have (non-canonically) that

$$(G^0)^\perp \cong C_d \times \{1\} \times \{1\} \times \{1\} \subseteq C_d \times C_z \times C_{p^r}^m \times C_{p^{\min\{\xi,r\}}} \cong \hat{G},$$

we must count the number of subgroups isomorphic to C_d, generated by an element of the form (x,y) with $x \in C_d$ and $y \in C_z \times C_{p^r}^m \times C_{p^{\min\{\xi,r\}}}$ say, such that the intersection with $(G^0)^\perp$ is isomorphic to C_f. The order of $e \cdot x$ must be equal to f, and since the map of multiplication by e from C_d to C_d is e-to-1 and has image isomorphic to C_f we have that the number of possible x is e times the number of generators of C_f, and hence is equal to $e\phi(f)$.

The y coordinate on the other hand should have order precisely equal to e, which we write $e = p^s h$ with $(h,p) = 1$, and this is impossible if $h \nmid z$, while if $h \mid z$ we have

$$\phi(h) \cdot \Pi_p(m,s,\xi)$$

possibilities for y, where for all p, m, s, ξ we define for convenience

$$\Pi_p(m,s,\xi) = \begin{cases} 1 & \text{if } s = 0, \\ p^{ms+\min\{\xi,s\}} - p^{m(s-1)+\min\{\xi,s-1\}} & \text{if } s > 0, \end{cases} \tag{5.2}$$

which counts the number of elements of order p^s in a group isomorphic to $C_{p^r}^m \times C_{p^{\min\{\xi,r\}}}$ (for any $r \geq s$).

Since we counted the number of good generators, to obtain the number of good groups we must divide by $\phi(ef)$ obtaining

$$\mathcal{C}(F,e,f) = \frac{e\phi(h)\phi(f)}{\phi(ef)} \cdot \Pi_p(m,s,\xi) \tag{5.3}$$

if $h \mid (p^{f(F/\mathbb{Q}_p)} - 1)$, while $\mathcal{C}(F,e,f) = 0$ if $h \nmid (p^{f(F/\mathbb{Q}_p)} - 1)$.

The total number of cyclic extensions of degree $d = p^r k$ can be deduced similarly, considering that

$$G \cong C_k \times C_z \times C_{p^r}^{m+1} \times C_{\min\{\xi,r\}}.$$

Let's consider the function $\psi(u, v)$ which for natural u, v counts the number of elements with order u in the group $C_u \times C_v$, and can be expressed as

$$\psi(u,v) = u \cdot (u,v) \cdot \prod_{\substack{\ell \text{ prime} \\ \ell | u/(u,v)}} \left(1 - \frac{1}{\ell}\right) \cdot \prod_{\substack{\ell \text{ prime} \\ \ell | u,\ \ell \nmid u/(u,v)}} \left(1 - \frac{1}{\ell^2}\right). \tag{5.4}$$

A computation similar to what done above tells us that the total number of C_d-extensions is

$$\mathcal{C}(F,d) = \frac{\psi(k, p^{f(K/\mathbb{Q}_p)} - 1)}{\phi(d)} \cdot \Pi_p(m+1, r, \xi). \tag{5.5}$$

5.3 Formula for isomorphism classes

Let's recall Krasner formula for the number $\mathcal{N}(K, e, f)$ of extensions with ramification $e = p^s h$ (with $(p,h) = 1$) and inertia f of a field K having absolute degree $n_0 = [K : \mathbb{Q}_p]$. The formula is

$$\mathcal{N}(K,e,f) = e \cdot \sum_{i=0}^{s} p^i \left(p^{\varepsilon(i)N} - p^{\varepsilon(i-1)N}\right),$$

where $N = n_0 e f$ and

$$\varepsilon(i) = \begin{cases} -\infty & \text{if } i = -1, \\ 0 & \text{if } i = 0, \\ p^{-1} + p^{-2} + \cdots + p^{-i} & \text{if } i > 0. \end{cases}$$

Denote by convenience with $\Sigma_p(N, s)$ the sum in the Krasner formula

$$\Sigma_p(N,s) = \sum_{i=0}^{s} p^i \left(p^{\varepsilon(i)N} - p^{\varepsilon(i-1)N}\right), \tag{5.6}$$

so that it can be written as $\mathcal{N}(K,e,f) = e \cdot \Sigma_p(N,s)$.

If we ignore for a moment the dependence of $\mathcal{C}(F,e,f)$ on the group of p-power roots of the unit, we can count the number of isomorphism classes of extensions iterating on all the towers $L/F/K$ with F/K having ramification e' and inertia f', and L/F with ramification e'' and inertia f'', with $e'e'' = e$ and $f'f'' = f$. Indicating with $F^{e',f'}$ a "generic" extension with ramification e' and inertia f' over K, we obtain

$$\mathcal{I}(K,e,f) = \frac{1}{n} \sum_{\substack{f'f''=f \\ e'e''=e}} \phi(e''f'') \cdot \mathcal{N}(K,e',f') \cdot \mathcal{C}(F^{e',f'}, e'', f'')$$

$$= \frac{1}{f} \sum_{\substack{f'f''=f \\ e'e''=e \\ h'' \left| \left(p^{f_0 f'}-1\right)\right.}} \phi(h'')\phi(f'') \cdot \Sigma_p(n_0 e' f', s') \cdot \Pi_p(n_0 e' f', s'', \xi),$$

where in all the sum we always put $e' = p^{s'}h'$, $e'' = p^{s''}h''$ with $(p, h') = (p, h'') = 1$.

But unluckily the ξ describing the order of the group of p-power roots of the unity in our "generic" extension $F^{e',f'}$ is not well defined, and depends on the particular extension $F^{e',f'}/K$. If we start putting $\xi = 0$ while counting all the towers $L/F/K$, each factor $\Pi_p(\cdot,\cdot,0)$ should be corrected by a term $\Pi_p(\cdot,\cdot,1) - \Pi_p(\cdot,\cdot,0)$ for all towers with $F \supseteq K(\zeta_p)$, another correction term $\Pi_p(\cdot,\cdot,2) - \Pi_p(\cdot,\cdot,1)$ is required for all $F \supseteq K(\zeta_{p^2})$, and so on.

Consequently, let's define for convenience the quantity $\Delta_p(m, s, 0) = \Pi_p(m, s, 0)$, and $\Delta_p(m, s, i) = \Pi_p(m, s, i) - \Pi_p(m, s, i-1)$ for $i > 0$, that gives the main contribution and all the correction terms, and can be written explicitly as

$$\Delta_p(m, s, i) = \begin{cases} 1 & \text{if } s = i = 0, \\ (p^m - 1)p^{m(s-1)} & \text{if } s > i = 0, \\ (p-1)(p^m - 1)p^{m(s-1)+i-1} & \text{if } s > i > 0, \\ (p-1)p^{ms+s-1} & \text{if } s = i > 0, \\ 0 & \text{if } i > s. \end{cases} \tag{5.7}$$

Adding all correctiong terms for all tower where F contains all the various extension $K(\zeta_{p^i})$ for $i \leq s$, we have

Theorem 5.3.1. *The number of isomorphism classes of extensions with ramification e and inertia f of a field K of absolute degree $n_0 = [K : \mathbb{Q}_p]$ and absolute inertia $f_0 = f(K/\mathbb{Q}_p)$ is*

$$\mathcal{I}(K, e, f) = \frac{1}{f} \sum_{\substack{0 \leq i \leq s \\ f'f''f^{(i)}=f \\ e'e''e^{(i)}=e \\ h'' \left| \left(p^{f_0 f^{(i)} f'}-1\right)\right.}} \frac{\phi(h'')\phi(f'')}{e^{(i)}} \cdot \Sigma_p(N', s') \cdot \Delta_p(N', s'', i),$$

where Σ_p and Δ_p are respectively defined in the (5.6) *and* (5.7)*, we have put*

$$e^{(i)} = e(K(\zeta_{p^i})/K), \quad f^{(i)} = f(K(\zeta_{p^i})/K), \quad n^{(i)} = e^{(i)} f^{(i)},$$

and where throughout the sum (for all i, e', f', etc) we have put

$$N' = n_0 n^{(i)} e' f'$$

and

$$e = p^s h, \quad e' = p^{s'} h', \quad e'' = p^{s''} h''$$

with h, h', h'' all prime with p.

Remark 5.3.2. *When $s = 0$ (i.e. $p \nmid e$) the formula has the much simpler form*

$$\begin{aligned}\mathcal{I}(K,e,f) &= \frac{1}{f} \sum_{\substack{f'f''=f \\ e'e''=e \\ e'' \left| \left(p^{f_0 f'}-1\right)\right.}} \phi(f'') \cdot \phi(e'') \\ &= \frac{1}{f} \sum_{f'f''=f} \phi(f'') \cdot \left(e, p^{f_0 f'} - 1\right)\end{aligned}$$

because we are adding $\phi(e'')$ for all e'' that divide both e and $p^{f_0 f'} - 1$,

$$= \frac{1}{f} \sum_{i=0}^{f-1} \left(e, p^{f_0 (f',i)} - 1\right)$$

because each divisor f' of f appears precisely $\phi(f/f') = \phi(f'')$ times in the set of the (f,i) for $i = 0, \ldots, f-1$. This is precisely the formula obtained in [HK04, Remark 4.2, pag. 27] when $p \nmid e$.

With a computation similar to what done for Theorem 5.3.1, we obtain

Theorem 5.3.3. *The total number of isomorphism classes of extensions with degree n of a field K of absolute degree $n_0 = [K : \mathbb{Q}_p]$ and absolute inertia $f_0 = f(K/\mathbb{Q}_p)$ is*

$$\mathcal{I}(K,n) = \frac{1}{n} \sum_{\substack{0 \le i \le t \\ de'f'n^{(i)}=n}} e'\psi(k, p^{f_0 f^{(i)} f'} - 1) \cdot \Sigma_p(N', s') \cdot \Delta_p(N'+1, r, i),$$

where we are keeping the same notation as in Theorem 5.3.1, $\psi(u,v)$ is defined in the (5.4), p^t is the biggest power of p dividing n, and moreover throughout the sum we have written $d = p^r k$ with $(k,p) = 1$.

Chapter 6

Eisenstein polynomials generating p-extensions

In this chapter we explore the techniques that can be used to deduce necessary and sufficient conditions for a polynomial to have a certain Galois group as group of the splitting field over a $\mathfrak{p}$-adic field.

Lbekkouri gave in [Lbe09] congruence conditions for Eisenstein polynomials of degree p^2 with coefficients in the rational $\mathfrak{p}$-adic field $\mathbb{Q}_p$, and these conditions are satisfied if and only if the generated extension is Galois. Since the multiplicative group $U_{1,\mathbb{Q}_p}$ of 1-units of $\mathbb{Q}_p$ has rank 1 as $\mathbb{Z}_p$-module and in particular ${}^{U_{1,\mathbb{Q}_p}(\mathbb{Q}_p^\times)^p}/_{(\mathbb{Q}_p^\times)^p} \cong {}^{\mathbb{Z}}/_{p\mathbb{Z}}$, we have by local class field theory that every Galois totally ramified extension of degree p^2 over $\mathbb{Q}_p$ is cyclic, and consequently over $\mathbb{Q}_p$ the problem is reduced to finding conditions for Eisenstein polynomials of degree p^2 to generate a cyclic extension.

If the base field K is a proper extension of $\mathbb{Q}_p$ this is no longer true, so the restriction of considering polynomials that generate cyclic extensions has to be added explicitly. If K is ramified over $\mathbb{Q}_p$ even the characterization of the possible upper ramification breaks is a non-trivial problem (see [Mau71, Mik81]) and the problem seems to be very difficult for a number of other reasons, so we will only consider fields K that are finite unramified extensions over $\mathbb{Q}_p$, with residual degree $f = f(K/\mathbb{Q}_p) = [K : \mathbb{Q}_p]$. In this setting the problem is still tractable without being a trivial generalization of the case over $\mathbb{Q}_p$, and we will show a technique allowing to handle very easily the case of degree p^2.

During the proof the Artin-Hasse exponential function comes into play, and we use it to clarify the connection between the image of the norm map and the coefficients of the Eisenstein polynomial.

While some conditions are necessary to force the splitting field to be a p-extension, the remaining conditions can be tested in order, and the first that fails gives information on the Galois group of the splitting field. Taking into account another family of polynomials that can never provide a cyclic extension of degree p^2, we give a full classification of the polynomials of degree p^2 whose normal closure is a p-extension, providing a complete description of the Galois group of the normal closure with its ramification filtration. See Chapter 4 for a classification of the possible Galois groups.

We then show how the same methods apply to characterize Eisenstein polynomials of degree p^3 generating a cyclic extension. In this case the characterization is substantially more complicated, but the strategy used in degree p^2 can still be applied in a relatively straightforward way. It should be quite easy to apply the same methods to other abelian groups, and should even be possible to obtain a characterization for some non-abelian group.

In the last section we give a combinatorial interpretation of certain sums of roots of the unity appearing during the proof, it is actually much more than needed but it has some interest on its own.

The general strategy

We explain abstractly how our strategy works. Let K be a p-adic field that is unramified over $\mathbb{Q}_p$, so that p is a uniformizing element of K. Let $f(T)$ be an Eisenstein polynomial of degree n say, and π be a root. Let $L = K(\pi)$ be the extension by a root π over K.

Let G be an abelian group of order n. Then by local class field theory the extension L/K is Galois with group G if and only if $N_{L/K}(U_L)$ has index n in U_K, with quotient $U_K/N_{L/K}(U_L)$ isomorphic to G. When n is a power of p, the groups U_K and U_L can be replaced with the 1-units $U_{1,K}$ and $U_{1,L}$, so we are reduced to verifying that $U_{1,K}/N_{L/K}(U_{1,L})$ be isomorphic to G.

When G is a cyclic group of order p^k, it turns out that $N = N_{L/K}(U_{1,L})$ should have a special form. In particular it turns out that $U_{1,K}/N$ is cyclic of order p^k if and only if $N \cap U_{i,K}$ is contained in $1 + p^i V$, for all $1 \leq i \leq k$, and some $\mathfrak{p}_K \subseteq V \subseteq \mathcal{O}_k$ such that the reduction $V/\mathfrak{p}_K$ is a subspace of codimension 1 in κ_K as $\mathbb{F}_p$ vector space. A similar characterization is possible for general abelian p-groups, but here we will restrict to the case of cyclic group.

In particular $N \mod \mathfrak{p}_K^2$ is already sufficient to determine uniquely V. So after determining it, and testing whether it has codimension 1, we can just check that $N \cap U_{i,K} \subset 1 + p^i V$ for $2 \leq i \leq k$.

Now by the structure of the norm map over local fields (see §3.2.1, Chap. 3), we have that $j = \psi_{L/K}(k)$ is the biggest index such that $N_{L/K}(U_{j,L})$ is not identically contained in $U_{k+1,K}$, while $N_{L/K}(U_{j+1,L}) \subseteq U_{k+1,K}$. Since each condition has to be tested modulo $U_{k+1,K}$, we can just consider the subgroup of $U_{1,K}/U_{k+1,K}$ generated by elements $N_{L/K}(\alpha_m)$, for a set α_m of generators of $U_{1,L}/U_{j+1,L}$. If the generated group has the requested form, that is, each combination in $U_{i,K}$ turns out to be also in $1+p^i V$, then the extension is verified to be Galois with group G.

To do so, we can take as generators elements of the form $1 + \theta\pi^m$ with $(m, p) = 1$ and $\theta \in U_K$, and consider the group generated by their norms in $U_{1,K}/U_{k+1,K}$. Clearly $N_{K(\pi)/K}(1 + \theta\pi^m)$ can be expressed as function of the coefficients of the minimal polynomial of $f(T)$, so it is possible to translate the constraints on the structure of $N/U_{k,K}$ into conditions on the coefficients of $f(T)$.

Now $N_{K(\pi)/K}(1+\theta\pi^m)$ will have a certain expression in terms of the coefficients. Let $E(x)$ be the Artin-Hasse exponential function, then the $E(\theta\pi^m)$ give also a set of generators of $U_{1,L}/U_{j+1,L}$, and it turns out that their norms can be written really easily in terms of the coefficients of $f(T)$. So if $N_{K(\pi)/K}(1+\theta\pi^m)$ has a complicated expression, it is only because $1+\theta\pi^m$ is a complicated product of elements of the form $E(\eta\pi^\ell)$. Passing to the norms of the $E(\theta\pi^m)$, we decompose the terms appearing in $N_{K(\pi)/K}(1+\theta\pi^m)$, and the condition on the coefficients of $f(T)$ can be expressed easily.

We describe now how it is possible to extend this information to classify completely the polynomials of degree p^2 whose splitting field is p-extension. In degree p^2, some condition on the coefficients for having a cyclic extension is clearly related to the request that L/K be decomposable in a double cyclic extension, that is, we need the existence of an intermediate extension F such that L/F and F/K are cyclic of degree p.

This condition is verified if an only if the Galois closure is a p-extension, and the group of the normal closure $\tilde{L}$ is characterized uniquely by the length of $\mathrm{Gal}(\tilde{L}/F)$ as $\mathrm{Gal}(F/K)$-module, and by its exponent (see Prop. 2.2.1, Chap. 2). If K is unramified over $\mathbb{Q}_p$, it turns out that the ramification breaks can be equal to those of a cyclic extension of degree p^2 if and only if the exponent of $\mathrm{Gal}(\tilde{L}/K)$ is p^2. Furthermore, after requesting $N \cap U_{1,K} \subseteq 1+pV$, the other conditions on the coefficients allow to recover the biggest i (if any) such that the condition $N_{L/K}(U_{i,L}) \cap U_{2,K} \subseteq 1+p^2V$ fails. This i can be related to the length of $\mathrm{Gal}(\tilde{L}/F)$, applying the functorial properties of the reciprocity map.

When L has a suitable intermediate extension but the ramification breaks do not coincide with those of a cyclic extension then the problem turns out to be slightly easier, because $\mathrm{Gal}(\tilde{L}/K)$ is always a semidirect product, and the ramification data give almost complete information about the group. In this way we obtain a characterization of all polynomials of degree p^2 whose Galois group is a p-group.

6.1 Preliminaries

Let K be a $\mathfrak{p}$-adic field. As usual we will denote with $[K^\times]_K$ the group of p-th power classes ${}^{K^\times}\!/_{(K^\times)^p}$. For integers a, b, we will denote by $[\![a,b]\!]$ the set of integers $a \leq i \leq b$ such that $(i,p)=1$.

We start computing modulo which power of p we must consider the coefficients of an Eisenstein polynomial (this computation is very well known, see [Kra62] for example): let $f(X)=\sum_{i=0}^n f_{n-i}X^i$ and $g(X)=\sum_{i=0}^n g_{n-i}X^i$ be Eisenstein polynomials of degree n say, ρ a root of g, $\pi=\pi_1,\pi_2,\dots$ the roots of f with π the most near to ρ, and put $L=K(\pi)$. Let v be the biggest lower ramification break and $\mathscr{D}_f = f'(\pi)$ be the different, if

$$\left|(f_{n-i}-g_{n-i})\pi^i\right| < \left|\pi^{v+1}\mathscr{D}_f\right|$$

then being

$$f(\rho) = f(\rho) - g(\rho) = \sum_{i=0}^{n} (f_{n-i} - g_{n-i})\,\rho^i$$

we obtain $|f(\rho)| < |\pi^v \mathscr{D}_f|$. We have

$$\left|(\rho - \pi) \cdot \prod_{i=2}^{n}(\pi - \pi_i)\right| \le \left|\prod_{i=1}^{n}(\rho - \pi_i)\right| < \left|\pi^{v+1}\mathscr{D}_f\right|,$$

in fact $|\pi - \pi_i| \le |\rho - \pi_i|$ for $i \ge 2$ or we would contradict the choice of $\pi = \pi_1$. Consequently $|\rho - \pi| < |\pi^{v+1}|$, which is equal to the minimum of the $|\pi - \pi_i|$, and hence $K(\rho) \subseteq K(\pi)$ by Krasner's lemma, and $K(\rho) = K(\pi)$ having the same degree.

Let now K be unramified over $\mathbb{Q}_p$, then $U_{1,K}^{p^i} = U_{i+1,K}$, and consequently by local class field theory the upper ramification breaks of a cyclic p-extension are $1, 2, 3, \ldots$, and the lower ramification breaks are $1, p+1, p^2+p+1, \ldots$.

For an extension of degree p^k with lower ramification breaks $t_0 \le t_1 \le \cdots \le t_{k-1}$ we can compute $v_L(\mathscr{D}_{L/K})$ as $\sum_{i=1}^{k}(p^i - p^{i-1})t_{k-i}$, which for a cyclic L/K of degree p^2 or p^3 is $3p^2 - p - 2$ (resp. $4p^3 - p^2 - p - 2$), while $v_L(\pi^{v+1}\mathscr{D}_{L/K})$ is respectively $3p^2 = v_L(p^3)$ and $4p^3 = v_L(p^4)$. Hence we obtain the condition on the precision of the coefficients, that we state in a proposition for convenience:

Proposition 6.1.1. *Let L/K be a totally ramified cyclic extension of degree $n = p^2$ (resp. $n = p^3$) determined by the Eisenstein polynomial $f(X) = \sum_{i=0}^{n} f_{n-i}X^n$. Then the lower ramification breaks are $1, p+1$ (resp. $1, p+1, p^2+p+1$), $v_L(\mathscr{D}_{L/K})$ is equal to $3p^2 - p - 2$ (resp. is $4p^3 - p^2 - p - 2$), and the extension is uniquely determined by the classes of $f_n \pmod{p^4}$ and $f_i \pmod{p^3}$ for $0 \le i < n$ (resp. by the classes of $f_n \pmod{p^5}$ and $f_i \pmod{p^4}$ for $0 \le i < n$, for $n = p^3$).*

6.1.1 Additive polynomials

We will need a few facts about additive polynomials, and in particular some formulæ to express in terms of the coefficients the condition that an additive polynomial has range contained in the range of some other additive polynomial. We resume what we need in the following

Proposition 6.1.2. *Let $A(Y) = a_pY^p + a_1Y$ be an additive polynomial in $\kappa_K[Y]$ such that $A'(0) \neq 0$ and all the roots of $A(Y)$ are in κ_K, and let $B(Y) = b_pY^p + b_1Y$, $C(Y) = c_{p^2}Y^{p^2} + c_pY^p + c_1Y$ and $D(Y) = d_{p^3}Y^{p^3} + d_{p^2}Y^{p^2} + d_pY^p + d_1Y$ be any three other additive polynomials in $\kappa_K[Y]$. Then*

- *$B(\kappa_K) \subseteq A(\kappa_K)$ if and only if $b_p = a_p({}^{b_1}/{}_{a_1})^p$, and in this case $B(Y)$ is equal to $A({}^{b_1}/{}_{a_1}Y)$,*
- *$C(\kappa_K) \subseteq A(\kappa_K)$ if and only if $c_p = a_p({}^{c_1}/{}_{a_1})^p + a_1({}^{c_{p^2}}/{}_{a_p})^{1/p}$, and in this case $C(Y)$ can be written as $A(\beta Y^p + {}^{c_1}/{}_{a_1}Y)$ with $\beta = ({}^{c_{p^2}}/{}_{a_p})^{1/p}$ or equivalently $\beta = {}^{c_p}/{}_{a_1} - {}^{a_p}/{}_{a_1}({}^{c_1}/{}_{a_1})^p$.*

- $D(\kappa_K) \subseteq A(\kappa_K)$ *if and only if* $a_1/a_p(d_{p^3}/a_p)^{1/p} + (d_p/a_1)^p = d_{p^2}/a_p + (a_p/a_1)^p(d_1/a_1)^{p^2}$.

Note that being κ_K finite and hence perfect the map $x \mapsto x^p$ is an automorphism, and we just denote by $x \mapsto x^{1/p}$ the inverse automorphism.

Proof. Since $A'(0) \neq 0$ and all the roots of $A(Y)$ are in κ_K we have from the theory of additive polynomials (see [FV02, Chap. 5, §2, Corollary 2.4]) that if $B(\kappa_K) \subseteq A(\kappa_K)$ then $B(Y) = A(G(Y))$ for some other additive polynomial $G(Y)$, which should be linear considering the degrees, $G(Y) = \alpha Y$ say. Consequently it has to be $B(Y) = a_p\alpha^p Y^p + a_1\alpha Y$, and comparing the coefficients we obtain that $\alpha^p = (b_1/a_1)^p$ and should also be equal to b_p/a_p. Similarly if $C(\kappa_K) \subseteq A(\kappa_K)$ we should have

$$C(Y) = A(\beta Y^p + \alpha Y) = a_p\beta^p Y^{p^2} + (a_p\alpha^p + a_1\beta)Y^p + a_1\alpha Y,$$

and we deduce $\alpha = c_1/a_1$, $\beta^p = c_{p^2}/a_p$, and we obtain the condition substituting α, β in $c_p = a_p\alpha^p + a_1\beta$. If $D(\kappa_K) \subseteq A(\kappa_K)$ then $D(Y)$ should be $A(\gamma Y^{p^2} + \beta Y^p + \alpha Y)$ and hence

$$a_p\gamma^p Y^{p^3} + (a_p\beta^p + a_1\gamma)Y^{p^2} + (a_p\alpha^p + a_1\beta)Y^p + a_1\alpha Y,$$

$\alpha = d_1/a_1$, $\gamma = (d_{p^3}/a_p)^{1/p}$, and β^p can be written in two different ways as

$$d_{p^2}/a_p - a_1/a_p(d_{p^3}/a_p)^{1/p} = (d_p/a_1 - a_p/a_1(d_1/a_1)^p)^p.$$

The condition is clearly also sufficient. □

The following proposition will also be useful, it gives a criterion to verify if the splitting field of an additive polynomial of degree p^2 is a p-extension (that is, either trivial of cyclic of degree p) that is slightly easier to test than the condition itself.

Proposition 6.1.3. *Let* $A(Y) = Y^{p^2} + aY^p + bY$ *be an additive polynomial in* $\kappa_K[Y]$*, than the splitting field is a* p*-extension over* κ_K *precisely when* $A(Y)$ *has a root in* $\kappa_K^\times$*, and* $b \in (\kappa_K^\times)^{p-1}$.

Proof. If the Galois group is a p-group then its orbits have cardinality divisible by p and the action on the roots of $A(Y)$ should clearly have some fixed point other than 0, $\eta \in \kappa_K^\times$ say. If $\beta = \eta^{p-1}$ then the roots of $Y^p - \beta Y$ are roots of $A(Y)$, so by [FV02, Chap. 5, §2, Prop. 2.5] $A(Y)$ is $B(Y^p - \beta Y)$ for some additive polynomial $B(Y)$, which has to be monic too, $B(Y) = Y^p - \alpha Y$ say. The roots of $B(Y)$ have to be in κ_K or it, and hence $A(Y)$, would generate an extension of order prime with p, and consequently α has to be in $(\kappa_K^\times)^{p-1}$, and $b = \alpha\beta$ as well. On the other hand if a root η is in κ_K we can write $A(Y) = B(Y^p - \beta Y)$ for $\beta = \eta^{p-1}$, and replacing Y by ηZ we can consider $B(\eta^p(Z^p - Z))$, and the extension is obtained as an Artin-Schreier extension over the extension determined by $B(Y)$. Consequently we only need the extension determined by $B(Y)$ to be trivial, and this condition is verified when $b \in (\kappa_K^\times)^{p-1}$. □

6.1.2 Sum of roots of the unity

Let ζ_ℓ be a primitive ℓ-th root of the unity for some ℓ, we define for each tuple $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_r)$ of r integers the sum

$$\Sigma_\lambda(\ell) = \sum_{\iota=(\iota_1,\dots,\iota_r)} \zeta_\ell^{\iota_1\lambda_1+\iota_2\lambda_2+\cdots+\iota_r\lambda_r},$$

where the sum ranges over all the r-tuples $\iota = (\iota_1, \dots, \iota_r)$ such that $0 \le \iota_i \le \ell-1$ for each i, and the ι_i are all distinct.

We deduce some property of the sums $\Sigma_\lambda(\ell)$ to help expanding the expressions that will appear. For each $\lambda = (\lambda_1, \lambda_2, \dots)$ and integer k put $k\lambda$ for the partition $(k\lambda_1, k\lambda_2, \dots)$. For integers ℓ, k, m let's define the functions

$$\delta_{\ell,k}^{[m]} = \begin{cases} \ell & \text{if } \ell \ge m \text{ and } \ell \mid k, \\ 0 & \text{in any other case,} \end{cases}$$

and put $\delta_{\ell,k} = \delta_{\ell,k}^{[1]}$ for short. Then we have

Proposition 6.1.4. *Assume $(\ell, p) = 1$, $\ell > 1$. For any partition λ we have $\Sigma_{p\lambda}(\ell) = \Sigma_\lambda(\ell)$. For $k \ge 1$ we have $\Sigma_{(k)}(\ell) = \delta_{\ell,k}$, and $\Sigma_{(k,1)}(\ell) = \delta_{\ell,k+1}^{[2]}$, and if $(k, p) = 1$ we also have $\Sigma_{(k,p)}(\ell) = \delta_{\ell,k+p}^{[2]}$ and $\Sigma_{(k,p^2)}(\ell) = \delta_{\ell,k+p^2}^{[2]}$. We also have $\Sigma_{(1,1,1)}(\ell) = \delta_{\ell,3}^{[3]}$, $\Sigma_{(p,1,1)}(\ell) = \delta_{\ell,p+2}^{[3]}$ and $\Sigma_{(p,p,1)}(\ell) = \delta_{\ell,2p+1}^{[3]}$.*

The proof can be obtained via an easy computation, but we omit it being also an immediate consequence of the more general Lemma 6.5.1 proved in the last section.

6.2 Polynomials of degree p^2 generating a cyclic extension

Since the different $f'(\pi)$ has valuation $3p^2 - p - 2$ it must come from a term $f_{p+1}X^{p^2-p-1}$ with $v_p(f_{p+1}) = 2$, and we must have $v_p(f_i) \ge 2$ for all $(i, p) = 1$, and $v_p(f_i) \ge 3$ if furthermore $i > p + 1$.

Since the first break is at 1, the p-th coefficient of the ramification polynomial $f(X + \pi)$ needs to have valuation exactly equal to $(p^2 - p) \cdot 2 = 2p^2 - 2p$, and observe that a monomial $f_{p^2-i}(X + \pi)^i$ contributes at most one term $\binom{i}{p} f_{p^2-i}\pi^{i-p}X^p$ in X^p. The valuations of these terms have different remainders modulo the degree p^2, and consequently the minimal valuation of the $\binom{i}{p} f_{p^2-i}\pi^{i-p}$ has to be $2p^2 - 2p$, is achieved for $i = p^2 - p$ and we must have $v_p(f_p) = 1$, while $v_p(f_{pk}) \ge 2$ for all $2 \le k \le p - 1$.

So we have to respect the following

Condition 6.2.1. *We must have*

- *$v_p(f_p) = 1$, and $v_p(f_{pi}) \ge 2$ for $i \in [\![2, p-1]\!]$,*

- $v_p(f_i) \geq 2$ *for* $i \in [\![1, p-1]\!]$, $v(f_{p+1}) = 2$ *and* $v_p(f_i) \geq 3$ *for* $i \in [\![p+2, p^2-1]\!]$.

In other words, turning to 0 all the f_i divisible by p^3 for $i \neq p^2$, that we are allowed to do by Prop. 6.1.1, $f(X)$ can be written as

$$f(X) = X^{p^2} + \underbrace{f_p X^{p^2-p} + f_{p^2}}_{\overset{\Cap}{p\mathcal{O}[X]}} + \underbrace{\sum_{j\in[\![2,p-1]\!]} f_{pj} X^{p^2-pj} + \sum_{k\in[\![1,p+1]\!]} f_k X^{p^2-k}}_{\overset{\Cap}{p^2\mathcal{O}[X]}} . \qquad (6.1)$$

Suppose now that L is an arbitrary extension determined by a root π of the polynomial $f(X)$, by local class field theory it is a totally ramified abelian extension precisely when $N_{L/K}(L^\times) \cap U_{1,K} = N_{L/K}(U_{1,L})$ has index p^2 in $U_{1,K}$ and the corresponding quotient is cyclic.

Being $U_{i+1,K} = U_{1,K}^{p^i}$ for $i \geq 1$, to have a cyclic extension $N_{L/K}(U_{1,L})U_{2,K}$ shall have index p in $U_{1,K}$, and $N_{L/K}(U_{1,L}) \cap U_{2,K}$ index p in $U_{2,K}$.

Let's recall that for each $i \geq 0$ we have a natural map $(\times p) : {}^{\mathfrak{p}_K^i}/_{\mathfrak{p}_K^{i+1}} \to {}^{\mathfrak{p}_K^{i+1}}/_{\mathfrak{p}_K^{i+2}}$ induced by multiplication by p, and for $i \geq 1$ being $(1 + \theta p^i)^p \equiv 1 + \theta p^{i+1} + \ldots$ we have a natural map $(\uparrow p) : {}^{U_{i,K}}/_{U_{i+1,K}} \to {}^{U_{i+1,K}}/_{U_{i+2,K}}$ induced by taking p-th powers and a commutative diagram

$$\begin{tikzcd}
{}^{\mathfrak{p}_K^i}/_{\mathfrak{p}_K^{i+1}} \arrow[r, "\times p"] \arrow[d, "\mu_i"'] & {}^{\mathfrak{p}_K^{i+1}}/_{\mathfrak{p}_K^{i+2}} \arrow[d, "\mu_{i+1}"'] \\
{}^{U_{i,K}}/_{U_{i+1,K}} \arrow[r, "\uparrow p"] & {}^{U_{i+1,K}}/_{U_{i+2,K}}
\end{tikzcd} \qquad (6.2)$$

where μ_i is induced by $x \mapsto 1 + x$.

So $N_{L/K}(U_{1,L}) \cap U_{2,K}$ will certainly contain $N_{L/K}(U_{1,L})^p U_{3,K}$, which has index p in $U_{2,K}$, and consequently has to be equal to it. For L/K to be Galois cyclic we need

$$N_{L/K}(U_{1,L}) \subseteq 1 + pV, \qquad N_{L/K}(U_{1,L}) \cap U_{2,K} \subseteq 1 + p^2 V \qquad (6.3)$$

for some $\mathbb{F}_p$-subspace V of ${}^{\mathcal{O}_K}/_{\mathfrak{p}_K}$ of codimension 1. Note that V is uniquely determined by $N_{L/K}(U_{1,L})U_{2,K}$ as a subgroup of $U_{1,L}$, we commit the abuse of denoting also as V its preimage in $\mathcal{O}_L$, and the meaning of the expressions $1 + p^i V$ should be clear.

If $i \geq 1$ then $N_{L/K}(U_{i+1,L}) \subseteq U_{\phi_{L/K}(i)+1,K}$ (see [FV02, Chap. 3, §3.3 and §3.4]), and in our case we have $N_{L/K}(U_{2,L}) \subseteq U_{2,K}$ and $N_{L/K}(U_{p+2,L}) \subseteq U_{3,K}$.

Consequently we can prove that L/K is Galois by showing that the norms of elements whose images generate ${}^{U_{1,L}}/_{U_{2,L}}$ are contained in $1 + pV$ for some V, and that for any x obtained as combination of a set of elements whose images generate ${}^{U_{1,L}}/_{U_{p+2,L}}$, and such that $N_{L/K}(x) \in U_{2,K}$, we actually have $N_{L/K}(x) \in 1 + p^2 V$. We will take as generators the elements of the form $(1 - \theta\pi^\ell)$

for $\ell \in [\![1, p+1]\!]$, plus those of the forms $(1-\theta\pi)^p$ for θ in the set of multiplicative representative. Those of the form $(1-\theta\pi)^p$ can be discarded considering that we are already requesting $N_{L/K}(1-\theta\pi) \in 1+pV$, so their norm will certainly be in $1+p^2V$.

The norm of an element of the form $1-\theta\pi^\ell$ can be expressed as

$$N_{L/K}(1-\theta\pi^\ell) = \prod_{\pi_i | f(\pi_i)=0} (1-\theta\pi_i^\ell) = \mathrm{Res}_X(1-\theta X^\ell, f(X)),$$

where π_i are the roots of $f(X)$ and we denote by Res_X the resultant in X.

For a polynomial $a(X)$ of degree d let's denote by $\tilde{a}(X)$ the conjugate polynomial $X^d a(X^{-1})$. Then for each pair of polynomials $a(X), b(X)$ we have $Res_X(a(X), b(X)) = Res_X(\tilde{b}(X), \tilde{a}(X))$.

Consequently $N_{L/K}(1-\theta\pi^\ell)$ can also we written as

$$\mathrm{Res}_X(\tilde{f}(X), X^\ell - \theta) = \prod_{i=0}^{\ell-1} \tilde{f}(\zeta_\ell^i \theta^{1/\ell})$$

for some primitive ℓ-th root of the unity. In the expansion of the second term only integral powers of θ appear being invariant under the substitution $\theta^{1/p} \to \zeta_\ell \theta^{1/\ell}$. In the same way while the terms in the right hand side live in $K(\zeta_\ell)$ the result always lives in K, and the above expansion should be rather considered as a combinatorial expedient.

Put $T = \theta^{1/\ell}$ and consider it as an indeterminate, from the expression for $f(X)$ in the (6.1) we have that $N_{L/K}(1-\theta\pi^\ell)$ is

$$\prod_{i=0}^{\ell-1}\left(1 + \underbrace{f_p\zeta_\ell^{ip}T^p + f_{p^2}\zeta_\ell^{ip^2}T^{p^2}}_{\in\, \mathfrak{p}_K} + \underbrace{\sum_{j\in[\![2,p-1]\!]} f_{pj}\zeta_\ell^{ipj}T^{pj} + \sum_{k\in[\![1,p+1]\!]} f_k\zeta_\ell^{ik}T^k}_{\in\, \mathfrak{p}_K^2}\right).$$

For each tuple $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_r)$ of r integers put $f_\lambda T^{|\lambda|}$ for the term $\prod_{i=1}^r f_{\lambda_i}T^{\lambda_i}$ of the expansion. For each $k \geq 0$ let $m_k(\lambda)$ denote the number of parts λ_i equal to k. Then the coefficient of $f_\lambda T^{|\lambda|}$ in the expression can be computed over all the ways we can partitioning the $1, \zeta_\ell, \zeta_\ell^2, \dots$ in sets of cardinality $m_k(\lambda)$. Computing the ratio to the ordered choices of r distinct elements, which is the collection over which we are iterating while computing $\Sigma_\lambda(\ell)$, we have that the coefficient of $f_\lambda T^{|\lambda|}$ in the expansion is $\frac{1}{\prod_{k\geq 1} m_k(\lambda)!} \cdot \Sigma_\lambda(\ell)$.

In particular, discarding the terms with valuation ≥ 3 and subtracting 1, we have that the above product can be expanded modulo p^3 as

$$\mathfrak{p}_K \ni \Big[\qquad \Sigma_{(p)}(\ell) \cdot f_p T^p + \Sigma_{(p^2)}(\ell) \cdot f_{p^2} T^{p^2}$$

$$\mathfrak{p}_K^2 \ni \left[\begin{array}{l} +\frac{1}{2}\Sigma_{(p,p)}(\ell)\cdot f_p^2T^{2p} + \Sigma_{(p^2,p)}(\ell)\cdot f_pf_{p^2}T^{p^2+p} + \frac{1}{2}\Sigma_{(p^2,p^2)}(\ell)\cdot f_{p^2}^2T^{2p^2} \\ \qquad + \sum\limits_{j\in[\![2,p-1]\!]} \left(\Sigma_{(pj)}(\ell)\cdot f_{pj}T^{pj}\right) + \sum\limits_{k\in[\![1,p+1]\!]} \left(\Sigma_{(k)}(\ell)\cdot f_kT^k\right), \end{array}\right.$$

which applying Prop. 6.1.4 can be rewritten as

$$\begin{array}{l} \mathfrak{p}_K \ni \left[\qquad \delta_{\ell,1}f_pT^p + \delta_{\ell,1}f_{p^2}T^{p^2} \right. \\ \mathfrak{p}_K^2 \ni \left[\begin{array}{l} -\frac{1}{2}\delta_{\ell,2}^{[2]}f_p^2T^{2p} - \delta_{\ell,p+1}^{[2]}f_pf_{p^2}T^{p^2+p} - \frac{1}{2}\delta_{\ell,2}^{[2]}f_{p^2}^2T^{2p^2} \\ \qquad + \sum\limits_{j\in[\![2,p-1]\!]} \delta_{\ell,j}f_{pj}T^{pj} + \sum\limits_{k\in[\![1,p+1]\!]} \delta_{\ell,k}f_kT^k. \end{array}\right. \end{array} \tag{6.4}$$

The expansion for $\ell = 1$ and modulo p^2 tells us that the norms in $U_{1,K}$ are of the form $1 + f_pT^p + f_{p^2}T^{p^2} + \mathcal{O}(p^2)$ for some T, consequently put $F_p = \overline{f_p/p}$, $F_{p^2} = \overline{f_{p^2}/p}$ and consider the additive polynomial

$$A(Y) = F_{p^2}Y^p + F_pY \tag{6.5}$$

over the residue field. It defines a linear function, if V is the range $A(\kappa_K)$ then $N_{L/K}(U_{1,L})U_{2,K}$ is contained in $1 + pV$, and V has codimension 1 precisely when the map defined by A has a kernel of dimension 1, that is when $-F_p/F_{p^2}$ is a $(p-1)$-th power (if $K = \mathbb{Q}_p$ we shall have $V = 0$ and the condition is $F_{p^2} = -F_p$).

Condition 6.2.2. *We must have* $-F_p/F_{p^2} \in \kappa_K^{p-1}$.

Now for $\ell \geq 2$ the first part of the expansion (6.4) is 0, while the remaining part shall be contained in p^2V for each ℓ and each specialization of $T^\ell = \theta$.

Note that we only consider the ℓ prime with p, and all the $\delta_{\ell,i}^{[m]}$ appearing for some m, i have been reduced with no loss of generality to have $(i,p) = 1$. Consequently for $\ell \geq 2$ the expansion can be written as a polynomial $C_\ell(T^\ell) = \ell\sum_{(k,p)=1} c_{k\ell}(T^{k\ell})$, where for each ℓ prime with p we denote by $c_\ell(T^\ell)$ the polynomial of T^ℓ obtained by the evaluating equation (6.4), but changing the definition of $\delta_{a,b}^{[m]}$ to be 1 if $a = b$, and 0 if $a \neq b$.

Fix ℓ, then $c_\ell(T^\ell)$ can be obtained via a sort of Möbius inversion

$$\begin{aligned} \sum_{(k,p)=1} \mu(k)\frac{C_{k\ell}(T^{k\ell})}{k\ell} &= \sum_{(k,p)=1} \left(\mu(k)\cdot \sum_{(j,p)=1} c_{jk\ell}(T^{jk\ell})\right) \\ &= \sum_{(i,p)=1} \left(c_{i\ell}(T^{i\ell})\cdot \sum_{k|i}\mu(k)\right) \end{aligned}$$

by change of variable $i = jk$, obtaining $c_\ell(T^\ell)$ by the properties of the Möbius function μ. In view of the isomorphism $\mathfrak{p}_K^2/\mathfrak{p}_K^3 \to U_{2,K}/U_{3,K}$ induced by $x \mapsto 1+x$

and specializing the argument $T^{k\ell}$ of $C_{k\ell}(T^{k\ell})$ to $\theta' = \frac{1}{\ell}\theta^k$ we have that

$$1 + \frac{1}{k\ell} C_{k\ell}(\theta^k) \equiv N_{L/K}\left(1 - \frac{1}{\ell}\theta^k \pi^{k\ell}\right)^{1/k} \pmod{p^3},$$

for each ℓ, k prime with p and each $\theta = T^\ell$. Consequently $1 + c_\ell(\theta)$ is congruent modulo p^3 to the norm of

$$\prod_{(k,p)=1} \left(1 - \frac{1}{\ell}\theta^k \pi^{k\ell}\right)^{\mu(k)/k} \equiv E(\theta\pi^\ell) \pmod{\mathfrak{p}_K^3},$$

where $E(x)$ is the Artin-Hasse exponential function (in its original form, according to [FV02, Chap. 3, §9.1]). Note that we can equivalently require all the $N_{L/K}(E(\theta\pi^\ell))$ to be in $1 + p^2 V$, for $\ell \in [\![2, p+1]\!]$ and $\theta \in U_K$.

Put $A_\ell(Y) = \overline{c_\ell(Y)/p^2}$, we obtain depending on ℓ the additive polynomials

$$\begin{aligned} -F_p F_{p^2} Y^p + G_{p+1} Y & \qquad \ell = p+1, \\ G_{p\ell} Y^p + G_\ell Y & \qquad \ell \in [\![3, p-1]\!], \\ -\frac{1}{2} F_{p^2}^2 Y^{p^2} + \left(G_{2p} - \frac{1}{2} F_p^2\right) Y^p + G_2 Y & \qquad \ell = 2, \end{aligned}$$

where for convenience we have put $G_i = \overline{f_i/p^2}$ for each $i \neq p, p^2$.

Hence we have obtained the

Condition 6.2.3. *For each $\ell \in [\![2, p+1]\!]$ we shall have $A_\ell(\kappa_K) \subseteq A(\kappa_K)$.*

We are left to ensure that norms are in $1 + p^2 V$, when taking $\ell = 1$ and $T = \theta$ for some θ such that $\theta^{p^2-p} \equiv -f_p/f_{p^2} \pmod{p}$. Consider again the (6.4), considering the definition of the $c_k(T)$ we have that $\sum_{(k,p)=1} c_k(T^k)$ differs from $C_1(T) = N_{L/K}(1 - T\pi) - 1$ by the extra term

$$-\frac{1}{2} f_p^2 T^{2p} - f_p f_{p^2} T^{p^2+p} - \frac{1}{2} f_{p^2}^2 T^{2p^2} = -\frac{1}{2}\left(f_p T^p + f_{p^2} T^{p^2}\right)^2,$$

which is however even contained in $\mathfrak{p}^4$ for $T = \theta$. Since we already required the polynomials $c_k(Y^k)$ to take values in $p^2 V$ identically for $k \geq 2$, our requirement becomes that

$$c_1(\theta) = f_{p^2}\theta^{p^2} + f_p \theta^p + f_1 \theta$$

shall be contained in $p^2 V$ too. Hence we have the

Condition 6.2.4. *Let θ be such that $\theta^{p^2-p} \equiv -f_p/f_{p^2} \pmod{p}$, then we must have $\overline{c_1(\theta)/p^2} \in V$.*

Collecting all the above conditions, and applying Prop. 6.1.2 to obtain conditions on the coefficients, we have the following theorem.

Theorem 6.2.5. *The Eisenstein polynomial $f(X) = X^{p^2} + f_1 X^{p^2-1} + \cdots + f_{p^2-1} X + f_{p^2}$ determines a Galois extension of degree p^2 over K if and only if*

1. *$v_p(f_p) = 1$, and $v_p(f_{pi}) \geq 2$ for $i \in [\![2, p-1]\!]$,*
2. *$v_p(f_i) \geq 2$ for $i \in [\![1, p-1]\!]$, $v(f_{p+1}) = 2$ and $v_p(f_i) \geq 3$ for $i \in [\![p+2, p^2 - 1]\!]$,*

putting $F_p = \overline{{}^{f_p}/_{p}}$, $F_{p^2} = \overline{{}^{f_{p^2}}/_{p}}$, and $G_i = \overline{{}^{f_i}/_{p^2}}$ for all $i \neq p, p^2$ we have

3. *$-{}^{F_p}/_{F_{p^2}} \in \kappa_K^{p-1}$,*
4. *$G_{p+1}^p = -F_p^{p+1}$,*
5. *$G_{p\ell} = F_{p^2} \left({}^{G_\ell}/_{F_p}\right)^p$, for all $\ell \in [\![3, p-1]\!]$,*
6. *$G_{2p} = F_{p^2} \left({}^{G_2}/_{F_p}\right)^p + \frac{1}{2} F_p \left(F_p - F_{p^2}^{1/p}\right)$,*

if θ is such that $\bar{\theta}^{p(p-1)} = -{}^{F_p}/_{F_{p^2}}$ we have that (for any choice of θ)

7. *$F_{p^2} X^p + F_p X - \overline{\frac{1}{p^2}\left(f_{p^2}\theta^{p^2} + f_p\theta^p\right)} - G_1\bar{\theta}$ has a root in κ_K.*

6.3 Polynomials of degree p^2 whose Galois group is a p-group

In the proof of Theorem 6.2.5 we obtained a list of requirements on an Eisenstein equation of degree p^2 that guarantee that the generated extension is Galois cyclic over K. Let's keep the hypotheses on the ramification numbers (and consequently conditions 1 and 2 of the theorem), it is a natural question to describe the Galois group of the normal closure when some of these hypotheses are not satisfied.

Put $L = K(\pi)$, we will also keep the condition 3, which we can see immediately to be satisfied if and only if L contains a Galois extension of degree p of K, which is a necessary condition for the normal closure of L/K to be a p-group. Note that this hypothesis is always satisfied for $f(X)$ if K is replaced with a suitable unramified extension.

We can notice from the proof that the first unsatisfied requirement among the conditions 4, 5 with ℓ as big as possible, 6 and 7 in Theorem 6.2.5 gives us information about the biggest possible ℓ such that $N_{L/K}(U_{\ell,L}) \cap U_{2,K}$ is not contained in $1 + p^2 V$, with V defined as in the proof. We expect this fact to allow us to deduce information about the Galois group of the normal closure.

Let F be the Galois extension of degree p of K contained in L, it is unique or $\mathrm{Gal}(L/K)$ would be elementary abelian, which is not possible considering the ramification breaks. Then F/K has ramification number 1 and L/F ramification number $p+1$.

Before continuing we prove a proposition that will also be of use later, and where we only assume that L/F has ramification break > 1 and F/K to be Galois with break at 1, with group generated by σ say. Similarly we have that the only f_i with $v_p(f_i) = 1$ are f_p and f_{p^2}. For some $\theta \in K$ we can write

$$\pi_F^{(\sigma-1)} = 1 - \theta^p \pi_F + \ldots$$

$$= N_{L/F}(1-\theta\pi) + \mathcal{O}(\pi_F^2)$$

in view of §3.2.1, Chap. 3, and having L/F ramification break > 1. Since $\pi_F^{(\sigma-1)}$ is killed by $N_{F/K}$ and $N_{F/K}(U_{2,F}) \subseteq U_{2,K}$ we should have $N_{L/K}(1-\theta\pi) \in U_{2,K}$ and hence $\bar{\theta}^{p(p-1)} = -{}^{F_p}/{}_{F_{p^2}}$, as we have expanding $\tilde{f}(\theta) = N_{L/F}(1-\theta\pi)$ like in the proof of Theorem 6.2.5.

We obtain inductively that

Proposition 6.3.1. *For each $1 \leq \ell < p$ we have*

$$\pi_F^{(\sigma-1)^\ell} = 1 - k\theta^{p\ell}\pi_F^\ell + \dots,$$

for some integer k prime with p, where $\bar{\theta}^{p(p-1)} = -{}^{F_p}/{}_{F_{p^2}}$.

We return to our main problem, so let L/F have ramification break at $p+1$. We require L/F to be Galois: by local class field theory this is the case precisely when the map ${}^{U_{p+1,L}}/{}_{U_{p+2,L}} \to {}^{U_{p+1,F}}/{}_{U_{p+2,F}}$ induced by $N_{L/F}$ is not surjective. Since the map ${}^{U_{p+1,F}}/{}_{U_{p+2,F}} \to {}^{U_{2,K}}/{}_{U_{3,K}}$ induced by $N_{F/K}$ is an isomorphism by §3.2.1, Chap. 3, we are reduced to study the image of ${}^{U_{p+1,L}}/{}_{U_{p+2,L}}$ in ${}^{U_{2,K}}/{}_{U_{3,K}}$. Considering the norms of the usual $1+\theta\pi^{p+1}$, we have from the proof of Theorem 6.2.5 that this map is described by the additive polynomial $A_{p+1}(Y)$, and is non-surjective precisely when ${}^{G_{p+1}}/{}_{F_pF_{p^2}}$ is in κ_K^{p-1}. Consequently we will always assume the

Condition 6.3.2. *We require ${}^{G_{p+1}}/{}_{F_pF_{p^2}} \in \kappa_K^{p-1}$.*

This condition is necessary and sufficient for the Galois closure of L/K to be a p-group, and again is always satisfied if we replace K by a suitable unramified extension.

For an $\mathbb{F}_p[G]$-module M we respectively denote by $\mathrm{soc}^i(M)$ and $\mathrm{rad}^i(M)$ the i-th socle and radical of M. If σ is a generator of G, the radical of $\mathbb{F}_p[G]$ is generated by $\sigma - 1$, and we have

$$\mathrm{rad}^i(M) = M^{(\sigma-1)^i}, \qquad \mathrm{soc}^i(M) = \left\{ x : x^{(\sigma-1)^i} = 0 \right\}.$$

Let $G = \mathrm{Gal}(F/K)$ and $\tilde{L}$ be the Galois closure of L over K, we want to compute the length of $\mathrm{Gal}(\tilde{L}/F)$ as a $\mathbb{F}_p[G]$-module, which we will also show to determine completely $\mathrm{Gal}(\tilde{L}/K)$ in the present case. If $F^{(p)}$ is the maximal abelian elementary p-extension of F, this amounts to computing the smallest m such that $\mathrm{rad}^m(\mathrm{Gal}(F^{(p)}/F))$ is contained in $\mathrm{Gal}(F^{(p)}/L)$.

For $0 \leq i \leq p$ let's consider the submodules $S_i = \mathrm{soc}^{p-i}(P_F)$ of $P_F = [F^\times]_F$ (which is canonically identified with $\mathrm{Gal}(F^{(p)}/F)$ via local class field theory), and let K_i be the class field corresponding to S_i over F. For $0 \leq i < p$ we have $[U_{i+1,F}] \subseteq S_i$ and thus the highest upper ramification break of $\mathrm{Gal}(K_i/F)$ is i for $i < p$, and in particular being $p+1$ the unique ramification break of L/F we have that $K_i \not\supseteq L$ for $i < p$. Note also that K_1 is the maximal elementary abelian p-extension of K.

Let K' be the field corresponding to $\mathrm{rad}^1(P_F)$, it is the maximal p-elementary abelian extension of F that is abelian over K, and it corresponds to $N_{F/K}(F^\times)^p$ via the class field theory of K. Considering the structure of $P_F \cong \mathbb{F}_p[G]^{\oplus f} \oplus \mathbb{F}_p$ as a Galois module we have that

$$\mathit{rad}^i(P_F) = \mathrm{soc}^{p-i}(P_F) \cap \mathrm{rad}^1(P_F) = S_i \cap \mathrm{rad}^1(P_F),$$

for each i, and $\mathit{rad}^i(P_F)$ corresponds to $K'K_i$ via class field theory, so we are looking for the smallest m such that $L \subset K'K_m$. Since L and K' are never contained in K_i for $i < p$ and K' has degree p over K_1, this inclusion holds if and only if L and K' generate the same extension over K_m (and $\tilde{L}$ will too, being $K'K_m$ Galois over K). This is the case if and only if $K' \subset LK_m$, and this condition is consequently equivalent to the $\mathbb{F}_p[G]$-module $\mathrm{Gal}(\tilde{L}/F)$ having length $\leq m$

We can now show that if $K' \subset LK_m$ for some $m < p$, then $\mathrm{Gal}(\tilde{L}/K)$ cannot be the semidirect product: indeed $\mathrm{Gal}(K_{m+1}/K)$ lives in the exact sequence

$$1 \to {}^{P_F}\!/_{S_{m+1}} \to \mathrm{Gal}(K_{m+1}/K) \to G \to 1,$$

and all p-th powers in $\mathrm{Gal}(K_{m+1}/K)$ are clearly G-invariant elements of ${}^{P_F}\!/_{S_{m+1}}$, and hence contained in ${}^{S_m}\!/_{S_{m+1}}$, and this shows that the quotient $\mathrm{Gal}(K_m/K)$ has exponent p since we quotiented out all p-th powers. On the other hand $\mathrm{Gal}(K'/K)$ has exponent p^2 so if $K' \subset LK_m$ then also $\mathrm{Gal}(\tilde{L}K_m/K)$ does, and $\mathrm{Gal}(\tilde{L}/K)$ should also have exponent p^2 or the p-th power of any element of the absolute Galois group would act trivially on $\tilde{L}$, K_m, and consequently on $\tilde{L}K_m$, which is impossible. Note that if $\mathrm{Gal}(\tilde{L}/F)$ has maximal length $m = p$ there is only one possible isomorphism class of possible p-groups, which is the wreath product of two cyclic groups of order p, see Prop. 2.2.1, Chap. 2.

The above observation can be viewed as the fact that, for $m < p$, K_m is the compositum of all the extensions of degree p whose normal closure has group over F of length $\leq m$ as $\mathbb{F}_p[G]$-module, and whose group over K is the semidirect product extension (and hence has exponent p). The extensions whose group of the normal closure over K is not the semidirect product are obtained via a sort of twist with K', which is non-trivial when $L \nsubseteq K_m$.

Now K' is not contained in LK_m precisely when there exist an element in $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ fixing LK_m but not K', and any such element can be lifted to $\mathrm{Gal}(L^{\mathrm{ab}}/L)$. Since the image of the Artin map $\Psi_L : L^\times \to \mathrm{Gal}(L^{\mathrm{ab}}/L)$ is dense in $\mathrm{Gal}(L^{\mathrm{ab}}/L)$ we can take such element of the form $\Psi_L(\alpha)$ for some $\alpha \in L^\times$. Having to fix K_1 we will have $N_{L/K}(\alpha) \in (K^\times)^p$ by the functoriality of the reciprocity map (see §3.4, Chap. 3), $[N_{L/F}(\alpha)]_F \in S_m$ because K_m is fixed, and $N_{L/K}(\alpha) \notin N_{F/K}(F^\times)^p$ because the action is non-trivial on K'. On the other hand the existence of such an element ensures that $K' \notin LK_m$.

If L and K are as above, we have proved the following proposition.

Proposition 6.3.3. *Let $1 \leq m \leq p$ be the smallest possible integer such that for all $\alpha \in L^\times$ such that $N_{L/K}(\alpha) \in (K^\times)^p$ and $[N_{L/F}(\alpha)]_F \in S_m$ we also have $N_{L/K}(\alpha) \in N_{F/K}(F^\times)^p$. Then $\mathrm{Gal}(\tilde{L}/K)$ is the unique p-group that has* *exponent p^2 and is an extension of $G = \mathrm{Gal}(F/K)$ by an indecomposable $\mathbb{F}_p[G]$-module of length m.*

We now determine the $(p-m)$-th socle S_m of P_F for each $0 \leq m \leq p$, and deduce the ramification breaks of the normal closure.

Consider the images $V_i = [U_{i,F}]_F$ of the $U_{i,F}$ in P_F for $i \geq 1$, and put $V_0 = P_F$ for convenience. If G is generated by σ say, the radical of $\mathbb{F}_p[G]$ is generated by $(\sigma - 1)$ and we have $V_i^{\sigma-1} \subseteq V_{i+1}$. Since $V_p = V_{p+1}$ and $V_{p+2} = 1$ we have that V_p is killed by $\sigma - 1$, V_{p-1} by $(\sigma-1)^2$ and so on, so that $V_{k+1} \subseteq \mathrm{soc}^{p-k} P_F = S_k$ for $0 \leq k < p$, while clearly $S_p = 0$. Furthermore if π_F is a uniformizing element of F we have $\pi_F^{(\sigma-1)^k} \in V_k \setminus V_{k+1}$ and $\pi_F^{(\sigma-1)^k} \in S_k$ for $0 \leq k < p$, so comparing the dimensions we have that

$$S_k = \langle \pi_F^{(\sigma-1)^k} \rangle + V_{k+1}.$$

If m is like in the proposition and ≥ 2, take in $L^\times$ an element α contradicting the proposition for $m-1$ and such that $t = v_L(1 - N_{L/F}(\alpha))$ is as big as possible. Then $\psi_{LK_{m-1}/F}(t)$ is the ramification break of $K'LK_{m-1}/LK_{m-1}$, which is also equal to that of $LK'K_{m-1}/K'K_{m-1}$ considering that $K'K_{m-1}/K_{m-1}$ and LK_{m-1}/K_{m-1} have the same ramification break equal to $\psi_{K_{m-1}/F}(p+1)$, and the total set of breaks has to be preserved. By the definition of S_{m-1} and S_m we have that t can be either $m-1$ or m, unless $m = p$ where t is either $p-1$ or $p+1$.

By local class field theory $K'K_{m-1}/F$ corresponds to the subgroup $A = rad^{m-1}(P_F)$ of P_F, and $LK'K_{m-1}/F$ to another subgroup B with index p in A, and t is the biggest t such that some $x \in V_t \cap A$ has non-trivial image in A/B. Passing to the groups A' and B' of the elements sent by $\sigma - 1$ into A and B respectively, $A' = soc^{p-m+2}(P_F)$ corresponds to K_{m-2}, and B' to $L'K_{m-2}$ where L' is the subfield of $\tilde{L}$ corresponding to $\mathrm{soc}^1(\mathrm{Gal}(\tilde{L}/F))$ as $\mathbb{F}_p[G]$-module. The upper ramification break of the new relative extension is $\psi_{K_{m-2}/F}(s)$ where s is the biggest so that some $y \in V_s \cap A'$ is nontrivial in A'/B'. Being $A = rad^{m-1}(P_F)$ each $x \in A \setminus B$ is of the form $x = y^{\sigma-1}$ for some $y \in A' \setminus B'$, so $s = t - 1$ unless $t = p + 1$ where it becomes $s = p - 1$.

Since $\mathrm{Gal}(L'/F)$ has length $m-1$ and the field L'' corresponding to $\mathrm{soc}^1(\mathrm{Gal}(L'/L))$ is contained in K_{m-2}, and $V_{m-2} \supseteq A' \supseteq V_{m-1}$, we have that s is also the ramification number of L'/L'' with respect to F, that is the break is $\psi_{L''/F}(s)$. Repeating this observation for $m-1$ steps we have that the upper ramification breaks over F are either $1, 2, \ldots, m-1, p+1$, either $0, 1, \ldots, m-2, p+1$ depending on whether an element $\alpha \in S_{m-1}$ contradicting the proposition can be found in V_m or not, where for convenience a “ramification break” of 0 indicates an unramified extension.

We proved the

Proposition 6.3.4. *Let $1 \leq m \leq p$ be like in the Prop. 6.3.3, if we can find an α such that $N_{L/K}(\alpha) \in (K^\times)^p \setminus N_{F/K}(F^\times)^p$ such that $[N_{L/F}(\alpha)]_F \in V_m$, then the normal closure $\tilde{L}/F$ is totally ramified with breaks $1, 2, \ldots, m-1, p+1$. If* *not, then $\tilde{L}/F$ is formed by an unramified extension of degree p and an extension with upper breaks $1, 2, \dots, m-2, p+1$.*

We will look for the biggest $1 \leq m \leq p-1$ such that we can find an α contradicting the requests of the Prop. 6.3.3. For all $\ell = p-1, \dots, 2, 1$ in descending order, if we cannot find a suitable α with $[N_{L/F}(\alpha)]_F \in V_{\ell+1}$, we inductively test $S_\ell \supset V_{\ell+1}$ (and $\mathrm{Gal}(\tilde{L}/F)$ has length $\ell+1$ and there is an unramified part), and then $V_\ell \supseteq S_\ell$ (and in this case $\mathrm{Gal}(\tilde{L}/F)$ has length ℓ and the extension is totally ramified).

Verifying that we cannot find α with $[N_{L/F}(\alpha)]_F \in V_{\ell+1}$ is easy, and is the condition of the theorem connected to $A_{p+1}(Y)$ for $\ell = p-1$, or to $A_{\ell+1}$ if $\ell < p-1$. We then allow $[N_{L/F}(\alpha)]_F$ to be in $S_\ell = \langle \pi_F^{(\sigma-1)^\ell} \rangle + V_{\ell+1}$: by Prop. 6.3.1 for $\bar{\theta}^{p(p-1)} = -{}^{F_p}/_{F_{p^2}}$ and for some k prime with p we have

$$\begin{aligned} \pi_F^{(\sigma-1)^\ell} &= 1 - k\theta^{p\ell}\pi_F^\ell + \dots \\ &= N_{L/F}(1 - k\theta^\ell \pi^\ell) + \mathcal{O}(\pi_F^{\ell+1}), \end{aligned}$$

in view of §3.2.1, Chap. 3, and being ℓ smaller than the ramification break $p+1$. In particular the image of $N_{L/F}(1 - \theta^\ell \pi^\ell)$ generates ${}^{S_\ell}/_{V_{\ell+1}}$, and testing the condition for S_ℓ is equivalent to verifying that $A_\ell(\bar{\theta}^\ell) \in V$.

Note that $A_2(\bar{\theta}^2)$ has the simplified form $G_{2p}\bar{\theta}^{2p} + G_2\bar{\theta}^2$, and testing if $F_{p^2}X^p + F_pX = A_\ell(\bar{\theta}^\ell)$ has solution in κ_K is equivalent to checking, after replacing X by $\bar{\theta}^\ell X$ and dividing by $\bar{\theta}^\ell$, if there are solutions to

$$F_{p^2}({-}^{F_p}/_{F_{p^2}})^{\ell/p}X^p + F_pX - G_{p\ell}({-}^{F_p}/_{F_{p^2}})^{\ell/p} - G_\ell = 0.$$

Note that for $\ell = 1$ we just test if $\overline{{}^{c_1(\theta)}/_{p^2}}$ is in V, like in the last condition of Theorem 6.2.5.

We have the

Theorem 6.3.5. *Assume that $f(X)$ satisfies conditions 1, 2, 3 of Theorem 6.2.5, and keeping the notation assume additionally that*

1. ${}^{G_{p+1}}/_{F_pF_{p^2}} \in \kappa_K^{p-1}$.

Let L be the extension determined by $f(X)$, $\tilde{L}$ the normal closure over K, and F the unique subextension of degree p contained in L. Then $\mathrm{Gal}(\tilde{L}/K)$ is an extension of $G = \mathrm{Gal}(F/K)$ by the indecomposable $\mathbb{F}_p[G]$-module $M = \mathrm{Gal}(\tilde{L}/F)$, $\mathrm{Gal}(\tilde{L}/K)$ has exponent p^2 and is a non-split extension unless M has length p. Furthermore

2. *if $G_{p+1}^p \neq -F_p^{p+1}$ then M has length p and L/F is totally ramified with upper ramification breaks $1, 2, \dots, p-1, p+1$;*

assuming equality in the previous condition,

3. *if* $G_{p\ell} \neq F_{p^2} \left({}^{G_\ell}\!/_{F_p}\right)^p$ *for some* $\ell \in [\![3, p-1]\!]$ *that we take as big as possible, or* $G_{2p} \neq F_{p^2} \left({}^{G_2}\!/_{F_p}\right)^p + \frac{1}{2} F_p \left(F_p - F_{p^2}^{1/p}\right)$ *and we put* $\ell = 2$*, let*

$$U(X) = F_{p^2} \left(-{}^{F_p}\!/_{F_{p^2}}\right)^{\ell/p} X^p + F_p X - G_{p\ell} \left(-{}^{F_p}\!/_{F_{p^2}}\right)^{\ell/p} - G_\ell.$$

   We have that

   - *if* $U(X)$ *has no root in* κ_K*, then* M *has length* $\ell+1$ *and* $\tilde{L}/F$ *is formed by an unramified extension followed by a totally ramified extension with upper ramification breaks* $1, 2, \ldots, \ell-1, p+1$,
   - *if* $U(X)$ *has some root in* κ_K*, then* M *has length* ℓ *and* $\tilde{L}/F$ *is a totally ramified extension with upper ramification breaks* $1, 2, \ldots, \ell-1, p+1$,

assuming equality in the previous conditions, and for $\bar{\theta}^{p(p-1)} = -{}^{F_p}\!/_{F_{p^2}}$,

4. *if* $F_{p^2} X^p + F_p X - \overline{\frac{1}{p^2} \left(f_{p^2} \theta^{p^2} + f_p \theta^p\right)} - G_1 \bar{\theta}$ *has no root in* κ_K*, then* M *has length* 2 *and* $\tilde{L}/F$ *is formed by an unramified extension followed by a totally ramified extension with upper ramification break* $p+1$.

All conditions pass precisely when all requirements of Theorem 6.2.5 are satisfied, and in this case L/F *is Galois cyclic.*

It turns out that we just worked out the hard case of the classification of all polynomials of degree p^2 whose Galois group is a p-group.

We keep the notation of the previous part of this section. We have classified in Theorem 6.3.5 all polynomials such that L/F has ramification break at $p+1$ and the normal closure is a p-group, and it turned out that the condition on the ramification number is sufficient to guarantee that the Galois group of the normal closure has exponent p^2. Conversely if the ramification number is $\leq p-1$ then either $L \subset K_m$ for some $m < p$ and $\mathrm{Gal}(\tilde{L}/F)$ has length $\leq m$, and $\mathrm{Gal}(\tilde{L}/K)$ is the splitting extension of G, either $\mathrm{Gal}(\tilde{L}/F)$ has length p, and there is only one possibility for $\mathrm{Gal}(\tilde{L}/K)$, which is both a split extension and has exponent p^2, and is a wreath product of two cyclic groups of order p.

Again as above, let ℓ be the smallest integer such that $[N_{L/F}(L^\times)]_F$ contains $V_{\ell+1}$. The ramification number of L/F is ℓ, and the length of $\mathrm{Gal}(\tilde{L}/K)$ as G-module can be ℓ when the norms also contain S_ℓ, or $\ell+1$ if this is not the case. Since $S_\ell = \langle \pi_F^{(\sigma-1)^\ell} \rangle + V_{\ell+1}$ to resolve this ambiguity we should test whether $[\pi_F^{(\sigma-1)^\ell}]_F \in [N_{L/F}(L^\times)]_F$. Since $\pi_F^{(\sigma-1)^\ell} \in U_{\ell,F}$ and $N_{L/F}(L^\times) \supset U_{\ell+1,F}$ we can just test if

$$N_{L/F}(1 + \theta \pi^\ell) = \pi_F^{(\sigma-1)^\ell} + \ldots$$

for some unit $\theta \in U_K$.

Factorizing in L the ramification polynomial $f(X+\pi)$ over the Newton polygon we have that $f(X+\pi) = Xg(X)h(X)$, where $g(X)$ has degree $p-1$ with roots of valuation $\ell+1$ and $h(X)$ degree p^2-p and roots with valuation 2. We can take $g(X)$ to be monic and with roots $\tau^i(\pi) - \pi$, where τ is an automorphism of order p of the normal closure of L over F and $1 \leq i < p$, and L/F is Galois if and only if $g(X) = X^{p-1} + \cdots + g_1 X + g_0$ splits in linear factors in L. If we can write $\tau(\pi) - \pi = \eta\pi^{\ell+1} + \ldots$ with $\eta \in U_K$, then $\tau(\pi)$ can be approximated in L better than by any other conjugate, and consequently L/F is Galois by Krasner lemma. On the other hand if L/K is Galois we certainly have such an expression for some η. Since

$$g_0 = \prod_{i=1}^{p-1} (\tau^i \pi - \pi) \tag{6.6}$$

$$\equiv \prod_{i=1}^{p-1} i\eta\pi^{\ell+1} \equiv -\eta^{p-1}\pi^{(p-1)(\ell+1)} \tag{6.7}$$

we have that L/F is Galois if and only if $-g_0$ is a $(p-1)$-th power.

The monomial in X^p of $f(X+\pi)$ is

$$\binom{p^2-p}{p} f_p \pi^{p^2-2p} X^p = h_0 X^p$$

where h_0 is the constant term of $h(X)$, while the monomial in X is

$$X f'(\pi) = (p^2 - r) f_r \pi^{p^2-r-1} X = g_0 h_0 X$$

where r should be $p^2 - (p-1)\ell + p$ and $v_p(f_r) = 2$, considering that $f'(\pi)$ is the different and has valuation $(p^2 - p) \cdot 2 + (p-1) \cdot (\ell + 1)$.

Since $\binom{p^2-p}{p} \equiv -1 \pmod{p}$, by the definition of r we have taking the ratio of the coefficients of the monomials above that

$$\begin{aligned} \frac{g_0}{\pi^{(p-1)(\ell+1)}} &= \frac{-r f_r \pi^{(p-1)\ell-p-1}}{-f_p \pi^{p^2-2p}} \cdot \pi^{-(p-1)(\ell+1)} + \ldots \\ &= {}^{rf_r}/_{f_p} \cdot \pi^{-p^2} + \cdots = -{}^{rf_r}/_{f_p f_{p^2}} + \ldots, \end{aligned}$$

being $\pi^{p^2} = -f_0 + \ldots$.

Since $r \equiv \ell \pmod{p}$ we obtained that $\bar{\eta}^{p-1}$ is equal to $\overline{{}^{\ell f_r}/_{f_p f_{p^2}}}$, and it is contained in κ_K^{p-1} if and only if g_0 is a $(p-1)$-th power. Put again $F_p = \overline{{}^{f_p}/_p}$, $F_{p^2} = \overline{{}^{F_{p^2}}/_p}$ and $G_i = \overline{{}^{f_i}/_{p^2}}$ for $i \neq p, p^2$.

Condition 6.3.6. *L/F is Galois if and only if ${}^{\ell G_r}/_{F_p F_{p^2}}$ is in κ_K^{p-1}, where r is equal to $p^2 - (p-1)\ell + p$.*

Let's recall that from §3.2.1, Chap. 3 we have that

$$N_{L/F}(1 + \theta\pi^\ell) = 1 + (\theta^p - \eta^{p-1}\theta)\pi_F^\ell + \ldots,$$

while

$$\pi_F^{(\sigma-1)^\ell} = 1 - k\rho^\ell \pi_F^\ell + \ldots$$

for $\bar{\rho}^{p-1} = -{}^{F_p}/_{F_{p^2}}$ and some integer k prime with p, by Prop. 6.3.1. From what observed at the beginning, we obtain that the length of $\mathrm{Gal}(\tilde{L}/K)$ is ℓ when $X^p - {}^{\ell G_r}/_{F_p F_{p^2}} X = \bar{\rho}^\ell$ has solution in κ_K, and $\ell + 1$ if this is not the case. Replacing X by $\bar{\rho}^\ell X$ and dividing by $\bar{\rho}^\ell$ this is equivalent to testing if

$$(-{}^{F_p}/_{F_{p^2}})^\ell X^p - {}^{\ell G_r}/_{F_p F_{p^2}} X = 1$$

has solution in κ_K.

Consequently we obtain

Theorem 6.3.7. *Let $2 \leq \ell \leq p-1$ an let $r = p^2 - (p-1)\ell + p$, and assume that $f(X)$ is such that*

1. *$v_p(f_p) = 1$, and $v_p(f_{pi}) \geq 2$ for $i \in [\![2, p-1]\!]$,*
2. *$v_p(f_i) \geq 2$ for $i \in [\![1, r-1]\!]$, $v(f_r) = 2$ and $v_p(f_i) \geq 3$ for $i \in [\![r+1, p^2-1]\!]$,*

putting $F_p = \overline{{}^{f_p}/_p}$, $F_{p^2} = \overline{{}^{f_{p^2}}/_p}$, and $G_i = \overline{{}^{f_i}/_{p^2}}$ for all $i \neq p, p^2$ we have

3. *$-{}^{F_p}/_{F_{p^2}} = \bar{\rho}^{p-1}$ for some $\bar{\rho} \in \kappa_K^\times$,*
4. *${}^{\ell G_r}/_{F_p F_{p^2}} = \bar{\eta}^{p-1}$ for some $\bar{\eta} \in \kappa_K^\times$.*

Let L be the extension determined by $f(X)$, $\tilde{L}$ the normal closure over K, and F the unique subextension of degree p contained in L. Then $\mathrm{Gal}(\tilde{L}/K)$ is a split extension of $G = \mathrm{Gal}(F/K)$ by the indecomposable $\mathbb{F}_p[G]$-module $M = \mathrm{Gal}(\tilde{L}/F)$ and furthermore defining

$$U(X) = (-{}^{F_p}/_{F_{p^2}})^\ell X^p - {}^{\ell G_r}/_{F_p F_{p^2}} X - 1$$

we have that if

- *$U(X)$ has no root in κ_K, then M has length $\ell + 1$ and $\tilde{L}/F$ is formed by an unramified extension followed by a totally ramified with upper ramification breaks $1, 2, \ldots, \ell$,*
- *$U(X)$ has some root in κ_K, then M has length ℓ and $\tilde{L}/F$ is totally ramified with upper ramification breaks $1, 2, \ldots, \ell$.*

What is left is the easy case for $\ell = 1$, which is considered separately. In this case L/K has 1 as unique ramification break, $v_p(f_1) = 1$ while $v_p(f_i) \geq 2$ for $i \in [\![2, p^2-1]\!]$, and consequently put $F_i = \overline{{}^{f_i}/_p}$ for $i = 1, p, p^2$. The map ${}^{U_{1,L}}/_{U_{2,L}} \to {}^{U_{1,K}}/_{U_{2,K}}$ induced by $N_{L/K}$ is described by the additive polynomial $A(Y) = F_{p^2} Y^{p^2} + F_p Y^p + F_1 Y$, and L/K is Galois precisely when $N_{L/K}(U_{1,L}) = 1 + pW$ for a subspace W of codimension 2 in κ_K, that is when $A(Y)$ splits completely in κ_K. On the other hand the normal closure $\tilde{L}/K$ is a p-extension if and only if L becomes abelian elementary over the unique unramified extension of degree p of K, or equivalently if $A(Y)$ splits completely over the unique extension of degree p of κ_K.

Theorem 6.3.8. *Assume that $f(X)$ is such that*

1. $v_p(f_p) \leq 1$, *and* $v_p(f_{pi}) \geq 2$ *for* $i \in [\![2, p-1]\!]$,
2. $v_p(f_1) = 1$, *and* $v(f_i) \geq 2$ *for* $i \in [\![2, p^2-1]\!]$,

and putting $F_i = \overline{f_i/p}$ *for* $i = 1, p, p^2$

3. *the polynomial* $F_{p^2}Y^{p^2} + F_pY^p + F_1Y$ *has a root in* $\kappa_K^\times$, *and* ${F_1}/{F_{p^2}} \in (\kappa_K^\times)^{p-1}$.

Let L be the extension determined by $f(X)$, and $\tilde{L}$ be the normal closure over K. Then

- *if* $F_{p^2}Y^{p^2} + F_pY^p + F_1Y$ *does not split in* κ_K *then* L/K *has a unique subextension* F, $\mathrm{Gal}(\tilde{L}/F)$ *has length* 2, $\tilde{L}/F$ *is formed by an unramified extension followed by a totally ramified extension with upper ramification break* 1, *and* $\mathrm{Gal}(\tilde{L}/K)$ *is a split extension of* $\mathrm{Gal}(F/K)$ *by* $\mathrm{Gal}(\tilde{L}/F)$,
- *if* $F_{p^2}Y^{p^2} + F_pY^p + F_1Y$ *has all roots in* κ_K *then* L/K *is an abelian elementary* p*-extension.*

Theorems 6.3.5, 6.3.7 and 6.3.8 cover all possible ramification breaks of the extension L/F, so they completely describe the Galois groups of polynomials of degree p^2 whose splitting field is a p-extension.

6.4 Polynomials of degree p^3 generating a cyclic extension

We proceed with the same strategy used for the polynomials of degree p^2, starting from the conditions on the valuations of the coefficients.

Let $f(X) = X^{p^3} + \cdots + f_{p^3-1}X + f_{p^3}$, since the different has now valuation $4p^3 - p^2 - p - 2$ it will be determined by the monomial $f_{p^2+p+1}X^{p^3-p^2-p-1}$, $v_p(f_{p^2+p+1}) = 3$, $v_p(f_i) \geq 3$ if $(i,p) = 1$ and $v_p(f_i) \geq 4$ if furthermore $i > p^2 + p + 1$. Let π be a root, the coefficients of the term of degree p of the ramification polynomial $f(X+\pi)$ will have valuation $(p^3 - p^2) \cdot 2 + (p^2 - p) \cdot (p+1) = 3p^3 - p^2 - 2p$ and has to come from a monomial $f_{p^3-i}(X+\pi)^i$ contributing the term $\binom{i}{p} f_{p^3-i}X^p\pi^{i-p}$, and we deduce the i has to be $i = p^3 - p^2 - p$, that $v_p(f_{p^2+p}) = 2$, that $v_p(f_{pi}) \geq 2$ for $(i,p) = 1$ and $v_p(f_{pi}) \geq 3$ if furthermore $i \geq p+2$. Similarly considering the coefficient of the term of degree p^2 of the ramification polygon, which shall have valuation $2p^3 - 2p^2$, we obtain that $v_p(f_{p^2}) = 1$ and $v_p(f_{p^2i}) \geq 2$ for all indices such that $(i,p) = 1$.

Condition 6.4.1. *We must have*

1. $v_p(f_{p^2}) = 1$ *and* $v_p(f_{p^2i}) \geq 2$ *for* $i \in [\![2, p-1]\!]$,

2. $v_p(f_{pi}) \geq 2$ *for all* $i \in \llbracket 1, p-1 \rrbracket$, $v_p(f_{p^2+p}) = 2$, *and* $v_p(f_{pi}) \geq 3$ *for all* $i \in \llbracket p+1, p^2-1 \rrbracket$,

3. $v_p(f_i) \geq 3$ *for all* $i \in \llbracket 1, p^2+p-1 \rrbracket$, $v_p(f_{p^2+p+1}) = 3$ *and* $v_p(f_i) \geq 4$ *for all* $i \in \llbracket p^2+p+2, p^3-1 \rrbracket$.

Again working like in degree p^2, we shall require $N_{L/K}(U_{1,L})^{p^{i-1}} \cap U_{i+1,L}$ to be contained in $1 + p^i V$ for $1 \leq i \leq 3$ and some $\mathbb{F}_p$-vector space V, and after determining V we will have to verify the condition on the combinations of the norms of elements of the form $1 + \theta\pi^\ell$ for a unit θ, and $1 \leq \ell \leq p^2+p+1$ and $(\ell, p) = 1$.

Let's expand again $\prod_{i=0}^{\ell} \tilde{f}(\zeta_\ell^i T)$ modulo p^4, taking into account the valuations of the f_i and evaluating directly the $\Sigma_\lambda(\ell)$ via Prop. 6.1.4 it can be written with the terms in increasing valuation as

$$\mathfrak{p}_K \ni \Big[\quad +\delta_{\ell,1} f_{p^2} T^{p^2} + \delta_{\ell,1} f_{p^3} T^{p^3} \tag{6.8}$$

$$\mathfrak{p}_K^2 \ni \left[\begin{aligned} &+\frac{1}{2}\delta^{[2]}_{\ell,2} f_{p^2}^2 T^{2p^2} + \delta^{[2]}_{\ell,p+1} f_{p^2} f_{p^3} T^{p^3+p^2} + \frac{1}{2}\delta^{[2]}_{\ell,2} f_{p^3}^2 T^{2p^3} \\ &+ \sum_{j \in \llbracket 2,p-1 \rrbracket} \delta_{\ell,j} f_{p^2 j} T^{p^2 j} + \sum_{k \in \llbracket 1,p+1 \rrbracket} \delta_{\ell,k} f_{pk} T^{pk} \end{aligned} \right. \tag{6.9}$$

$$\mathfrak{p}_K^3 \ni \left[\begin{aligned} &+\frac{1}{3}\delta^{[3]}_{\ell,3} f_{p^2}^3 T^{3p^2} + \delta^{[3]}_{\ell,p+2} f_{p^3} f_{p^2}^2 T^{p^3+2p^2} + \delta^{[3]}_{\ell,2p+1} f_{p^3}^2 f_{p^2} T^{2p^3+p^2} + \frac{1}{3}\delta^{[3]}_{\ell,3} f_{p^3}^3 T^{3p^3} \\ &+ \sum_{j \in \llbracket 2,p-2 \rrbracket} \delta^{[2]}_{\ell,j+1} f_{p^2} f_{p^2 j} T^{p^2+p^2 j} + \delta^{[2]}_{\ell,1} f_{p^2} f_{p^3-p^2} T^{p^3} + \sum_{k \in \llbracket 1,p+1 \rrbracket} \delta^{[2]}_{\ell,k+p} f_{p^2} f_{pk} T^{p^2+pk} \\ &+ \sum_{j \in \llbracket 2,p-1 \rrbracket} \delta^{[2]}_{\ell,j+p} f_{p^3} f_{p^2 j} T^{p^3+p^2 j} + \sum_{k \in \llbracket 1,p+1 \rrbracket} \delta^{[2]}_{\ell,k+p^2} f_{p^3} f_{pk} T^{p^3+pk} \\ &+ \sum_{j \in \llbracket p+2,p^2-1 \rrbracket} \delta_{\ell,j} f_{pj} T^{pj} + \sum_{k \in \llbracket 1,p^2+p+1 \rrbracket} \delta_{\ell,k} f_k T^k \end{aligned} \right. \tag{6.10}$$

While this expansion looks scary we can start noticing that since raising to a p-th power induces an automorphism on the set of multiplicative representatives we have considering the expansion modulo p^3 that the conditions stated in Theorem 6.2.5 must be satisfied with f_{pi}in place of f_i. Consequently put $F_i = \overline{f_i/p}$ for $i = p^2, p^3$, $G_i = \overline{g_i/p^2}$ for $i \in p\llbracket 1, p+1 \rrbracket$ or $i \in p^2\llbracket 2, p-1 \rrbracket$, let $A(Y) = F_{p^3} Y^p + F_{p^2} Y$ and put $V = A(\kappa_K)$. Such conditions are satisfied if and only if V has codimension 1 in κ_K and the norms contained in $U_{1,K}$ or $U_{2,K}$ are respectively in $1 + pV$ and $1 + p^2 V$.

Similarly to the case in degree p^2, for $\ell \geq 2$ this sum can be written as $D_\ell(\theta) = \ell \cdot \sum_{\ell | k} d_k(\theta^k)$ where the $d_\ell(T^\ell)$ are the polynomial obtained if every $\delta^{[m]}_{\ell,i}$ is interpreted as a Kronecker's delta and $1 + d_\ell(\theta) \equiv N(E(\theta\pi^\ell)) \pmod{p^4}$. For $\ell = 1$ there are exceptions because $\delta^{[m]}_{\ell,i} = 0$ for $\ell < m$.

We require the norms in $U_{3,K}$ to be in $1+p^3V$, and let's concentrate first on the case of $\ell \in [\![p+2, p^2+p+1]\!]$ so that the norms $N_{L/K}(1+\theta\pi^\ell)$ already live in $U_{3,K}$, and the first few terms of the expansion disappear. For such indices ℓ, $d_\ell(\theta)$ shall be in p^3V for each representative θ, and dividing by p^3 we can consider the additive polynomials $A_\ell(Y) = \overline{d_\ell(Y)/p^3}$, which, depending on ℓ, are

$$\begin{array}{cr} -G_{p(\ell-p^2)}F_{p^3}Y^p + H_\ell Y & \ell \in [\![p^2+1, p^2+p+1]\!], \\ H_{p\ell}Y^p + H_\ell Y & \ell \in [\![2p+2, p^2-1]\!], \\ F_{p^3}^2 F_{p^2}Y^{p^2} + (H_{p\ell} - F_{p^2}G_{p(p+1)})Y^p + H_\ell Y & \ell = 2p+1, \\ -F_{p^3}F_{p^2(\ell-p)}Y^{p^2} + (H_{p\ell} - F_{p^2}G_{p(\ell-p)})Y^p + H_\ell Y & \ell \in [\![p+3, 2p-1]\!], \\ (F_{p^3}F_{p^2}^2 - F_{p^3}F_{2p^2})Y^{p^2} + (H_{p\ell} - F_{p^2}G_{2p})Y^p + H_\ell Y & \ell = p+2, \end{array}$$

where we have put $H_k = \overline{f_k/p^3}$ for $k \in [\![1, p^2+p+1]\!]$ and $k \in p[\![p+2, p^2-1]\!]$.

Condition 6.4.2. *For each $\ell \in [\![p{+}2, p^2{+}p{+}1]\!]$ we shall have $A_\ell(\kappa_K) \subseteq A(\kappa_K)$.*

For $\ell \leq p+1$ the question is a bit more complicated because in general the norms of $1-\theta\pi^\ell$ will not be contained in $U_{3,K}$, but a proper combination of norms of elements of this form may be, and we should require it to be in $1+p^3V$. However for η varying the elements $N_{L/K}(1-\eta\pi)^p$ have norms covering all classes in $U_{2,K}/U_{3,K}$, and consequently each $N_{L/K}(1-\theta\pi^\ell)$ can be reduced into $U_{3,K}$ by multiplication by an suitable $N_{L/K}(1-\eta\pi)^p$ for some η, and we should verify that all such reduction are actually in $1+p^3V$. The condition for more complicated combinations will certainly also be ensured.

Since the map $\mathfrak{p}_K^2/\mathfrak{p}_K^4 \to U_{2,K}/U_{4,K}$ induced by $x \mapsto 1+x$ is still an isomorphism we have that a proper combination of the of $1+\theta\pi^\ell$ (e.g. via the Artin-Hasse exponential) has norm of the form $1+d_\ell(\theta)$. In other words depending on $2 \leq \ell \leq p+1$ we have that the remaining term, which we call $g_\ell(Y)$, is

$$\begin{array}{cr} \left\{-f_{p^3}f_{p^2}Y^{p^2} + f_{p^2+p}Y^p\right\} - f_{p^2}f_pY^p + f_{p+1}Y & [p+1], \\ \left\{f_{p^2\ell}Y^{p^2} + f_{p\ell}Y^p\right\} - f_{p^2}f_{p^2(\ell-1)}Y^{p^2} + f_\ell Y & [4, p-1], \\ \left\{f_{3p^2}Y^{p^2} + f_{3p}Y^p\right\} + \frac{1}{3}f_{p^3}^3Y^{p^3} + \frac{1}{3}f_{p^2}^3Y^{p^2} - f_{p^2}f_{2p^2}Y^{p^2} + f_3Y & [3], \\ \left\{-\frac{1}{2}f_{p^3}^2Y^{p^3} + \left(f_{2p^2} - \frac{1}{2}f_{p^2}^2\right)Y^{p^2} + f_{2p}Y^p\right\} + f_2Y & [2], \end{array}$$

where under braces are the terms that are not identically in $\mathfrak{p}_K^3$. On the other hand

$$N(1+\eta\pi) = 1 + f_{p^3}\eta^{p^3} + f_{p^2}\eta^{p^2} + f_p\eta^p \mod p^2V$$

and consequently

$$N(1+\eta\pi)^p = 1 + \left\{pf_{p^3}\eta^{p^3} + pf_{p^2}\eta^{p^2}\right\} + pf_p\eta^p \mod p^3V,$$

with again under braces are the terms that are not identically in $\mathfrak{p}_K^3$. Consequently let's consider the polynomial

$$h(Z) = \{pf_{p^3}Z^{p^2} + pf_{p^2}Z^p\} + pf_pZ,$$

we are looking for values of $Z = \phi_\ell(Y)$, that will be the lifting of some additive polynomials in Y, such that $g_\ell(Y) - h(\phi_\ell(Y)) \in \mathfrak{p}_K^3$, to impose the condition that it shall be in p^3V as well.

The additive polynomials $\overline{{}^{g_\ell(Y)}/_{p^2}}$, which we denote by $B_\ell(Y^p)$ replacing Y^p by Y, are forced to have image contained V, that is the image of $\overline{{}^{h(Y)}/_{p^2}} = A(Y^p)$, and the condition is that $B_\ell(Y) = A(D_\ell(Y))$ for some other additive polynomial $D_\ell(Y)$ whose coefficients can be deduced easily.

In particular, being $A(Y) = F_{p^3}Y^p + F_{p^2}Y$ and $B_\ell(Y)$ the polynomials

$$\begin{array}{cc} -F_{p^2}F_{p^3}Y^p + G_{p^2+p}Y & [p+1], \\ G_{p^2\ell}Y^p + G_{p\ell}Y & [3,\ p-1], \\ -\tfrac{1}{2}F_{p^3}^2Y^{p^2} + \left(G_{2p^2} - \tfrac{1}{2}F_{p^2}^2\right)Y^p + G_{2p}Y & [2], \end{array} \tag{6.11}$$

in view of Prop. 6.1.2 we can take as $D_\ell(Y)$ respectively the polynomials

$$\begin{array}{cc} {}^{G_{p\ell}}/_{F_{p^2}}Y & [3,\ p+1], \\ -\tfrac{1}{2}F_{p^3}^{1/p}Y^{p^2} + {}^{G_{2p}}/_{F_{p^2}}Y & [2]. \end{array} \tag{6.12}$$

Now, $B_\ell(Y^p) = A((D_\ell^{1/p}(Y))^p)$ where $D_\ell^{1/p}(Y)$ is $D_\ell(Y)$ with the map $x \mapsto x^{1/p}$ applied to the coefficients. Given the definitions of $A(Y)$ and $B_\ell(Y)$ in terms of the $h(Y)$ and $g_\ell(Y)$, we have that we can take as $\phi_\ell(Y)$ any lifting of $D_\ell^{1/p}(Y)$ to $\mathcal{O}_K[Y]$.

For $3 \leq \ell \leq p+1$ let's take a $\rho \in \mathcal{O}_K$ such that $\bar{\rho}^p = {}^{G_{p\ell}}/_{F_{p^2}} = \overline{{}^{f_{p\ell}}/_{pf_{p^2}}}$, then $D_\ell(Y) = \bar{\rho}^pY$ and we can take $\phi_\ell(Y) = \rho Y$, and the polynomials $\overline{\frac{1}{p^3}(g_\ell(Y) - h(\phi_\ell(Y)))}$ should take values in V. Considering that

$$h(\phi_\ell(Y)) = \left\{pf_{p^3}\rho^{p^2}Y^{p^2} + pf_{p^2}\rho^pY^p\right\} + pf_p\rho Y,$$

depending on ℓ they are

$$\begin{aligned} &\overline{\left(-{}^{f_{p^3}f_{p^2}}/_{p^3} - {}^{f_{p^3}\rho^{p^2}}/_{p^2}\right)}Y^{p^2} \\ &+ \left[\overline{({}^{f_{p^2+p}}/_{p^3} - {}^{f_{p^2}\rho^p}/_{p^2})} - F_{p^2}G_p\right]Y^p + (H_{p+1} - G_p\bar{\rho})Y \end{aligned}$$

for $\ell = p+1$,

$$\begin{aligned} &\left[\overline{\left(-{}^{f_{p^2\ell}}/_{p^3} - {}^{f_{p^3}\rho^{p^2}}/_{p^2}\right)} - F_{p^2}G_{p^2(\ell-1)}\right]Y^{p^2} \\ &+\overline{({}^{f_{p\ell}}/_{p^3} - {}^{f_{p^2}\rho^p}/_{p^2})}Y^p + (H_\ell - G_p\bar{\rho})Y, \end{aligned}$$

for $4 \leq \ell = p-1$, and

$$\begin{aligned} &\frac{1}{3}F_{p^3}^3Y^{p^3} + \left[\overline{\left({}^{f_{3p^2}}/_{p^3} - {}^{f_{p^3}\rho^{p^2}}/_{p^2}\right)} + \frac{1}{3}F_{p^2}^3 - F_{p^2}G_{2p^2}\right]Y^{p^2} \\ &+\overline{({}^{f_{3p}}/_{p^3} - {}^{f_{p^2}\rho^p}/_{p^2})}Y^p + (H_3 - G_p\bar{\rho})Y \end{aligned}$$

for $\ell = 3$.

For $\ell = 2$ let's take $\rho, \tau \in \mathcal{O}_K$ such that $\bar{\rho}^p = {}^{G_{p2}}/_{F_{p^2}} = \overline{{}^{f_{p2}}/_{pf_{p^2}}}$ and $\bar{\tau}^{p^2} = -\frac{1}{2}F_{p^3} = -\frac{1}{2}\overline{{}^{f_{p^3}}/_{p^3}}$. Then $D_\ell(Y) = \bar{\tau}^p Y^p + \bar{\rho}^p Y$ so that we can take $\phi_2(Y) = \tau Y^p + \rho Y$, and we have

$$h(\phi_2(Y)) = \Big\{ pf_{p^3}(\tau Y^p + \rho Y)^{p^2} + pf_{p^2}(\tau Y^p + \rho Y)^p \Big\} + pf_p(\tau Y^p + \rho Y)$$
$$= pf_{p^3}\tau^{p^3}Y^{p^3} + pf_{p^3}\rho^{p^2}Y^{p^2} + pf_{p^3}\sum_{i=1}^{p-1}\binom{p^2}{ip}\tau^{ip}\rho^{(p-i)p}Y^{ip^2+(p-1)p} + \mathcal{O}(p^4)$$
$$+pf_{p^2}\tau^{p^2}Y^{p^2} + pf_{p^2}\rho^p Y^p + pf_{p^2}\sum_{i=1}^{p-1}\binom{p}{i}\tau^i\rho^{(p-i)}Y^{ip+(p-1)}$$
$$+pf_p\tau Y^p + pf_p\rho Y.$$

Considering that $\frac{1}{p}\binom{p}{i} \equiv \frac{1}{p}\binom{p^2}{ip} \pmod{p}$ and the terms in the sums can be paired in elements that are $pf_{p^3}\binom{p^2}{ip}Z^p + pf_{p^2}\binom{p}{i}Z$ for $Z = \tau^i\rho^{(p-i)}Y^{ip+(p-1)}$ and hence in p^3V for each Z, we have that up to some element in p^3V we can write $h(\phi_2(Y))$ as

$$pf_{p^3}\tau^{p^3}Y^{p^3} + (pf_{p^3}\rho^{p^2} + pf_{p^2}\tau^{p^2})Y^{p^2} + (pf_{p^2}\rho^p + pf_p\tau)Y^p + pf_p\rho Y.$$

Consequently up to some element of V the polynomial $\overline{\frac{1}{p^3}(g_2(Y) - h(\phi_2(Y)))}$ is the

$$\overline{\left(-\frac{1}{2}{}^{f_{p3}^2}/_{p^3} - {}^{f_{p3}\tau^{p^3}}/_{p^2}\right)}Y^{p^3} + \overline{\left({}^{f_{2p2}}/_{p^3} - \frac{1}{2}{}^{f_{p2}^2}/_{p^3} - {}^{f_{p3}\rho^{p^2}}/_{p^2} - {}^{f_{p2}\tau^{p^2}}/_{p^2}\right)}Y^{p^2}$$
$$+ \left(\overline{({}^{f_{2p}}/_{p^3} - {}^{f_{p2}\rho^p}/_{p^2})} - G_p\tau\right)Y^p + (H_2 - G_p\bar{\rho})\,Y,$$

which is required to take values in V.

One last effort is required: for $\ell = 1$ in the case that $1 - \theta\pi$ has norm in $U_{2,K}$ (and hence in $1 + p^2V$), that is when θ is such that $A(\bar{\theta}^{p^2}) = 0$, we should also have that taking η such that $(1 - \theta\pi)(1 - \eta\pi)^{-p}$ has norm in $U_{3,K}$, than that norm is required to be actually in $1 + p^3V$.

Let $\theta = T$ be as required, the terms that disappear because $\ell = 1$ are

$$\frac{1}{2}f_{p^2}^2T^{2p^2} + f_{p^3}f_{p^2}T^{p^3+p^2} + \frac{1}{2}f_{p^3}^2T^{2p^3} = \frac{1}{2}\left(f_{p^2}T^{p^2} + f_{p^3}T^{p^3}\right)^2,$$

then

$$\frac{1}{3}f_{p^2}^3T^{3p^2} + f_{p^3}f_{p^2}^2T^{p^3+2p^2} + f_{p^3}^2f_{p^2}T^{2p^3+p^2} + \frac{1}{3}f_{p^3}^3T^{3p^3} = \frac{1}{3}\left(f_{p^2}T^{p^2} + f_{p^3}T^{p^3}\right)^3,$$

and the sums can be decomposed as sums of $(f_{p^2}T^{p^2} + f_{p^3}T^{p^3})f_{p^2j}T^{p^2j}$ and of $(f_{p^2}T^{p^2} + f_{p^3}T^{p^3})f_{pk}T^{pk}$, and in particular all such terms are in $\mathfrak{p}_K^4$ considering the hypotheses on T.

Consequently such terms can be assumed to be present, and removing the extra terms we already studied (or considering the norm of $E(\theta\pi)$) the remaining terms are

$$w(T) = f_{p^3}T^{p^3} + f_{p^2}T^{p^2} - f_{p^2}f_{p^3-p^2}T^{p^2} + f_pT^p + f_1T.$$

Assume $\overline{\frac{1}{p^2}\left(f_{p^3}\theta^{p^3} + f_{p^3}\theta^{p^2} + f_p\theta^p\right)}$ can be written as $F_{p^3}\bar{\alpha}^{p^2} + F_{p^2}\bar{\alpha}^p$ for some $\bar{\alpha}$, then taking any lift α of $\bar{\alpha}$ we can consider $w(\theta) - h(\alpha)$, which comes from a norm of the required type, and should be in p^3V.

At last, we can state the

Theorem 6.4.3. *The Eisenstein polynomial $f(X) = X^{p^3} + f_1X^{p^3-1} + \cdots + f_{p^3-1}X + f_{p^3}$ determines a Galois extension of degree p^3 over K if and only if*

1. *$v_p(f_{p^2}) = 1$ and $v_p(f_{p^2i}) \geq 2$ for $i \in \llbracket 2, p-1 \rrbracket$,*
2. *$v_p(f_{pi}) \geq 2$ for all $i \in \llbracket 1, p-1 \rrbracket$, $v_p(f_{p^2+p}) = 2$, and $v_p(f_{pi}) \geq 3$ for all $i \in \llbracket p+1, p^2-1 \rrbracket$,*
3. *$v_p(f_i) \geq 3$ for all $i \in \llbracket 1, p^2+p-1 \rrbracket$, $v_p(f_{p^2+p+1}) = 3$ and $v_p(f_i) \geq 4$ for all $i \in \llbracket p^2+p+2, p^3-1 \rrbracket$,*

putting $F_{p^2} = \overline{f_{p^2}/p}$, $F_{p^3} = \overline{f_{p^3}/p}$, and $\overline{G_i = f_i/p^2}$ for all i in $p^2\llbracket 2, p-1 \rrbracket$ or in $p\llbracket 1, p+1 \rrbracket$ we have

4. *$-F_{p^2}/F_{p^3} \in \kappa_K^{p-1}$,*
5. *$G_{p(p+1)}^p = -F_{p^2}^{p+1}$,*
6. *$G_{p^2\ell} = F_{p^3}\left(G_{\ell p}/F_{p^2}\right)^p$ for $\ell \in \llbracket 3, p-1 \rrbracket$,*
7. *$G_{2p^2} = F_{p^3}\left(G_{2p}/F_{p^2}\right)^p + \frac{1}{2}F_{p^2}\left(F_{p^2} - F_{p^3}^{1/p}\right)$,*

if ρ is such that $\bar{\rho}^{p(p-1)} = -F_{p^2}/F_{p^3}$ we have (independently of ρ)

8. *$\overline{\frac{1}{p^2}\left(f_{p^3}\rho^{p^2} + f_{p^2}\rho^p + f_p\rho\right)} = F_{p^3}\alpha^p + F_{p^2}\alpha$ for some $\alpha \in \kappa_K$,*

putting $H_i = \overline{f_i/p^3}$ for i in $\llbracket 1, p^2+p+1 \rrbracket$ or in $p\llbracket p+2, p^2-1 \rrbracket$ we have

9. *$-G_{p(\ell-p^2)}F_{p^3} = F_{p^3}(H_\ell/F_{p^2})^p$ for $\ell \in \llbracket p^2+1, p^2+p+1 \rrbracket$,*
10. *$H_{p\ell} = F_{p^3}(H_\ell/F_{p^2})^p$ for $\ell \in \llbracket 2p+2, p^2-1 \rrbracket$,*
11. *$H_{p(2p+1)} - F_{p^2}G_{p(p+1)} = F_{p^3}(H_{2p+1}/F_{p^2})^p + F_{p^2}(F_{p^3}F_{p^2})^{1/p}$,*
12. *$H_{p\ell} - F_{p^2}G_{p(\ell-p)} = F_{p^3}(H_\ell/F_{p^2})^p - F_{p^2}(F_{p^2(\ell-p)})^{1/p}$ for $\ell \in \llbracket p+3, 2p-1 \rrbracket$,*
13. *$H_{p(p+2)} - F_{p^2}G_{2p} = F_{p^3}(H_{p+2}/F_{p^2})^p + F_{p^2}(F_{p^2}^2 - F_{2p^2})^{1/p}$,*

for each $\ell \in \llbracket 3, p+1 \rrbracket$, let ρ_ℓ be such that $\bar{\rho}_\ell^p = G_{p\ell}/F_{p^2}$. Then

14. *putting* $P_{p+1} = H_{p+1} - G_p\bar{\rho}_{p+1}$,

$$Q_{p+1} = \overline{({}^{f_{p^2+p}}/_{p^3} - {}^{f_{p^2}\rho^p_{p+1}}/_{p^2})} - F_{p^2}G_p, \qquad R_{p+1} = \overline{\left(-{}^{f_{p^3}f_{p^2}}/_{p^3} - {}^{f_{p^3}\rho^{p^2}_{p+1}}/_{p^2}\right)},$$

we have $Q_{p+1} = F_{p^3}({}^{P_{p+1}}/_{F_{p^2}})^p + F_{p^2}({}^{R_{p+1}}/_{F_{p^3}})^{1/p}$,

15. *for each* $4 \leq \ell \leq p-1$ *putting* $P_\ell = H_\ell - G_p\bar{\rho}_\ell$,

$$Q_\ell = \overline{({}^{f_{p\ell}}/_{p^3} - {}^{f_{p^2}\rho^p_\ell}/_{p^2})} - F_{p^2}G_p, \qquad R_\ell = \overline{\left(-{}^{f_{p^2\ell}}/_{p^3} - {}^{f_{p^3}\rho^{p^2}_\ell}/_{p^2}\right)} - F_{p^2}G_{p^2(\ell-1)},$$

we have $Q_\ell = F_{p^3}({}^{P_\ell}/_{F_{p^2}})^p + F_{p^2}({}^{R_\ell}/_{F_{p^3}})^{1/p}$,

16. *putting putting* $P_3 = H_3 - G_p\bar{\rho}_3$,

$$Q_3 = \overline{({}^{f_{3p}}/_{p^3} - {}^{f_{p^2}\rho^p_3}/_{p^2})}, \qquad R_3 = \overline{\left({}^{f_{3p^2}}/_{p^3} - {}^{f_{p^3}\rho^{p^2}_3}/_{p^2}\right)} + \frac{1}{3}F^3_{p^2} - F_{p^2}G_{2p^2}$$

we have $\frac{1}{3}F_{p^2}(F^2_{p^3})^{1/p} + F_{p^3}({}^{Q_3}/_{F_{p^2}})^p = R_3 + F_{p^3}({}^{F_{p^3}}/_{F_{p^2}})^p({}^{P_3}/_{F_{p^2}})^{p^2}$,

let $\rho_2, \tau_2 \in \mathcal{O}_K$ *such that* $\bar{\rho}^p_2 = {}^{G_{p^2}}/_{F_{p^2}}$ *and* $\bar{\tau}^{p^2}_2 = -\frac{1}{2}F_{p^3}$. *Then*

17. *putting*

$$P_2 = H_2 - G_p\bar{\rho}, \qquad Q_2 = \overline{({}^{f_{2p}}/_{p^3} - {}^{f_{p^2}\rho^p}/_{p^2})} - G_p\bar{\tau},$$

$$R_2 = \overline{\left({}^{f_{2p^2}}/_{p^3} - \frac{1}{2}{}^{f^2_{p^2}}/_{p^3} - {}^{f_{p^3}\rho^{p^2}}/_{p^2} - {}^{f_{p^2}\tau^{p^2}}/_{p^2}\right)}, \qquad S_2 = \overline{\left(-\frac{1}{2}{}^{f^2_{p^3}}/_{p^3} - {}^{f_{p^3}\tau^{p^3}}/_{p^2}\right)}$$

we have $F_{p^2}({}^{S_2}/_{F_{p^3}})^{1/p} + F_{p^3}({}^{Q_2}/_{F_{p^2}})^p = R_2 + F_{p^3}({}^{F_{p^3}}/_{F_{p^2}})^p({}^{P_2}/_{F_{p^2}})^{p^2}$,

if ρ, ξ *are such that* $\bar{\rho}^{p^2(p-1)} = -{}^{F_{p^2}}/_{F_{p^3}}$ *and*

$$\overline{\frac{1}{p^2}\left(f_{p^3}\rho^{p^3} + f_{p^2}\rho^{p^2} + f_p\rho^p\right)} = F_{p^3}\bar{\xi}^{p^2} + F_{p^2}\bar{\xi}^p,$$

18. *we have that*

$$\overline{\frac{1}{p^3}\left(f_{p^3}(\rho^{p^3} - \xi^{p^2}) + f_{p^2}(\rho^{p^2} - \xi^p) + f_p(\rho^p - \xi) - f_{p^2}f_{p^3-p^2}\rho^{p^2} + f_1\rho\right)}$$

is also of the form $F_{p^3}\bar{\omega}^p + F_{p^2}\bar{\omega}$ *for some* $\bar{\omega} \in \kappa_K$.

6.5 Sums of roots of unity

We finally prove the lemma about the $\Sigma_\lambda(\ell)$, it is actually much more than needed but nevertheless is has a nice statement, which could still be useful in similar circumstances:

Lemma 6.5.1. *Let $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_r)$ be a partition, then*

$$\Sigma_\lambda(\ell) = \sum_{\lambda = \sqcup_{j\in J}\lambda^{(j)}} \ell^{\#J} \cdot \prod_{j\in J} (-1)^{\#\lambda^{(j)}-1}(\#\lambda^{(j)}-1)!$$

where the sum is over all the partitions $\lambda = \bigsqcup_{j\in J}\lambda^{(j)}$ (as set) such that for each $j \in J$ the sum $|\lambda^{(j)}|$ of the elements in $\lambda^{(j)}$ is multiple of ℓ and $\#\lambda^{(j)}$ is the cardinality of the subset $\lambda^{(j)}$.

Proof. Let $A_{(i,j)}$ be the sets (indexed by the pairs (i,j)) of indices $(\iota_1, \dots, \iota_r)$ such that $\iota_i = \iota_j$, let A_0 be the set of all possible indices, and for $A \subseteq A_0$ denote by $\Sigma(A)$ the sum over all the indices in A. By inclusion-exclusion we have that

$$\begin{aligned}\Sigma_\lambda(\ell) &= \Sigma(A_0) - \Sigma(\cup_{(i,j)}A_{(i,j)}) \\ &= \Sigma(A_0) - \sum_{(i,j)}\Sigma(A_{(i,j)}) + \sum_{(i,j)\neq(i',j')}\Sigma(A_{(i,j)}\cap A_{(i',j')}) - \dots\end{aligned}$$

Now let A be the intersection of all the sets $A_{(i_k,j_k)}$ for a collection of pairs $P = \{(i_1,j_1),\dots,(i_s,j_s)\}_{s\in S}$, if we consider the graph with $R = \{1,\dots,r\}$ as vertices and the (i_k,j_k) as edges we have that if we split R in connected components $R = \sqcup_{t\in T}R_t$ then the allowed indices ι are those constant on each R_t, and calling ι_t the value taken on R_t the sum $\Sigma(A)$ becomes

$$\Sigma(A) = \prod_{t\in T}\sum_{\iota_t=0}^{\ell-1}\zeta_\ell^{\iota_t(\sum_{r\in R_t}\lambda_r)},$$

and this sum is $\ell^{\#T}$ when all the $\sum_{r\in R_t}\lambda_r$ are multiple of ℓ and 0 if not. Note that $\Sigma(A)$ appears with sign equal to $(-1)^{\#S}$ in the inclusion-exclusion, so for each partition of R in sets R_t such that the sum of λ_r for $r \in R_t$ is multiple of ℓ we have that to consider the all graphs with set of vertices R and such that each R_t is a connected component, and count the number of graphs with an even number of edges minus those with a odd number of edges. Now the total difference is the product of the differences over all the connected components, so we have

$$\Sigma_\lambda(\ell) = \sum_{\lambda=\sqcup_{j\in J}\lambda^{(j)}} \ell^{\#J} \cdot \prod K_{\#\lambda^{(j)}}$$

where for each i we denote by K_i the difference of the number of connected graphs on i vertices having an even and odd number of edges.

The difference of the number of connected graphs K_i on i vertices with an even or odd number of vertices can be computed fixing an edge, and considering the graphs obtained adding or removing that edge. Those such that with or without it are connected come in pairs with an even and odd number of edges, the other graphs are obtained connecting two other connected graphs on j and $i-j$ vertices. In particular choosing $j-1$ vertices to make one component with the first vertex of our distinguished edges we obtain

$$K_{i+2} = -\sum_{j}^{i} \binom{i}{j} K_{i-j+1} K_{j+1}$$

for $i \geq 0$, and $K_1 = 1$. Calling $G(X)$ the exponential generating function $\sum_{i=0}^{\infty} \frac{K_{i+1}}{i!} X^i$ we obtain that

$$\frac{d}{dX} G(X) = -G(X)^2$$

with the additional condition that $K_1 = 1$, and this equation is clearly satisfied by ${}^{1}/_{(1+X)}$, which can be the only solution. Consequently $K_{i+1} = (-1)^i \cdot i!$ and the lemma is proved. □

Chapter 7

Special Eisenstein polynomials

In this chapter we show how it is possible to define a normal form for Eisenstein polynomials, which can be used for quickly enumerating totally ramified extensions of a local field, for selecting a special defining polynomial to represent extensions, and for identification of the extensions. Unluckily it doesn't seem possible to produce easily exactly one special polynomial for each isomorphism class of extensions, but we show how to obtain a very restricted set of polynomials generating each extension. The number of special polynomials generating a fixed extension L/K is not greater than the number of conjugates of L over K, so that each Galois extensions is generated by exactly one polynomial. In fact, the problem of selecting exactly one generating polynomial for each isomorphism class appears to be as hard as that of determining the cardinality of the group of automorphisms of the extension generated by a polynomial.

As shown in [PR01], it is possible to enumerate and identify the extensions generated by Eisenstein polynomials selecting one polynomial for each neighborhood with respect to a suitable distance, and applying Panayi root finding algorithm to collect the polynomials generating the same extension. The search space can be drastically reduced by just taking into account Eisenstein polynomials in normal form.

Furthermore, for each Eisenstein polynomial generating an extension L/K of degree n there exists a quick way to recover all the special polynomials attached to the extension. The procedure does not require an exhaustive search over the space of all extensions of degree n of K, not even a search within the set of polynomials generating extensions with fixed ramification data.

Indeed, any Eisenstein polynomial can be put into normal form by applying greedily a reduction algorithm, which however allows some free choices during the reduction. The full set of special polynomials is obtained as the set of all possible outputs of the reduction algorithm, over all possible choices.

A family of unique representatives for Eisenstein polynomials was already defined long time ago by Krasner [Kra37], and it turns out that Krasner special representative is one of the special polynomials we consider, when the sets of representatives in the definition are taken to force as many terms to be 0 in the p-adic expansions of the coefficients. The unique Krasner representative is not easy to characterize in terms of the coefficients, while from our point of view we have a very restricted set of polynomials that can be easily described. Curiously Krasner work appears to be unknown to many people working in the field, and is not taken into account in many recent works, such as in [PR01, JR06].

We exhibit a criterion for establishing *a priori* that an Eisenstein polynomial $f(T)$ may not be converted to another polynomial $g(T)$ via such a reduction applied greedily, and when $f(T)$ and $g(T)$ are any two Eisenstein polynomials such that one of them is known to generate a Galois extension then the criterion can be used to show that $f(T)$ and $g(T)$ generate non-isomorphic extensions. The criterion takes into account the higher order terms appearing in the p-adic expansion of the coefficients, not just the valuation (or first-order expression) of $f(\pi) - g(\pi)$ for a uniformizer π of an extension L/K of degree n. The criterion established in [Yos11] for totally ramified Galois extensions over $\mathbb{Q}_p$ is also recovered in a more general context.

In the last section we describe an algorithm that allows to construct the unique special Eisenstein polynomial generating a totally ramified class field, given a suitable description of a norm subgroup. In particular, we show that there exists an ordering of the terms appearing in the p-adic expansions of the coefficients allowing to recover all the terms of the special polynomial, by solving inductively linear equations over the residue field. An algorithm for the construction of polynomials generating class field was described in [Pau06] for cyclic extensions, where an extension of degree p^m is constructed inductively by steps of degree p. In our construction an Eisenstein polynomial generating an arbitrary totally ramified class field is constructed directly. For each closed subgroup we obtain exactly one extension of degree equal to the index, which has additionally to be Galois, so we also obtain an alternate and constructive proof of the Existence Theorem of local class field theory.

Notation

We will assume that K has finite residue field, and set $e_K = v_K(p)$ as usual. If L/K is any totally ramified extension of degree n, with k distinct ramification breaks say, we will usually denote with $t_1 < t_2 < \cdots < t_k$ the ramification breaks. We will denote as $\gamma_0 > \gamma_1 > \cdots > \gamma_k$ the cardinalities of the corresponding ramification subsets (see §3.3, Chap. 3), so that $\gamma_0 = \#\Gamma = n$ and $\gamma_i = \#\Gamma_{t_i^+}$ for $1 \leq i \leq k$. The γ_i are all powers of π, except possibly for $\gamma_0 = n$. We will denote by L_{t_i} and $L_{t_i^+}$ the fields fixed by Γ_{t_i} and $\Gamma_{t_i^+}$ respectively.

If p^s is the biggest power of p dividing n, for each $0 \leq \ell \leq s$ it will also be convenient putting τ_ℓ to be equal to the smallest real t such that $n\phi_{L/K}(x)$ has slope $\leq p^\ell$ for $x \geq t$, it will be equal to either 0, or some ramification break t_i. The τ_ℓ are weakly decreasing and exhaust all the lower ramification breaks t_i, and one break $t_i > 0$ is repeated r times if $(\Gamma_{t_i} : \Gamma_{t_i^+})$ is equal to p^r, so each ramification break is taken "with its multiplicity" in a suitable sense. It will also be convenient defining

$$\xi_\ell = n\phi_{L/K}(\tau_\ell) - p^\ell \tau_\ell, \qquad \sigma_\ell = n\phi_{L/K}(\tau_\ell),$$

for each $0 \leq \ell \leq s$. Up to a factor n the σ_ℓ are the upper ramification breaks of the extension.

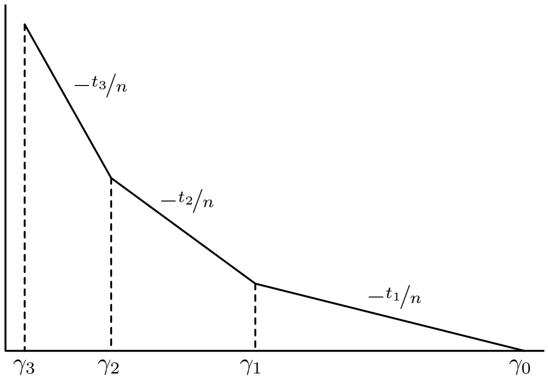
7.1 Reduction algorithm and the family of reduced polynomials

Let $f(T) = T^n + f_{n-1}T^{n-1} \dots f_1 T + f_0$ be a monic Eisenstein polynomial of degree n, let π be a root in a fixed algebraic closure K^{alg} and put $L = K(\pi)$. Then clearly $f(T)$ is the minimal polynomial of π, which is a uniformizing element of the extension determined by $f(T)$, and we are interested in understanding how the coefficients of the minimal polynomial of a uniformizer change when π is replaced by another uniformizer $\rho = \pi + \theta\pi^{m+1} + \dots$, for some unit $\theta \in U_K$ and integer $m \geq 1$. Since the following computation only depends on θ at the first order, θ may be taken to be a multiplicative representative.

Let us consider the ramification polynomial $\Phi(T) = \pi^{-n} f(\pi T + \pi)$, its Newton polygon is fully described by the lower ramification breaks. For $\alpha \in \mathcal{O}_K$ we can compute a lower bound for the valuation of $\Phi(\alpha)$ as function of $v_L(\alpha)$ starting from the Newton polygon of $\Phi(T)$. The construction produces naturally the *Newton copolygon*, which is essentially the dual convex body of the Newton polygon, and is connected to the Hasse-Herbrand transition function as already observed in [Lub81, Li97]; in such references $f(T + \pi)$ was used instead so the function obtained was slightly different from the classical Hasse-Herbrand defined in [FV02, Ser79].

Indeed, the Newton polygon of the polynomial $\Phi(\pi^m T)$ resulting by the substitution $T \to \pi^m T$ can obtained from the polygon of $\Phi(T)$ moving the points with abscissa x up by $\frac{m}{n}x$. In other words, if $N : [1, n] \to \mathbb{R}$ is the real function describing the polygon of $\Phi(T)$, the polygon of $\Phi(\pi^m T)$ is described by $N(x) + \frac{m}{n}x$.

The function $N(x)$ is convex and piecewise linear, and by the well known properties of Newton polygons the slopes are $-{t_k}/{n}, \dots, -{t_1}/{n}$ where $t_1 < t_2 < \dots < t_k$ are the lower ramification breaks of the extension generated by a root, and it has slope $-{t_i}/{n}$ in the interval $[\gamma_i, \gamma_{i-1}]$ where $\gamma_0 > \gamma_1 > \dots > \gamma_k$ are the cardinalities of the corresponding ramification subsets. We put $t_0 = +\infty$, $t_{k+1} = -\infty$ for convenience.



Let's consider the minimum achieved by the function $N(x) + \frac{m}{n}x$ in the interval $[1, n]$, as a function of the real parameter m. It is again a piecewise linear function with slope γ_i/n for $t_i \leq m \leq t_{i+1}$, and we obtain that this minimum value function is exactly the Hasse-Herbrand function $\phi_{L/K}(m)$. Hence this is the smallest valuation (with respect to K) of the coefficients of $\Phi(\pi^m T)$, and $\pi^{-n\phi_{L/K}(m)}$ is the exact power of π such that $\pi^{-n\phi_{L/K}(m)}\Phi(\pi^m T)$ is in $\mathcal{O}_L[T]$ and non trivial modulo $\mathfrak{p}_L$.

Let's define the valuation of a polynomial to be the smallest valuation of the coefficients, we can resume what proved in the following

Proposition 7.1.1. *Let $f(T)$ be an Eisenstein polynomial, π a root, $L = K(\pi)$ and $\Phi(T) = \pi^{-n}f(\pi T + \pi)$ its ramification polynomial. Then*

$$v_L(\Phi(\pi^m T)) = n\phi_{L/K}(m).$$

It will also be convenient to deduce an expression for the values $N(p^\ell)$ for each $\ell \geq 0$ such that $p^\ell \mid n$. Starting from p^ℓ the function $N(x)$ has slope $-\tau_\ell/n$, so $N(x) + \frac{\tau_\ell}{n}x$ has infimum equal to $\phi_{L/K}(\tau_\ell)$, which is achieved for $x = p^\ell$ and is also equal to $N(p^\ell) + \frac{\tau_\ell}{n}p^\ell$, so we obtain

$$N(p^\ell) = \phi_{L/K}(\tau_\ell) - \frac{\tau_\ell}{n}p^\ell = \frac{\xi_\ell}{n}.$$

Lemma 7.1.2. *For each $\ell \geq 0$ such that $p^\ell \| n$ we have $N(p^\ell) = \xi_\ell/n$.*

We will also prove another Lemma, which will be needed require later. If p^ℓ is the abscissa of a vertex of the Newton polygon we have that the terms contributing to the coefficient of T^{p^ℓ} in the ramification polynomial give to the coefficient of T^{p^j} contributions having K-valuation at most $e_K(\ell - j)$ bigger, for $j < \ell$. In other words we have that $N(p^j) < e_K(\ell - j) + N(p^\ell)$, for each $j \leq \ell$. Considering the last vertex of one side of the Netwon polygon, and since for each ℓ the slope is equal to $-\tau_\ell/n$ in the interval $[p^\ell, p^{\ell+1}]$ and $N(p^\ell) < e_K + N(p^{\ell+1})$, we have that then τ_ℓ has to be at most $n\frac{e_K}{(p^{\ell+1} - p^\ell)} = e_L/(p^{\ell+1} - p^\ell)$. Hence we have

Lemma 7.1.3. *We have*

$$\xi_j \leq e_L(\ell - j) + \xi_\ell$$

for each $j < \ell$, and furthermore

$$\tau_\ell \leq {}^{e_L}\!/\!_{(p^{\ell+1}-p^\ell)}$$

for each ℓ.

We now study the points $(j, v_K(\Phi_j))$, coming from a monomial $\Phi_j T^j$, that may lie on the boundary of the Newton polygon of $\Phi(T) = \sum_{i=0}^n \Phi_i T^i$. We claim that either their ordinate j is a power of p, either $\gamma_1 \mid j$, and the latter is only possible when $\gamma_0 = n$ is not a power of p, so that γ_1 is the biggest power of p dividing n, and the polygon of $\Phi(T)$ has slope 0 in the interval $[\gamma_1, \gamma_0]$.

Indeed, for each r we have

$$\Phi_r = \sum_{i=r}^{n} \binom{i}{r} f_i \pi^{i-n},$$

and since the summands have different valuations modulo n the valuation of Φ_r has to be equal to the minimal valuation of such terms. Consider $v_K(\binom{i}{r} f_i \pi^{i-n})$ as a function of r: then its minimum is obtained when r is the biggest power of p dividing i, and if $p^\ell|i$ then $v_K(\binom{i}{r} f_i \pi^{i-n})$ is at least $v_K(\binom{i}{p^\ell} f_i \pi^{i-n})$ when $p^{\ell+1} \nmid r$, and strictly bigger if $p^\ell \nmid r$. So when $p^\ell \| r$ we have that $v_L(\Phi_r) \geq v_L(\Phi_{p^\ell})$, and $(r, v_K(\Phi_r))$ cannot be on the boundary of the polygon unless possibly when the segment containing p^ℓ has horizontal slope, $p^\ell = \gamma_1$ and $p^\ell \mid r$.

For integer $m \geq 0$ let's consider the polynomials

$$S_m(T) = \overline{\pi^{-n\phi_{L/K}(m)} \Phi(\pi^m T)}.$$

If $m \geq 1$, or n is a power of p, then $S_m(T)$ is of the form

$$S_m(T) = \sum_{i=a}^{b} c_i T^{p^i}$$

for some coefficients c_i, where $p^a = p^b = \gamma_i$ when m is not a ramification break and $m \in (t_{i+1}, t_i)$ say, while $\gamma_i = p^a$ and $\gamma_{i-1} = p^b$ if $m = t_i$ for some i. In particular they are additive polynomials.

On the other hand if $m = 0$ and n is not a power of p (and hence L has a non-trivial tamely ramified subextension) the terms appearing in $S_0(T) = \overline{\Phi(T)}$ are all coming from the leading monomial T^n, so that putting $n' = {}^{n}\!/\!_{\gamma_1}$ we have

$$\begin{aligned} S_0(T) &= \sum_{j=1}^{n'} \binom{n}{\gamma_1 j} T^{\gamma_1 j} \\ &= \sum_{j=1}^{n'} \binom{n'}{j} T^{\gamma_1 j} \end{aligned}$$

$$= (1 + T^{\gamma_1})^{n'} - 1.$$

We collect these facts in the following proposition.

Proposition 7.1.4. *If $m \geq 1$ the polynomial $S_m(T)$ is an additive polynomial, which is composed by more than one monomial if and only if m is a lower ramification break. For $m = 0$ we have $S_0(T) = (1 + T^{p^s})^{n'} - 1$, where $n = p^s n'$ and $(p, n) = 1$.*

When the context is clear, we will abuse of notation and also denote by S_m the induced map $\theta \mapsto S_m(\theta)$ over the residue field or an extension thereof.

7.1.1 Change induced on the coefficients by a substitution

We study now the effect of replacing the minimal polynomial $f(T)$ of π with the minimal monic polynomial $g(T)$ of a different uniformizer ρ.

Let's take $\rho = \pi + \theta\pi^{m+1} + \dots$, we will identify the term $(f_i - g_i)\rho^i$ that has minimal valuation for general θ, which gives information about the most significant change induced on the coefficients $f_i \to g_i$ as consequence of the substitution $\pi \to \rho$.

The non-zero terms $(f_i - g_i)\rho^i$ have valuations with different remainders modulo n, and furthermore we have

$$\begin{aligned}\sum_{i=0}^{n-1}(f_i - g_i)\rho^i &= f(\rho) - g(\rho) \\ &= f(\rho) = \pi^n\Phi(\theta\pi^m + \dots),\end{aligned}$$

considering the definition of ρ. If $m \geq 1$, being $\rho \equiv \pi \pmod{\mathfrak{p}_K^2}$ we obtain the following Lemma, after dividing by $\pi^{n(\phi_{L/K}(m)+1)}$ and reducing the expression modulo $\mathfrak{p}_K$.

Lemma 7.1.5. *If $m \geq 1$ and $g(T)$ is the minimal monic polynomial of an element of the form $\rho = \pi + \theta\pi^{m+1} + \dots$ we have*

$$\overline{(f(\pi) - g(\pi)) \cdot \pi^{-n(\phi_{L/K}(m)+1)}} = S_m(\theta).$$

Since $n \mid v_L(f_i - g_i)$ for each i, the unique term $(f_i - g_i)\pi^i$ of $f(\pi) - g(\pi)$ that may contribute to the left hand side is for i satisfying

$$i \equiv n(\phi_{L/K}(m) + 1) \pmod{n},$$

so i is uniquely determined being $0 \leq i < n$. We observe that if $m \geq 1$ is not a lower ramification break then S_m is surjective being κ_K finite and hence perfect, while if $m = t_i$ for some i then it may not be surjective, when the additive polynomial $S_{t_i}(T)$ has a root over the residue field κ_K.

Assume that t_i is an integer, we will later show that the polynomial $S_{t_i}(T)$ only depends on the field extension L/K and on the class of $\pi \mod \mathfrak{p}^2$, as a consequence of a stronger result, Theorem 7.2.5, which is proved independently. For the moment we can give a definition of reduced polynomial without assuming this invariance, even though the definition will be less manageable from a practical point of view.

Let I_m be the image of S_m, and also its preimage in $\mathcal{O}_L$ when the context is clear. Lemma 7.1.5 says that passing to the minimal polynomial of an element of the form $\pi + \theta\pi^{m+1} + \dots$, if $n(\phi_{L/K}(m)+1) = jn+i$ with $0 \leq i \leq n$, we can change the corresponding term f_i by an element of $\pi^{nj} I_m$ while all other terms $f_r \pi^r$ are unchanged modulo π^{jn+i+1}. Since the polynomials S_r for $r \leq m$ are certainly unchanged too, this observation motivates the following definition.

Definition 7.1.6. Let $f(x)$ be an Eisenstein polynomial, and assume that each coefficient f_i has an expansion

$$f_i = \sum_{j \geq 1}^{\infty} f_{i,j} \pi_K^j$$

with $f_{i,j} \in R$ for a fixed set of residue representatives R, and where π_K is a fixed uniformizer of K, and let $\bar{\eta}_f = \overline{{-f_0}/{\pi_K}}$. Assume the choice of a set $A_0 \subset \kappa_K^\times$ of representatives of $\kappa_K^\times/(\kappa_K^\times)^n$, and for each additive polynomial $S_m(T)$ for $m \geq 1$ a set of elements $A_m \subset \kappa_K$ that are representatives of the cokernel of the map $\theta \mapsto \eta_f^j S(\theta)$, where $j = [\phi_{L/K}(m)+1]$.

We say that $f(x)$ is *reduced* (with respect to the choice of the A_i) when we have

1. $\bar{\eta}_f = \overline{-{f_0}/{\pi_K}}$ is in A_0,
2. for each $m \geq 1$, if $n(\phi_{L/K}(m)+1) = jn+i$ for positive integers i, j with $i < n$, then we have $\overline{f_{i,j}} \in A_m$

We say that $f(x)$ is *reduced up to the level* r when condition 1 is satisfied, and condition 2 holds for all $m \leq r$.

If $f(T)$ is any Eisenstein polynomial, it's easy to see that the polynomial $\theta^n f(\theta^{-1}T)$ satisfies condition 1 for some suitable θ. A polynomial reduced up to level 0 can be obtained by the following algorithm.

Algorithm 1 Reduction (step 0)

```
$\bar{\alpha} \leftarrow \overline{{-f_0}/{\pi_K}}$,
$\bar{\beta} \leftarrow Representative(\bar{\alpha}, (\kappa_K^\times)^n)$,
$\bar{\theta} \leftarrow Solve(T^n = \bar{\beta}/\bar{\alpha})$,
$\theta \leftarrow Lift(\bar{\theta})$,
return $\theta^n f(\theta^{-1}T)$.
```

If i, j are as above, we have shown above $f_{i,j}\pi_K^j$ can be changed by any element in $\pi^{nj} I_m$ modulo π^{nj+1}, so $\overline{f_{i,j}}$ can be changed by any element of

$\overline{({}^{\pi^n}/_{\pi_K})^j I_m}$. Since $\pi^n = -f_0 + \dots$ we have that $\overline{({}^{\pi^n}/_{\pi_K})} = \bar{\eta}_f$, so $\overline{f_{i,j}}$ is changed by an element of $\bar{\eta}_f^j I_m$, while η_f is unchanged when passing to the minimal polynomial of an uniformizer of the form $\pi + \theta\pi^{m+1} + \dots$.

In particular, if $f(x)$ is reduced up to the level $m-1$ we can obtain a polynomial reduced up to the level m via the following reduction step.

Algorithm 2 Reduction (step m)

```
$j \leftarrow \lfloor \phi_{L/K}(m) + 1 \rfloor$,
$i \leftarrow n \cdot \{\phi_{L/K}(m) + 1\}$,
$\bar{\alpha} \leftarrow \overline{f_{i,j}}$,
$\bar{\beta} \leftarrow \mathit{Representative}(\bar{\alpha}, \mathrm{image}(\bar{\eta}_f^j S_m))$,
$\bar{\theta} \leftarrow \mathit{Solve}(\bar{\eta}_f^j S_m(T) = \bar{\alpha} - \bar{\beta})$,
$\theta \leftarrow \mathit{Lift}(\bar{\theta})$,
$F(T) \leftarrow T + \theta T^{m+1} + \{\text{any terms of degree} \geq m+2\}$,
return $\mathit{Resultant}_U(f(U), T - F(U))$.
```

Indeed, if $g(T)$ is the returned polynomial we have

$$\overline{(f_{i,j} - g_{i,j})\pi_K^j \pi^{i-n(\phi_{L/K}(m)+1)}} = \overline{(f_{i,j} - g_{i,j})}\bar{\eta}_f^{-j} = S_m(\bar{\theta}),$$

and consequently $\overline{g_{i,j}} = \bar{\beta} \in A_m$. Since we allow any higher order term in the choice of $F(T) = T + \theta T^{m+1} + \dots$, we anticipate that for a suitable $F(T)$ it will not be necessary to compute the resultant appearing in the algorithm as the determinant of a big matrix with coefficients in $K[T]$, see Remark 7.2.6.

Remark 7.1.7. *If m is bigger than the biggest lower ramification break t_k, then $S_m(x)$ is surjective, and the function $n(\phi_{L/K}(m)+1)$ assumes as possible values all integers $> n(\phi_{L/K}(t_k)+1)$. Consequently we can arbitrarily change all the representatives $f_{i,j}$ whenever*

$$v_L(\pi_K^j \pi^i) = nj + i > n(\phi_{L/K}(t_k) + 1), \tag{7.1}$$

without affecting the generated extension, turning them all to 0 for instance. In this way we recover the well known quantitative criterion on the distance of two Eisenstein polynomials ensuring that they generate the same extension, as considered in [Kra62, PR01, Yos11].

7.1.2 Characterizing reduced polynomials

We start with a few remarks about Definition 7.1.6. Since we allow a different choice of the representing sets A_m for each m, where the 0 element of the image of the map is not even requested to be represented by 0, we have that each Eisenstein polynomial is reduced for a suitable choice of the A_m. This choice is very far from what would be recommended in a computer algebra system, but it will be useful to be able to consider each Eisenstein polynomial as already reduced.

On the other hand on a computer algebra system we can expect to have a more or less canonical way for selecting representing elements of a quotient, and selecting 0 as representative of the zero element in the quotient. Under this hypothesis we clarify here how a reduced polynomial looks like. In particular we will see that, for each $\ell \geq 0$ such that p^ℓ divides n, the possible valuations of the terms $f_{i,j}\pi_K^j\pi^i$ such $p^\ell \| i$ belong to one fixed interval, *with some exception.*

Fix ℓ and let us consider the terms $f_{i,j}\pi_K^j T^i$ with $p^\ell \| i$, we deduce a lower bound for the value of $nj + i$ from the shape of the Newton polygon of the ramification polynomial. Indeed, the contribution to the coefficient of T^{p^ℓ} in $\Phi(T)$ is

$$\pi^{-n} f_{i,j}\pi_K^j \pi^i \binom{i}{p^\ell},$$

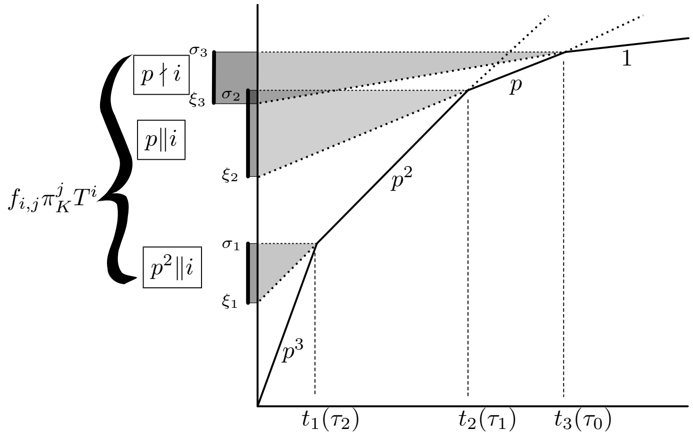
and since the contributions coming from different monomials of $f(T)$ have different valuations modulo n then their smallest valuation should be at least $nN(p^\ell) = \xi_\ell$. In the same way we obtain that any term $f_{i,j}\pi_K^j T^i$ with $p^\ell \| i$ and $nj - n + i \geq \xi_\ell$ is compatible with the ramification data, and when $p^\ell \| \xi_\ell$ and p^ℓ is the abscissa of a vertex of the ramification polygon then there should be a term $f_{i,j}\pi_K^j T^i$ such that the valuation $nj - n + i$ of the contributed term is exactly ξ_ℓ, this case corresponds to a vertex of the Netwon polygon and hence the minimum is reached.

We will show now that all the terms $f_{i,j}\pi_K^j T^i$ with $p^\ell \| i$ and such that $nj + i$ is big enough are turned to 0 by the reduction algorithm, with a few exceptions. Indeed, we claim that the integers that are multiple of p^ℓ and $> n\phi(\tau_\ell) = \sigma_\ell$ are all of the form $n\phi_{L/K}(m)$ for some $m > t_\ell$ (note that σ_ℓ may not be a multiple of p^ℓ itself, we are considering non-Galois extensions and the t_r and $\phi(t_r)$ may not be integers).

To show the claim we work by induction on the number of ramification breaks. If $p^\ell < \gamma_{k-1}$ then $\tau_\ell = t_k$, and $nN(1)$ is certainly an integer being equal to $v_L(\mathscr{D}_{L/K})$, and $n\phi_{L/K}(m)$ for integer m assumes as values all integers that are $> n\phi_{L/K}(t_k)$, being $n\phi_{L/K}(x)$ equal to $nN(1) + x$ for integer $m > t_k$. Assume instead $p^\ell \geq \gamma_{k-1}$, then by induction $\frac{n}{\gamma_{k-1}}\phi_{L_{t^+_{k-1}}/K}(m)$ takes as values any multiple of p^ℓ/γ_{k-1} bigger than $\frac{n}{\gamma_{k-1}}\phi_{L_{t^+_{k-1}}/K}(\tau_\ell)$ for integer $m > \tau_\ell$. So $n\phi_{L_{t^+_{k-1}}/K}(x)$ satisfies the required property with respect to p^ℓ, and so does $n\phi_{L/K}(x)$, which is obtained as the minimum of $n\phi_{L_{t^+_{k-1}}/K}(x)$ and $nN(1) + x$.

Consequently we have from the claim that all the terms $f_{i,j}\pi_K^j$ with $p^\ell \| i$ and $nj - n + i \geq \sigma_\ell$ can be forced to satisfy $f_{i,j} = 0$, except possibly when $nj - n + i$ is itself equal to σ_r for some $r \leq \ell$, in this case we can only force $f_{i,j}$ to be a suitable representative depending on the image of the polynomial $S_{\tau_r}(T)$, which may not be surjective as a function over κ_K.

In the case of three breaks we have the following figure representing the values $nj - n + i$ of the terms of a reduced polynomial.



We state the above results in the following proposition.

Proposition 7.1.8. *Let $f(x)$ be a reduced Eisenstein polynomial, and assume that each coefficient f_i has an expansion*

$$f_i = \sum_{j\geq 1}^{\infty} f_{i,j}\pi_K^j.$$

Assume $p^\ell \| i$, then $f_{i,j}$ is non-zero only when

$$\xi_\ell \leq nj - n + i < \sigma_\ell,$$

or when $nj-n+i$ is equal to some σ_r and the corresponding additive polynomial $S_{\tau_r}(T)$ has a root in κ_K.

In other words we have that starting from a certain points all terms $f_{i,j}\pi_K^j$ for $p^\ell \| i$ can all be simplified to 0, except at upper ramification breaks. We will later see how this phenomenon can be interpreted in terms of local class field theory for abelian extensions, or in connection with Serre mass formula [Ser78] in some simple case.

7.1.3 Representation of automorphism as power series

Applying such substitutions for increasing m we are taking into account all transformations $F(\pi)$ of π by a power series without constant coefficient $F(T) = \theta_1 T + \theta_2 T^2 + \dots$ that may provide an element whose minimal polynomial is reduced, because any such power series can be written as a composition of polynomials of the form θT and $T(1+\theta T^m)$. Applying the above reduction step for increasing m, when m is not equal to a ramification break t_i we have a unique possible choice for the class $\bar{\theta}$ of θ in the substitution $\pi \to \pi(1+\theta\pi^m)$. When $m = t_i$ for some i, the choice for $\bar{\theta}$ is defined up to an element that is a root of $S_{t_i}(T)$, and taking into account representatives θ for all possible choices for $\bar{\theta}$ we can track all possible outputs. We can run this algorithm starting from the set $\{f(T)\}$ and replacing each polynomial with the set of all possible outputs, which may not be unique at the ramification breaks t_i, and do so up to the level t_k. After this last step we obtain reduced polynomials turning to 0 all the $f_{i,j}$ for i, j such that $nj + i > n(\phi_{L/K}(t_k) + 1)$.

Algorithm 3 All reduced polynomials

```
$\{t_1, \dots, t_k\} \leftarrow \mathit{LowerRamificationBreaks}(f(T))$
$A \leftarrow \{f(T)\}$
for $m = 0 \to t_k$ do
  $B \leftarrow \emptyset$
  for $g(T) \in A$ do
    $B \leftarrow B \cup \mathit{AllReductions}(g(T), m)$
  end for
  $A \leftarrow B$
end for
$a \leftarrow [\phi_{L/K}(t_k) + 1]$
$b \leftarrow n \cdot \{\phi_{L/K}(t_k) + 1\}$
return $A \mod (\pi^{a+1}, \pi^a T^b)$
```

Since some outputs may be repeated we end with a multiset of reduced polynomials. Clearly different power series $F(T)$, $G(T)$ may give the same value $F(\pi) = G(\pi)$ when evaluated in π, but we will show that we took into account all the different *values* $F(\pi) \in L$ such that the minimal polynomial of $F(\pi)$ is reduced.

Indeed, in step 0 we considered all possible values for $F(\pi)$ modulo $\mathfrak{p}_L^2$, and assume by induction that all the $F(\pi)$ taken into account up to step $m-1$ cover all possible values modulo $\mathfrak{p}_L^{m+1}$. The values $F(\pi) + \theta F(\pi)^{m+1} + \dots$ covered in step m, for all admissible representatives θ, will provide all possible values modulo $\mathfrak{p}_L^{m+2}$.

Let $\rho_i(\kappa_K)$ be the cardinality of $\kappa_K^\times/(\kappa_K^\times)^n$ if $t_i = 0$, and let it be the number of roots of $S_{t_i}(x)$ contained in κ_K if t_i is an integer and > 0. The cardinality of the multiset of polynomials obtained as output of the algorithm can be computed counting for each m the number of possible choices, which is indeed equal to $\rho_i(\kappa_K)$ for $t_i = m$ when there is no unique choice. The total cardinality is equal to the product of the $\rho_i(\kappa_K)$ over all i such that t_i is an integer, that is

$$B_{L/K} = \prod_{\substack{1 \le i \le k \\ t_i \in \mathbb{Z}}} \rho_i(\kappa_K).$$

We give now an interpretation of the $\rho_i(\kappa_K)$ as the number of automorphism of intermediate extensions. Indeed, if $t_i = 0$ then $\rho_i(\kappa_K)$ counts the number of n-th roots of the unity in κ_K, or equivalently of n'-th roots if $n = p^s n'$ with $(n', p) = 1$, which is also the number of automorphisms of a tame extension of degree n' of K, like L_{0^+}/K is.

For $t_i > 0$ let's consider the intermediate extension $L_{t_i^+}/L_{t_i}$: if $g(T)$ is the minimal polynomial of π over L_{t_i} (which is a factor of $f(T)$) then

$$\overline{\pi^{-n(\phi_{i-1}(t_i)+1)}g(\pi^{t_i+1}T+\pi)} = S_{t_i}(T),$$

and consequently representatives θ of the roots of $S_{t_i}(T)$ are exactly those such that

$$\sigma(\pi)/\pi = 1 + \theta\pi^{t_i} + \dots$$

for some L_{t_i}-automorphism $\sigma \in \operatorname{Aut}(L^{\mathrm{sep}}/L_{t_i})$. Now after extending the elements of $\Gamma_{t_i^+}$ to the normal closure we have $\Gamma_{t_i^+}(\sigma|_L) = \sigma\Gamma_{t_i^+}$, this is immediate considering $\Gamma_{t_i^+}$ as the image of elements of a ramification (normal) subgroup of a bigger Galois extension containing L. Consequently averaging over $\Gamma_{t_i^+}$ we obtain

$$\sigma(\pi_{L_{t_i^+}})/\pi_{L_{t_i^+}} = 1 + \theta^{\gamma_i}\pi_{L_{t_i^+}}^{t_i} + \dots,$$

where $\pi_{L_{t_i^+}} = N_{L/L_{t_i^+}}(\pi)$. The equality holds because t_i is smaller than the all ramification numbers of the extension $L/L_{t_i^+}$, by keeping into account the properties of the norm map $N_{L/L_{t_i^+}}$ (see §3.2.1, Chap. 3, and [FV02, Chap. 3, §1, Prop. 1.5]).

If $\sigma(\pi_{L_{t_i^+}}) \in L_{t_i^+}$ then $\bar{\theta}$ is in κ_K, and on the other hand if $\bar{\theta} \in \kappa_K$ then $\sigma(\pi_{L_{t_i^+}})$ can be approximated better than any other conjugate of $\pi_{L_{t_i^+}}$ having $L_{t_i^+}/L_{t_i}$ only one ramification break, and consequently $\sigma(\pi_{L_{t_i^+}}) \in L_{t_i^+}$ by Krasner Lemma. In other words we have one root of $S_{t_i}(T)$ in κ_K for each conjugate of $\pi_{L_{t_i^+}}$ contained in $L_{t_i^+}$, and $\rho_i(\kappa_K) = \#\operatorname{Aut}(L_{t_i^+}/L_{t_i})$.

So we have that $B_{L/K}$ is an invariant of the extension L/K. Considering the subgroups $\operatorname{Aut}(L/L_{t_i})$ of $\operatorname{Aut}(L/K)$ and the corresponding quotients as subgroups of $\operatorname{Aut}(L_{t_i^+}/L_{t_i})$, we observe that $B_{L/K}$ provides a "naive" upper bound to the cardinality of $\operatorname{Aut}(L/K)$, but which is in general tighter than the full degree $[L : K]$.

Let $f_1(x), \dots, f_r(x)$ be all the reduced polynomials obtained applying the above algorithm. The number of times we obtain the same polynomial $f_i(x)$ is equal to the number of distinct $F_j(\pi)$ such that $f_1(F_j(\pi)) = 0$, and is consequently equal to the number of roots of $f_i(x)$ contained in L, in another words to the cardinality of $\operatorname{Aut}(L/K)$.

Theorem 7.1.9. *Each extension L/K is generated by a reduced polynomial, and the number of reduced polynomials generating a fixed extension L/K is*

$$B_{L/K}/\#\operatorname{Aut}(L/K).$$

If $f(x)$ is an Eisenstein polynomial such that a root generates an extension isomorphic to L, then the reduction algorithm outputs a multiset of cardinality $B_{L/K}$ formed by the reduced polynomials, each having multiplicity $\#\operatorname{Aut}(L/K)$.

We remark that if $F(T)$ is a power series such that $F(\pi)$ is a conjugate of π, the algorithm giving the set of special polynomials can collect all the θ used in the substitutions $\pi \to \pi + \theta\pi^{m+1}$ to produce an expression of

$$F(T) \mod (f(T), T^{t_k+1}),$$

which can be used to realize the group $\mathrm{Aut}(L/K)$ as group of truncated power series under composition, we omit the details of the construction.

Note that there is a unique reduced representative for Eisenstein polynomials generating Galois extensions, while in general we have a set of polynomials with cardinality equal to the ratio of the “naive” bound on the number of automorphisms to the real number of automorphisms. We remark that extinguishing the redundancy from the above family of reduced polynomials seems to be at least as hard as computing the cardinality of the automorphism group. This can probably be done in a few particular cases, possibly for polynomials of degree p^2 over an unramifed extension of $\mathbb{Q}_p$, but a criterion to determine the cardinality of the group of automorphisms is required.

When L/K has only one ramification break, or when L/K is Galois, then we have a unique representative, so the unique Krasner representative is easily described in terms of the coefficients. This was already remarked in the original Krasner paper [Kra37, page 167, after the proof of Theorem V].

7.1.4 Amano polynomials and Serre mass formula

We provide here some qualitative observation, without being completely rigorous. First, if the degree n is prime with p it's easy to say what are reduced polynomials, and they are all of the form $T^n + \theta\pi_K$ for some representative $\theta \in R$ such that $\bar{\theta} \in A_0$, where A_0 is the chosen set of representatives of $K^\times/(K^\times)^n$.

When $n = p$, Amano defined in [Ama71] a set of special generating polynomials composed by trinomials. The equations considered here turn out to look much more complicated “visually” because they are no longer trinomials, but the number of parameters is clearly the same, and nevertheless Amano polynomials do not seem to be easily generalizable to higher degree.

Reduced polynomials of degree p are of the form

$$T^p + \sum_{i=1}^{p} \left(\sum_{\substack{pj+i \geq (p-1)t+p \\ pj+i < pt+p}} f_{i,j}\pi_K^j \right) \cdot T^i + \pi_K \left(+ f_{0,t+1}\pi_K^{t+1} \right),$$

for some ramification break t such that either $t = {}^{pe_K}/_{p-1}$, either t is $< {}^{pe_K}/_{p-1}$ and $(p-1)t$ is an integer prime with p. Furthermore the term $f_{0,t+1}\pi_K^{t+1}$ is present only when t is an integer and the additive polynomial $S_t(T)$ has a root in κ_K, which is precisely the case of the extensions being Galois.

We remark that given an extension L/K of degree p, then in the Galois cyclic case the uniformizer π_K may not be a norm by class field theory, so in general an additional term is indeed required. On the other hand if L/K is not Galois then π_K is always in $N_{L/K}(L^{\times})$.

We give one last interpretation of this fact, under the light of the proof of Serre “mass formula”. Considering the map

$$\left\{\begin{array}{l}\text{uniformizers of ex-}\\ \text{tensions of degree } p\end{array}\right\} \xrightarrow{\text{“minimal polynomial”}} \left\{\begin{array}{l}\text{Eisenstein polyno-}\\ \text{mials of degree } p\end{array}\right\}$$

we have a p-to-1 correspondence between measure spaces, whose scaling factor turns out to be determined by the discriminant of the extensions as proven in [Ser78]. Let’s restrict the map to the uniformizers of a fixed extension L/K in the algebraic closure, then either the extension is Galois and the map is still p-to-1, either the extension is not Galois and the map becomes 1-to-1, but in this case the image has bigger measure.

In other words, for fixed degree and restricting to extensions with fixed discriminant, the smaller is the space of polynomials generating one fixed isomorphism class of extensions, the bigger will be the automorphism group of these extensions. When applying the reduction algorithm to a polynomial of degree p generating L/K, we have that when the unique ramification break t is an integer and the additive polynomial $S_t(T)$ is not surjective we can do *less simplifications* to the coefficients of the Eisenstein polynomial. Since any Eisenstein polynomial generating L is a possible output of the reduction algorithm (for a suitable choice of the A_i) we have that the set of possible polynomials generating L turns out to be “smaller”, and that L/K is Galois having some non trivial automorphism and degree p.

For higher degree, and in particular when there are more ramification breaks, it becomes difficult to generalize this observation, because a modification that appears to be trivial at the first order may actually provoke some change to the higher order terms in the expansions. This fact also justifies the claim that reducing the family to have exactly one polynomial for each isomorphism class appears to be at least as hard as the computation of the number of isomorphisms for the extension determined by one Eisenstein polynomial.

7.2 A criterion to rule out possible reductions

To complement the above reduction algorithm we give a synthetic criterion to exclude an Eisenstein polynomial from generating an extension of which we know the set of all the reduced polynomials. In particular given two polynomials $f(T)$ and $g(T)$ we can often rule out early the possibility that a sequence of substitutions $\pi \to \pi + \theta\pi^{m+1} + \dots$, starting from level $m = r$ say, may transform the minimal polynomial $f(T)$ of π into the new minimal polynomial $g(T)$, without having to compute the complete reduction.

Let’s consider the monomial $(f_i - g_i)\pi^i$ having smallest valuation, which determines the valuation of $f(\pi) - g(\pi)$, and assume that its valuation is equal to $v = n(\phi_{L/K}(r)+1)$ for some real number r. Let’s select sets of representatives A_m that make $g(T)$ reduced, then we say that $f(T)$ can be reduced to $g(T)$

greedily if $g(T)$ is a possible output of the reduction algorithm applied to $f(T)$ starting from step $m = r$. The proof of the following proposition is clear.

Proposition 7.2.1. *If r is not an integer than $f(T)$ cannot be reduced greedily to $g(T)$.*

We also have the following proposition, whose proof is immediate as well.

Proposition 7.2.2. *If r is an integer equal to a lower ramification break and $(f_i - g_i)\pi^{i-v}$ is not in the image of $S_{t_i}(T)$, then $f(T)$ cannot be reduced greedily to $g(T)$.*

These observations are well complemented by the following proposition, which makes them particularly effective in the case of Galois extensions.

Proposition 7.2.3. *Assume that one of $f(T)$ or $g(T)$ is known to generate a Galois extension, then $f(T)$ and $g(T)$ generate the same extensions if and only if one polynomial can be greedily reduced to the other.*

Proof. For a suitable choice of representatives $g(T)$ is already reduced, and for Galois extensions there is only one reduced polynomial in view of Theorem 7.1.9, so applying greedily the reduction algorithm to $f(T)$ we obtain $g(T)$ as unique possible output. The other implication is clear. □

In other words for Galois extensions if $g(T)$ can be obtained in some way from $f(T)$, then it can also be obtained in the greedy way.

When considering wildly ramified Galois extensions over $\mathbb{Q}_p$ the $S_{t_i}(T)$ are the zero map over the residue field $\mathbb{F}_p$, so if r is a ramification break then $f(T)$ and $g(T)$ certainly generate non-isomorphic extensions, and we essentially recovered the main result of [Yos11].

However, it is possible to give a deeper criterion, which is more selective than what can be obtained via an inspection of $f(\pi) - g(\pi)$ at the first order.

Consider the range of monomials $f_{i,j}\pi_K^j T^i$ corresponding to one ramification break as described in Prop. 7.1.8, then the intuitive idea is that if we can obtain $f(T)$ from $g(T)$ applying reductions of parameter $m \geq r$ then the first r terms in each such interval must be equal, because such terms are not going to be changed by any reduction of order $\geq r$. Such ranges can be independently "brought up to the front" (with respect to the p-adic valuation) computing formally a ramification polynomial of $f(T) - g(T)$, and considering the coefficients of $T, T^p, T^{p^2}, \ldots$, as we can see observing the contributions to the coefficient of T^{p^ℓ} in the ramification polynomial. Consequently taking into account a ramification polynomial for $f(T) - g(T)$ provides a synthetic and effective formalism to describe how some sets of coefficients must be equal in order to be able to pass from $f(T)$ to $g(T)$ via reduction step.

What we are going to prove is closely related to what was done in [Hei96] and Theorem 4.6 in particular, and shares the philosophy that the sets of monomials $f_i T^i$ with a fixed valuation of i live an independent life from the other monomials, up to a certain extent, and that when a uniformizer is changed

$\pi \to \pi + \theta\pi^{m+1} + \dots$ the change induced on minimal polynomial satisfies a certain continuity (in [Hei96] a different kind of defining equation formed by a power series with coefficients in a set of representatives was used rather than Eisenstein polynomials, but the underlying principle is the same). From a more effective point of view, such a continuity provides an easily verifiable criterion to exclude a polynomial from generating one fixed extension, which is particularly effective in the case of Galois extensions thanks to Prop. 7.2.3. What we need seems not to follow directly from the results of [Hei96] and additional steps would be needed to switch to power series and back to Eisenstein polynomials, so we will avoid using the slightly cumbersome notation of [Hei96] and prove our result directly.

For integers $a \geq 0$ and w let's define P_{p^a}, resp. $P_{p^a}(w)$, as the module generated over $\mathcal{O}_K$ by the monomials cT^i such that $p^a \mid i$, resp. those monomials such that additionally $v_L(c) + i \geq w$. If $cT^i \in P_{p^a}(w)$ for some w, than we have

$$c\left(T + \theta T^{m+1} + \dots\right)^i - cT^i \in \sum_{j=0}^{a} P_{p^j}(w + e_L(a-j) + p^j m) \qquad (7.2)$$

as we can verify at once expanding the left hand side. Furthermore if $g \in P_{p^a}(w)$ and $h \in P_{p^b}(z)$ than clearly we have $gh \in P_{p^{\min\{a,b\}}}(w+z)$.

Lets consider the ramification polynomial $\Phi(T) = \pi^{-n} f(\pi T + \pi)$, then the coefficient of T^{p^a} is has valuation at least ξ_a. Assume $p^a \| i$, from a monomial $f_i T^i$ we have a contribution $\binom{i}{p^a} f_i \pi^{i-n} T^{p^a}$ to the coefficient of T^{p^a} in $\Phi(T)$, so $v_L(f_i) + i - n$ should be at least ξ_a, and consequently the monomial $f_i T^i$ is contained in $P_{p^a}(\xi_a + n)$, being $v_L(f_i) + i \geq \xi_a + n$.

Consequently we have obtained that

$$f(T) \in \sum_{j=0}^{s} P_{p^j}(\xi_j + n), \qquad (7.3)$$

where s is the biggest integer such that $p^s \mid n$ (recall that $\xi_s = 0$).

What observed above we obtain the following.

Proposition 7.2.4. *Let $F(T) = T + \theta_{m+1}T^{m+1} + \theta_{m+2}T^{m+2} + \dots$, then*

$$f(T) \equiv f(F(T)) \mod \sum_{j=0}^{s} P_{p^j}(\xi_j + n + p^j m). \qquad (7.4)$$

Proof. Let's consider $f(T) - f(F(T))$, we will show that a monomial $f_i T^i$, which is contained in $P_{p^a}(\xi_a + n)$ by (7.3) say, yields various terms each having valuation at least $\xi_j + n + p^j m$ and in P_{p^j}, for some $j < a$. But we obtain terms in $P_{p^j}(\xi_a + n + e_L(a-j) + p^j m)$ by (7.2), and $\xi_a + e_L(a-j) \geq \xi_j$ by Lemma 7.1.3. □

Assume $\pi = F(\rho)$ for a root ρ of $g(T)$, we have now obtained a congruence property for the power series $f(F(T))$, which clearly satisfies $f(F(\rho)) = 0$. The minimal polynomial of ρ is clearly a factor of $f(F(T))$ of degree n, and observe that the valuation the coefficient of T^n is 0 while the constant term has valuation 1, so its Newton polygon has exactly one side of length n and slope $-{}^1\!/_n$. In particular $g(T)$ is obtained by the factorization along the Newton polygon, or equivalently collecting the roots with positive valuation, which is exactly what is provided by p-adic Weierstrass Preparation Theorem.

We will however show a reduction that allows to approximate the minimal monic polynomial of ρ starting from $f(F(T))$, and keeping the congruence (7.4). Let's start putting $h_1(T) = f(F(T))$, and consider the polynomial $H_1(T)$ obtained taking the monomials of degree $\geq n$ of $h_1(T) - T^n$. If $H(T) = 0$ then there is no such monomial, and $g(T)$ is a monic polynomial of degree n, which is Eisenstein being $F(\pi)$ a root.

Let cT^r a monomial of $H_1(T)$ that minimizes the quantity $v_L(c) + r$, and take the monomial with r as big as possible among those achieving the minimum of $v_L(c) + r$, which are in a finite number. In other words, consider the higher valuation $\mathcal{F}$ on $\mathcal{O}_L[[T]]$ defined as

$$\mathcal{F}(cT^r) = (\mathcal{F}_1(cT^r), \mathcal{F}_2(cT^r)) = (v_L(c) + r,\ -r) \in \mathbb{Z}^2$$

where $\mathbb{Z}^2$ is ordered lexicographically. We take cT^r to be the monomial of $H_1(T)$ minimizing $\mathcal{F}(cT^r)$.

Let's replace now $h_1(T)$ with the new polynomial

$$h_2 = h_1(T) - h_1(T) \cdot cT^{r-n} = h_1(T) \cdot \left(1 - cT^{r-n}\right).$$

Apply iteratively such step. At the i-th step say, either the minimum of the quantity $v_L(c) + r$ for the monomials of degree $\geq n$ of $H_i(T)$ is increased, either is decreased the biggest degree of the monomials achieving the minimum. Since the whole computation is done in $\mathcal{O}_K[[T]]$, the latter can only happen a finite number of times, and such minimum is increased after a finite number of steps.

Algorithm 4 Lifting step

```
  $H_i(T) \leftarrow \{$sum of monomials of degree $\geq n$ of $h_i(T) - T^n\}$
  $cT^r \leftarrow$ (monomial of $H_i(T)$ minimizing $\mathcal{F}$)
  return $h_i(T) \cdot (1 - cT^{r-n})$
```

After a sufficient number of iterations we can replace $h_i(T)$ with the polynomial $h(T)$ formed by T^n plus the monomials of degree $< n$ of $h_i(T)$. We obtain an Eisenstein polynomial such that $h(F(\pi))$ is arbitrarily small, so $h(T)$ is itself an arbitrarily good approximation of the minimal polynomial of $F(\pi)$.

We need to show that while the above procedure approximating $g(T)$ is carried on the congruence satisfied by $f(F(T))$ is preserved. Indeed, assume that the congruence is satisfied by $h_i(T)$ and let $h_{i+1}(T) = h_i(T)(1 - cT^{r-n})$. Then $cT^r \in P_{p^\ell}(\xi_\ell + n + p^\ell m)$ for some ℓ, being cT^r a monomial of $H_i(T)$ and in view of the congruence that we assume to be satisfied by $f(T)$ and $h_i(T)$. Let bT^s be a monomial of $h_i(T)$, then $bT^s \in P_{p^k}(\xi_k + n)$ for some k by equation (7.3) and by the congruence satisfied by $h_i(T)$. If $k < \ell$ we have

$$bT^s \cdot cT^{r-n} \in P_{p^k}(\xi_k + n + \xi_\ell + n + p^\ell m - n) \subseteq P_{p^k}(\xi_k + n + p^k m),$$

while when $k \geq \ell$ we have

$$bT^s \cdot cT^{r-n} \in P_{p^\ell}(\xi_k + n + \xi_\ell + n + p^\ell m - n) \subseteq P_{p^\ell}(\xi_\ell + n + p^\ell m).$$

We obtained that subtracting $h_i(T) \cdot cT^{r-n}$ from $h_i(T)$ preserves the congruence. Considering also an analogue of a ramification polynomial for $f(T) - g(T)$ we have the following theorem.

Theorem 7.2.5. *Let $f(T)$ be an Eisenstein polynomial of degree n and π a root, if $g(T)$ is another Eisenstein polynomial of degree n having $\rho \in K(\pi)$ as root, and $\pi = \rho + \theta\rho^{m+1} + \dots$ then we have that*

$$f(T) \equiv g(T) \mod \sum_{j=0}^{s} P_{p^j}(\xi_j + n + p^j m),$$

and the polynomial

$$f(\pi + \pi T) - f(\pi) - g(\pi + \pi T) + g(\pi)$$

has its Newton polygon contained in the Newton polygon of $f(\pi + \pi^{m+1}T)$.

Proof. We only need to prove the second assertion, but if cT^r is in $P_{p^j}(\xi_j + n + p^j m)$ then for each $k \leq j$ the contribution of $c(\pi + \pi T)^r$ to the coefficient of T^{p^k} has valuation at least $\xi_j + n + p^j m + (j-k)e_L$, which is at least $\xi_k + n + p^k m$ as shown above. □

Remark 7.2.6. *We point out that the algorithm used during the proof to recover (an approximation of) the minimal polynomial of $\rho = F^{-1}(\pi)$ can be used to produce the minimal polynomial of a uniformizing element obtained deforming π in a much quicker way than by computing a resultant $Res_U(g(U), T - (U + \theta U^{m+1}))$ as the determinant of a $(n+m) \times (n+m)$ matrix with coefficients in $\mathcal{O}_K(T)$. Consequently taking $F(T) = T - \theta T^{m+1}$ and computing via the above approximation the minimal polynomial of the uniformizer ρ such that $\pi = \rho - \theta\rho^{m+1}$, we obtain the minimal polynomial of a uniformizer $\rho = \pi + \theta\pi^{m+1} + \dots$, and this observation allows to exploit the free choice of $F(T)$ in Algorithm 2 to avoid the computation of the resultant.*

7.3 Construction of totally ramified class fields

In this section we show how it is possible to convert a norm subgroup, representing a totally ramified abelian extension via local class field theory, into the unique reduced Eisenstein polynomial generating the extension.

We suppose given a finite index closed subgroup $N \subset K^\times$ such that $NU_{0,K} = K^\times$, so that the corresponding extension by local class field theory is totally ramified. Being closed we have $N \supset U_u$ for u sufficiently big, this hypothesis is automatically satisfied when K is a finite extension of $\mathbb{Q}_p$ and N has finite index.

We assume that N is described by a set of linear maps, one for each upper ramification break. That is for all $u \geq 0$ such that $U_{u,K} \nsubseteq NU_{u+1,K}$ we assume given a surjective homomorphism

$$\nu_u : NU_{u,K} \to V_u$$

having kernel exactly equal to $NU_{u+1,K}$, for some abstract group V_u, which is naturally an $\mathbb{F}_p$-vector space for $u \geq 1$. Take ν_u to be the trivial map to the trivial group 1 when u is not an upper break, that is $NU_{u,K} = NU_{u+1,K}$. Note that the knowledge of all the maps ν_u determines uniquely the group N.

The map ν_0, when non-trivial, gives a condition on the representative $f_{0,1}$, or equivalently on the residue class $\overline{f_0/\pi_K}$, this correspond to the well known explicit description of local class field theory for tamely ramified extensions. On the other hand the terms appearing in a reduced polynomial in connection to the cokernels of the polynomials $S_{t_i}(T)$ attached to the lower breaks t_i are all of the form $f_{0,j}\pi_K^j$, because the upper breaks are integers by Hasse-Arf Theorem.

Consequently the choice of such representatives $f_{0,j}$ is determined by the condition that f_0 should be a norm from the extension determined by N, and a suitable f_0 can be selected changing appropriately π_K.

The ramification data is described by the upper breaks $u \geq 1$ and the dimensions of the corresponding V_u. After selecting f_0 we have a well defined skeleton for the reduced Eisenstein polynomial, formed by a set of terms $f_{i,j}\pi_K^j T^i$ with $i \neq 0$, where the $f_{i,j}$ will be considered as unknowns in the set of representatives R. We will describe how it is possible to recover the $f_{i,j}$ from the maps ν_u.

The terms $f_{i,j}$ in a fixed range as in Prop. 7.1.8 can be evaluated at the level σ_ℓ when $p^\ell \| i$ say, making use the map $\nu_{\sigma_\ell/n-1}$ as we will now show. If m is such that $nj + i + p^\ell m = n\sigma_\ell + n$ it will be possible to describe the dependence of $N_{K(\pi)/K}(1 - \theta\pi^m)$ on the coefficient $f_{i,j}$ at the first order, obtaining a linear system from $\nu_{\sigma_\ell/n-1}$.

Definition 7.3.1. If $p^{\ell+1}|n$, we define R_ℓ to be the set of pairs (i,j) such that $j \geq 1$, $0 \leq i < n$, $p^\ell \| i$ and

$$\xi_\ell + n \leq nj + i < \sigma_\ell + n.$$

We assume that R_ℓ is ordered depending on the value of $nj + i$. We define $M(i,j)$ to be the number m such that

$$nj + i + p^\ell m = \sigma_\ell + n.$$

We remark that if the extension is abelian then $n|\sigma_\ell$ by Hasse-Arf theorem, so the m defined above is always an integer $\leq \tau_\ell$ and prime with p.

7.3.1 Dependence of norms on a $f_{i,j}$

We will now track the dependence of a norm $N_{K(\pi)/K}(1-\theta\pi^m)$ on a representative $f_{i,j}$ appearing in the expansion of a coefficient. To do so, let's treat $f_{i,j}$ as an indeterminate, and apply a sufficient number of steps of Algorithm 4 to pass from $f(T+\theta T^{m+1})$ to the minimal polynomial $g(T)$ of ρ, where $\pi = \rho + \theta\rho^{m+1}$.

Clearly $\rho = \pi - \theta\pi^{m+1} + \dots$, and g_0/f_0 will be the norm of an element of the form $1 - \theta\pi^m + \dots$. For some $r > m$, the changes induced changing $f_{i,j}$ on all $N_{K(\pi)/K}(1 - \theta\pi^r + \dots)$ turn out to be even smaller p-adically, so it will be possible to ignore any term that is $\mathcal{O}(\pi^{m+1})$.

In the expansion of $f(T + \theta T^{m+1})$ a term $f_{i,j}\pi_K^j(T + \theta T^{m+1})^i$ appears, and it has $f_{i,j}\pi_K^j T^i$ as main term. In the algorithm we start with $h_0(T) = f(T+\theta T^{m+1})$, and at the i-th step we subtract $h_i(T) \cdot cT^{r-n}$ from $h_i(T)$, where $cT^{r-n} \in P_{p^k}(\xi_k + p^k m)$ for some $k \leq s$. From the monomial $f_{i,j}\pi_K^j T^i$ the other terms in $f_{i,j}$ that may appear in the algorithm have coefficient with valuation at least

$$nj + i + \min_{0\leq k\leq s}\{\xi_k + p^k m\} = nj + i + n\phi_{L/K}(m),$$

with respect to the mixed valuation $\digamma_1(\pi_K^a T^b) = na + b$ on $\mathcal{O}_L[[T]]$.

Note that the minimum of $\xi_k + p^k m$ is obtained as the minimum of the piecewise linear function $nN(x) + mx$, which is $n\phi_{L/K}(m)$ in view of what proved before proposition 7.1.1. We will denote for convenience this quantity as

$$A_{i,j}(m) = nj + i + n\phi_{L/K}(m).$$

The term $f_{i,j}\pi_K^j T^i$ is the main term coming from $f_{i,j}\pi_K^j(T + \theta T^{m+1})^i$, and the second contribution can be found considering the expansion

$$(1+\theta T^m)^i = 1 + \binom{i}{p^\ell}(\theta T^m)^{p^\ell} + \binom{i}{p^{\ell-1}}(\theta T^m)^{p^{\ell-1}} + \dots.$$

Putting as usual $p^\ell \| i$, we denote the valuation of the second term as

$$B_{i,j}(m) = nj + i + \min_{0\leq k\leq \ell}\left\{e_L(\ell - k) + p^k m\right\}.$$

Such term is equal to

$$\binom{i}{p^\ell}\pi_K^j T^i \cdot (\theta T^m)^{p^\ell}$$

as long as $mp^\ell < e_L + mp^{\ell-1}$, that is $m < {}^{e_L}/_{(p^\ell - p^{\ell-1})}$, and if $m \leq M(i,j) \leq \tau_\ell$ this condition is certainly satisfied because

$$m \leq \tau_\ell \leq {}^{e_L}/_{(p^{\ell+1} - p^\ell)}$$

by Lemma 7.1.3.

By Proposition 7.1.8 we can assume $\ell < s$, and if $m \leq \tau_\ell$ we always have

$$B_{i,j}(m) = nj + i + p^\ell m < A_{i,j}(m).$$

So the main contribution to $N_{K(\pi)/K}(1 - \theta\pi^m) = g_0/f_0$ originated from $f_{i,j}\pi_K^j T^i$ is only coming from $f_{i,j}\binom{i}{p^\ell}\pi_K^j T^i \cdot (\theta T^m)^{p^\ell}$.

When $m = M(i,j)$ we obtain a condition on $f_{i,j}$ to have $N_{K(\pi)/K}(1-\theta\pi^m)$ in the norm group for each θ, which can be used to determine the representative $f_{i,j}$.

This can be made to work when only one representative $f_{i,j}$ is unknown, but a more refined study is needed if we have to determine them all. In particular, we will see that there exists an ordering of such unknowns that allows to determine them all inductively. What complicates this idea is that it will to be necessary to interleave in a suitable way the ranges of representatives considered in Prop. 7.1.8.

It will be convenient to write down a comfortable lower bound for the functions $A_{i,j}$ and $B_{i,j}$, obtaining a function describing the biggest quotient $\mathcal{O}_K/\mathfrak{p}_K^u$ where we can ignore the value of $f_{i,j}$ while computing $N_{K(\pi)/K}(\pi - \theta\pi^{m+1})$. In particular we can take

$$C_{i,j}(m) = nj + i + \min_{0\le k\le \ell} \left\{\xi_k - \xi_\ell + p^k m\right\},$$

where $\ell = v_p(i)$ as usual. We resume the properties proved in the following Lemma.

Lemma 7.3.2. *Denote with π a root of $f(T)$, and let $(i,j) \in R_\ell$. Then, for each $\theta \in U_K$, the value of*

$$N_{K(\pi)/K}(1-\theta\pi^m) \mod \mathfrak{p}_K^u$$

does not depend on $f_{i,j}$, whenever u is $\le C_{i,j}(m)/n - 1$. If $m = M(i,j)$ then $C_{i,j}(m) = \sigma_\ell + n$, and for $u = C_{i,j}(m)/n - 1 = \phi_{L/K}(\tau_\ell)$ we have

$$N_{K(\pi)/K}(1-\theta\pi^m) = N_{K(\pi_0)/K}(1-\theta\pi_0^m) + \pi_K^u f_{i,j}\lambda_{i,j}\theta^{p^\ell} + \dots, \tag{7.5}$$

where $\lambda_{i,j}$ is a fixed unit defined as

$$\lambda_{i,j} = \binom{i}{p^\ell} \cdot \left({}^{-f_0}/_{\pi_K}\right)^{(i+p^\ell m)/n-1},$$

and π_0 is a root of the polynomial obtained from $f(T)$ setting $f_{i,j}$ to 0.

Proof. We just have to prove the (7.5). For $m = M(i,j)$ the variation of the constant term comes from the monomial $f_{i,j}\binom{i}{p^\ell}\pi_K^j T^i \cdot (\theta T^m)^{p^\ell}$ in the expansion of $f(T+\theta T^{m+1})$, and during the reduction each T^n is transformed into $-f_0$. Dividing by f_0 we obtain that the variation for $N_{K(\pi)/K}(1-\theta\pi^m)$, which modulo π_K^{u+1} is

$$f_{i,j}\pi_K^j \binom{i}{p^\ell}(-f_0)^{(i+p^\ell m)/n-1}\theta^{p^\ell} = \pi_K^u f_{i,j}\lambda_{i,j}\theta^{p^\ell}. \qquad \square$$

We will now assume that some $f_{i,j}$ have been determined and some not yet, and will show that it is possible to determined some of the unknown ones. For ℓ such that $p^{\ell+1}\|n$, consider the range of terms R_ℓ like in Prop. 7.1.8, and let (i_ℓ, j_ℓ) be the smallest pair $(i,j) \in R_\ell$ (i.e. the pair in R_ℓ with $nj+i$ as small as possible) such that the corresponding $f_{i,j}$ has not been identified yet.

We first prove a couple of technical lemmas about the functions $C_{i,j}(x)$.

Lemma 7.3.3. *The functions $C_{i,j}(x)$ are strictly increasing, and for $(i,j) \neq (i',j')$ then the functions $C_{i,j}(x)$ and $C_{i',j'}(x)$ are always different except possibly at one point. The difference $C_{i,j}(x) - C_{i',j'}(x)$ is constant when $v_p(i) = v_p(i')$, and $C_{i',j'}(x)$ can surpass $C_{i,j}(x)$ only when $v_p(i') > v_p(i)$.*

Proof. Follows directly from the definition. □

Lemma 7.3.4. *Let $\Pi_L(x)$ be the real function $x \mapsto \min\{px, x + e_L\}$, and let $\Pi^{[h]}$ denote the h-times composition. Let $m, h \in \mathbb{N}$, and let $y = C_{i,j}(m) - n$ for some $(i,j) \in R_\ell$. Then assuming $p^{h-1}m \leq {}^{e_L}/_{(p-1)}$ we have*

$$\Pi^{[h]}(y) \geq C_{i,j}(p^h m) - n.$$

Proof. It's enough to prove that $\Pi(y) \geq C_{i,j}(pm) - n$ for $m \leq {}^{e_L}/_{(p-1)}$, and we can do so proving that both py and $y + e_L$ are bigger. The first inequality is clear from the definition of $C_{i,j}(m)$, for the second one we can observe that

$$nj + i + \xi_0 - \xi_\ell + pm \leq nj + i + \xi_0 - \xi_\ell + m + e_L,$$

and furthermore

$$nj + i + \xi_{i-1} - \xi_\ell + p^i m \leq nj + i + \xi_i - \xi_\ell + p^i m + e_L$$

for $1 \leq i \leq \ell$ by Lemma 7.1.3, so $C_{i,j}(pm) \leq C_{i,j}(m) + e_L$. □

Let $K(x)$ be the function defined as

$$K(x) = \min_{0 \leq \ell < s} C_{i_\ell, j_\ell}(x), \tag{7.6}$$

it is again a strictly increasing function which for each m describes up to which precision we can compute $N_{K(\pi)/K}(\pi - \theta\pi^{m+1})$, with the given information about the coefficients of $f(T)$.

Let I_ℓ be the set of real x where $K(x) = C_{i_\ell, j_\ell}(x)$, since two functions $C_{i,j}(x)$ can only cross once we have that I_ℓ is a (possibly infinite) topologically closed real interval, and taking into account the conditions under which a surpass may happen of Lemma 7.3.3 we obtain that I_k lies before I_ℓ if $k > \ell$. Let's merge in a unique bigger interval the I_ℓ such that the value of τ_ℓ is the same, and let J_r be formed by the union of the I_ℓ such that $\tau_\ell = t_r$. Let's also put $k_r = K^{-1}(n\phi(t_r) + n)$ for each r, then k_r is contained in the *interior* of J_r for some r, thanks to the following Lemma.

Lemma 7.3.5. *Let $A_1, \ldots, A_m$ be a sequence of intervals with extrema $\mathbb{R} \cup \{\pm\infty\}$, such that A_{i+1} begins exactly where A_i ends. Let $a_1 < a_2 < \cdots < a_m$ be real numbers contained in the interior of $\bigcup_{i=1}^m A_i$. Then a_i is contained in the interior of A_i, for some $1 \leq i \leq m$.*

Proof. The thesis is trivial when $m = 1$. If $m > 1$, then either a_m is in the interior of A_m, either we have that $a_1, a_2, \ldots, a_{m-1}$ are contained in the interior of $\bigcup_{i=1}^{m-1} A_i$ and the thesis follows by induction. □

So, let r be such that k_r is in the interior of J_r, and let $L_1 \leq L_2$ be the integers such that $\tau_\ell = t_r$ if and only if $\ell \in [L_1, L_2]$. Then we have that $C_{i_\ell, j_\ell}(k_r)$ is at least $n\phi_{L/K}(t_r) + n$ for $\ell \in [L_1, L_2]$, and strictly bigger for $\ell \notin [L_1, L_2]$. Put $m = k_r$.

For $L_1 \leq \ell \leq L_2$ let's redefine (i_ℓ, j_ℓ) to be the unique pair (i, j) in R_ℓ that $C_{i,j}(m) = n\phi_{L/K}(t_r) + n$. Then some pairs (i_ℓ, j_ℓ) will be unchanged while some others may be set to correspond to representatives f_{i_ℓ, j_ℓ} that are already known. This makes no harm since all these representatives will now be determined simultaneously. Since the equality need to hold already for some of the original (i_ℓ, j_ℓ) we obtain that $m = M(i_\ell, j_\ell)$ is an integer $< \tau_\ell = t_r$ and prime with p.

Let's consider the terms $f_{i_\ell, j_\ell} \pi_K^{j_\ell} T^{i_\ell}$ for ℓ in the given range, and lets vary the f_{i_ℓ, j_ℓ}. Put $u = \phi_{L/K}(t_r)$.

Lemma 7.3.6. *If the $f_{i,j}$ already known were determined inductively we already have*

$$N_{K(\pi)/K}(1 - \theta\pi^m) \in U_u N,$$

and the class modulo $U_{u+1}N$ is a linear function of $\bar{\theta}$.

Proof. Indeed let $u' = \phi_{L/K}(t_{r'}) \leq u$ be an upper ramification break and $m' \geq m$, and assume that at least one of these inequality is strict. We will show that there was a previous step where we computed some currently known coefficient, by requesting $N_{K(\pi)/K}(1 - \theta\pi^{m'})$ to be in $U_{u'+1}N$ for each θ.

If $\phi_{L/K}(m') > u'$ then we always have $N_{K(\pi)/K}(1 - \theta\pi^{m'}) \in U_{u'+1}$, by the properties of the norm map [FV02, Chap 3, Prop 3.1]. Consequently assume $\phi_{L/K}(m') \leq u'$, or $m' \leq \psi_{L/K}(u') = t_{r'}$ applying $\psi_{L/K}$, so in particular $m' \leq {}^{e_L}\!/\!_{(p-1)}$ by Lemma 7.1.3.

If $(m', p) = 1$, let $[L_1', L_2']$ be the interval of possible ℓ such that $\tau_\ell = t_{r'} \geq m'$, and for each ℓ we have a pair (i_ℓ', j_ℓ'), for $L_1' \leq \ell \leq L_2'$, which has the property that $m' = M(i_\ell', j_\ell')$, and $C_{i_\ell', j_\ell'}(m') = nu' + n \leq K(m)$. Thus the corresponding $C_{i_\ell', j_\ell'}(x)$ is certainly not $\geq K(x)$ and cannot appear in the (7.6). This means that the $f_{i_\ell', j_\ell'}$ for $L_1' \leq \ell \leq L_2'$ have been determined at a previous step, where we guaranteed that $N_{K(\pi)/K}(1 - \theta\pi^{m'}) \in U_{u'+1}$.

When $p \mid m'$, and $p^w \| m'$ say, let's consider the elements of the form $(1 + \theta\pi^{m'/p^w})^{p^w}$ as generators of $U_{m'}/U_{m'+1}$ (see [FV02, Chap. 1, Prop. 5.7], and note that $m' \lneq {}^{pe_L}\!/\!_{(p-1)})$. We are done if we show that $N(1 + \theta\pi^{m''}) \in NU_{u''+1}$ for $m'' = m'/p^w$ and each upper break $u'' \leq \Pi_K^{[-w]}(u')$, where $\Pi_K(x) = \min\{px, x + e_K\}$.

We can assume $m'' \leq \psi_{L/K}(u'') = t_{r''}$ as above. Consider as above an ℓ such that $\tau_\ell = t_{r''} = \psi_{L/K}(u'')$, and a pair $(i_\ell'', j_\ell'') \in R_\ell$ with $m'' = M(i_\ell'', j_\ell'')$. Then $C_{i_\ell'', j_\ell''}(m'') = nu'' + n$, and $C_{i_\ell'', j_\ell''}(m')$ is certainly

$$\leq \Pi_L^{[w]}(nu'') + n = n\Pi_K^{[w]}(u'') + n \leq nu' + n$$

by Lemma 7.3.4. We have that $C_{i_\ell'', j_\ell''}(x)$ is not $\geq K(x)$, and the condition $N(1 + \theta\pi^{m''}) \in NU_{u''+1}$ was verified in a previous step. $\square$

We have from the Lemma 7.3.2, applied once for each pair (i_ℓ, j_ℓ) for $L_1 \leq \ell \leq L_2$, that changing the f_{i_ℓ,j_ℓ} we have

$$N_{K(\pi)/K}(1-\theta\pi^m) = N_{K(\pi_0)/K}(1-\theta\pi_0^m) + \sum_{\ell=L_1}^{L_2} \pi_K^u f_{i_\ell,j_\ell}\lambda_{i_\ell,j_\ell}\theta^{p^\ell} + \dots,$$

where π_0 is a root of the polynomial with all unknown f_{i_ℓ,j_ℓ} set to 0.

Now for some choice of the f_{i_ℓ,j_ℓ} we want $N_{K(\pi)/K}(1-\theta\pi^m)$ be in the kernel of $\nu_u : NU_u/NU_{u+1} \xrightarrow{\sim} V_u$, for each residue representative θ. The condition only depends on the reductions $\bar{\theta}$ and $\overline{f_{i_\ell,j_\ell}}$ and is $\mathbb{F}_p$-linear in them, so we can impose it to hold only for a set of values for $\bar{\theta}$ that generate κ_K over $\mathbb{F}_p$. Let $\bar{\alpha}_1, \dots, \bar{\alpha}_{f_K}$ be such a basis for $f_K = [\kappa_K : \mathbb{F}_p]$, then we can decompose each

$$\overline{f_{i_\ell,j_\ell}} = \sum_{k=1}^{f_K} \overline{f_{i_\ell,j_\ell,k}}\bar{\alpha}_k$$

and consider the $\overline{f_{i_\ell,j_\ell,k}}$ as unknowns over $\mathbb{F}_p$.

Fix a lifting $\alpha_k \in \mathcal{O}_K$ for each $\bar{\alpha}_k$, we have an equation

$$\nu_u(N_{K(\pi_0)/K}(1-\theta\pi_0^m) + \sum_{\ell=L_1}^{L_2} \pi_K^u \left[\sum_{k=1}^{f} f_{i_\ell,j_\ell,k}\alpha_k\right] \lambda_{i_\ell,j_\ell}\theta^{p^\ell}) = 0$$

in V_u for each generator $\theta = \alpha_k$. The codomain V_u has $\mathbb{F}_p$-dimension equal to the "multiplicity" of the ramification break $\Lambda = L_2 - L_1 + 1$. So we have an inhomogeneous system formed by $f_K \cdot \Lambda$ equations over $\mathbb{F}_p$, for the same number of unknowns $\overline{f_{i_\ell,j_\ell,k}}$.

Consequently we have a unique solution for the $\overline{f_{i_\ell,j_\ell,k}}$ if we can prove that the system is non-degenerate. We can equivalently prove that the connected homogeneous system

$$\nu_u\left(1 + \sum_{\ell=L_1}^{L_2} \pi_K^u \left[\sum_{k=1}^{f_K} f_{i_\ell,j_\ell,k}\alpha_k\right] \lambda_{i_\ell,j_\ell}\theta^{p^\ell}\right) = 0, \qquad \text{for all } \theta$$

has no non-trivial solution. Subtracting 1 and dividing by a suitable power of π_K, the system can be interpreted as the request that the additive polynomial

$$A(\bar{\theta}) = \sum_{\ell=L_1}^{L_2} \overline{f_{i_\ell,j_\ell}\lambda_{i_\ell,j_\ell}}\bar{\theta}^{p^\ell}$$

should have range contained in a subspace of codimension $L_2 - L_1 + 1$. Since the powers of $\bar{\theta}$ appearing are p-th powers ranging from p^{L_1} to p^{L_2}, we have that its corank as linear map is at most $L_2 - L_1$ (see [FV02, Chap. 5, §2]). Consequently such a non-trivial solution of the homogeneous system is impossible, and the original system is non-degenerate.

Theorem 7.3.7. *Given a closed finite index subgroup $N \subset K^\times$ corresponding to a totally ramified class field, there exists an ordering of the representatives $f_{i,j}$ appearing in the expansion of the coefficients of a generic Eisenstein polynomial that allows to determine the coefficients of the reduced Eisenstein polynomial generating the extensions corresponding to N.*

It is indeed clear that the above procedure where the $f_{i,j}$ are obtained solving linear equations can be converted into an algorithm to construct explicitly a minimal equation corresponding to a class field. The $f_{i,j}$ allowed by the ramification data, but with $(i,j) \notin R_\ell$ for each ℓ, can be assumed to be all 0, or set to any arbitrary value (indeed, they are exactly the terms that are set to an arbitrary value by the reduction algorithm). On the other hand, during the construction we guarantee that for each $m > 0$ and prime with p, and for each θ, we have $N_{K(\pi)/K}(1 - \theta\pi^m) \in N$, because the condition $\nu_u(N_{K(\pi)/K}(1 - \theta\pi^m)) = 0$ is verified for all u at some point of the algorithm, implying that all norms are contained in N.

Remark 7.3.8. *We observe that this construction produces an alternative and constructive proof of the Existence Theorem of class field theory for totally ramified extensions, because for each finite index closed subgroup N of $K^\times$ with index n we construct an extensions of degree n having norm subgroup contained in N. We can construct precisely one reduced polynomial of degree $(K^\times : N)$ for each N, and considering all possible reduction steps we have easily that the group of norms has to be exactly equal to N, and that all intermediate fields $L_{t_r^+}/L_{t_r}$ are Galois, so the generated field L/K has to be Galois by Theorem 7.1.9.*

It would be interesting to extend this construction to recover the Artin map from $K^\times/N$ to $\mathrm{Gal}(K/L)$, proving that these two groups are indeed isomorphic and describing explicitly the isomorphism. The above methods do not even give an easy proof that the extension obtained is abelian, without assuming local class field theory.

Bibliography

[Alb35] A. A. Albert, *On cyclic fields*, Transactions of the American Mathematical Society **37** (1935), no. 3, 454–462.

[Alp93] J. L. Alperin, *Local representation theory: Modular representations as an introduction to the local representation theory of finite groups*, Cambridge Univ. Press, 1993.

[Ama71] S. Amano, *Eisenstein equations of degree p in a $\mathfrak{p}$-adic field*, J. Fac. Sci. Univ. Tokyo Sect. IA Math **18** (1971), 1–21.

[BD11] A. Bartel and T. Dokchitser, *Brauer relations in finite groups*, 2011. arXiv:1103.2047

[Bro82] K. S. Brown, *Cohomology of groups*, vol. 87, Springer, 1982.

[Cap07] L. Caputo, *A classification of the extensions of degree p^2 over $\mathbb{Q}_p$ whose normal closure is a p-extension*, Journal de théorie des nombres de Bordeaux **19** (2007), no. 2, 337–355.

[CMR10] S. Chebolu, J. Mináč, and C. Reis, *Reciprocity laws for representations of finite groups*, Ann. Sci. Math. Québec **34** (2010), no. 1, 37–61.

[Dal10] C. S. Dalawat, *Serre's formule de masse in prime degree*, Monatshefte für Mathematik (2010), 1–20.

[DCD07] I. Del Corso and R. Dvornicich, *The Compositum of Wild Extensions of Local Fields of Prime Degree*, Monatshefte für Mathematik **150** (2007), no. 4, 271–288.

[Del84] P. Deligne, *Les corps locaux de caractéristique p, limites de corps locaux de caractéristique* 0, Representations of reductive groups over a local field, Travaux en Cours, Hermann, Paris, 1984, pp. 119–157.

[FV02] I. B. Fesenko and S. V. Vostokov, *Local fields and their extensions*, American Mathematical Society, 2002.

[Gor80] D. Gorenstein, *Finite groups*, Chelsea Pub. Co., 1980.

[Gre10] C. Greve, *Galoisgruppen von Eisensteinpolynomen über p-adischen Körpern*, Ph.D. thesis, Universität Paderborn, 2010, pp. 1–114.

[Has30] H. Hasse, *Bericht über neuere untersuchungen und probleme aus der theorie der algebraischen zahlkörper*, Teubner, 1930.

[Hei96] V. Heiermann, *De nouveaux invariants numériques pour les extensions totalement ramifiées de corps locaux*, Journal of Number Theory **59** (1996), no. 1, 159–202.

[Hel91] C. Helou, *On the ramification breaks*, Communications in Algebra **19** (1991), no. 8, 2267–2279.

[HK04] X.-D. Hou and K. Keating, *Enumeration of isomorphism classes of extensions of p-adic fields*, Journal of Number Theory **104** (2004), no. 1, 14–61.

[Iwa55] K. Iwasawa, *On Galois groups of local fields*, Trans. Amer. Math. Soc **80** (1955), 448–469.

[Jak68] A. V. Jakovlev, *The Galois group of the algebraic closure of a local field*, Izv. Akad. Nauk SSSR Ser. Mat. **32** (1968), 1283–1322. MR 0236155 (38 #4453)

[JR04] J. W. Jones and D. P. Roberts, *Nonic 3-adic fields*, Algorithmic Number Theory (2004), 293–308.

[JR06] ______, *A database of local fields*, Journal of Symbolic Computation **41** (2006), no. 1, 80–97.

[JW83] U. Jannsen and K. Wingberg, *Die Struktur der absoluten Galoisgruppe $\mathfrak{p}$-adischer Zahlkörper*, Invent. Math. **70** (1982/83), no. 1, 71–98.

[Kra37] M. Krasner, *Sur la primitivité des corps $\mathfrak{p}$-adiques*, Mathematica, Cluj **13** (1937), 72–191 (French).

[Kra62] ______, *Nombre des extensions d'un degré donné d'un corps $\mathfrak{p}$-adique*, C. R. Acad. Sc. Paris **254** (1962), 3470–3472, *ibidem* **255** (1962), 224–226, 1682–1684, 2342–2344, 3095–3097.

[Lab67] J. P. Labute, *Classification of Demushkin groups*, Canad. J. Math. **19** (1967), 106–132.

[Lan02] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[Lbe09] A. Lbekkouri, *On the construction of normal wildly ramified extensions over $\mathbb{Q}_p$, $(p \neq 2)$*, Archiv der Mathematik **93** (2009), no. 4, 331–344.

[Li97] H.-C. Li, *p-adic power series which commute under composition*, Transactions of the American Mathematical Society **349** (1997), no. 4, 1437–1446.

[Lub81] J. D. Lubin, *The local Kronecker-Weber theorem*, Transactions of the American Mathematical Society **267** (1981), no. 1, 133–138.

[Mau67] E. Maus, *Arithmetisch disjunkte Körper*, J. Reine Angew. Math. **226** (1967), 184–203.

[Mau71] ______, *On the jumps in the series of ramifications groups*, Bull. Soc. math. France **25** (1971), 127–133.

[Med08] A. Mednykh, *Counting conjugacy classes of subgroups in a finitely generated group*, J. Algebra **320** (2008), no. 6, 2209–2217.

[Mik81] H. Miki, *On the ramification numbers of cyclic p-extensions over local fields*, Journal für die Reine und Angewandte Mathematik (1981), 99–115.

[Mon11] M. Monge, *Determination of the number of isomorphism classes of extensions of $\mathfrak{p}$-adic field*, Journal of Number Theory **131** (2011), no. 8, 1429–1434.

[MS03] J. Mináč and J. Swallow, *Galois module structure of pth-power classes of extensions of degree p*, Israel Journal of Mathematics **138** (2003), no. 1, 29–42.

[MS05] ______, *Galois embedding problems with cyclic quotient of order p*, Israel Journal of Mathematics **145** (2005), no. 1, 93–112.

[MSS06] J. Mináč, A. Schultz, and J. Swallow, *Galois module structure of pth-power classes of cyclic extensions of degree p^n*, Proceedings of the London Mathematical Society **92** (2006), no. 2, 307.

[MSS11] ______, *Cyclic algebras, Schur indices, norms, and Galois modules*, Ann. Sci. Math. Québec **35** (2011), no. 1, 123–136.

[Neu99] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften, vol. 322, Springer-Verlag, Berlin, 1999.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer-Verlag, Berlin, 2008.

[Ore28] Ö. Ore, *Abriß einer arithmetischen Theorie der Galoisschen Körper*, Math. Ann. **100** (1928), 650–673, *ibidem* **102** (1930), 283–304.

[Pau06] S. Pauli, *Constructing class fields over local fields*, Journal de théorie des nombres de Bordeaux **18** (2006), no. 3, 627–652.

[PR01] S. Pauli and X.-F. Roblot, *On the computation of all extensions of a p-adic field of a given degree*, Mathematics of Computation **70** (2001), no. 236, 1641–1660.

[Ser78] J.-P. Serre, *Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local*, C.R. Acad. Sci. Paris Sér. A-B **286** (1978), 1031–1036.

[Ser79] ———, *Local fields*, Springer, 1979.

[Sha47] I. R. Shafarevitch, *On p-extensions*, Rec. Math. [Mat. Sbornik] N.S. **20(62)** (1947), 351–363.

[Wat94] W. C. Waterhouse, *The normal closures of certain Kummer extensions*, Canad. Math. Bull **37** (1994), no. 1, 133–139.

[Wym69] B. F. Wyman, *Wildly Ramified Gamma Extensions*, American Journal of Mathematics **91** (1969), no. 1, 135.

[Yam68] S. Yamamoto, *On a property of the Hasse's function in the ramification theory*, Memoirs of the Faculty of Science, Kyushu University. Series A, Mathematics **22** (1968), no. 2, 96–109.

[Yam95] M. Yamagishi, *On the number of Galois p-extensions of a local field*, Proc. Amer. Math. Soc. **123** (1995), no. 8, 2373–2380.

[Yos11] M. Yoshida, *An ultrametric space of Eisenstein polynomials and ramification theory*, Proc. Amer. Math. Soc. (to appear) (2011), 1–11.