Classification of Weakly Ramified Extensions of the p-adic Numbers

Dominik Bullach

Mathematisches Institut • Ludwig-Maximilians-Universität München

Classification of Weakly Ramified Extensions of the p-adic Numbers

Dominik Bullach

Master's Thesis supervised by
Prof. Dr. Werner Bley

Ludwig-Maximilians-Universität München

No animals were harmed in the making of this thesis.

Last time modified: 15th May 2018, 00:37

Printed in Bavaria.

Contents

1 Introduction **7**

2 Group-theoretic Preliminaries **13**
2.1 Characters 14
2.2 Non-abelian groups of order p^3 and l^2p 18
2.3 Idempotents 26

3 Local Considerations **31**
3.1 Higher ramification groups 32
3.2 Some results from local class field theory 36
3.3 Weakly ramified extensions 38
3.4 Kummer theory 40
3.5 Non-abelian and weakly ramified extensions of degree l^2p 41
3.6 Local extensions with Galois group $\mathrm{SL}_2(\mathbb{F}_3)$ 52

4 Global Considerations **61**
4.1 Embedding problems 62
4.2 Some results from global class field theory 72
4.3 Weakly ramified and non-abelian extensions of degree l^2p 74

5 Bibliography **81**

1 Introduction

Introduction

Let $L|K$ be a Galois extension of number fields with Galois group G, further denote by $\mathcal{O}_L$ and $\mathcal{O}_K$ the ring of integers of L and K, respectively. The ring $\mathcal{O}_L$ is naturally a $\mathbb{Z}[G]$-module and its structure as such has been a matter of interest for a long time.
One knows by a theorem of Noether that $\mathcal{O}_L$ is locally $\mathbb{Z}[G]$-free whenever $L|K$ is a tame extension and M. Taylor was able to express the class $[\mathcal{O}_L]$ defined by $\mathcal{O}_L$ in the class group $\mathrm{cl}(\mathbb{Z}[G])$ of projective $\mathbb{Z}[G]$-modules in terms of Artin root numbers (cf. [Tay81]). The latter result is commonly regarded as the highlight of classical Galois module theory.
Other $\mathbb{Z}[G]$-modules that have been studied include the inverse different of $L|K$, which is defined as

$$\mathfrak{C}_{L|K} = \{x \in L \mid \forall y \in \mathcal{O}_L : \mathrm{Tr}_{L|K}(xy) \in \mathcal{O}_K\},$$

as well as, if it exists, the square root $\mathcal{A}_{L|K}$ of $\mathfrak{C}_{L|K}$. Note that Hilbert's valuation formula ensures the existence of $\mathcal{A}_{L|K}$ if, for example, $[L : K]$ is odd. Define the dual of an ideal $\mathfrak{a}$ of L with respect to trace form of $L|K$ by

$$\mathfrak{a}^{\#} = \{x \in L \mid \forall a \in \mathfrak{a} : \mathrm{Tr}_{L|K}(xa) \in \mathcal{O}_K\} \cong \mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{a}, \mathcal{O}_K),$$

then $\mathfrak{C}_{L|K} = \mathcal{O}_L^{\#}$ and one can show that $\mathcal{A}_{L|K}$ is the only ideal of L satisfying $\mathcal{A}_{L|K} = \mathcal{A}_{L|K}^{\#}$. One is therefore interested in comparing the $\mathbb{Z}[G]$-module structures of those two modules with the structure of $\mathcal{O}_L$.

The detailed study of the $\mathbb{Z}[G]$-module structure of $\mathcal{A}_{L|K}$ was initiated by Erez, who showed in [Ere91b] that $\mathcal{A}_{L|K}$, whenever it exists[1], is a locally free $\mathbb{Z}[G]$-module if and only if the extension $L|K$ is weakly ramified, i. e. the second ramification group of any prime ideal in K vanishes. Moreover, he proved that $\mathcal{A}_{L|K}$ is a free $\mathbb{Z}[G]$-module if $L|K$ is tamely ramified and of odd degree. Those were the first general results on the $\mathbb{Z}[G]$-module structure of a module other than the ring of integers $\mathcal{O}_L$.

Recall that $\mathbb{Z}[G]$ admits locally free cancellation if we assume $|G|$ to be odd ([CR87, (51.3) and (51.24)]), so under this assumption a locally free $\mathbb{Z}[G]$-module is free if and only if its class in $\mathrm{cl}(\mathbb{Z}[G])$ is trivial. Thus, the statements mentioned above combine to yield for a tame extension $L|K$ the equality

$$[\mathcal{A}_{L|K}] = [\mathcal{O}_L]$$

in $\mathrm{cl}(\mathbb{Z}[G])$, where both classes in fact are trivial. Caputo and Vinatier showed in [VC16] that this equality also extends to locally abelian tame extensions of even degree, but does not necessarily take the value of the trivial class. In some more detail,

[1] In Erez's original work, this theorem is stated only for $L|K$ being of odd degree. However, Caputo and Vinatier point out in [VC16, footnote on p. 6] that his proof also works for even degree extensions such that $\mathcal{A}_{L|K}$ exists.

they exhibit an extension having Galois group $\mathrm{SL}_2(\mathbb{F}_3)$ such that the class $[\mathcal{A}_{L|K}]$ of $\mathcal{A}_{L|K}$ in $\mathrm{cl}(\mathbb{Z}[G])$ is non-trivial and subsequently prove that this example is minimal in the sense that $[\mathcal{A}_{L|K}]$ is trivial for all extensions of degree $[L:K] \leq 24$ and Galois group $G \ncong \mathrm{SL}_2(\mathbb{F}_3)$. One might therefore ask if such extensions having Galois group $\mathrm{SL}_2(\mathbb{F}_3)$ also fail other properties related to $\mathcal{A}_{L|K}$ that are known to hold in the case of $[L:K]$ being odd.

Some time before that Vinatier showed in [Vin01] that $\mathcal{A}_{L|\mathbb{Q}}$ is $\mathbb{Z}[G]$-free, if $[L:\mathbb{Q}]$ is locally abelian. This, and some numerical computations, encouraged him to make in [Vin03] the following

Conjecture (Vinatier)**.** If $L|\mathbb{Q}$ is a finite Galois extension with Galois group G such that $\mathcal{A}_{L|\mathbb{Q}}$ exists, then $\mathcal{A}_{L|\mathbb{Q}}$ is a free $\mathbb{Z}[G]$- module.

Bley, Burns and Hahn approached this conjecture in [BBH17] using a fairly general principle. Roughly speaking, one seeks distinguished elements of a relative algebraic K_0-group $K_0(\mathbb{Z}[G], \overline{\mathbb{Q}}[G])$, respectively its subgroup $K_0(\mathbb{Z}[G], \mathbb{Q}[G])$, that project to arithmetic invariants that have been considered previously. One can then hope to prove, or at least conjecture, relations in $K_0(\mathbb{Z}[G], \overline{\mathbb{Q}}[G])$ that provide refinements of existing results or conjectures. One advantage of such a refinement is that we have a canonical decomposition

$$K_0(\mathbb{Z}[G], \mathbb{Q}[G]) \cong \bigoplus_p K_0(\mathbb{Z}_p[G], \mathbb{Q}_p[G]), \tag{$*$}$$

where p ranges over all primes, so previously entirely globally formulated problems might now turn into problems that admit a local decomposition and hence become easier to study. Secondly, the fairly abstract point of view may help to uncover relationships between earlier results explaining previously known but not yet understood parallelisms.

Concretely, Bley, Burns and Hahn consider weakly ramified global extensions $L|K$ of odd degree and assign an element $\mathfrak{a}_{L|K} \in K_0(\mathbb{Z}[G], \mathbb{Q}[G])$ to each of these defined using Galois-Gauss sums. Subsequently they show that $\mathfrak{a}_{L|K}$ projects to $[\mathcal{A}_{L|K}]$ under the natural map

$$K_0(\mathbb{Z}[G], \mathbb{Q}[G]) \to \mathrm{cl}(\mathbb{Z}[G]),$$

hence $\mathcal{A}_{L|K}$ is $\mathbb{Z}[G]$-free if and only if $\mathfrak{a}_{L|K}$ projects to the trivial class. Bley, Burns and Hahn also investigate the local components under the decomposition $(*)$ and prove that every component associated to an (at most) tamely ramified place of $L|K$ projects to zero in $\mathrm{cl}(\mathbb{Z}[G])$. Thus, if we prescribe the wildly ramified primes of $L|K$, it suffices to verify Vinatier's Conjecture for a (finite) representative set of extensions realising

this local behaviour. This makes the conjecture accessible for numerical computations and Bley, Burns and Hahn used this to obtain the following result:

Theorem ([BBH17], Thm. 10.1 and 10.6)**.** Vinatier's Conjecture holds true in the following cases:

(a) $L|\mathbb{Q}$ is non-abelian of degree 27,

(b) the only wildly ramified prime is 7, the decomposition group $G_\mathfrak{p}$ has order 63 for all $\mathfrak{p} \mid 7$ and $G_\mathfrak{p}/P \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, where $P \trianglelefteq G_\mathfrak{p}$ denotes the unique 7-Sylow group of $G_\mathfrak{p}$.

The main objective of this thesis is to provide preparational work needed to treat the case of $G_\mathfrak{p}/P \cong \mathbb{Z}/9\mathbb{Z}$ similarly. Strictly speaking,

- in the first chapter we will explore the irreducible characters of groups of order p^3 and l^2p, where l, p denote odd primes such that $l \mid (p-1)$, as well as collect some entirely group-theoretic statements about those groups needed later on,
- in the second chapter we will classify all non-abelian and weakly ramified extensions $L_p|\mathbb{Q}_p$ of degree l^2p and prove there is no local Galois extension $L_p|\mathbb{Q}_p$ having Galois group $\mathrm{SL}_2(\mathbb{F}_3)$,
- in the third chapter we will describe how to find a set of representative extensions $L|\mathbb{Q}$ realising these local extensions mentioned above.

Acknowledgment

This thesis concludes my studies so far, therefore there is a whole bunch of people I owe thanks for their invaluable contribution over the years and I apologise for only naming those directly involved into the formation of this thesis.

Firstly, I want to thank my advisor, Prof. Dr. Werner Bley, who suggested the subject to me and has been generously supporting me not only during the time writing this thesis, but also on several other occasions.

I also want to thank Nguyen Quang Do for pointing out to me Fröhlich's condition (3.42), without which I still would not have a proof of the non-existence of a local Galois extension $L_p|\mathbb{Q}_p$ having Galois group $\mathrm{SL}_2(\mathbb{F}_3)$ yet[2].

Moreover, I owe gratitude to my surpassing colleagues and friends that make showing up at office every day much easier. More precisely, I thank Chris "deBergh" Geishauser

[2] See the discussion at `https://math.stackexchange.com/questions/2760640/tate-cohomology-of-squares`

for his enthusiasm and companionship, Pascal "π" Stucky for his patience in sharing an office with me, which also includes listening to my newest ideas almost all the time, Martin Hofer for always being open-minded about discussing all kinds of mathematical as well as non-mathematical stuff, aka a "tea break", Harald Koppen for simply being *the* Harald and Johannes "hannibunny" Funk for, although not being a model student when it comes to staying in touch, instantly texting back at important occasions like those concerned with proof-reading.

It has been a pleasure writing this thesis. D.B.

2 Group-theoretic Preliminaries

2 **Group-theoretic Preliminaries** 13
2.1 Characters
2.2 Non-abelian groups of order p^3 and l^2p
2.3 Idempotents

2.1 Characters

This section contains a short overview of (ordinary) character theory of finite groups with emphasis on the interplay between characters of a group and of its (normal) subgroups. This will be needed in section 2.2 to classify all irreducible characters of groups of order p^3 and l^2p, respectively, where l, p denote odd primes satisfying $l \mid (p-1)$. For more details on the general theory the reader might consult [Isa76], which served as main source thereof.

Group Representations

Let G be a finite group.. A map $\chi\colon G \to \mathbb{C}$ is called an (ordinary) ***character*** of G if there is a homomorphism $\mathfrak{X}\colon G \to \mathrm{GL}_n(\mathbb{C})$ for some $n \in \mathbb{N}$ such that $\chi(g) = \mathrm{Tr}(\mathfrak{X}(g))$ for all $g \in G$. In this case, one says that χ is ***afforded*** by $\mathfrak{X}$ and the number n is called the ***degree*** of χ, denoted by $\deg\chi$. Note also that $\deg\chi = \chi(1)$.

(2.1) Example. The characters of degree 1 of G are exactly the homomorphisms $G \to \mathbb{C}^\times$. These characters are called ***linear***. In particular, the map taking constant value 1 on G is a linear character, which will be referred to as the ***trivial character***. ■

A character χ is called ***irreducible*** if it is afforded by a homomorphism $\mathfrak{X}\colon G \to \mathrm{GL}_n(\mathbb{C})$ that turns $\mathbb{C}^n$ into a simple $\mathbb{C}[G]$-module. The set of all irreducible characters, which is finite by Wedderburn's theorem, will be denoted by $\mathrm{Irr}(G)$.

Now the following fundamental formula holds:

$$|G| = \sum_{\chi \in \mathrm{Irr}(G)} (\deg\chi)^2.$$

Furthermore, $|\mathrm{Irr}(G)|$ equals the number of conjugacy classes of G, so G is abelian if and only if every irreducible character of G is linear.

Recall that characters are class functions, i. e. constant on conjugacy classes, since for a character of G afforded by $\mathfrak{X}$ we have

$$\chi(xgx^{-1}) = \mathrm{Tr}(\mathfrak{X}(xgx^{-1})) = \mathrm{Tr}\left(\mathfrak{X}(x)\cdot\mathfrak{X}(g)\cdot\mathfrak{X}(x)^{-1}\right) = \mathrm{Tr}(\mathfrak{X}(g)) = \chi(g).$$

One now has the following (see [Isa76, Thm 2.8] for a proof)

(2.2) Theorem. The set of class functions $G \to \mathbb{C}$ carries the structure of a $\mathbb{C}$-vector space and $\mathrm{Irr}(G)$ forms a basis of this vector space. Moreover, a class function is a character if and only if it is a nonzero linear combination in $\mathrm{Irr}(G)$ with integer coefficients.

Note that the product $\chi_1 \cdot \chi_2$ of characters $\chi_1, \chi_2 \colon G \to \mathbb{C}$ is a character again. In fact, the product character $\chi_1 \cdot \chi_2$ is afforded by the tensor product of the representations affording the characters χ_1 and χ_2, respectively.

(2.3) Definition. Let χ, φ be class functions of a finite group G, then

$$[\chi, \varphi] = \frac{1}{|G|} \sum_{g \in G} \varphi(g) \cdot \chi(g^{-1})$$

defines an inner product on the set of class functions of G.

One now can show that $\mathrm{Irr}(G)$ forms an orthogonal basis with respect to this inner product (cf. [Isa76, Cor. (2.14)]). In particular, if ϕ is a character and

$$\phi = \sum_{\chi \in \mathrm{Irr}(G)} n_\chi \chi$$

is its unique decomposition as a sum of irreducible characters, then $n_\chi = [\chi, \phi]$ for all $\chi \in \mathrm{Irr}(G)$. Those $\chi \in \mathrm{Irr}(G)$ satisfying $[\chi, \phi] > 0$ are called the ***irreducible constituents*** of ϕ.

Characters on Subgroups

Let G be a finite group and $U \subseteq G$ a subgroup. If χ is a character of G, then its restriction χ_U to U is a character of U. Note that if $\chi_U \in \mathrm{Irr}(U)$, then $\chi \in \mathrm{Irr}(G)$. Of course, the converse of this statement is false.

We now consider a process that resembles a dual to restriction.

(2.4) Definition. Let χ be a class function of U, then

$$\mathrm{ind}_U^G(\chi) \colon G \to \mathbb{C}, \quad g \mapsto \frac{1}{|U|} \sum_{x \in G} \chi^0(xgx^{-1}), \quad \text{where} \quad \chi^0(y) = \begin{cases} \chi(y) & \text{if } y \in U, \\ 0 & \text{otherwise,} \end{cases}$$

is called the ***induced class function*** of χ on G.

We will see shortly that characters induce characters.

(2.5) Lemma (Frobenius reciprocity)**.** Let $U \subseteq G$ be a subgroup and suppose that φ is a class function on U and θ is a class function on G. Then

$$[\varphi,\ \theta_U] = [\mathrm{ind}_U^G(\varphi),\ \theta].$$

Proof. We calculate:

$$\begin{aligned}[\mathrm{ind}_U^G(\varphi), \theta] &= \frac{1}{|G|} \sum_{g \in G} \mathrm{ind}_U^G(\varphi)(g^{-1}) \cdot \theta(g) = \frac{1}{|G| \cdot |H|} \sum_{g \in G} \sum_{x \in G} \varphi^0(xg^{-1}x^{-1})\theta(g) = \\ &= \frac{1}{|G| \cdot |H|} \sum_{g \in G} \sum_{x \in G} \varphi^0(g^{-1})\theta(xgx^{-1}) \overset{(*)}{=} \frac{1}{|G| \cdot |H|} \sum_{g \in G} \sum_{x \in G} \varphi^0(g^{-1})\theta(g) = \\ &= \frac{|G|}{|G| \cdot |H|} \sum_{g \in U} \varphi(g^{-1})\theta(g) = [\varphi, \theta_U]\end{aligned}$$

Here equality $(*)$ uses that θ is constant on conjugacy classes. □

(2.6) Corollary. Let $U \subseteq G$ be a subgroup and χ a character of U, then $\mathrm{ind}_U^G(\chi)$ is a character of G.

Even more can be said about the relationship between characters of G and those of a subgroup if one considers a normal subgroup.

Recall that the kernel of a character χ of G is defined as

$$\ker \chi = \{g \in G \mid \chi(g) = \deg \chi\}.$$

Note that one recovers the known notion of a kernel in the case of linear characters. If N denotes a normal subgroup of G, the following holds:

$$\mathrm{Irr}\left(G/N\right) = \{\chi \in \mathrm{Irr}(G) \mid N \subseteq \ker \chi\},$$

where we identify a character φ of G/N with the character $\hat{\varphi}$ of G given by $\hat{\varphi}(g) = \varphi(gN)$ for all $g \in G$. An application of this equality is that the number of linear characters of G equals $(G : [G, G])$, where $[G, G]$ denotes the commutator subgroup of G.

(2.7) Lemma. Let G be a group and $N \subseteq G$ a normal subgroup. If $\chi \in \mathrm{Irr}(G)$, then

$$\mathrm{ind}_N^G(\chi_N) = \chi \cdot \sum_{\varphi \in \mathrm{Irr}(G/N)} (\deg \varphi) \cdot \varphi.$$

Proof. Let $g, x \in G$, then

$$xgx^{-1} \in N \quad \Leftrightarrow \quad g \in x^{-1}Nx = N,$$

so we have

$$\mathrm{ind}_N^G(\chi_N)(g) = \begin{cases} (G : N)\chi(g) & \text{if } g \in N, \\ 0 & \text{otherwise.} \end{cases}.$$

Let $\rho = \sum_{\varphi \in \mathrm{Irr}(G/N)} \deg \varphi \cdot \varphi$, then

$$\rho(g) = \begin{cases} (G:N) & \text{if } g \in N, \\ 0 & \text{otherwise,} \end{cases}$$

by [Isa76, Lemma (2.10) and (2.11)], so the lemma follows. □

Let $N \subseteq G$ be a normal subgroup and $\chi \in \mathrm{Irr}(N)$, then for $x \in G$ we can define

$$\chi^x \colon N \to K, \quad g \mapsto xgx^{-1},$$

which is again an irreducible character of N. We say that χ^x is ***conjugate*** to χ.

(2.8) Theorem (Clifford)**.** Let $N \trianglelefteq G$ be a normal subgroup and $\chi \in \mathrm{Irr}(G)$. Let θ be an irreducible constituent of χ_N and $\theta = \theta_1, \ldots, \theta_t$ its distinct conjugates in G. Then

$$\chi_N = e \sum_{i=1}^{t} \theta_i,$$

where $e = [\chi_N, \theta]$.

Proof. Let $n \in N$, then

$$\mathrm{ind}_N^G(\theta)(n) = \frac{1}{|N|} \sum_{x \in G} \theta^x(n),$$

since $xnx^{-1} \in N$ for all $x \in G$. Thus, the irreducible constituents of $\left(\mathrm{ind}_N^G(\theta)\right)_N$ are exactly the conjugates of θ in G. Now χ is a constituent of $\mathrm{ind}_N^G(\theta)$ by Frobenius reciprocity (2.5), so χ_N appears as a summand in $\left(\mathrm{ind}_N^G(\theta)\right)_N$. In particular, every irreducible constituent of χ_N is also a conjugate of θ and it remains to show that

$$[\chi_N, \theta^x] = [\chi_N, \theta]$$

for all $x \in G$. This is done via the following calculation:

$$\begin{aligned} [\chi_N, \theta^x] &= \frac{1}{|N|} \sum_{n \in N} \chi_N(n^{-1}) \cdot \theta(xnx^{-1}) = \frac{1}{|N|} \sum_{n \in N} \chi_N(xn^{-1}x^{-1}) \cdot \theta(n) = \\ &= \frac{1}{|N|} \sum_{n \in N} \chi_N(n^{-1}) \cdot \theta(n) = [\chi_N, \theta] \end{aligned}$$

□

The following corollary is a slightly stronger version of Clifford's theorem for normal subgroups of prime index and will be crucial to our applications of the theory.

(2.9) Corollary. Let $N \trianglelefteq G$ be a normal subgroup of index p, where p is a prime, and $\chi \in \mathrm{Irr}(G)$. Then either

(a) χ_N is irreducible or

(b) $e = 1$ and $t = p$ in Theorem (2.8).

Proof. Assume that χ_N is reducible. Consider $\rho = \sum_{\varphi \in \mathrm{Irr}(G/N)} \varphi$, then $\mathrm{ind}_N^G(\chi_N) = \chi\rho$ by Lemma (2.7) as G/N is abelian, therefore every $\varphi \in \mathrm{Irr}(G/N)$ is linear. Moreover, we have

$$\begin{aligned}[\varphi\chi, \varphi\chi] &= \frac{1}{|G|} \sum_{g \in G} \Big(\varphi(g^{-1})\chi(g^{-1})\Big) \cdot (\varphi(g)\chi(g)) = \\ &= \frac{1}{|G|} \sum_{g \in G} \Big(\varphi(g^{-1}) \cdot \varphi(g)\Big) \cdot \Big(\chi(g^{-1}) \cdot \chi(g)\Big) = \\ &= [\chi, \chi] = 1.\end{aligned}$$

Consequently, every summand $\varphi\chi$ in

$$\mathrm{ind}_N^G(\chi_N) = \rho\chi = \sum_{\varphi \in \mathrm{Irr}(G/N)} \varphi\chi$$

is irreducible. Due to

$$[\mathrm{ind}_N^G(\chi_N), \varphi\chi] = [\chi_N, (\varphi\chi)_N] = [\chi_N, \chi_N] = e^2 t,$$

every irreducible constituent $\chi\varphi$ appears with multiplicity $e^2 t$ in $\mathrm{ind}_N^G(\chi_N)$. Let s be the number of *distinct* summands $\varphi\chi$, then

$$(G : N) \deg \chi = \deg \mathrm{ind}_N^G(\chi_N) = s \cdot e^2 t \cdot \deg \chi.$$

Hence $p = se^2 t$. We therefore must have $e = 1$ and $p = st$. If $t = 1$, then χ_N would be irreducible, so we can conclude that $t = p$. □

2.2 Non-abelian groups of order p^3 and $l^2 p$

The aim of this section is to classify all irreducible characters of non-abelian groups of order p^3 and $l^2 p$, where p denotes a prime and, in the latter case, p and l are odd primes satisfying $l \mid (p - 1)$. Along the way we will also gather some basic properties of these groups that will be useful later as the non-abelian groups of order $l^2 p$ will occur repeatedly throughout chapters 2 and 3.

Non-abelian groups of order p^3

Non-abelian groups of order p^3 are, in some sense, the easiest non-abelian groups. One can even show there exist only two isomorphism classes of such groups (cf. [Hal63, 4.4]) and describe those explicitly. However, we will need neither this statement nor the resulting explicit representation.

(2.10) Lemma. Let p be a prime, G a non-abelian group order p^3 and $Z(G)$ its centre. We have

$$|Z(G)| = p \quad \text{and} \quad G/Z(G) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Moreover, $Z(G) = [G, G]$.

Proof. As G is a p-group, $Z(G)$ must at least contain p elements. Now the first two statements follow from the general fact that $G/Z(G)$ being cyclic implies G is abelian. Since $G/Z(G)$ is abelian, we have $[G, G] \subseteq Z(G)$. Since G is abelian, this has to be an equality. □

(2.11) Remark. A p-group G with the property that its centre $Z(G)$ has order p and $G/Z(G)$ is abelian of exponent p is also called ***extra special*** and most of what follows could also be done for such groups.

We begin the investigation of the character theory of non-abelian groups of order p^3 by establishing a fairly general lemma.

(2.12) Lemma. Let G be a group, $A \trianglelefteq G$ an abelian normal subgroup of index p, where p is a prime, and $\chi \in \mathrm{Irr}(G), \theta \in \mathrm{Irr}(A)$.

(a) χ is a linear character if and only if χ_A is irreducible,

(b) if χ_A is reducible, then $\varphi \in \mathrm{Irr}(A)$ is a constituent of χ_A if and only if $\mathrm{ind}_A^G(\varphi) = \chi$. In particular, χ is of degree p,

(c) let $B \subseteq A$ be another subgroup, then

$$\{\varphi \in \mathrm{Irr}(A) \mid \varphi_B = \theta_B\} = \{\theta\rho \mid \rho \in \mathrm{Irr}\left(A/B\right)\},$$

(d) θ is fixed by conjugation on G if and only if $[G, G] \subseteq \ker\theta$.

Proof. (a): If χ is linear, χ_A is linear as well. In particular, χ_A is irreducible. Conversely, suppose χ_A is irreducible. Since A is abelian, χ_A is linear and so is χ.

(b): Assume φ is an irreducible constituent of χ_A, then by Corollary (2.9), we have

$$\chi_A = \sum_{i=i}^{p} \varphi_i,$$

where $\varphi = \varphi_1, ..., \varphi_p$ are the distinct conjugates of φ. In particular, χ is of degree p. Frobenius reciprocity yields

$$[\chi, \operatorname{ind}_A^G(\varphi)] = [\chi_A, \varphi] = 1,$$

so χ is an irreducible constituent of $\operatorname{ind}_A^G(\varphi)$. Since

$$\deg \chi = p = (G : A) = \operatorname{ind}_A^G(\varphi),$$

we must have $\chi = \operatorname{ind}_A^G(\varphi)$.

Now suppose $\chi = \operatorname{ind}_A^G(\varphi)$, then

$$1 = [\chi, \operatorname{ind}_A^G(\varphi)] = [\chi_A, \varphi].$$

This shows that φ is an irreducible constituent of χ_A.

(c): Let φ be in the set on the left hand side. We have

$$1 = [\varphi_B, \theta_B] = [\varphi, \operatorname{ind}_B^A(\theta_B)],$$

so φ is an irreducible constituent of $\operatorname{ind}_B^A(\theta_B)$. Applying Lemma (2.7) gives that $\operatorname{ind}_B^A(\theta_B) = \sum_{\rho \in \operatorname{Irr}(A/B)} \theta\rho$ is a decomposition into distinct irreducible characters, because A is abelian. It follows $\varphi = \theta\rho$ for some $\rho \in \operatorname{Irr}(A/B)$.

(d): The following holds:

$$\begin{aligned} \forall x \in G : \theta^x = \theta \quad &\Leftrightarrow \quad \forall x \in G, a \in A : \theta(xax^{-1}) = \theta(a) \\ &\Leftrightarrow \quad \forall x \in G, a \in A : \theta(xax^{-1}a^{-1}) = 1. \end{aligned}$$

It therefore suffices to show $[G, G] = [G, A]$. Let $xyx^{-1}y^{-1}$ be a generator of $[G, G]$. We may assume $x, y \notin A$, so xA generates G/A and we can write $y = x^n a$ for some $a \in A$ and $n \in \mathbb{N}$. Now

$$xyx^{-1}y^{-1} = x(x^n a)x^{-1}(a^{-1}x^{-n}) = x(x^n a x^{-n})x^{-1}(x^n a x^{-n})^{-1} \quad \in [G, A].$$

□

(2.13) Proposition. Let p be a prime and G a non-abelian group of order p^3. Moreover, let $Z \subseteq G$ be its centre and choose a normal subgroup $A \trianglelefteq G$ of order p^2 containing Z.

(a) $\mathrm{Irr}(G)$ consists of p^2 linear characters and $(p-1)$ characters of degree p,

(b) every $\varphi \in \mathrm{Irr}(A)$ that is non-trivial on Z induces an irreducible character of G of degree p and all degree p characters of G are of this form,

(c) $\mathrm{ind}_A^G(\chi) = \mathrm{ind}_A^G(\varphi)$ for characters $\mathrm{Irr}(A)$ being non-trivial on Z if and only if $\varphi_Z = \chi_Z$.

Proof. (a): Since the commutator subgroup $[G,G]$ of G equals Z, there are exactly $(G:Z) = p^2$ linear characters of G. By Lemma (2.12) (b), all non-linear characters of G are of degree p, therefore we get from

$$p^3 = |G| = \sum_{\chi \in \mathrm{Irr}(G)} (\deg \chi)^2$$

that the number of irreducible degree p characters is $\frac{p^3-p^2}{p^2} = p-1$.

(b): Let $\varphi \in \mathrm{Irr}(A)$ be non-trivial on Z and choose an irreducible constituent χ of $\mathrm{ind}_A^G(\varphi)$, then we have

$$0 < [\chi, \mathrm{ind}_A^G(\varphi)] = [\chi_A, \varphi],$$

so φ is an irreducible constituent of χ_A. As $Z \not\subseteq \ker\varphi$, we get from Lemma (2.12) (d) that φ is not fixed by conjugation on G. Applying Theorem (2.8) shows that χ_A is reducible, so $\chi = \mathrm{ind}_A^G(\varphi)$ by Lemma (2.12) (b).
Conversely, if $\chi \in \mathrm{Irr}(G)$ is of degree p, it is induced by an $\varphi \in \mathrm{Irr}(A)$ according to Lemma (2.12) (b). Suppose $Z \subseteq \ker\varphi$, then also $Z \subseteq \ker \mathrm{ind}_A^G(\varphi)$ and therefore χ defines an irreducible character of the abelian group A/Z. Hence χ is linear, contradiction.

(c): Let $\varphi \in \mathrm{Irr}(A)$ be non-trivial on Z. We first show the following equality:

$$\{\theta \in \mathrm{Irr}(A) \mid \theta_Z = \varphi_Z\} = \{\varphi^x \mid x \in G\}.$$

Take θ from the set on the left hand side. By Lemma (2.12) (c), we have $\theta = \varphi\rho$ for some $\rho \in \mathrm{Irr}(A/Z)$. Thus, the cardinality of the left hand side set is $(A:Z) = p$. We have shown above that $\chi = \mathrm{ind}_A^G(\varphi)$ is irreducible of degree p and so χ_A is the sum of the p distinct conjugates of φ by Corollary (2.9). In particular, the right hand side set above also consists of p elements. Since "$\supseteq$" is clear, this shows equality.

Now suppose $\mathrm{ind}_A^G(\chi) = \mathrm{ind}_A^G(\varphi)$. Because of

$$[\chi, (\mathrm{ind}_A^G(\varphi))_A] = [\mathrm{ind}_A^G(\chi), \mathrm{ind}_A^G(\varphi)] = 1,$$

χ is an irreducible constituent of $(\mathrm{ind}_A^G(\varphi))_A$. As already mentioned, $(\mathrm{ind}_A^G(\varphi))_A$ is the sum of the p distinct conjugates of φ, so χ and φ must be conjugate to each other. Conversely, suppose χ and φ are conjugate to each other. Since $\mathrm{ind}_A^G(\varphi)$ is an irreducible character of degree p, the restriction $(\mathrm{ind}_A^G(\varphi))_A$ is reducible and therefore the sum of all conjugates of φ by Corollary (2.9). In particular, χ is an irreducible constituent of $(\mathrm{ind}_A^G(\varphi))_A$ and Lemma (2.12) (b) gives $\mathrm{ind}_A^G(\varphi) = \mathrm{ind}_A^G(\chi)$. □

Non-abelian Groups of Order l^2p

Let l, p denote odd primes satisfying $l \mid (p-1)$. We now investigate non-abelian groups of order l^2p, which should be thought of as slightly more complicated than non-abelian groups of order p^3.

(2.14) Lemma. Let G be a group of order l^2p, then

(a) G has a unique p-Sylow group,

(b) G is abelian if and only if there is a unique l-Sylow group.

Proof. (a): Let ν_p and ν_l be the number of p- and l-Sylow groups, respectively. Sylow's theorems yield

$$\nu_p \mid l^2 \quad \Rightarrow \quad \nu_p \in \{1, l, l^2\}$$

and $\nu_p \equiv 1 \mod p$. Because of $l \mid (p-1)$ we have $l \leq (p-1)$ and $l \equiv 1 \mod p$ would force $l = 1$. In the case of $l^2 \equiv 1 \mod p$ we would either encounter the case of $l \equiv 1 \mod p$ again or get $l \equiv -1 \mod p$. However, the latter contradicts l being odd.

(b): If there is a unique l-Sylow group, G decomposes as a direct product of its l- and p-Sylow group. In particular, G is abelian. The converse is clear from the fact that a Sylow group is unique if and only if it is a normal subgroup. □

(2.15) Lemma. Let G be a non-abelian group of order l^2p. If $l^2 \nmid (p-1)$ or no l-Sylow group of G is cyclic, then G contains a cyclic normal subgroup of order lp.

Proof. Let P denote the unique p-Sylow group and L an arbitrary l-Sylow group of G. We have $G \cong P \rtimes_\phi L$, where the semi-direct product is formed with respect to

$$\phi\colon L \to \mathrm{Aut}(P) \cong \mathbb{Z}/(p-1)\mathbb{Z}, \quad x \mapsto \left\{ g \mapsto xgx^{-1} \right\}.$$

Since G is non-abelian, ϕ has to be non-trivial. Now our assumption implies that ϕ cannot be injective, so $\ker\phi$ is a subgroup of order l and

$$\langle P, \ker\phi \rangle = P \rtimes_\phi \ker\phi$$

is a cyclic subgroup of order lp. As $G/P \cong L$ is abelian, this is also a normal subgroup. □

(2.16) Remark. Using the same notation as in the proof of Lemma (2.15) we can describe the conjugacy class of an element $g \in P$ as the set

$$\{\phi(x)(g) \mid x \in L\}.$$

This description will be used later.

The normal subgroup described in Lemma (2.15) can be characterised in more detail:

(2.17) Lemma. Let G be a non-abelian group of order l^2p and $N \subseteq G$ a subgroup. The following statements are equivalent:

(a) N is a cyclic subgroup of order lp,

(b) $N = P \cdot Z(G)$, where $P \trianglelefteq G$ is the unique p-Sylow group and $Z(G)$ the centre of G.

Proof. "(a) ⇒ (b)": Let $N \subseteq G$ be an abelian subgroup of order lp. Take an element $x \in N$ of order l and choose an l-Sylow group L containing x. The element x commutes with all elements in L and all elements in the unique p-Sylow group $P \subseteq N$. Thus, $x \in Z(G)$ due to $G = P \cdot L$ and it suffices to show $Z(G) = \langle x \rangle$.

Since G is non-abelian, we have $|Z(G)| \neq l^2p$. We also cannot have $|Z(G)| = lp$, because in this case $G/Z(G)$ would be cyclic, hence G would be abelian. Since $x \in Z(G)$ is an element of order l, the only possible case remaining is $|Z(G)| = l$.

"(b) ⇒ (a)": Clear since $P \cdot Z(G)$ is obviously abelian. □

We now explore the irreducible characters of non-abelian groups of order lp, as this will be useful when considering non-abelian groups of order l^2p. Note that a non-abelian group of order lp exists only for $l \mid (p-1)$.

(2.18) Lemma. Let l, p be primes satisfying $l \mid (p-1)$ and G a non-abelian group of order lp with unique p-Sylow group $P \trianglelefteq G$.

(a) G has l linear and $\frac{p-1}{l}$ non-linear irreducible characters,

(b) every non-linear character of G is induced by a non-trivial character of P. In particular, they are of degree l.

Proof. G being non-abelian implies $[G,G] \neq 1$, so from G/P being abelian follows $P = [G,G]$. The number of linear characters of G is therefore $(G:P) = l$.

Let $\chi \in \mathrm{Irr}(G)$ be non-trivial. Then $\chi = \mathrm{ind}_P^G(\lambda)$ for some $\lambda \in \mathrm{Irr}(P)$ by Lemma (2.12) (a) and (b). Suppose $\lambda = 1_P$, then

$$\chi = \mathrm{ind}_P^G(1_P) = \sum_{\rho \in \mathrm{Irr}(G/P)} \rho$$

is not irreducible, hence λ must be non-trivial. Moreover, χ being induced by λ implies that χ is of degree l and so the number of non-linear irreducible characters can be calculated from the equation

$$lp = |G| = \sum_{\chi \in \mathrm{Irr}(G)} (\deg \chi)^2.$$

□

We are finally in a position to state our main result on the character theory of non-abelian groups of order $l^2 p$.

(2.19) Proposition. Let l, p be odd primes with $l \mid (p-1)$, and G a non-abelian group of order $l^2 p$.

(a) G has l^2 linear characters,

(b) every non-linear character of G has degree l or l^2 and we have

$$p = 1 + s_1 + s_2 l^2,$$

where s_1 and s_2 denote the number of irreducible degree l and degree l^2 characters, respectively,

(c) $s_1 s_2 = 0$, where $s_2 = 0$ if and only if G has an abelian normal subgroup N of order lp.

(2.20) Remark. The proof of Proposition (2.19) shows:

- If $s_2 = 0$, every irreducible character of N that is non-trivial on the p-Sylow group P induces an irreducible character of G of degree l, where the induced characters only depend on the restriction to P, and all non-linear character of G are of this form,
- if $s_1 = 0$, every non-trivial character of P induces an irreducible character of G and every non-linear character of G is of this form.

Proof. (a): Let P be the unique p-Sylow group of G. The factor group G/P is abelian, hence $[G, G] \subseteq P$. Since G is non-abelian, we must have $P = [G, G]$. Consequently, G has $(G : P) = l^2$ linear characters.

(b): Let χ be a non-linear irreducible character of G and $N \subseteq G$ a subgroup of order lp. Applying Lemma (2.12) (a) and (b) yields $\chi = \operatorname{ind}_N^G(\varphi)$ for any irreducible constituent φ of χ_N. Thus, χ has degree l or l^2 by Lemma (2.18).

Let the numbers s_1 and s_2 be defined as above, then

$$l^2p = |G| = l^2 + s_1l^2 + s_2l^4 \quad \Leftrightarrow \quad p = 1 + s_1 + s_2l^2.$$

(c): Assume there is an abelian normal subgroup $N \trianglelefteq G$ of order lp. Every irreducible character of N is linear, so the same argument as given in (b) shows that $s_2 = 0$.

Now consider the case that every subgroup of order lp is non-abelian. Choose any l-Sylow group L of G, then we may assume L to be cyclic by Lemma (2.15). Moreover, we have $G = P \rtimes_\phi L$, where ϕ is defined by

$$\phi\colon L \to \operatorname{Aut}(P), \quad y \mapsto \left\{x \mapsto yxy^{-1}\right\}.$$

Let $\alpha \in L$ and $x \in P$ be generators. Then $\phi(\alpha)$ must be of order l^2 because otherwise ϕ would have a non-trivial kernel and we would get an abelian subgroup of order lp (cf. the proof of Lemma (2.15)). Furthermore, we have

$$\phi(\alpha^i)(x) = \phi(\alpha^j)(x) \quad \Leftrightarrow \quad \phi(\alpha^i) = \phi(\alpha^j) \quad \Leftrightarrow \quad l^2 \mid j - i.$$

Hence $\phi(\alpha^i)(x) \neq \phi(\alpha^j)(x)$ for all $0 \leq i, j \leq l^2 - 1$. This shows that the conjugacy class of x in G consists of (at least) l^2 elements.

Let $\lambda \neq 1$ be a linear character of P. Then $\lambda(x)$ determines λ uniquely. Let gxg^{-1} be conjugate to x, then

$$\lambda^g \colon P \to \mathbb{C}^\times, \quad x \mapsto \lambda(gxg^{-1})$$

also defines a linear character of P. Since λ is injective, we get (at least) l^2 distinct G-conjugates of λ.

Let φ be an irreducible character of N of degree l, then φ_P is reducible and Lemma (2.12) (b) gives $\varphi = \operatorname{ind}_P^N(\lambda)$ for a non-trivial character $\lambda \in \operatorname{Irr}(P)$. More precisely, $\varphi = \operatorname{ind}_P^N(\theta)$ if and only if θ and λ are conjugate to each other. Let $g \in G$ and $n \in N$, then

$$\begin{aligned}\varphi^g(n) = \varphi(gng^{-1}) = \operatorname{ind}_P^N(\lambda)(gng^{-1}) = \\ = \frac{1}{|P|} \sum_{m \in N} \lambda^0(mgng^{-1}m^{-1}) \overset{(*)}{=} \\ = \frac{1}{|P|} \sum_{m \in N} \lambda^0(gmnm^{-1}g^{-1}) = \operatorname{ind}_P^N(\lambda^g)(n),\end{aligned}$$

where $Ng = gN$ was used at $(*)$. We have seen above that λ has at least l^2 conjugates, of which l each induce the same character on N. As a consequence, φ has at least l conjugates in G.

Now let χ be an irreducible constituent of $\operatorname{ind}_N^G(\varphi)$, then φ is an irreducible constituent of χ_N and so is every conjugate of φ. In particular, χ_N is reducible and Lemma (2.12) (b) yields

$$\chi = \operatorname{ind}_N^G(\varphi) = \operatorname{ind}_P^G(\lambda).$$

Since there are $\frac{p-1}{l}$ irreducible characters of degree l of N and each l of them induce an irreducible character of degree l^2 of G, we have constructed $\frac{p-1}{l^2}$ of them in total. Comparing with the equation in (b), we get $s_2 = \frac{p-1}{l^2}$ and $s_1 = 0$ as desired. □

2.3 Idempotents

The aim of this section is to collect all results on idempotents that will be necessary in the next chapter.

Let G be an abelian group of order n and K a field such that $|G| \in K^\times$. We set $\widehat{G} = \operatorname{Hom}(G, K^\times)$, which coincides with the previous definition of $\operatorname{Irr}(G)$ in the case of $K = \mathbb{C}$.

(2.21) Lemma. Let G be an abelian group of finite order n and K a field. If $\chi, \varphi \in \widehat{G}$, then

(a) $$\sum_{g\in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = 1, \\ 0 & \text{otherwise,} \end{cases}$$

(b) $$\sum_{g\in G} \chi(g)\varphi(g^{-1}) = \begin{cases} |G| & \text{if } \chi = \varphi, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. (a): Assume $\chi \neq 1$, then there is $x \in G$ such that $\chi(x) \in K^\times \setminus \{1\}$. We therefore get

$$\chi(x) \sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(xg) = \sum_{g\in G} \chi(g),$$

which gives $\sum_{g\in G} \chi(g) = 0$.

(b): Follows from (a) as the product of (linear) characters is again a (linear) character. □

(2.22) Lemma. Let G be an abelian group of finite order n and K a field such that $|G| = |\widehat{G}|$ and $\mathrm{char}(K) \nmid n$. If $g, h \in G$, then

(a) $$\sum_{\chi\in\widehat{G}} \chi(g) = \begin{cases} |G| & \text{if } g = 1, \\ 0 & \text{otherwise,} \end{cases}$$

(b) $$\sum_{\chi\in\widehat{G}} \chi(g)\chi(h^{-1}) = \begin{cases} |G| & \text{if } g = h, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. (b): Write $G = \{g_1, ..., g_n\}$ and $\widehat{G} = \{\chi_1, ..., \chi_n\}$, then Lemma (2.21)(b) is equivalent to stating that

$$\sum_{k=1}^{n} \chi_i(g_k)\chi_j(g_k^{-1}) = \delta_{ij} \cdot |G| \qquad (*)$$

for all $1 \leq i, j \leq n$. Let $A = (a_{ik})$ and $B = (b_{ik})$ be the $(n \times n)$-matrices with entries

$$a_{ik} = \chi_i(g_k) \quad \text{and} \quad b_{ik} = \chi_i(g_k^{-1}),$$

respectively. Now $(*)$ gives

$$A \cdot B^t = |G| \cdot I,$$

where I denotes the identity matrix. Since $|G|$ is a unit in K, we also have $B^t A =$

$|G| \cdot I$, which is equivalent to

$$\sum_{k=1}^{n} \chi_k(g_i)\chi_k(g_j^{-1}) = |G|\delta_{ij}$$

for all $1 \leq i, j \leq n$.

(a): Follows from (b) by evaluating at $h = 1$. □

(2.23) Remark. The condition $|G| = |\widehat{G}|$ in Lemma (2.22) is fulfilled if, for example, K is a finite field and G is an abelian finite group such that the exponent of G divides $|K^\times|$ or if K is algebraically closed.

(2.24) Definition. Let G be an abelian finite group and K a field such that $|G| \in K^\times$. For every $\chi \in \widehat{G}$ we set

$$e_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g)g^{-1} \quad \in K[G].$$

The next lemma collects some useful properties of these elements e_χ, among which is also the explanation why one usually refers to them as ***idempotents***.

(2.25) Lemma. Let G be a finite abelian group and K a field such that $|G| \in K^\times$ and $|G| = |\widehat{G}|$.

(a) $\sum_{\chi \in \widehat{G}} e_\chi = 1_G$,

(b) $g \cdot e_\chi = \chi(g)e_\chi$ for any $g \in G$,

(c) $e_\chi e_\varphi = \begin{cases} e_\chi & \text{if } \chi = \varphi, \\ 0 & \text{otherwise.} \end{cases}$

Proof. (a): We calculate:

$$\sum_{\chi \in \widehat{G}} e_\chi = \sum_{\chi \in \widehat{G}} \frac{1}{|G|} \sum_{g \in G} \chi(g)g^{-1} \overset{(2.22)(a)}{=} \frac{1}{|G|} \cdot (|G| \cdot 1_G) = 1_G.$$

(b): This is again a short calculation:

$$g \cdot e_\chi = \frac{1}{|G|} \sum_{h \in G} \chi(h)gh^{-1} = \frac{1}{|G|} \sum_{h \in G} \chi(hg^{-1})\chi(g)(hg^{-1})^{-1} = \chi(g)e_\chi.$$

(c): One last calculation:

$$e_\chi e_\varphi = \frac{1}{|G|}\sum_{g\in G}\chi(g)g^{-1}e_\varphi \overset{(b)}{=} \frac{1}{|G|}\sum_{g\in G}\chi(g)\varphi(g^{-1})e_\varphi \overset{(2.21)(b)}{=} \begin{cases} e_\chi & \text{if } \chi = \varphi, \\ 0 & \text{otherwise.} \end{cases}$$

□

We are now able to prove the main result of this section, the decomposition of $K[G]$-modules using idempotents.

(2.26) Theorem. Let G be a finite abelian group and K a field such that $|G| \in K^\times$ and $|G| = |\widehat{G}|$. If A is a $K[G]$-module, the maps

$$f\colon A \to \bigoplus_{\chi\in\widehat{G}} e_\chi A, \quad a \mapsto (e_\chi a)_\chi \quad \text{and} \quad g\colon \bigoplus_{\chi\in\widehat{G}} e_\chi A \to A, \quad (e_\chi a_\chi)_\chi \mapsto \sum_{\chi\in\widehat{G}} e_\chi a_\chi$$

define $K[G]$-ismorphisms that are inverse to each other.

Proof. Let $a \in A$, then

$$(g\circ f)(a) = g\left((e_\chi a)_\chi\right) = a\cdot\sum_{\chi\in\widehat{G}} e_\chi \overset{(2.25)(a)}{=} a.$$

Conversely, if $(e_\chi a_\chi)_\chi$ is an element in $\bigoplus_{\chi\in\widehat{G}} e_\chi A$, we have

$$(f\circ g)\big((e_\chi a_\chi)_\chi\big) = f\Big(\sum_{\chi\in\widehat{G}} e_\chi a_\chi\Big) = \left(\Big(\sum_{\chi\in\widehat{G}} e_\chi a_\chi\Big)e_\varphi\right)_\varphi \overset{(2.25)(c)}{=} (e_\varphi a_\varphi)_\varphi.$$

□

3 Local Considerations

3 **Local Considerations** 31
3.1 Higher ramification groups
3.2 Some results from local class field theory
3.3 Weakly ramified extensions
3.4 Kummer theory
3.5 Non-abelian and weakly ramified extensions of degree l^2p
3.6 Local extensions with Galois group $\mathrm{SL}_2(\mathbb{F}_3)$

3.1 Higher ramification groups

In this section we state some well-known facts about higher ramification groups needed later on. For a more comprehensive discussion of these see [Ser79, Ch. IV] or [Neu92, Ch. II, 10].
By a local field we will always mean a non-archimedean local field.

(3.1) Definition. Let $L|K$ be a Galois extension of local fields with Galois group G and valuation v_L on L, then

$$G_s = \{\sigma \in G \mid \forall x \in \mathcal{O}_L : v_L(\sigma x - x) \geq s+1\}, \quad s \geq -1$$

is called the s-th ***ramification group***.

Observe that $G_{-1} = G$ and G_0 is the inertia subgroup of G.

(3.2) Lemma. Let $L|K$ be a finite Galois extension of local fields.

(a) The G_s form a decreasing sequence of normal subgroups,

(b) there is $s_0 \in \mathbb{Z}$ such that $G_s = 1$ for all $s \geq s_0$.

Proof. (a): Let $\sigma, \tau \in G_s$ and $x \in \mathcal{O}_L$, then

$$v_L(\sigma\tau x - x) = v_L(\sigma\tau x - \tau x + \tau x - x) \geq \min\{v_L(\sigma\tau x - \tau x), v_L(\tau x - x)\} \geq s+1.$$

This shows that G_s is a subgroup of G. Now take $\rho \in G$ arbitrary. We have

$$v_L(\rho\tau\rho^{-1}x - x) = v_L(\tau\rho^{-1}x - \rho^{-1}x) \geq s+1,$$

so G_s is indeed a normal subgroup.

(b): By [Neu92, Lemma II.10.4], there is $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Set

$$s_0 = \max_{\sigma \in G\setminus\{1\}} v_L(\sigma\alpha - \alpha),$$

then s_0 is finite, because $\sigma x - x = 0$ would imply $\sigma = 1$. This shows that the identity is the only element of G_s for $s \geq s_0$. □

(3.3) Lemma. Let $L|K$ be a finite Galois extension of local fields with Galois group G and $H \subseteq G$ a subgroup. If $M = L^H$ is the fixed field of H, then

$$H_s = G_s \cap H \quad \text{for all } s \geq -1.$$

Proof. An element $\sigma \in G$ is in $G_s \cap H$ if and only if

$$\sigma \in H \quad \text{and} \quad v_L(\sigma x - x) \text{ for all } x \in \mathcal{O}_L,$$

which is exactly the condition of σ belonging to H_s. □

For each $n \in \mathbb{N}$ we put $U_L^{(n)} = 1 + \mathfrak{p}_L^n$, where $\mathfrak{p}_L$ denotes the maximal ideal of the p-adic number field L, and call $U_L^{(n)}$ the group of ***principal units*** of level n.

(3.4) Proposition. Let $L|K$ be a finite Galois extension of local fields with Galois group G and $\pi_L \in \mathcal{O}_L$ a uniformising element. For every integer $s \geq 0$, the map

$$G_s/G_{s+1} \to U_L^{(s)}/U_L^{(s+1)}, \quad \sigma \mapsto \frac{\sigma\pi_L}{\pi_L}$$

is an injective homomorphism independent of the choice of π_L.

(3.5) Remark. If λ denotes the residue field of L, we have

$$U_L^{(0)}/U_L^{(1)} \cong \lambda^\times \quad \text{and} \quad U_L^{(s)}/U_L^{(s+1)} \cong \lambda$$

for every integer $s \geq 1$. Thus, G_1 is the unique p-Sylow subgroup of G_0 and G_s is a p-group for $s \geq 1$.

Proof. We first check the described map is well-defined. Let $\sigma \in G_s$ for some $s \geq 0$, then

$$v_L(\sigma\pi_L - \pi_L) \geq 1 + s \quad \Leftrightarrow \quad \sigma\pi_L - \pi_L \in \mathfrak{p}_L^{1+s} \quad \Leftrightarrow \quad \frac{\sigma\pi_L}{\pi_L} - 1 \in \mathfrak{p}_L^s,$$

which shows $\frac{\sigma\pi_L}{\pi_L} \in U_L^{(s)}$. The same argument shows that the map only depends on the coset in G_s/G_{s+1} as soon as we show it to be a homomorphism. In order to do this, take $\sigma, \tau \in G_s$. We now have:

$$\frac{\sigma\tau\pi_L}{\pi_L} = \frac{\sigma\tau\pi_L}{\tau\pi_L} \cdot \frac{\tau\pi_L}{\pi_L}.$$

It therefore suffices to show the independence of the choice of uniformising element. Let $\pi_L' = \varepsilon\pi_L$, where $\varepsilon \in \mathcal{O}_L^\times$, be another choice of uniformiser. Then

$$\sigma\varepsilon - \varepsilon \in \mathfrak{p}_L^{s+1} \quad \Leftrightarrow \quad \frac{\sigma\varepsilon}{\varepsilon} - 1 \in \mathfrak{p}_L^{s+1},$$

hence

$$\frac{\sigma\pi_L'}{\pi_L'} \cdot \frac{\pi_L}{\sigma\pi_L} = \frac{\sigma\varepsilon}{\varepsilon} \in U_L^{(s+1)}.$$

It remains to check injectivity. The following equivalence holds:

$$\frac{\sigma\pi_L}{\pi_L} \in U_L^{(s+1)} \quad \Leftrightarrow \quad \sigma\pi_L - \pi_L \in \mathfrak{p}_L^{s+2}.$$

We show that this already implies $\sigma x - x \in \mathfrak{p}_L^{s+2}$ for all $x \in \mathcal{O}_L$. Firstly, by Lemma (3.3) we may assume that $L|K$ is totally ramified. In this case, we have $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ (see [Ser79, I§6, Prop. 18]) and writing $x = \sum_{k=0}^{n} a_k \pi_L^k$, we get

$$v_L(\sigma x - x) = v_L\left(\sum_{k=0}^{n} a_k(\sigma\pi_L^k - \pi_L^k)\right) \geq \min_{0\leq k\leq n} v_L(a_k) + v_L(\sigma\pi_L^k - \pi_L^k) \geq s+2.$$

□

Herbrand's Theorem

Let $L|K$ be a finite Galois extension of local fields and M an intermediate field. A natural question to ask is whether the higher ramification groups of $L|M$ and $M|K$ are determined by those of $L|K$, as it is the case when considering inertia subgroups only. We saw in Lemma (3.3) that higher ramification groups behave well when passing to subgroups, which is, unfortunately, not the case when passing to quotients. However, one can nonetheless obtain a compatibility statement for this case if one twists the numbering of the G_s. In order to do this, define the following function:

$$\eta_{L|K}\colon [-1,\infty[\longrightarrow [-1,\infty[, \quad s \mapsto \int_0^s \frac{1}{(G_0 : G_x)}\mathrm{d}x,$$

where we set $(G_0 : G_x) = (G_x : G_0)^{-1}$ for $x \leq 0$. In other words, $\eta_{L|K}(s) = s$ for $-1 \leq s \leq 0$ and

$$\eta_{L|K}(s) = \frac{1}{|G_0|}\left((\sum_{i=1}^{\lfloor s\rfloor}|G_i|) + (s - \lfloor s\rfloor)\cdot|G_{\lceil s\rceil}|\right) \quad \text{for } s \geq 0$$

using the floor and ceiling functions. Observe that $\eta_{L|K}$ is a continuous and strictly increasing function, hence a homeomorphism of $[-1,\infty[$ into itself. Denote by $\psi_{L|K}$ its inverse.

We can now define the ***upper numbering*** of higher Ramification subgroups by setting

$$G^s = G_{\psi_{L|K}(s)} \quad \text{or equivalently} \quad G^{\eta_{L|K}(s)} = G_s$$

for all $s \geq -1$.

One can also express $\psi_{L|K}(s)$ as an integral involving higher Ramification subgroups in upper numbering.

(3.6) Lemma. Let $L|K$ be a finite Galois extension of local fields. Let $s \geq -1$, then

$$\psi_{L|K}(s) = \int_0^s (G_0 : G^x)\mathrm{d}x.$$

Proof. Let $f(s)$ denote the integral above, then we have

$$(f \circ \eta)'(s) = \frac{\mathrm{d}}{\mathrm{d}s}\int_0^{\eta(s)} (G_0 : G^x)\mathrm{d}x = (G_0 : G^{\eta(s)}) \cdot \eta'(s) = (G_0 : G_s) \cdot \frac{1}{(G_0 : G_s)} = 1.$$

Moreover, $(f \circ \eta)(0) = 0$, so $f \circ \eta = \mathrm{id}$ by integration. Evaluating this equation at $\psi(s)$ gives $f = \psi$. □

An important result which makes dealing with the upper numbering in most cases much easier is

(3.7) Theorem (Hasse-Arf)**.** Let $L|K$ be a finite abelian extension of local fields. If $s \geq -1$ is a ***jump*** in the upper numbering, i. e. $G^{s+\varepsilon} \neq G^s$ for all $\varepsilon > 0$, then $s \in \mathbb{Z}$.

Proof. See [Ser79, Chapter V, §7]. □

Using the Theorem of Hasse-Arf we can rephrase Lemma (3.6) for an abelian extension $L|K$ as

$$\psi_{L|K}(s) = |G_0| \cdot \left((\sum_{i=1}^{\lfloor s \rfloor} \frac{1}{|G^i|}) + \frac{s - \lfloor s \rfloor}{|G^{\lceil s \rceil}|} \right) \qquad \text{for } s \geq 0.$$

The statement commonly refered to as Herbrand's Theorem is now the following

(3.8) Theorem (Herbrand)**.** Let $L|K$ be a finite Galois extension with Galois group G and $L|M$ an intermediate extension with Galois group H. Let $s \geq -1$, then

$$(G_s \cdot H)/H = \left(G/H\right)_t, \quad \text{where } t = \eta_{L|M}(s).$$

Proof. See [Neu92, Ch. II, Thm. (10.7)] or [Ser79, IV§3, Lemma 5]. □

A somehow more natural way of stating this result is given below.

(3.9) Corollary. Let $L|K$ be a finite Galois extension with Galois group G and $L|M$ an intermediate extension with Galois group H. Let $s \geq -1$, then

$$(G^s \cdot H)/H = \left(G/H\right)^s.$$

Proof. See [Neu92, Ch. II, Thm. (10.9)] or [Ser79, IV§3, Proposition 14]. □

The following two Lemmas comprise two statements that will be crucial to our purposes.

(3.10) Lemma. Let $L|K$ be a Galois extension of local fields with Galois group G. If G is a simple group and $s \geq -1$, then

$$G_s = 0 \quad \Leftrightarrow \quad G^s = 0.$$

Proof. "⇒": We have $\Psi_{L|K}(s) \geq s$ for all $s \geq -1$, so $G^s = G_{\Psi_{L|K}(s)} \subseteq G_s = 0$.

"⇐": We proceed by contraposition. Assume $G_s \neq 0$, then

$$G = G_{-1} = ... = G_s$$

and we have

$$\eta_{L|K}(s) = \int_0^s \frac{1}{(G_0 : G_x)} \mathrm{d}x = s.$$

Hence $G^s = G^{\eta_{L|K}(s)} = G_s \neq 0$. □

(3.11) Lemma. Let $L|K$ be a finite abelian extension of local fields with Galois group G and set $n = |G_0/G_1|$. If $s \geq -1$ is an integer such that $n \nmid s$, then $G_s = G_{s+1}$.

Proof. See [Ser79, IV§2, Corollary 2]. □

3.2 Some results from local class field theory

We use this section to state some rather special results of local class field theory we will need later on. We begin with the relationship of higher Ramification groups and the local reciprocity map. If $L|K$ is an abelian extension of local fields, the latter will be denoted by $(-,\ L|K)$.

(3.12) Proposition. Let $L|K$ be a finite abelian extension of local fields and $s \geq -1$ an integer. Then

$$(U_K^{(s)},\ L|K) = G^s.$$

Proof. See [Iwa86, Thm. 7.12]. □

Next we want to explore the interaction of local class field theory and Galois actions.

(3.13) Lemma. Let $L|K$ be a finite extension of local fields and let M be an intermediary field such that $L|M$ and $M|K$ are both abelian extensions. Then $L|K$ is Galois if and only if $N_{L|M}(L^\times)$ is stable under the action of $G_{M|K}$.

Proof. Let $\overline{K}$ be an algebraic closure of K and $\tau \in \mathrm{Hom}_K(L, \overline{K})$, then $\tau L|M$ is also Galois and

$$G_{L|M} \to G_{\tau L|M}, \quad \sigma \mapsto \tau\sigma\tau^{-1}$$

is an isomorphism. Hence $N_{\tau L|M}(\tau L^\times) = \tau N_{L|M}(L^\times)$.

Since τ was chosen arbitrarily, $L|K$ is Galois if and only if $\tau L = L$, which is equivalent to $N_{L|M}(L^\times) = N_{\tau L|M}(\tau L^\times)$ by local class field theory. Comparing with the calculation above now gives the result. □

If L, M, K are as in Lemma (3.13) and the extension $L|K$ is Galois, then we have a well-defined natural action on the quotient $M^\times/N_{L|M}(L^\times)$.

(3.14) Lemma. Let $L|K$ be a finite Galois extension of local fields and M an intermediary field such that $L|M$ is an abelian and $M|K$ a cyclic extension. Then $L|K$ is abelian if and only if $G_{M|K}$ acts trivially on $M^\times/N_{L|M}(L^\times)$.

Proof. Let $G = G_{L|K}$ and $H = G_{L|M}$. Now H is a normal subgroup of G, so G acts on H by conjugation. This action coincides with the action of G/H on H by conjugation because H is abelian by assumption. Thus, H is contained in the centre $Z(G)$ of G if and only if G/H acts trivially on H. On the other hand, the former holds if and only if $G/Z(G)$ is a quotient of G/H. Since $M|K$ is assumed to be a cyclic extension, we get that $G/Z(G)$ is cyclic and G therefore abelian. It therefore suffices to show that the action of G/H on H by conjugation is the same as the action of $G_{M|K}$ on $M^\times/N_{L|M}(L^\times)$. However, this is exactly [Neu11, II§5, Satz (5.10)]. □

(3.15) Corollary. Let $L|K$ be a finite Galois extension of local fields and M an intermediary field such that $L|M$ is unramified and $M|K$ is cyclic. Then $L|K$ is abelian.

Proof. Let $\pi \in M^\times$ be a uniformising element of M, then we have a decomposition

$$M^\times = \langle \pi \rangle \times U_M^{(0)}$$

and $N_{L|M}(L^\times) = \langle \pi^n \rangle \times U_M^{(0)}$, where $n = [L : M]$. Now if $\sigma \in G_{M|K}$, we have $\sigma\pi = \varepsilon\pi$ for some $\varepsilon \in U_M^{(0)}$. Thus, $\sigma\pi \equiv \pi \mod N_{L|M}(L^\times)$. This shows that $G_{M|K}$ acts trivially on $M^\times / N_{L|M}(L^\times)$. □

3.3 Weakly ramified extensions

Recall that a finite Galois extension $L|K$ of local fields with Galois group G is called ***unramified*** if G_0 vanishes and ***tamely ramified*** if G_1 vanishes.

(3.16) Definition (Erez)**.** A finite Galois extension $L|K$ of local fields with Galois group G is called ***weakly ramified*** if $G_2 = 0$.

In particular, any unramified or tamely ramified extension is weakly ramified. We will see later that if p is a prime and $n \in \mathbb{N}$ is divisible by p, then there is a wildly and weakly ramified extension $L|\mathbb{Q}_p$ of degree n (cf. Proposition (3.29)).

(3.17) Lemma. Every Galois sub-extension of a weakly ramified extension is itself weakly ramified.

Proof. Let $L|K$ be a weakly ramfied extension with Galois group G and M an intermediate field. Lemma (3.3) then gives that $L|M$ is weakly ramified.
Observe that $\psi_{L|M}(2) \geq 2$, hence $G_{\psi_{L|M}(2)} \subseteq G_2 = 0$. Applying Herbrand's Theorem (3.8) yields

$$(G_{M|K})_2 = (G_{\psi_{L|M}(2)} \cdot G_{L|M}) \big/ G_{L|M} = 0.$$

□

(3.18) Remark. Note that the composite of weakly ramified extensions is not necessarily weakly ramified. As an example for this phenomenon, let p be an odd prime and $\zeta_p, \zeta_{p^2} \in \overline{\mathbb{Q}_p}$ be a primitive p-th and p^2-th root of unity, respectively, and consider the cyclotomic extension $L = \mathbb{Q}_p(\zeta_{p^2})$. Put $G = G_{L|\mathbb{Q}_p}$. According to [Ser79, IV4, Prop. 18], we have

$$G = G_0, \quad G_1 = \ldots = G_{p-1}, \quad G_p = 0,$$

where G_1 is the unique subgroup of order p. In particular, $L^{G_1} = \mathbb{Q}_p(\zeta_p)$ is a tamely ramified extension field of $\mathbb{Q}_p$. Let $H \subseteq G$ be the unique subgroup of index p, then $H_1 = 0$ and thus $\eta_{L|L^H}(s) = \frac{s}{p-1}$ for all $s \geq 1$. Hence

$$\left(G/H\right)_2 = (G_{\psi_{L|L^H}(2)} \cdot H)/H = (G_{2(p-1)} \cdot H)/H = 0.$$

We have therefore shown that $L = L^H \cdot L^{G_1}|\mathbb{Q}_p$ is a not weakly ramified extension that is the composite of two weakly ramified extensions. See also Proposition (3.21) on this matter. ■

An immediate consequence of Proposition (3.12) and Lemma (3.10) is the following important

(3.19) Lemma. A finite abelian Galois extension $L|K$ of p-adic number fields of degree p is weakly ramified if and only if $U_K^{(2)} \subseteq N_{L|K}(L^\times)$.

If $L|K$ is a finite Galois extension of local fields and $L^{ur}|K$ its maximal unramified subextension, then Lemma (3.3) implies that $L|K$ is weakly ramified if and only if $L|L^{ur}$ is weakly ramified. Even more can be said if $L|L^{ur}$ is of degree p, where p is an odd prime such that $\mathbb{Q}_p \subseteq L$.

(3.20) Lemma. Let p be an odd prime and $K|\mathbb{Q}_p$ a finite unramified extension. If $L|K$ is a Galois extension of degree p, then $L|K$ is weakly ramified.

Proof. We have $(U_K^{(1)})^p \subseteq N_{L|K}(L^\times)$ according to local class field theory, so the statement follows from $(U_K^{(1)})^p = U_K^{(2)}$ using Lemma (3.19). □

We are now able to give a full description of abelian and weakly ramified extensions of $\mathbb{Q}_p$, where p denotes an odd prime.

(3.21) Proposition. Let p be an odd prime. For any finite abelian extension $L|\mathbb{Q}_p$ the following assertions are equivalent:

(a) $L|\mathbb{Q}_p$ is weakly ramified,

(b) the ramification degree of $L|\mathbb{Q}_p$ is either equal to p or coprime to p.

Proof. "(a) ⇒ (b)": Denote by G the Galois group of $L|\mathbb{Q}_p$ and suppose p divides the ramification index of $L|\mathbb{Q}_p$. Since $G_1 \neq G_2$, it follows from Lemma (3.11) that $|G_0/G_1|$ is a divisor of 1, hence $G_0 = G_1$. We have

$$G_0 = G_1 = G_1/G_2 \hookrightarrow U^{(1)}/U^{(2)} \cong \mathbb{F}_p$$

by Proposition (3.4), so $|G_0| = p$.

"(b) $\Rightarrow$ (a)": If the ramification degree of $L|\mathbb{Q}_p$ is coprime to p, the extension $L|\mathbb{Q}_p$ is tamely ramified. We therefore may assume that $|G_0| = p$ and the statement follows from the previous Lemma (3.20). □

3.4 Kummer theory

For the convenience of the reader, we briefly state the main results of Kummer theory needed shortly.

(3.22) Theorem (Kummer correspondence)**.** Let $n > 0$ be an integer and K a field such that $\operatorname{char} K \nmid n$ and $K^\times$ contains the n-th roots of unity μ_n. There is a bijective inclusion preserving correspondence defined by

$$\left\{\text{subgroups of } K^\times/(K^\times)^n\right\} \underset{\longleftarrow}{\longrightarrow} \left\{\begin{array}{c}\text{abelian Galois extensions } L|K \\ \text{of exponent dividing } n\end{array}\right\},$$

$$\Delta \longmapsto K(\sqrt[n]{a} \mid a \in \Delta),$$

$$(L^\times)^n \cap K^\times \longmapsfrom L.$$

Denoting the Galois group of $K(\sqrt[n]{a} \mid a \in \Delta)|K$ by G, we furthermore have an isomorphism

$$\Phi\colon G \to \operatorname{Hom}(\Delta, \mu_n), \quad \sigma \mapsto \left\{a \mapsto \tfrac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}\right\}.$$

In particular $\Delta \cong G$, if $|\Delta|$ is finite.

Proof. See, for example, [Bos09, 4.9, Thm. 3]. □

The following is the Kummer-theoretic version of Lemma (3.13).

(3.23) Lemma. Let $n > 0$ be an integer and M a field such that $\operatorname{char} K \nmid n$ and $K^\times$ contains the n-th roots of unity μ_n. Let further $M|K$ be a Galois extension, $\Delta \subseteq M^\times/(M^\times)^n$ a subgroup, and $L = M(\sqrt[n]{a} \mid a \in \Delta)$. The extension $L|K$ is Galois if and only if Δ is stable by the Galois group $G_{M|K}$.

Proof. Let $\overline{K}$ be an algebraic closure of K and $\tau \in \mathrm{Hom}_K(L, \overline{K})$, then, as τ was chosen arbitrarily, $L|K$ is Galois if and only if $\tau L = L$. Since $\tau L = M(\sqrt[n]{a} \mid a \in \tau\Delta)$, this is the case if and only if $\tau\Delta = \Delta$ by Kummer correspondence (3.22). □

Let K now be a local field satisfying the conditions of Theorem (3.22), then the isomorphism mentioned in Theorem (3.22) and the local reciprocity map team up with each other to give a non-degenerate bilinear map

$$\kappa\colon K^\times\!/(K^\times)^n \times K^\times\!/(K^\times)^n \to \mu_n, \quad (a,b) \mapsto \frac{(a,\ K(\sqrt[n]{b})|K)(\sqrt[n]{b})}{\sqrt[n]{b}},$$

which is called the ***Hilbert symbol***. This pairing admits the following properties.

(3.24) Proposition. Using the notations introduced above, we have

(a) $\kappa(a,b) = 1$ if and only if $a \in N_{K(\sqrt[n]{b})|K}$,

(b) $\kappa(a,b) = \kappa(b,a)^{-1}$,

(c) $\kappa(a,1-a) = 1$ and $\kappa(a,-a) = 1$.

Proof. See [Neu92, Ch. V, Satz (3.2)]. □

3.5 Non-abelian and weakly ramified extensions of degree l^2p

Let l, p be odd primes satisfying $l \mid (p-1)$. The aim of this section is to classify all local extensions $L|\mathbb{Q}_p$ of degree l^2p that are non-abelian and weakly ramified. To achieve this, we will use some of the results on non-abelian groups of order l^2p that have been proved in chapter II. In particular, recall that such a group contains a unique p-Sylow group.

The following was proved by Bley, Burns and Hahn in [BBH17, Prop. 9.8].

(3.25) Proposition. Let l, p be odd primes with $l \mid (p-1)$. Then there exist exactly l distinct non-abelian and weakly ramified Galois extension $L|\mathbb{Q}_p$ of degree l^2p such that $G_{E|\mathbb{Q}_p} \cong \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$, where $E = L^P$ denotes the fixed field of the unique p-Sylow group $P \trianglelefteq G_{L|\mathbb{Q}}$.

The rest of this section will therefore treat the case of $E|\mathbb{Q}_p$ being a cyclic extension.

(3.26) Lemma. Let $L|\mathbb{Q}_p$ be a non-abelian and weakly ramified Galois extensions of degree l^2p with Galois group G. Let further $P \trianglelefteq G$ be the unique p-Sylow group and $E = L^P$ its fixed field. If $l^2 \nmid (p-1)$ and all l-Sylow groups of G are cyclic, the extension $E|\mathbb{Q}_p$ is unramified.

Proof. Assume $E|\mathbb{Q}_p$ is of ramification degree at least l. By Lemma (2.15) there is a cylic normal subgroup $N \trianglelefteq G$ containing P. Let $E' = L^N$ be its fixed field, then $E|E'$ is the unique subextension of $E|\mathbb{Q}_p$ of degree l and therefore must be totally ramified by assumption. Now $L|E$ is totally ramified as well by Corollary (3.15), so $L|E'$ is a totally ramified extension. We have

$$\left|N_0 \diagup N_1\right| = \left|N \diagup G_{L|E}\right| = \frac{lp}{p} = l,$$

so $N_2 = N_1 \neq 0$ by Lemma (3.11) contradicting that $L|\mathbb{Q}_p$ is weakly ramified. □

Unramified case

We will now first treat the case of $E|\mathbb{Q}_p$ being unramified. As it does not require more effort, we will consider the slightly more general case of $[E : \mathbb{Q}_p] = n$, where $n \in \mathbb{N}$ is arbitrary. We begin with some preliminary results on $G_{\mathbb{F}_q|\mathbb{F}_p}$-stable subgroups of order p contained in $\mathbb{F}_q$, where q is a power of p.

(3.27) Lemma. Let $q = p^n$ for some $n \in \mathbb{N}$ and denote by $G = \langle \gamma \rangle$ the Galois group of $\mathbb{F}_q|\mathbb{F}_p$. Furthermore let $b \in \mathbb{F}_q$. The following are equivalent:

(a) $|\langle b \rangle| = p$ and $G \cdot \langle b \rangle \subseteq \langle b \rangle$,

(b) b is a root of $X^{p-1} - r$ for some $r \in \mathbb{F}_p^\times$,

(c) $b \neq 0$ and $\langle b \rangle$ is the zero set of $X^p - rX$ for some $r \in \mathbb{F}_p^\times$.

Proof. "(a) ⇒ (b)": As $\langle b \rangle$ is G-stable, we must have $\gamma b = rb$ for some $r \in \mathbb{F}_p$. Now $|\langle b \rangle| = p$ is equivalent to $b \neq 0$, so $\gamma b \neq 0$ as well. Hence $r \in \mathbb{F}_p^\times$. Thus

$$\gamma b = b^p = rb \quad \Leftrightarrow \quad b^{p-1} = r.$$

"(b) ⇒ (c)": As zero is not a root of $X^{p-1} - r$, we must have $b \neq 0$. Let $c \in \langle b \rangle$, that is $c = kb$ for some $k \in \mathbb{F}_p$, then

$$(kb)^p = b^p = rb.$$

Since $X^p - rX$ can have at most p zeros in $\mathbb{F}_q$, the statement follows.

"(c) $\Rightarrow$ (a)": Firstly, $|\langle b\rangle| = p$ is clear from $b \neq 0$. Let $c \in \langle b\rangle$, then

$$c^p - rc = 0 \quad \Leftrightarrow \quad \gamma c = rc,$$

so $\gamma^k c = r^k c \in \langle b\rangle$ for all $k \in \mathbb{N}$ by induction. □

Using Lemma (3.27) we therefore seek for all $r \in \mathbb{F}_p^\times$ such that the polynomial $X^{p-1} - r$ has a root in $\mathbb{F}_q$.

(3.28) Lemma. Let $q = p^n$ for some $n \in \mathbb{N}$ and $r \in \mathbb{F}_p^\times$. The polynomial $X^{p-1} - r$ has a root in $\mathbb{F}_q$ if and only if $\operatorname{ord} r \mid \gcd(n, p-1)$.

Proof. Let $\Delta \subseteq \mathbb{F}_p^\times$ be the set of elements $r \in \mathbb{F}_p^\times$ such that $X^{p-1} - r$ has a root in $\mathbb{F}_q$, i. e. the subgroup

$$\Delta = (\mathbb{F}_q^\times)^{p-1} \cap \mathbb{F}_p^\times.$$

Let $\Delta^{1/(p-1)} \subseteq \mathbb{F}_q^\times$ be the set of $(p-1)$-th roots of elements in Δ, then Kummer theory (Theorem (3.22)) tells us that

$$\Delta = \Delta \big/ (\mathbb{F}_p^\times)^{p-1} \cong G_{\mathbb{F}_p(\Delta^{1/(p-1)})|\mathbb{F}_p},$$

so we need to find $[\mathbb{F}_p(\Delta^{1/(p-1)}) : \mathbb{F}_p]$. Observe that $\mathbb{F}_{p^{p-1}}$ is the maximal abelian extension of exponent $(p-1)$ of $\mathbb{F}_p$, so $(\mathbb{F}_{p^{p-1}}^\times)^{p-1} \cap \mathbb{F}_p^\times = \mathbb{F}_p^\times$ by Kummer correspondence and we get

$$(\mathbb{F}_q^\times \cap \mathbb{F}_{p^{p-1}}^\times)^{p-1} \cap \mathbb{F}_p^\times = \Delta \cap \mathbb{F}_p^\times = \Delta.$$

Thus, $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^{p-1}} = \mathbb{F}_p(\Delta^{1/(p-1)})$ by Kummer correspondence, so

$$\mathbb{F}_p(\Delta^{1/(p-1)}) = \mathbb{F}_{p^{\gcd(p-1,n)}}.$$

Hence Δ is the unique subgroup of $\mathbb{F}_p^\times$ of order $\gcd(p-1, n)$. □

(3.29) Proposition. Let $n \in \mathbb{N}$ and $E|\mathbb{Q}_p$ be the unramified extension of degree n. The number of extension fields L of E such that $L|\mathbb{Q}_p$ is a non-abelian and weakly ramified extension of degree np is $\gcd(n, p-1) - 1$.

(3.30) Remark. The proof will show that for each of these fields L defining a non-abelian and weakly ramified extension $L|\mathbb{Q}_p$ there is a unique $r \in \mathbb{F}_p^\times \setminus \{1\}$ such that

$$N_{L|E}(L^\times) = (E^\times)^p \cdot U_E^{(2)} \cdot (1 + N(X^p - rX)^\perp \cdot \mathfrak{p}_E),$$

where $N(X^p - rX)$ denotes the zero set of the polynomial $X^p - rX$ and the orthogonal complement is formed with respect to the trace form of $\mathbb{F}_{p^n}|\mathbb{F}_p$.

Proof. By local class field theory (Lemma (3.13), Lemma (3.14) and Lemma (3.19)), every extension field L of E such that $L|\mathbb{Q}_p$ is a non-abelian and weakly ramified extension of degree np corresponds to a subgroup U of index p of

$$E^\times \big/ (E^\times)^p \cdot U_E^{(2)} \cong \mathbb{Z}\big/p\mathbb{Z} \times U_E^{(1)} \big/ U_E^{(2)} \qquad (*)$$

such that U is stable under the action of $G = G_{E|\mathbb{Q}_p}$ and G acts non-trivially on the quotient of $(*)$ by U. Observe that

$$U_E^{(1)} \big/ U_E^{(2)} \to \mathbb{F}_{p^n}, \quad (1 + xp)U_E^{(2)} \mapsto x + \mathfrak{p}_E$$

is an isomorphism of G-modules, since $E|\mathbb{Q}_p$ is unramified. Put

$$V = \mathbb{F}_p \times \mathbb{F}_{p^n}$$

and define

$$b\colon V \times V \to \mathbb{F}_p, \quad ((n, \alpha),\ (m, \beta)) \mapsto n \cdot m + \mathrm{Tr}(\alpha\beta),$$

then b is a non-degenerate and G-invariant bilinear form on V. Thus,

$$\left\{ \begin{array}{c} G\text{-stable subgroups} \\ U \subseteq V \text{ of index } p \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} G\text{-stable subgroups} \\ U \subseteq V \text{ of order } p \end{array} \right\},$$

$$U \longmapsto U^\perp,$$

where the orthogonal complement is formed with respect to b, defines a bijective correspondence. Let $U = \langle (n, \alpha) \rangle \subseteq V$ be a G-stable subgroup of V of order p. We have

$$V \big/ U^\perp = U \oplus U^\perp \big/ U^\perp \cong U,$$

so G acts non-trivially on the quotient if and only if it acts non-trivially on U. Let $\sigma \in G \setminus \{\mathrm{id}\}$. If $n \neq 0$, then

$$(n, \sigma\alpha) = \sigma(n, \alpha) = k(n, \alpha) \quad \text{for some } k \in \mathbb{F}_p^\times$$

implies $k = 1$. That is, G acts trivially on U and hence $U^\perp$ corresponds to an abelian extension of $\mathbb{Q}_p$. We therefore may, and do, assume that U is a G-stable subgroup of order p of $\mathbb{F}_{p^n}$. By Lemma (3.27) and Lemma (3.28) such subgroups are exactly the zero sets of the polynomials $X^p - rX$, where r ranges over all elements of $\mathbb{F}_p^\times$ satisfying $r^{\gcd(n,p-1)} = 1$. The action of G on the roots of one of these polynomials $X^p - rX$ is given by multiplication by r, so $r = 1$ is the only element we need to exclude to ensure a non-trivial G-action on the quotient $V/U^\perp$. □

Totally ramified case

Next we deal with the case that $E|\mathbb{Q}_p$ is a totally ramified extension and begin by determining such fields E. This turns out to be a Kummer-correspondence-type result.

(3.31) Lemma. Let $n \in \mathbb{N}$ be a divisor of $(p-1)$. Denote by $\mu' \subseteq \mathbb{Q}_p^\times$ the group of $(p-1)$-th roots of unity and let $\xi \in \mu'$, then $\xi \mapsto E_\xi = \mathbb{Q}(\sqrt[n]{\xi p})$ defines a bijective correspondence between $\mu'/(\mu')^n$ and the set of totally ramified cyclic extensions of $\mathbb{Q}_p$ of degree n.

Proof. Let $\xi \in \mu'$ and choose an n-th root $\sqrt[n]{\xi p}$ of ξp. We first check that $E_\xi = \mathbb{Q}_p(\sqrt[n]{\xi p})$ is indeed a totally ramified cyclic extension of $\mathbb{Q}_p$. Note that $X^n - \xi p \in \mathbb{Z}_p[X]$ is an Eisenstein polynomial, so $[E_\xi : \mathbb{Q}_p] = n$. Observe that

$$G_{E_\xi|\mathbb{Q}_p} \to \mu', \quad \sigma \mapsto \frac{\sigma(\sqrt[n]{\xi p})}{\sqrt[n]{\xi p}}$$

is an injective homomorphism, hence $G_{E_\xi|\mathbb{Q}_p}$ is cyclic of order n. Let e be the ramification degree of $E_\xi|\mathbb{Q}_p$, then comparing valuations gives

$$e \cdot v_{\mathbb{Q}_p}(\xi p) = v_{E_\xi}(\xi p) = n \cdot v_{E_\xi}(\sqrt[n]{\xi p}) \geq n.$$

Thus, $e = n$. It remains to show that $E_\xi = E_\zeta$ implies $\xi\zeta^{-1} \in (\mu')^n$ for $\xi, \zeta \in \mu'$. By Kummer correspondence (3.22), the assertion $E_\xi = E_\zeta$ is true if and only if ξp and ζp generate the same subgroup modulo $(\mathbb{Q}_p^\times)^n$. Suppose

$$\xi p(\zeta p)^{-k} \in (\mathbb{Q}_p^\times)^n = \langle p^n \rangle \times (\mu')^n \times U_{\mathbb{Q}_p}^{(1)}$$

for some $k \in \mathbb{Z}$, then $k - 1 \in n\mathbb{Z}$ by comparing valuations and $\xi\zeta^{-k} \in (\mu')^n$. These observations combine to give

$$\xi\zeta^{-1} \equiv \xi\zeta^{-k} \equiv 1 \mod (\mu')^n$$

as desired.

Now let $E|\mathbb{Q}_p$ be an arbitrary totally ramified cyclic extension of degree n. Let $\pi_E \in E$ be a uniformising element. Since $E|\mathbb{Q}_p$ is totally ramified, we have $\pi_E^n = \xi u p$ for some $\xi \in \mu'$ and $u \in U_E^{(1)}$. As n is coprime to p, we may write $u = v^n$ for some $v \in U_E^{(1)}$ and get $(\frac{\pi_E}{v})^n = \xi p$. That is, E contains an n-th root of ξp and we must have $E = \mathbb{Q}_p(\sqrt[n]{\xi p})$. □

Knowing now all totally ramified cyclic extensions $E|\mathbb{Q}_p$, we continue by investigating how such a field E can be extended by a field extension $L|E$ of degree p in order to obtain a non-abelian weakly ramified extension $L|\mathbb{Q}_p$.

(3.32) Lemma. Let $n \in \mathbb{N}$ be coprime to p and $E|\mathbb{Q}_p$ a totally ramified cyclic extension of degree n. Then

(a) we necessarily have $n \mid (p-1)$,

(b) there is exactly one extension field L of E such that $L|\mathbb{Q}_p$ is a non-abelian and weakly ramified extension of degree np.

Proof. (a): By [Neu11, Ch. II, Satz (7.17)], the norm group of $E|\mathbb{Q}_p$ contains a uniformising element π of $\mathbb{Q}_p$ and therefore corresponds to a subgroup of index n of

$$\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^n \cdot \langle \pi \rangle \cong \mu' / (\mu')^n \cong \mathbb{Z} / \gcd(n, p-1)\mathbb{Z},$$

where $\mu' \subseteq \mathbb{Q}_p^\times$ denotes the subgroup of $(p-1)$-th roots of unity. The existence of a subgroup of index n therefore forces n to be a divisor of $p-1$.

(b): Every such extension field L corresponds to a subgroup U of index p of

$$E^\times / (E^\times)^p \cdot U_E^{(2)} \cong \mathbb{Z}/p\mathbb{Z} \times U_E^{(1)} / U_E^{(2)} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \qquad (*)$$

that is stable under $G = G_{E|\mathbb{Q}_p}$ and such that G acts non-trivially on the quotient of $(*)$ by U. We therefore first investigate the action of G on $(*)$.

By Lemma (3.31) we have $E = \mathbb{Q}_p(\sqrt[n]{\xi p})$, where ξ is a $(p-1)$-th root of unity. Set $\pi_E = \sqrt[n]{\xi p}$ and choose a generator γ of G, then $\gamma \pi_E = \xi_\gamma \pi_E$ for some primitve n-th root of unity ξ_γ. In particular,

$$\gamma \pi_E \equiv \pi_E \mod (E^\times)^p,$$

so we may assume that G acts trivially on the first component of $(*)$. Consider

the isomorphism

$$\theta\colon U_E^{(1)}/U_E^{(2)} \to \mathbb{F}_p, \quad (1+x\pi_E)U_E^{(2)} \mapsto x+\mathfrak{p}_E,$$

which induces the following G-action on $\mathbb{F}_p$: Let $x+\mathfrak{p}_E \in \mathbb{F}_p$, then we have

$$\gamma(x+\mathfrak{p}_E) = \theta\left(\gamma(1+x\pi_E)U_E^{(2)}\right) = \xi_\gamma x+\mathfrak{p}_E,$$

where we used that $\gamma x \equiv x \mod \mathfrak{p}_E$ since $E|\mathbb{Q}_p$ is totally ramified. Let U be a G-stable subgroup of $(*)$ of order p and pick a generator $(a,b) \in U$. We have

$$\gamma b = b \quad \Leftrightarrow \quad \xi_\gamma b = b \quad \Leftrightarrow \quad b = 0 \text{ or } \xi_\gamma = 1.$$

As ξ_γ is a primtive n-th root, we get that

$$(a,b) - \gamma(a,b) = (0, b-\gamma b) \in U$$

is nonzero if $b \neq 0$. Hence $U = \langle (0,b-\gamma b)\rangle = \{0\}\times\mathbb{F}_p$. Now G acts trivially on the quotient of $(*)$ by U, so this U provides an abelian extension of E. We therefore may assume $b=0$, i. e. $U = \mathbb{F}_p \times \{0\}$. As seen above, G acts non-trivially on the quotient of $(*)$ by U, so this U indeed corresponds to a non-abelian extension of E. □

Lemma (3.31) and Lemma (3.32) in conjunction give

(3.33) Proposition. Let l, p be odd primes such that $l^2 \mid (p-1)$, then there are exactly l^2 non-abelian and weakly ramified extensions $L|\mathbb{Q}_p$ of degree l^2p with $L^P|\mathbb{Q}_p$ being totally ramified and cyclic, where P denotes the unique p-Sylow subgroup of the Galois group $G_{L|\mathbb{Q}_p}$.

Proof. Follows from Lemma (3.31) and Lemma (3.32) as every such extension $L|\mathbb{Q}_p$ contains a unique subextension $E|\mathbb{Q}_p$ of degree l^2. □

(3.34) Remark. The proof of Proposition (3.33) shows that each of these non-abelian and weakly ramified extension $L|\mathbb{Q}_p$ of degree l^2p with $E = L^P|\mathbb{Q}_p$ being totally ramified and cyclic, where P denotes the unique p-Sylow subgroup of the Galois group $G_{L|\mathbb{Q}_p}$, arises in the following way:

The unique subfield E is of the form $E = \mathbb{Q}_p(\sqrt[l^2]{\xi p})$, where ξ is a $(p-1)$-th root of unity of $\mathbb{Q}_p$. Now L is the unique extension field of E having norm group

$$N_{L|E}(L^\times) = \langle \sqrt[l^2]{\xi p} \rangle \cdot \mu' \cdot U_E^{(2)},$$

where $\mu' \subseteq \mathbb{Q}_p^\times$ denotes the subgroup of $(p-1)$-th roots of unity.

Ramification degree l case

It remains to look at the case that $E|\mathbb{Q}_p$ is a cyclic extension of degree l^2 and ramification index l. By Lemma (3.26) we may assume $l^2 \mid (p-1)$.

(3.35) Lemma. Let l, p be odd primes such that $l^2 \mid (p-1)$, then there are exactly $(l-1)$ distinct cyclic extensions $E|\mathbb{Q}_p$ of ramification index l such that $[E : \mathbb{Q}_p] = l^2$.

Proof. Let $E|\mathbb{Q}_p$ be such an extension and G its Galois group, then the inertia subgroup G_0 is the unique subgroup of order l, and $E' = E^{G_0}$, the unique subfield of degree l, is unramified over $\mathbb{Q}_p$. Hence

$$(\mathbb{Q}_p^\times)^{l^2} \subseteq N_{E|\mathbb{Q}_p}(E^\times) \subseteq N_{E'|\mathbb{Q}_p}\left((E')^\times\right) = \langle p^l \rangle \times \mathbb{Z}_p^\times$$

by local class field theory. If we pass to the quotient, this chain corresponds to a chain

$$\{0\} \subseteq \overline{N} \subseteq \overline{N'} \quad \text{in} \quad \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^{l^2} \cong \mathbb{Z}/l^2\mathbb{Z} \times \mathbb{Z}/l^2\mathbb{Z},$$

where

$$\overline{N'} = \langle (l,0),\ (0,1) \rangle \quad \subseteq \mathbb{Z}/l^2\mathbb{Z} \times \mathbb{Z}/l^2\mathbb{Z}$$

corresponds to the norm group of $E'|\mathbb{Q}_p$. Now $\overline{N}$ is a subgroup of index l^2 of $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^{l^2}$, so it is a subgroup of order l^2 of $\overline{N'}$. Firstly, $\overline{N'}$ contains $l(l-1) \cdot l$ elements of order l^2, therefore it contains l cyclic subgroups of order l^2, which are explicitely given by

$$U_k = \langle (kl,\ 1) \rangle, \quad \text{where } 0 \leq k \leq l-1.$$

If $U \subseteq \overline{N'}$ is a non-cyclic subgroup of order l^2, every of its non-trivial elements has order l. Counting elements yields that there is exactly one such subgroup, namely

$$U = \langle (l,0),\ (0,l) \rangle.$$

However, we have

$$(\mathbb{Z}/l^2\mathbb{Z} \times \mathbb{Z}/l^2\mathbb{Z})/U \cong \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z},$$

so U corresponds to a non-cyclic extension of $\mathbb{Q}_p$. Now U_0 corresponds to

$$\langle p^{l^2} \rangle \times \mu' \times U_{\mathbb{Q}_p}^{(1)},$$

i. e. the unramified extension of $\mathbb{Q}_p$. It follows that the remaining subgroups U_k for $k \in \{1, ..., l-1\}$ correspond to extensions of ramification index l and we only have to check these extensions to be cyclic as well. Take $(l, 1) \in \mathbb{Z}/l^2\mathbb{Z} \times \mathbb{Z}/l^2\mathbb{Z}$ and $k \in \{1, ..., l-1\}$, then

$$n \cdot (1,1) \in U_k \quad \Leftrightarrow \quad (n,n) = (rkl, r)$$

for some $r \in \mathbb{Z}$. The latter implies

$$rkl \equiv n \equiv r \mod l^2 \quad \Leftrightarrow \quad r(kl-1) \equiv 0 \mod l^2.$$

As $kl - 1 \not\equiv 0 \mod l$, we must have $n \equiv r \equiv 0 \mod l^2$. This shows that $(1,1)$ is an element of order l^2 in $(\mathbb{Z}/l^2\mathbb{Z} \times \mathbb{Z}/l^2\mathbb{Z})/U_k$. □

(3.36) Lemma. Let l, p be odd primes such that $l^2 \mid (p-1)$ and $E|\mathbb{Q}_p$ a cyclic extension of degree l^2 and ramification degree l. Then there are exactly l extension fields L of E such that $L|\mathbb{Q}_p$ is a non-abelian and weakly ramified extension of degree l^2p.

Proof. Let L be such a field, then its norm group over E corresponds to a subgroup U of index p of

$$E^\times \big/ (E^\times)^p \cdot U_E^{(2)} \cong \mathbb{Z}\big/p\mathbb{Z} \times \mathbb{F}_{p^l} \qquad (*)$$

that is stable under the action of $G = G_{E|\mathbb{Q}}$ and such that G acts non-trivially on the quotient of $(*)$ by U. We therefore first search for such groups.
Let V be the factor group $(*)$, then V is an $\mathbb{F}_p[G]$-module and we can apply Theorem (2.26) to obtain a decomposition

$$V = \bigoplus_{\chi \in \widehat{G}} e_\chi V,$$

where $\widehat{G} = \mathrm{Hom}(G, \mathbb{F}_p^\times)$. Every nonzero component of this decomposition is of order at least p. We now show that there are $(l+1)$ nonzero components, hence every nonzero component is of order p.

Let E' be the unique intermediary field of $E|\mathbb{Q}$, i. e. $E'|\mathbb{Q}_p$ is the unramified extension of degree l. Choose a generator $\gamma \in G$ such that γ is an extension of the Frobenius automorphism of $E'|\mathbb{Q}_p$. Since $E|E'$ is totally, but tamely, ramified, we can choose a uniformiser π_E of E such that $\pi_{E'} = \pi_E^l$ is a uniformiser of E'. We

now have $G_{E|E'} = \langle \gamma^l \rangle$ and hence $\gamma^l(\pi_E) = \xi\pi_E$ for some primitive l-th root of unity $\xi \in \mathbb{Z}_p^\times$, where we may assume $\xi = a^l$ for some primitive l^2-th root of unity $a \in \mathbb{Z}_p^\times$, i. e. $\gamma(\pi_E) = a^m\pi_E$ for an integer m satisfying $m \equiv 1 \mod l$. Now define

$$\psi\colon G \to \mathbb{F}_p^\times, \quad \gamma^i \mapsto a^i,$$

then $\widehat{G} = \langle \psi \rangle$. We furthermore define for $r \in (\mathbb{Z}/l^2\mathbb{Z})^\times$ an automorphism $f_r \in \mathrm{Aut}(G)$ by $f(\gamma) = \gamma^r$.

Pick r such that $r^l = 1$, which is the same as saying that $r \equiv 1 \mod l$, and set $\phi_r = \psi \circ f_r \in \widehat{G}$. We now have

$$\begin{aligned} e_{\phi_r} &= \frac{1}{l^2}\sum_{\sigma\in G}\phi_r(\sigma)\sigma^{-1} = \frac{1}{l^2}\sum_{\sigma\in G/G_{E|E'}}\sum_{\rho\in G_{E|E'}}\phi_r(\sigma\rho)(\sigma\rho)^{-1} = \\ &= \frac{1}{l^2}\sum_{i=0}^{l-1}\sum_{j=0}^{l-1}\phi_r(\gamma^i\gamma^{jl})\gamma^{-i}\gamma^{-jl} \overset{(**)}{=} \frac{1}{l^2}\sum_{i=0}^{l-1}\sum_{j=0}^{l-1}\psi(\gamma^{ir+jl})\gamma^{-i-jl} = \\ &= \frac{1}{l^2}\sum_{i=0}^{l-1}\sum_{j=0}^{l-1}a^{ir+jl}\gamma^{-i-jl} = \frac{1}{l^2}\left(\sum_{i=0}^{l-1}a^{ir}\gamma^{-i}\right)\cdot\left(\sum_{j=0}^{l-1}a^{jl}\gamma^{-jl}\right), \end{aligned}$$

where we used $r \equiv 1 \mod l$ at equality $(**)$. Consider the isomorphism

$$\theta\colon U_E^{(1)}/U_E^{(1)} \to \mathbb{F}_{p^l}, \quad (1 + x\pi_E)U_E^{(1)} \mapsto x + \mathfrak{p}_E,$$

which induces the following action of G on $\mathbb{F}_{p^l}$: Let $x + \mathfrak{p}_E \in \mathbb{F}_p$, then

$$\gamma^i \cdot (x + \mathfrak{p}_E) = \theta\left(\gamma^i(1 + x\pi_E)U_E^{(1)}\right) = \gamma^i(x)a^{im} + \mathfrak{p}_E$$

for all $i \in \mathbb{Z}$. In particular, we have

$$\gamma^{il} \cdot (x + \mathfrak{p}_E) = xa^{ilm} + \mathfrak{p}_E = xa^{il} + \mathfrak{p}_E,$$

since $x + \mathfrak{p}_E$ can be represented by an element $x \in E'$ and $m \equiv 1 \mod l$. Using

the expression obtained above, we therefore get

$$\begin{aligned} e_{\phi_r} \cdot (x + \mathfrak{p}_E) &= \frac{1}{l^2} \left(\sum_{i=0}^{l-1} a^{ir} \gamma^{-i} \right) \cdot \left(\sum_{j=0}^{l-1} a^{jl} \gamma^{-jl} \right) \cdot (x + \mathfrak{p}_E) = \\ &= \frac{1}{l^2} \left(\sum_{i=0}^{l-1} a^{ir} \gamma^{-i} \right) \cdot \sum_{j=0}^{l-1} a^{jl} \cdot a^{-jl} \cdot (x + \mathfrak{p}_E) = \\ &= \frac{1}{l} \sum_{i=0}^{l-1} a^{i(r-m)} \gamma^{-i} \cdot (x + \mathfrak{p}_E) = \frac{1}{l} \sum_{i=0}^{l-1} a^{ir} x^{p^{l-i}} + \mathfrak{p}_E \end{aligned}$$

If we choose a normal basis element $b \in \mathbb{F}_{p^l}$ of $\mathbb{F}_{p^l}|\mathbb{F}_p$, we thus get $e_{\phi_r} \cdot b \neq 0$. Moreover, if ψ^0 denotes the trivial character, we have

$$e_{\psi^0} \cdot p = \frac{1}{l^2} \sum_{\sigma \in G} \psi^0(\sigma) \sigma^{-1}(p) = \left(N_{E|\mathbb{Q}_p}(p) \right)^{1/l^2} = p \quad \notin (E^\times)^p \cdot U_E^{(2)},$$

so ψ^0 and ϕ_r for $r \in (\mathbb{Z}/l^2\mathbb{Z})^\times$ with $r^l = 1$ are the $(l+1)$ characters giving non-vanishing components in the decomposition of V above.
It follows that the subgroups of the form $(e_{\phi_r} - 1)V$ are of index p, G-stable and yield a quotient

$$V \big/ (e_{\phi_r} - 1)V \cong e_{\phi_r} V,$$

on which G acts non-trivially. This way we obtain by local class field theory l extension fields L of E such that $L|\mathbb{Q}_p$ is non-abelian, weakly ramified, and of degree l^2p.

Conversely, if L is a field with these properties, we have

$$G_{L|E} \cong E^\times \big/ N_{L|E}(L^\times) = \bigoplus_{\chi \in \widehat{G}} e_\chi \cdot \left(E^\times \big/ N_{L|E}(L^\times) \right).$$

As $|G_{L|E}| = p$, exactly one component is nonzero. Let χ_0 be the corresponding character, then we have

$$(e_{\chi_0} - 1) \left(E^\times \big/ N_{L|E}(L^\times) \right) = 0 \quad \Leftrightarrow \quad (e_{\chi_0} - 1)E^\times \subseteq N_{L|E}(L^\times).$$

Now $N_{L|E}(L^\times)$ corresponds to a subgroup of index p of

$$E^\times \big/ (e_{\chi_0} - 1)E^\times \cdot (E^\times)^p \cdot U_E^{(2)} = V \big/ (e_{\chi_0} - 1)V \cong e_{\chi_0} V.$$

We have seen above that this is only possible if $\chi_0 = \phi_r$ for some $r \in (\mathbb{Z}/l^2\mathbb{Z})^\times$ with $r^l = 1$ and

$$N_{L|E}(L^\times) = (e_{\chi_0} - 1)E^\times \cdot (E^\times)^p \cdot U_E^{(2)}.$$

□

Lemma (3.35) and Lemma (3.36) combine to give

(3.37) Proposition. Let l, p be odd primes such that $l^2 \mid (p-1)$, then there are exactly $l(l-1)$ non-abelian and weakly ramified extensions $L|\mathbb{Q}_p$ of degree $l^2 p$ with $L^P|\mathbb{Q}_p$ being cyclic of ramification degree l, where P denotes the unique p-Sylow subgroup of the Galois group $G_{L|\mathbb{Q}_p}$.

We summarise the Propositions (3.29), (3.33) and (3.37) by giving the following table that displays the respective number of non-abelian and weakly ramified extensions in each of the possible cases for the ramification index $e_{E|\mathbb{Q}_p}$:

$e_{E\|\mathbb{Q}_p}$	1	l	l^2
$l^2 \nmid (p-1)$	$l-1$	-	-
$l^2 \mid (p-1)$	l^2-1	$l(l-1)$	l^2

3.6 Local extensions with Galois group $\mathrm{SL}_2(\mathbb{F}_3)$

In this section we prove that for any prime p there is no Galois extension $L|\mathbb{Q}_p$ whose Galois group is $\mathrm{SL}_2(\mathbb{F}_3)$.

The Binary Tetrahedral Group

Recall that $\mathrm{SL}_2(\mathbb{F}_3)$, the ***Special Linear Group*** of dimension 2 with coefficients in $\mathbb{F}_3$, is defined as

$$\mathrm{SL}_2(\mathbb{F}_3) = \{A \in \mathrm{GL}_2(\mathbb{F}_3) \mid \det A = 1\}$$

and fits into an exact sequence

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{SL}_2(\mathbb{F}_3) \longrightarrow A_4 \longrightarrow 1,$$

where $A_4 \trianglelefteq S_4$ denotes the Alternating Group of four symbols. As A_4 is the symmetry group of the tetrahedron, $\mathrm{SL}_2(\mathbb{F}_3)$ is sometimes also called the ***Binary Tetrahedral Group*** and denoted by $\widetilde{A_4}$. However, we will stick to the notation $\mathrm{SL}_2(\mathbb{F}_3)$.

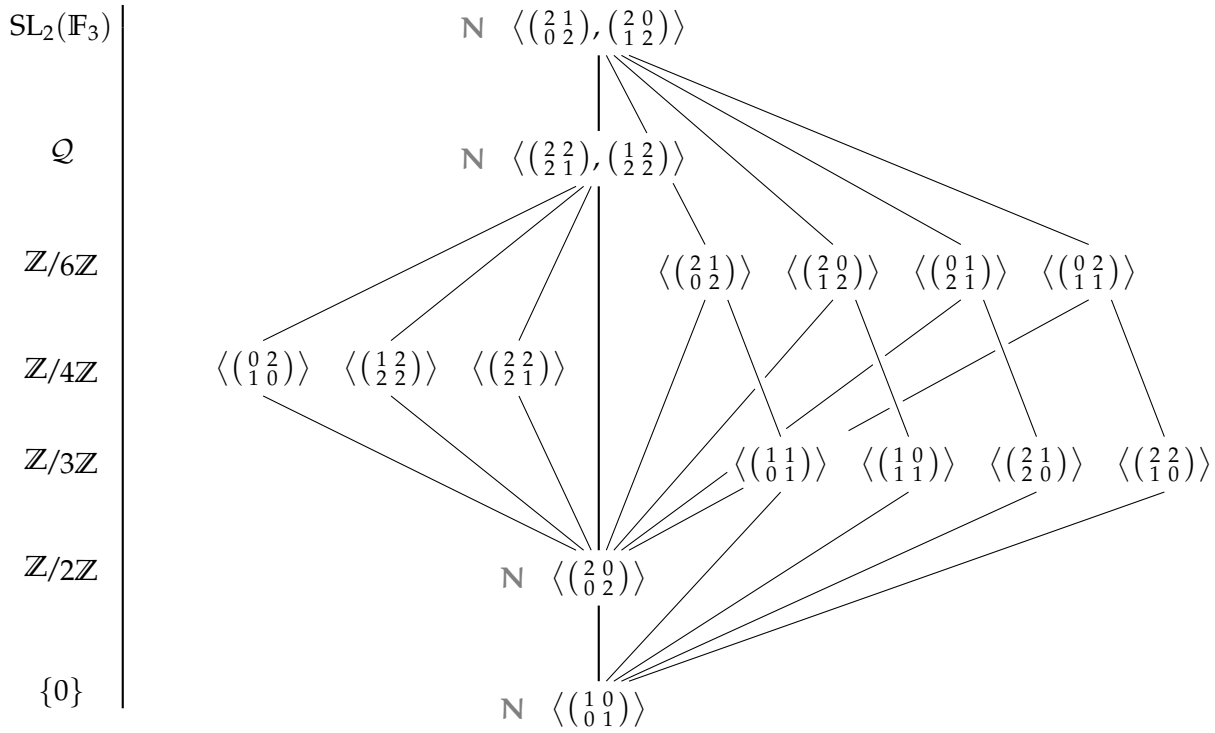


Figure (3.1): Subgroup lattice of $\mathrm{SL}_2(\mathbb{F}_3)$: On the left hand side the respective isomorphism type is given ($\mathcal{Q}$ denotes the Quaternion group). The symbol $\mathbb{N}$ indicates a normal subgroup. The diagram is taken from [Ros09, p. 175].

For more details on $\mathrm{SL}_2(\mathbb{F}_3)$ the reader is kindly referred to [Ros09, Chapter 8.2]. For example, we will make use of the subgroup structure of $\mathrm{SL}_2(\mathbb{F}_3)$ as displayed in Figure (3.1) and of the fact that $\mathrm{SL}_2(\mathbb{F}_3)$ is the unique non-abelian group of order 24 containing no normal subgroup of order 12.

The case of odd p

We will now show that if p is odd, there is not even Galois extension $L|\mathbb{Q}_p$ with Galois group A_4. In particular, no Galois extension with Galois group $\mathrm{SL}_2(\mathbb{F}_3)$ can exist. It is crucial for the proof that A_4 contains only one non-trivial normal subgroup, namely the Klein four-group (cf. Figure (3.1)).

(3.38) Proposition. Let p be an odd prime. There is no p-adic number field L such that $L|\mathbb{Q}_p$ is a Galois extension with Galois group A_4.

Proof. Suppose there is a Galois extension $L|\mathbb{Q}$ with Galois group $G \cong A_4$. Let $V_4 \trianglelefteq A_4$ be the Klein four-group, then $L^{V_4}|\mathbb{Q}_p$ is a Galois extension of degree 3 and $L|L^{V_4}$ is an extension of degree 4 and exponent 2. We have

$$(L^{V_4})^\times \big/ \big((L^{V_4})^\times\big)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mu' \big/ (\mu')^2 \times U^{(1)}_{L^{V_4}} \big/ (U^{(1)}_{L^{V_4}})^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

where $\mu' \subseteq (L^{V_4})^\times$ denotes the subgroup of $(p^f - 1)$-th roots of unity with f being the residue degree of $L^{V_4}|\mathbb{Q}_p$. Choose a uniformising element $\pi \in L^{V_4}$, then we have

$$N_{L|L^{V_4}}(L^\times) = \langle \pi^2 \rangle \times (\mu')^2 \times U^{(1)}_{L^{V_4}},$$

so the extension $L^{V_4}|L$ has ramification degree 2. It follows that $L|\mathbb{Q}_p$ has ramification degree 2 or 6. However, A_4 contains neither a normal subgroup of order 2 nor of order 6. □

The case $p = 2$

Unlike in the case of odd p, it turns out that there actually does exist a unique Galois extension $L|\mathbb{Q}_2$ with Galois group A_4. Before proving this, we first prove a preparational

(3.39) Lemma. Let $L|\mathbb{Q}_2$ be a Galois extension with Galois group A_4. Then $L^{V_4}|\mathbb{Q}_2$ is unramified and $L|L^{V_4}$ is totally ramified.

Proof. Observe that

$$\mathbb{Q}_2^\times \big/ (\mathbb{Q}_2^\times)^3 \cong \mathbb{Z}/3\mathbb{Z},$$

so there is a unique Galois extension of $\mathbb{Q}_2$ of degree 3, namely the unramified one.

The extension $L|L^{V_4}$ cannot be unramified, as this would mean that $L|\mathbb{Q}_2$ is unramified, hence abelian. So we must have $2 \leq e_{L|\mathbb{Q}_2} \leq 4$, where $e_{L|\mathbb{Q}_2}$ denotes the ramification index of $L|\mathbb{Q}_2$. Now the inertia subgroup of $L|\mathbb{Q}_2$ is a normal subgroup having degree $e_{L|\mathbb{Q}_2}$ and as V_4 is the only non-trivial normal subgroup of A_4, we must have $e_{L|\mathbb{Q}_2} = 4$. Thus, $L|L^{V_4}$ is a totally ramified extension. □

We now determine the unique extension field Z of $\mathbb{Q}_2$ such that $Z|\mathbb{Q}_2$ is a Galois extension with Galois group A_4.

(3.40) Proposition. There is a unique field Z such that $Z|\mathbb{Q}_2$ is a Galois extension with Galois group A_4. Let $E = Z^{V_4}$, i. e. $E|\mathbb{Q}_2$ is the unramified extension of degree 3, pick

a root $\alpha \in E^\times$ of $X^3 + X + 1$ and denote by $\varphi \in G_{E|\mathbb{Q}_2}$ the Frobenius automorphism, then we have

$$Z = E\left(\sqrt{5(1+2\alpha)},\ \sqrt{5(1+2\varphi(\alpha))}\right).$$

Moreover, the respective norm group is

$$N_{Z|E}(Z^\times) = \langle 2\rangle \times \mu_7 \times \langle -1, U_E^{(2)}\rangle \quad \subseteq E^\times.$$

Proof. It follows from the exact sequence

$$1 \longrightarrow U_E^{(2)}/(U_E^{(1)})^2 \longrightarrow U_E^{(1)}/(U_E^{(1)})^2 \longrightarrow U_E^{(1)}/U_E^{(2)} \longrightarrow 1$$

and [Neu11, Satz II.(3.7)] that $U_E^{(2)}/(U_E^{(1)})^2$ is of order 2, so it is generated by the class of a single element of $U_E^{(2)}$ that is not a square. Suppose $5 \in (U_E^{(1)})^2$, i. e. there is $x \in \mathcal{O}_E$ such that

$$1 + 2\cdot 2 = (1+2x)^2 \quad \Leftrightarrow \quad 1 + 4 = 1 + 4(x + x^2) \quad \Leftrightarrow \quad 1 = x + x^2.$$

In particular, $x + \mathfrak{p}_E$ would be a root of the polynomial $X^2 + X + 1$ in $\mathbb{F}_8$. However, $X^2 + X + 1$ is irreducible in $\mathbb{F}_8[X]$. The exact sequence above is a split exact sequence of $\mathbb{F}_2$-vector spaces, hence $\{-1, 1+2\alpha, 1+2\varphi(\alpha), 5\}$ is a $\mathbb{F}_2$-basis of $U_E^{(1)}/(U_E^{(1)})^2$ using the isomorphism

$$\theta\colon U_E^{(1)}\big/U_E^{(2)} \to \mathbb{F}_8, \quad (1+2x)U_E^{(2)} \mapsto x + \mathfrak{p}_E.$$

The polynomial $X^3 + X + 1$ encodes the following equations:

$$\begin{aligned} 0 &= \mathrm{Tr}_{E|\mathbb{Q}_2}(\alpha) \\ 1 &= \alpha\varphi(\alpha) + \alpha\varphi^2(\alpha) + \varphi(\alpha)\varphi^2(\alpha) \\ -1 &= N_{E|\mathbb{Q}_2}(\alpha) \end{aligned}$$

A short calculation now yields

$$\begin{aligned} N_{E|\mathbb{Q}_2}(1+2\alpha) &= (1+2\alpha)(1+2\varphi(\alpha))(1+2\varphi^2(\alpha)) = \\ &= 1 + 2\,\mathrm{Tr}_{E|\mathbb{Q}_2}(\alpha) + 4(\alpha\varphi(\alpha) + \alpha\varphi^2(\alpha) + \varphi(\alpha)\varphi^2(\alpha)) + 8N_{E|\mathbb{Q}_2}(\alpha) = \\ &= 1 + 4 - 8 = \\ &= -3. \end{aligned}$$

Observe that $-3 \in U_E^{(2)} \setminus (U_E^{(1)})^2$ by the same argument as was used above to show $5 \in U_E^{(2)} \setminus (U_E^{(1)})^2$. Consequently, the action of $G_{E|\mathbb{Q}_2}$ on $U^{(1)_E}/(U_E^{(1)})^2$ is defined by

$$\varphi(1+2\alpha) = 1+2\varphi^2(\alpha), \qquad \varphi(1+2\varphi(\alpha)) = 5(1+2\alpha)(1+2\varphi(\alpha)) \mod (E^\times)^2$$

and one immediately checks that

$$\begin{aligned} U^{(1)_E}\!/(U_E^{(1)})^2 = &\{1\} \cup \{-1\} \cup \{5\} \cup \{-5\} \\ &\cup \{(1+2\alpha),\ (1+2\varphi(\alpha)),\ 5(1+2\alpha)(1+2\varphi(\alpha))\} \\ &\cup \{-(1+2\alpha),\ -(1+2\varphi(\alpha)),\ -5(1+2\alpha)(1+2\varphi(\alpha))\} \\ &\cup \{5(1+2\alpha),\ 5(1+2\varphi(\alpha)),\ (1+2\alpha)(1+2\varphi(\alpha))\} \\ &\cup \{-5(1+2\alpha),\ -5(1+2\varphi(\alpha)),\ -(1+2\alpha)(1+2\varphi(\alpha))\} \end{aligned}$$

is the decomposition into disjoint $G_{E|\mathbb{Q}_2}$-orbits. From this explicit description it is obvious that the only $G_{E|\mathbb{Q}_2}$-stable subgroup of $E^\times/(E^\times)^2$ of order 4 on which $G_{E|\mathbb{Q}_2}$ acts non-trivially is

$$\langle 5(1+2\alpha), 5(1+2\varphi(\alpha))\rangle.$$

Observe that if $U = \langle a, b\rangle$ is a subgroup of $E^\times/(E^\times)^2$ generated by elements $a, b \in \mathbb{Q}_2$, then $E(\sqrt{a}, \sqrt{b}) = E \cdot \mathbb{Q}_2(\sqrt{a}, \sqrt{b})$ is the composite of two linearly disjoint abelian extensions of $\mathbb{Q}_2$, hence it is itself an abelian extension of $\mathbb{Q}_2$. Thus, Kummer correspondence (3.22) and Lemma (3.23) give that

$$Z = E\left(\sqrt{5(1+2\alpha)},\ \sqrt{5(1+2\varphi(\alpha))}\right)$$

is the only candidate for an extension $Z|E$ having Galois group V_4 such that $Z|\mathbb{Q}_2$ is a non-abelian Galois extension. Since $5(1+2\alpha)$ is not fixed by φ, the extension $E(\sqrt{5(1+2\alpha)})|\mathbb{Q}_2$ is not Galois by Lemma (3.23), hence $Z|\mathbb{Q}_2$ is indeed non-abelian. Thus, the Galois group $G_{Z|\mathbb{Q}_2}$ is a non-abelian group of order 12 having $G_{Z|E} \cong V_4$ as a normal subgroup. The only such group is A_4.

Now the norm group of an extension $K|E$ with $G_{K|E} = V_4$ and such that $K|\mathbb{Q}_2$ is non-abelian corresponds to a $G_{E|\mathbb{Q}_2}$-stable subgroup U of index 4 of $Z^\times/(Z^\times)^2$ such that $G_{E|\mathbb{Q}_2}$ acts non-trivially on the quotient $(Z^\times/(Z^\times)^2)/U$. We know from the previous discussion that there is exactly one such group, so we must have

$$U = \langle 2, -1, 5\rangle,$$

which concludes the proof. □

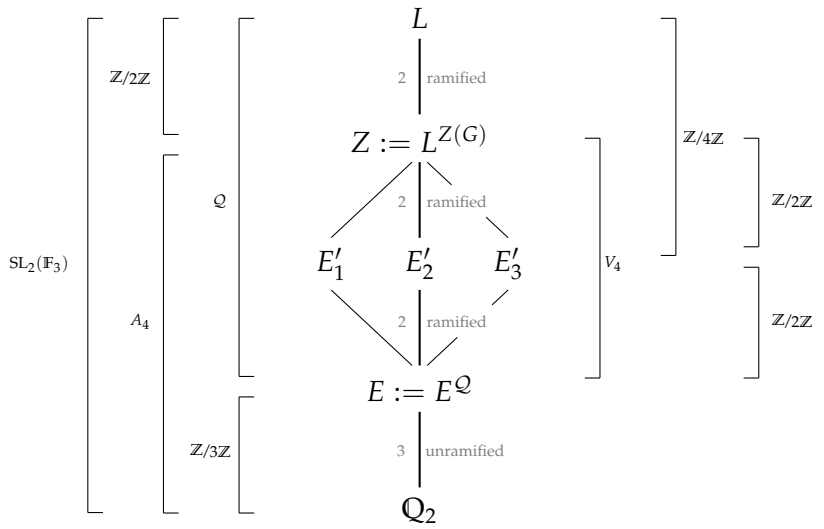


Figure (3.2): Illustration of a field extension $L|\mathbb{Q}_2$ with Galois group $G \cong \mathrm{SL}_2(\mathbb{F}_3)$. Here $Z(G)$ denotes the centre of G and $\mathcal{Q} \subseteq G$ the unique 2-Sylow group. All Galois subextensions are marked with a square bracket carrying the isomorphism type of the respective Galois group.

(3.41) Remark. According to the LMFDB database[3], the field Z determined in Proposition (3.40) is, as an extension of $\mathbb{Q}_2$, generated by the polynomial

$$X^{12} - 2X^{11} + 6X^{10} + 4X^9 + 6X^8 + 12X^7 - 4X^6 - 8X^3 + 16X^2 - 8.$$

Crucial to the remaining proof is now the following result.

(3.42) Theorem (Fröhlich)**.** Let K be a local field of characteristic $\neq 2$ and $a, b \in K^\times \setminus (K^\times)^2$. The field $K(\sqrt{a}, \sqrt{b})$ has an extension field L such that $L|K$ is a Galois extension with $G_{L|K} = \mathcal{Q}$, the quaternion group, if and only if

$$\kappa(a,b) \cdot \kappa(a,-1) \cdot \kappa(b,-1) = 1,$$

where $\kappa\colon K^\times/(K^\times)^2 \times K^\times/(K^\times)^2 \to \{\pm 1\}$ denotes the Hilbert symbol.

Proof. See [Frö85, (7.7)] □

(3.43) Theorem. There is no Galois extension $L|\mathbb{Q}_2$ such that $G_{L|\mathbb{Q}_2} \cong \mathrm{SL}_2(\mathbb{F}_3)$.

[3] See `http://www.lmfdb.org/LocalNumberField/2.12.18.59`

Proof. Suppose there is such an extension $L|\mathbb{Q}_2$, then $Z \subseteq L$, where Z denotes the unique field of Proposition (3.40), and $L|E$ is a Galois extension having Galois group $\mathcal{Q}$. It therefore suffices to show that such a field does not exist.

It also follows from Proposition (3.40) (using the notation introduced there) that

$$N_{E(\sqrt{5(1+2\alpha)})|E}\left(E(\sqrt{5(1+2\alpha)})^\times\right) = \langle 2\rangle \times \mu_7 \times \langle -1,\ 1+2\alpha,\ U_E^{(2)}\rangle,$$
$$N_{E(\sqrt{5(1+2\varphi\alpha)})|E}\left(E(\sqrt{5(1+2\varphi\alpha)})^\times\right) = \langle 2\rangle \times \mu_7 \times \langle -1,\ 1+2\varphi\alpha,\ U_E^{(2)}\rangle.$$

We thus have

$$\begin{aligned}\kappa\left(5(1+2\alpha),\ -1\right) &= \kappa(-1,5(1+2\alpha))^{-1} = 1,\\ \kappa(5(1+2\varphi(\alpha)),-1) &= \kappa(-1,5(1+2\varphi(\alpha)))^{-1} = 1,\\ \kappa(5(1+2\alpha),\ 5(1+2\varphi(\alpha)) &= -1.\end{aligned}$$

Now the statement follows from Theorem (3.42). □

Because of the following Lemma we have thereby also classified all Galois extensions $L|\mathbb{Q}_2$ of degree 24 containing Z as a subfield.

(3.44) Lemma. Let $M|K$ be a Galois extension with Galois group $G \cong A_4$ and L an quadratic extension field of M such that $L|K$ is Galois. Then either

(a) $G_{L|K} \cong \mathrm{SL}_2(\mathbb{F}_3)$ or

(b) there is a quadratic sub-extension $k|\mathbb{Q}_2$ of $L|K$ and $L = k \cdot M$. In this case, k is unique as quadratic subfield of L and $G_{L|K} \cong A_4 \times \mathbb{Z}/2\mathbb{Z}$.

Proof. Let $H = G_{L|M}$. As a non-abelian group of order 24, G is isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$ if and only if G contains no normal subgroup N of order 12.
Suppose there is such a normal subgroup $N \trianglelefteq G$ of order 12. If $H \subseteq N$, we have

$$N/H \hookrightarrow G/H \cong A_4.$$

However, A_4 contains no subgroup of order 6, so we must have $N \cap H = 1$. This implies $G = H \cdot N$ and

$$A_4 \cong G/H = HN/H \cong N/H \cap N \cong N.$$

Hence $G \cong N \times H \cong A_4 \times \mathbb{Z}/2\mathbb{Z}$. Now A_4 is the only subgroup of order 12

of $A_4 \times \mathbb{Z}/2\mathbb{Z}$ (cf. [Ros09, p. 290]), thence $k = L^{A_4}$ is the unique subfield of L satisfying $[k : K] = 2$. Moreover, k is not contained in M, whence $L = k \cdot M$. □

4 Global Considerations

4 **Global Considerations** 61
4.1 Embedding problems
4.2 Some results from global class field theory
4.3 Weakly ramified and non-abelian extensions of degree l^2p

5 **Bibliography** 81

4.1 Embedding problems

In this section we first define the notion of an embedding problem associated to a number field and subsequently prove a theorem about solvability of such an embedding problem with additional local conditions. This will be used later to construct non-abelian and weakly ramified extensions $L|\mathbb{Q}_p$ of degree l^2p, where l, p are odd primes satisfying $l \mid (p-1)$. The main source for the material presented in this section is [Neu73].

(4.1) Definition. Let $L|K$ be a finite Galois extension with Galois group $G_{L|K}$ and denote by Γ the absolute Galois group of K. An ***embedding problem*** $\mathscr{E}$ associated to $L|K$ consists of a diagram

$$\begin{array}{ccccccccc} & & & & & & \Gamma & & \\ & & & & & & \downarrow \varphi & & \\ 1 & \longrightarrow & A & \longrightarrow & B & \xrightarrow{j} & G_{L|K} & \longrightarrow & 1, \end{array}$$

where A, B are finite groups, the sequence at the bottom is exact, and $\varphi\colon \Gamma \to G_{L|K}$ is the natural homomorphism defined by restriction. The group A is sometimes also called the ***kernel*** of $\mathscr{E}$. A ***(proper) solution*** of this embedding problem is a (surjective) continuous homomorphism $\psi\colon \Gamma \to B$ such that $j \circ \Psi = \varphi$, i. e. the diagram

$$\begin{array}{ccccccccc} & & & & & & \Gamma & & \\ & & & & & \swarrow^{\psi} & \downarrow \varphi & & \\ 1 & \longrightarrow & A & \longrightarrow & B & \xrightarrow{j} & G_{L|K} & \longrightarrow & 1, \end{array}$$

commutes.

(4.2) Remark. Let $\mathscr{E}$ be an embedding problem given by

$$\begin{array}{ccccccccc} & & & & & & \Gamma & & \\ & & & & & & \downarrow \varphi & & \\ 1 & \longrightarrow & A & \longrightarrow & B & \xrightarrow{j} & G_{L|K} & \longrightarrow & 1, \end{array}$$

then $\mathscr{E}$ has a proper solution if and only if there is an extension field L' of L such that $L'|K$ is Galois and $G_{L'|K} \cong B$. Indeed, if $\psi\colon \Gamma \to B$ is a proper solution to $\mathscr{E}$ and we set L' to be the fixed field $\overline{K}^{\ker\psi}$ of $\ker\psi$, then the extension $L'|K$ is Galois with Galois group isomorphic to B. Moreover, $j \circ \psi = \varphi$, whence $\ker\psi \subseteq \ker\varphi = G_{\overline{K}|L}$. As a consequence, L is contained in L'.

Since we are mainly interested in the field theoretic interpretation as given in Remark (4.2), it is sufficient for our purposes to use the following, somehow slightly weaker, notion of a solution to an embedding problem, which does however not affect the field obtained by the procedure described in Remark (4.2).

(4.3) Definition. Let $\mathscr{E}$ be an embedding problem and $\psi, \psi' \colon \Gamma \to B$ two solutions of $\mathscr{E}$. We say that ψ and ψ' are ***equivalent***, if there is $a \in A$ such that

$$\psi(\sigma) = a\psi'(\sigma)a^{-1} \quad \text{for all } \sigma \in \Gamma.$$

Every equivalence class $[\psi]$ is now called a ***solution*** to $\mathscr{E}$ and the set of all such solutions is called the ***space of solutions***, denoted by $\mathscr{L}(\mathscr{E})$. If in addition ψ is proper, the equivalence class $[\psi]$ is also called ***proper***.

If $\mathscr{E}$ is an embedding problem given by

$$\begin{array}{ccccccccc} & & & & & & \Gamma & & \\ & & & & & & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & A & \longrightarrow & B & \xrightarrow{j} & C & \longrightarrow & 1 \end{array}$$

with abelian kernel A, then A is equipped with a C-module structure given by

$$C \times A \to A, \quad (c, a) \mapsto j^{-1}(c) \cdot a \cdot j(c).$$

One immediately convinces oneself that this definition does not depend on the choice of preimage $j^{-1}(c)$. In particular, A is a Γ-module.

(4.4) Lemma. Let $\mathscr{E}$ be a solvable embedding problem with abelian kernel A. Then

$$H^1(\Gamma, A) \times \mathscr{L}(\mathscr{E}) \to H^1(\Gamma, A), \quad ([\xi], \psi) \mapsto {}^{\xi}\psi,$$

where ${}^{\xi}\psi(\sigma) = \xi(\sigma) \cdot \psi(\sigma)$ for all $\sigma \in \Gamma$, is a well-defined map defining a simply transitive group action of $H^1(\Gamma, A)$ on $\mathscr{L}(\mathscr{E})$.

Proof. Let $[\xi] \in H^1(\Gamma, A)$ and $\psi \in \mathscr{L}(\mathscr{E})$, then also ${}^{\xi}\psi \in \mathscr{L}(\mathscr{E})$, since ξ maps into the kernel of j. If ζ is a cocycle representing $[\xi]$, there is $a \in A$ such that $\xi(\sigma) \cdot \zeta^{-1}(\sigma) = (\sigma a) \cdot (a^{-1})$ for all $\sigma \in \Gamma$ and the calculation

$$\begin{aligned} {}^{\zeta}\psi(\sigma) &= \zeta(\sigma)\psi(\sigma) = (a \cdot (\sigma a)^{-1})\xi(\sigma)\psi(\sigma) = (a \cdot \psi(\sigma)a^{-1}\psi(\sigma^{-1}))\xi(\sigma)\psi(\sigma) = \\ &= a\xi(\sigma) \cdot (\psi(\sigma)a^{-1}\psi(\sigma^{-1}\psi(\sigma)) = a\big(\xi(\sigma)\psi(\sigma)\big)a^{-1}, \end{aligned}$$

where we used $\sigma a = \psi(\sigma)a\psi(\sigma^{-1}) \in A$, shows that ${}^{\xi}\psi$ and ${}^{\zeta}\psi$ are equivalent solutions. It is immediate that this action also respects the equivalence relation on $\mathscr{L}(\mathscr{E})$.

Now let $\psi' \in \mathscr{L}(\mathscr{E})$ an arbitrary solution, then

$$\xi\colon \Gamma \to A, \quad \sigma \mapsto \psi'(\sigma) \cdot \psi(\sigma^{-1})$$

defines a cocycle satisfying ${}^{\xi}\psi = \psi'$. If ψ and ψ' are equivalent, there is $a \in A$ such that

$$\xi(\sigma) = \psi'(\sigma) \cdot \left(a\psi'(\sigma^{-1})a^{-1}\right) = (\sigma a)a^{-1},$$

i. e. ξ is a coboundary. Conversely, if ξ is a coboundary, there is $a \in A$ such that

$$\begin{aligned}\psi'(\sigma) = \xi(\sigma)\psi(\sigma) = (\sigma a)a^{-1}\psi(\sigma) = \left(\psi(\sigma)a\psi(\sigma^{-1})\right)a^{-1}\psi(\sigma) = \\ = a^{-1}\left(\psi(\sigma)a\psi(\sigma^{-1})\right)\psi(\sigma) = a^{-1}\psi(\sigma)a.\end{aligned}$$

As a consequence, the action defined above is indeed simply transitive. □

Let $L|K$ be a finite Galois extension of number fields and $\mathscr{E}$ an embedding problem associated to $L|K$ using the notations of above. Let moreover $\mathfrak{P}$ be a prime of L lying over a prime $\mathfrak{p}$ of K and choose an extension $\overline{\mathfrak{p}}$ of $\mathfrak{p}$ to $\overline{K}$, then we can regard the decomposition group $\Gamma_{\mathfrak{p}}$ of $\overline{\mathfrak{p}}$ as absolute Galois group of the completion $K_{\mathfrak{p}}$ and therefore obtain a new local embedding problem $\mathscr{E}_{\mathfrak{p}}$ given by

$$\begin{array}{ccccccccc} & & & & & & \Gamma_{\mathfrak{p}} & & \\ & & & & & & \downarrow{\scriptstyle \varphi'} & & \\ 1 & \longrightarrow & A & \longrightarrow & B' & \xrightarrow{j} & G_{L_{\mathfrak{P}}|K_{\mathfrak{p}}} & \longrightarrow & 1, \end{array}$$

where φ' is again given by restriction and $B' = j^{-1}(G_{L_{\mathfrak{P}}|K_{\mathfrak{p}}})$.

If ψ is a solution of $\mathscr{E}$, then its restriction to $\Gamma_{\mathfrak{p}}$ defines a solution of $\mathscr{E}_{\mathfrak{p}}$. We therefore have a canonical restriction map

$$\mathscr{L}(\mathscr{E}) \to \mathscr{L}(\mathscr{E}_{\mathfrak{p}})$$

in the case of $\mathscr{L}(\mathscr{E}) \neq \varnothing$. Clearly, if L' is the field defined by a solution $[\psi] \in \mathscr{L}(\mathscr{E})$ in the sense of Remark (4.2), then the completion of L' at the prime $\overline{\mathfrak{p}} \cap L'$ is determined by the restriction $[\psi_{\Gamma_{\mathfrak{p}}}] \in \mathscr{L}(\mathscr{E}_{\mathfrak{p}})$. We can therefore control the local behaviour of the extension $L'|K$ by supplementing the embedding problem $\mathscr{E}$ with additional conditions in terms of the local embedding problem $\mathscr{E}_{\mathfrak{p}}$. Now the map

$$\lambda\colon \mathscr{L}(E) \to \prod_{\mathfrak{p}} \mathscr{L}(\mathscr{E}_{\mathfrak{p}}), \quad [\psi] \mapsto [\psi_{\Gamma_{\mathfrak{p}}}]$$

is of central interest and we first strive for substituting its codomain by a slightly smaller group.

Let $I_\mathfrak{p} \subseteq \Gamma_\mathfrak{p}$ be the inertia subgroup of $\overline{\mathfrak{p}}$. For any Γ-module A and $q \in \mathbb{Z}$ we put $H^q(K_\mathfrak{p}, A) = H^q(\Gamma_\mathfrak{p}, A)$ and

$$H^q_{\mathrm{nr}}(K_\mathfrak{p}, A) = \operatorname{im}\left\{H^q(\Gamma_\mathfrak{p}/I_\mathfrak{p}, A) \xrightarrow{\mathrm{Inf}} H^q(K_\mathfrak{p}, A)\right\}.$$

(4.5) Definition. Let K be a number field and $\mathscr{E}$ an embedding problem associated to K. We define the ***restricted product*** to be

$$\prod_\mathfrak{p} \mathscr{L}(\mathscr{E}_\mathfrak{p}) = \left\{([\psi_\mathfrak{p}])_\mathfrak{p} \in \prod_\mathfrak{p} \mathscr{L}(\mathscr{E}_\mathfrak{p}) \mid I_\mathfrak{p} \subseteq \ker\psi_\mathfrak{p} \text{ for almost all } \mathfrak{p}\right\},$$
$$\prod_\mathfrak{p} H^q(K_\mathfrak{p}, A) = \left\{(\xi_\mathfrak{p})_\mathfrak{p} \in \prod_\mathfrak{p} H^q(K_\mathfrak{p}, A) \mid \xi_\mathfrak{p} \in H^q_{\mathrm{nr}}(K_\mathfrak{p}, A) \text{ for almost all } \mathfrak{p}\right\}.$$

(4.6) Lemma. Let K be a number field and $\mathscr{E}$ an embedding problem associated to K.

(a) The image of $\lambda\colon \mathscr{L}(E) \to \prod_\mathfrak{p} \mathscr{L}(\mathscr{E}_\mathfrak{p})$ is contained in $\coprod_\mathfrak{p}\mathscr{L}(\mathscr{E}_\mathfrak{p})$,

(b) the image of $\rho\colon H^1(K, A) \to \prod_\mathfrak{p} H^1(K_\mathfrak{p}, A)$ is contained in $\coprod_\mathfrak{p} H^1(K_\mathfrak{p}, A)$.

Proof. (a): Let $[\psi] \in \mathscr{L}(\mathscr{E})$, then only finitely many primes ramify in the finite extension $\overline{K}^{\ker\psi}|K$. Hence $\overline{K}^{\ker\psi} \subseteq \overline{K}^{I_\mathfrak{p}}$ for almost all $\mathfrak{p}$, which is equivalent to $I_\mathfrak{p} \subseteq \ker\psi$. In particular, $I_\mathfrak{p} \subseteq \ker\psi_\mathfrak{p}$ for almost every $\mathfrak{p}$, where $\psi_\mathfrak{p}$ denotes the restriction of ψ to $\Gamma_\mathfrak{p}$.

(b): Let ξ represent a cohomology class in $H^1(K, A)$. Since $\xi\colon \Gamma \to A$ is a continuous map, the subgroup $\ker\xi \subseteq \Gamma$ is closed and of finite index, so $\overline{K}^{\ker\xi}|K$ is a finite extension and, like in (a), we must have $I_\mathfrak{p} \subseteq \ker\xi$ for almost all $\mathfrak{p}$. That is, $\xi_\mathfrak{p}$ is in the kernel of

$$\mathrm{Res}\colon H^1(K_\mathfrak{p}, A) \to H^1(I_\mathfrak{p}, A)$$

for nearly all $\mathfrak{p}$. Thus $\xi_\mathfrak{p} \in H^1_{\mathrm{nr}}(K_\mathfrak{p}, A)$ for all $\mathfrak{p}$ by exactness of the Inflation-Restriction sequence. □

(4.7) Definition. Let $M|K$ be a finite Galois extension of fields, $\mathscr{E}$ an embedding problem associated to $M|K$ and S a finite set of primes of K. A set of the form

$$L = \prod_{\mathfrak{p}\in S}\{[\psi_\mathfrak{p}]\} \times \coprod_{\mathfrak{p}\notin S} \mathscr{L}(\mathscr{E}_\mathfrak{p}) \quad \subseteq \quad \prod_\mathfrak{p} \mathscr{L}(\mathscr{E}_\mathfrak{p}),$$

where each $[\psi_\mathfrak{p}]$ is a solution of the local embedding problem $\mathscr{E}_\mathfrak{p}$, is called a ***local requirement*** and abbreviated to $L = ([\psi_\mathfrak{p}])_{\mathfrak{p}\in S}$. Accordingly, $(\mathscr{E}, L)$ is called an ***embedding problem with local requirement*** and $[\psi] \in \mathscr{L}(\mathscr{E})$ is called a solution

of $(\mathscr{E}, L)$, if

$$\lambda\colon \mathscr{L}(\mathscr{E}) \to \prod_{\mathfrak{p}} \mathscr{L}(\mathscr{E}_{\mathfrak{p}})$$

maps $[\psi]$ into L.

We now want to extend the group action introduced in Lemma (4.4) to restricted products of solution sets and cohomology groups, respectively.

(4.8) Lemma. Let K be a number field, $\mathscr{E}$ an embedding problem with abelian kernel A associated to K, and $L = ([\psi_{\mathfrak{p}}])_{\mathfrak{p}\in S}$ a local requirement for $\mathscr{E}$. The map

$$\prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}}, A) \times \prod_{\mathfrak{p}} \mathscr{L}(\mathscr{E}_{\mathfrak{p}}) \to \prod_{\mathfrak{p}} \mathscr{L}(\mathscr{E}_{\mathfrak{P}}), \quad ((\xi_{\mathfrak{p}})_{\mathfrak{p}},\ ([\phi_{\mathfrak{p}}])_{\mathfrak{p}}) \mapsto ([{}^{\xi_{\mathfrak{p}}}\phi_{\mathfrak{p}}])_{\mathfrak{p}}$$

gives a well-defined and simply-transitive group action.

Proof. Take $([\phi_{\mathfrak{p}}])_{\mathfrak{p}} \in \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}}, A)$ and $(\xi_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}} \mathscr{L}(\mathscr{E}_{\mathfrak{p}})$. By definition, the inertia group $I_{\mathfrak{p}}$ is contained in $\ker \xi_{\mathfrak{p}}$ and $\ker \phi_{\mathfrak{p}}$ for almost every $\mathfrak{p}$, hence $I_{\mathfrak{p}} \subseteq \ker {}^{\xi_{\mathfrak{p}}}\phi_{\mathfrak{p}}$ for almost every $\mathfrak{p}$. If $([\phi'_{\mathfrak{p}}])_{\mathfrak{p}} \in \prod_{\mathfrak{p}} \mathscr{L}(\mathscr{E}_{\mathfrak{p}})$ is another element, then there is a unique $\xi_{\mathfrak{p}} \in \mathscr{L}(\mathscr{E}_{\mathfrak{p}})$ such that ${}^{\xi_{\mathfrak{p}}}\phi_{\mathfrak{p}} = \phi'_{\mathfrak{p}}$ by Lemma (4.4). It therefore suffices to show that $(\xi_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}} \mathscr{L}(\mathscr{E}_{\mathfrak{p}})$. However,

$$\xi_{\mathfrak{p}} = \phi'_{\mathfrak{p}} \cdot \phi^{-1}$$

for every $\mathfrak{p}$, so the assertion holds. □

If $L = ([\psi_{\mathfrak{p}}])_{\mathfrak{p}\in S}$ is a local requirement, we consider the subgroup

$$\Lambda = \prod_{\mathfrak{p}\in S} \{0_{\mathfrak{p}}\} \times \prod_{\mathfrak{p}\notin S} H^1(\Gamma_{\mathfrak{p}}, A),$$

which is maximal with respect to $\Lambda \cdot L \subseteq L$, and the homomorphisms

$$\pi_S\colon \prod_{\mathfrak{p}} H^1(\Gamma_{\mathfrak{p}}, A) \to \prod_{\mathfrak{p}\in S} H^1(\Gamma_{\mathfrak{p}}, A) \quad \text{as well as} \quad \rho_S = \pi_S \circ \rho\colon H^1(\Gamma, A) \to \prod_{\mathfrak{p}\in S} H^1(\Gamma_{\mathfrak{p}}, A).$$

Moreover, we set $\Delta(\Gamma, A, S) = \operatorname{coker} \rho_S$.

(4.9) Lemma. Let $(\mathscr{E}, L)$ be a solvable embedding problem with local requirement and abelian kernel A.

(a) Let $l \in L$ and $[\psi] \in \mathscr{L}(\mathscr{E})$, then

$$\eta([\psi]) = \pi_S(\lambda([\psi]) \cdot l^{-1}) \quad \in \quad \prod_{\mathfrak{p}\in S} H^1(\Gamma_{\mathfrak{p}}, A)$$

does not depend on the choice of l and vanishes if and only if $\lambda([\psi]) \in L$,

(b) The image of $\eta([\psi])$ in $\Delta(\Gamma, A, S)$ does not depend on $[\psi]$ and vanishes if and only if $\lambda^{-1}(L) \neq \varnothing$. We denote it by $\eta(L)$.

Proof. (a): Let $k \in L$ be another element and $x = (x_\mathfrak{p})_\mathfrak{p} \in \Lambda$ be such that $l = {}^x k$. We now have

$$\pi_S(\lambda([\psi])l^{-1}) = \pi_S\left(\lambda([\psi]) \cdot^x (k^{-1})\right) = \pi_S\left(\lambda([\psi]) \cdot k^{-1}\right),$$

because $x_\mathfrak{p} = 0$ for all $\mathfrak{p} \in S$ by definition of Λ. In particular, if $\lambda([\psi])$ lies in L, then $\eta([\psi])$ vanishes. Conversely, if $\eta([\psi]) = 0$, then

$$\left(\lambda([\psi]) \cdot l^{-1}\right)_\mathfrak{p} = 0 \quad \text{for all} \quad \mathfrak{p} \in S.$$

This means $\lambda([\psi]) \cdot l^{-1} \in L$, hence $\lambda([\psi]) \in L$.

(b): Let $[\phi] \in \mathscr{L}(\mathscr{E})$ be another solution, then there is $\xi \in H^1(\Gamma, A)$ such that ${}^\xi\phi = \psi$ and a short calculation yields

$$\begin{aligned}\eta([\psi]) &= \pi_S\left(\lambda([\psi]) \cdot l^{-1}\right) = \pi_S\left(\lambda([{}^\xi\phi]) \cdot l^{-1}\right) = \pi_S\left({}^{\rho(\xi)}\lambda([\phi]) \cdot l^{-1}\right) = \\ &= \pi_S\left(\rho(\xi) \cdot \lambda([\phi]) \cdot l^{-1}\right) = \rho_S(\xi) \cdot \eta([\phi]).\end{aligned}$$

Thus, $\eta([\phi])$ and $\eta([\psi])$ are equal in $\Delta(\Gamma, A, S)$. Now $\eta(L)$ vanishes if and only if there is $[\psi] \in \mathscr{L}(\mathscr{E})$ such that $\eta([\psi])$ vanishes, which is equivalent to $[\psi] \in \lambda^{-1}(L)$ by (a). □

Our objective is henceforth to find suitable conditions that ensure $\Delta(\Gamma, A, S) = 0$. In order to do so, we will need Tate-Poitou duality.

(4.10) Theorem (Global Duality Theorem)**.** Let A be a finite Γ-module and $A' = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ its dual module. There is a canonical non-degenerate pairing

$$H^q(K_\mathfrak{p}, A) \times H^{2-q}(K_\mathfrak{p}, A') \to \mathbb{Q}/\mathbb{Z}, \quad 0 \le q \le 2$$

of finite groups such that the images of $H^q(K, A)$ and $H^q(K, A')$ are orthogonal complements of each other with respect to the pairing

$$\begin{array}{ccccc} H^q(K,A) & & & H^{2-q}(K,A') & \\ \downarrow & & & \downarrow & \\ \prod_\mathfrak{p} H^q(K_\mathfrak{p}, A) & \times & \prod_\mathfrak{p} H^{2-q}(K_\mathfrak{p}, A') & \longrightarrow \mathbb{Q}/\mathbb{Z}, & 0 \le q \le 2, \end{array}$$

Proof. The formulation relies on [Neu73, Satz (4.2)], a proof can be found in [Poi67, Exp. 15]. □

Using the maps ρ and ρ_S defined for a local requirement $L = ([\psi_\mathfrak{p}])_\mathfrak{p}$ above, we set

$$\nabla(\Gamma, A, S) = \ker \rho_S / \ker \rho.$$

(4.11) Lemma. Let A be a finite Γ-module, $A' = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ its dual module, and $\Lambda^\perp$ the orthogonal complement of Λ in $\prod_\mathfrak{p} H^1(K_\mathfrak{p}, A')$. There is a canonical non-degenerate pairing

$$\Delta(\Gamma, A, S) \times \nabla(\Gamma, A', S') \to \mathbb{Q}/\mathbb{Z},$$

where S' denotes the set of all primes of K not in S.

Proof. According to Theorem (4.10), the images of

$$\rho\colon H^1(K, A) \to \prod_\mathfrak{p} H^1(K_\mathfrak{p}, A) \quad \text{and} \quad \rho'\colon H^1(K, A') \to \prod_\mathfrak{p} H^1(K_\mathfrak{p}, A')$$

are orthogonal complements of each other with respect to the pairing

$$\prod_\mathfrak{p} H^1(K_\mathfrak{p}, A) \times \prod_\mathfrak{p} H^1(K_\mathfrak{p}, A') \to \mathbb{Q}/\mathbb{Z}.$$

Therefore we have

$$\begin{aligned} (\operatorname{im}\rho \cdot \Lambda)^\perp &= (\operatorname{im}\rho)^\perp \cap \Lambda^\perp = \operatorname{im}\rho' \cap \Lambda^\perp, \\ \operatorname{im}\rho \cdot \Lambda &= (\operatorname{im}\rho \cdot \Lambda)^{\perp\perp} = \left(\operatorname{im}\rho' \cap \Lambda^\perp\right)^\perp, \end{aligned}$$

whence we obtain a non-degenerate pairing

$$\prod_\mathfrak{p} H^1(K_\mathfrak{p}, A) / \operatorname{im}\rho \cdot \Lambda \times \left(\operatorname{im}\rho' \cap \Lambda^\perp\right) \to \mathbb{Q}/\mathbb{Z}.$$

Note that

$$\begin{aligned} \Delta(\Gamma, A, S) = \prod_{\mathfrak{p}\in S} H^1(K_\mathfrak{p}, A) / \operatorname{im}\rho_S &= \left(\prod_\mathfrak{p} H^1(K_\mathfrak{p}, A)/\Lambda\right) / (\operatorname{im}\rho \cdot \Lambda/\Lambda) = \\ &= \prod_\mathfrak{p} H^1(K_\mathfrak{p}, A) / \operatorname{im}\rho \cdot \Lambda \end{aligned}$$

and that the composite

$$\ker \rho'_{S'} \to H^1(K, A') \xrightarrow{\rho'} \operatorname{im}\rho' \cap \Lambda^\perp$$

is surjective, hence induces an isomorphism

$$\nabla(\Gamma, A', S') = \ker \rho'_{S'} / \ker \rho' \cong \operatorname{im} \rho \cap \Lambda^{\perp}.$$

□

(4.12) Definition. Let G be a finite group and A a G-module. We set

$$X(G, A) = \ker \left\{ H^1(G, A) \to \prod_{\sigma \in G} H^1(\langle \sigma \rangle,\ A) \right\}.$$

Apparently, if G is cyclic, then $X(G, A) = 0$ for every G-module A.

Let K be a number field and Γ, as before, its absolute Galois group. If A is a finite Γ-module and $A' = \operatorname{Hom}(A, \mathbb{Q}/\mathbb{Z})$ its dual module, we consider

$$\operatorname{Stab}_\Gamma(A') = \{\sigma \in \Gamma \mid \forall a \in A' : a^\sigma = a\} = \ker\{\Gamma \to \operatorname{Aut}(A')\}$$

and define $K(A')$ to be the fixed field $\overline{K}^{\operatorname{Stab}_\Gamma(A')}$. Let G be the Galois group of $K(A')|K$ and take a prime $\mathfrak{p}$, say, of $K(A')$. Denote by $G_\mathfrak{p}$ the respective decomposition group and define the homomorphisms

$$\bar{\rho}' \colon H^1(G, A') \to \prod_{\mathfrak{p}} H^1(G_\mathfrak{p}, A') \quad \text{as well as} \quad \bar{\rho}'_S \colon H^1(G, A) \to \prod_{\mathfrak{p} \notin S} H^1(G_\mathfrak{p}, A'),$$

where S is meant to be a finite set of primes.

(4.13) Lemma. Using the notation just introduced, the equality

$$\nabla(\Gamma, A', S') \cong \ker \bar{\rho}'_S / \ker \bar{\rho}'$$

holds and we have a canonical embedding

$$\nabla(\Gamma, A', S') \to \prod_{\mathfrak{p} \in S} X(G_\mathfrak{p}, A').$$

Proof. Recall that we defined $\nabla(\Gamma, A', S')$ to be $\ker \rho'_S / \ker \rho$, where the appearing maps are

$$\rho' \colon H^1(K, A') \to \prod_{\mathfrak{p}} H^1(K_\mathfrak{p}, A') \quad \text{and} \quad \rho'_S \colon H^1(K, A') \to \prod_{\mathfrak{p} \notin S} H^1(K_\mathfrak{p}, A).$$

Let T be the set of all primes of $k(A')$ lying over any prime contained in S, then we get a commutative diagram of the following sort:

$$\begin{array}{ccccccc}
1 & \longrightarrow & \ker\bar{\rho}'_S & \longrightarrow & \ker\rho'_S & \longrightarrow & \ker\rho'_T \\
 & & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & H^1(G, A') & \longrightarrow & H^1(K, A') & \longrightarrow & H^1(K(A'), A') \\
 & & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & \prod_{\mathfrak{p}\notin S} H^1(G_\mathfrak{p}, A') & \longrightarrow & \prod_{\mathfrak{p}\notin S} H^1(K_\mathfrak{p}, A') & \longrightarrow & \prod_{\mathfrak{P}\notin T} H^1(K(A')_\mathfrak{P}, A')
\end{array}$$

$K(A')$ is a trivial Γ'-module, where Γ' denotes the absolute Galois group of $K(A')$, so we have

$$H^1(K(A'), A') = \mathrm{Hom}(\Gamma', A') \quad \text{and} \quad H^1(K(A')_\mathfrak{P}, A') = \mathrm{Hom}(\Gamma'_\mathfrak{P}, A').$$

Pick $\varphi \in \ker\rho'_T$, then $\Gamma'_\mathfrak{P} \subseteq \ker\varphi$ for all $\mathfrak{P} \notin T$. Let N be the fixed field of $\ker\varphi$, then we have that the decomposition group $(G_{N|K(A')})_\mathfrak{q}$ vanishes for every prime $\mathfrak{q}$ lying over some prime not in T. Hence almost all primes in $N|K(A')$ are completely split and we must have $N = K(A')$ by the Frobenius Density Theorem [Neu92, Korollar VII. (13.7)]. In other words $\varphi = 0$, i. e. $\ker\rho'_T = 0$.

From the diagram we therefore get $\ker\bar{\rho}'_S \cong \ker\rho'_S$ and, by taking $S = \varnothing$, also $\ker\bar{\rho}' \cong \ker\rho'$. Thus,

$$\nabla(\Gamma, A', S') = \ker\rho'_S/\ker\rho' \cong \ker\bar{\rho}'_S/\ker\bar{\rho}'.$$

Considering the exact sequence

$$1 \longrightarrow \ker\bar{\rho}' \longrightarrow \ker\bar{\rho}'_S \longrightarrow \textstyle\prod_{\mathfrak{p}\in S} H^1(G_\mathfrak{p}, A')$$

it suffices to show that $\ker\bar{\rho}'_S$ is mapped into $\prod_{\mathfrak{p}\in S} X(G_\mathfrak{p}, A')$, which is equivalent to showing that the composite

$$\ker\bar{\rho}'_S \longrightarrow \prod_{\mathfrak{p}\in S} H^1(G_\mathfrak{p}, A') \longrightarrow \prod_{\mathfrak{p}\in S}\prod_{\sigma\in G_\mathfrak{p}} H^1(\langle\sigma\rangle,\ A') \qquad (*)$$

is the zero map. For every cyclic subgroup $\langle\sigma\rangle$ of G there are infinitely many primes not in S such that $\langle\sigma\rangle$ is the respective decomposition group by Cebotarev's Theorem, hence

$$\ker\bar{\rho}'_S \to H^1(\langle\sigma\rangle, A')$$

is the zero map by definition of $\ker\rho'_S$ for every such cyclic subgroup $\langle\sigma\rangle$. In particular, $(*)$ is the zero map. □

All that remains to do in order to obtain the desired result about solvability of embedding problems with a local requirement is reaping the harvest.

(4.14) Theorem. Let K be a number field and $(\mathscr{E}, L)$ an embedding problem with local requirement given by

$$\begin{array}{ccccccccc} & & & & & & \Gamma & & \\ & & & & & & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & A & \longrightarrow & B & \xrightarrow{j} & C & \longrightarrow & 1. \end{array}$$

If A is cyclic of odd order and the exact sequence at the bottom splits, there is a proper solution to $(\mathscr{E}, L)$.

Proof. We have $\mathscr{L}(\mathscr{E}) \neq \varnothing$, because by assumption the exact sequence at the bottom of $\mathscr{E}$ splits. To account for existence of a solution to $(\mathscr{E}, L)$, by Lemma (4.9)(b) it suffices to show that $\Delta(\Gamma, A, S)$ vanishes. By Lemma (4.11) the latter is true if $\nabla(\Gamma, A', S)$ vanishes, where $A' = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$. If A' is cyclic of odd order, then $\mathrm{Aut}(A')$ is also cyclic. The same therefore holds for

$$G = G_{K(A')|K} = \Gamma\!\diagup\!\mathrm{Stab}_\Gamma(A') \cong \mathrm{im}\left\{\Gamma \to \mathrm{Aut}(A')\right\}.$$

Now Lemma (4.13) provides us with an embedding

$$\nabla(\Gamma, A', S) \hookrightarrow \prod_{\mathfrak{p} \in S} X(G_\mathfrak{p}, A') = 0,$$

so the existence of a solution to $(\mathscr{E}, L)$ follows. It remains to show there even exists a surjective such solution. Choose a prime $\mathfrak{q} \notin S$ that splits completely in $L|K$ and consider the respective local embedding problem

$$\begin{array}{ccccccccc} & & & & & & \Gamma_\mathfrak{q} & & \\ & & & & & & \downarrow & & \\ 1 & \longrightarrow & A & \longrightarrow & A & \xrightarrow{j} & 1 & \longrightarrow & 1. \end{array}$$

As A is cyclic of odd order, the unramified extension of degree $|A|$ over $K_\mathfrak{q}$ defines a solution $\psi_\mathfrak{q}$ to this embedding problem. Let $S^\# = S \cup \{q\}$ and $L^\#$ be the new local requirement obtained by amending $\psi_\mathfrak{q}$ to L, then the previous discussion also applies to $(\mathscr{E}, L^\#)$. Now a solution to $(\mathscr{E}, L^\#)$ is automatically surjective. □

(4.15) Remark. There is actually a whole list of different possible conditions one could impose on A other than being cyclic of odd order and such that Theorem (4.14) holds, see [Neu73, Thm. (6.6)].

4.2 Some results from global class field theory

In the following sections we will need statements from global class field theory analogous to those from local class field theory from the previous chapter. We assume the reader is familiar with the core material of global class field theory as, for example, is contained in [Neu11, Ch. III] and will make repeated use of it. Let us fix some notation first.

For a number field K and a modulus $\mathfrak{m}$ of K we denote by

$$\begin{aligned} \mathrm{cl}_K(\mathfrak{m}) &= J_K(\mathfrak{m})/P_K(\mathfrak{m}) && \text{the ray class group mod } \mathfrak{m} \text{ of } K, \\ C_K(\mathfrak{m}) &= I_K(\mathfrak{m}) \cdot K^\times/K^\times && \text{the idèle ray class group mod } \mathfrak{m} \text{ of } K, \end{aligned}$$

where in both cases $\mathfrak{m}$ is dropped from the notation if $\mathfrak{m} = (1)$.

(4.16) Lemma. Let $M|K$ be a finite Galois extension of number fields and $L|M$ a finite abelian extension. Let $\mathfrak{m}$ be a modulus of definition for $L|M$ fixed by $G_{M|K}$ and $H = N_{L|M}(J_L(\mathfrak{m})) \cdot P_M(\mathfrak{m}) \subseteq J_M(\mathfrak{m})$ the subgroup corresponding to L. Then

(a) the extension $L|K$ is Galois if and only if H is stable by the action of $G_{M|K}$,

(b) if (a) holds, then $G_{L|M}$ is contained in the centre of $G_{L|K}$ if and only if $G_{M|K}$ acts trivially on $J_M(\mathfrak{m})/H$.

Proof. (a): Let $\sigma \in \mathrm{Hom}_K(L, \mathbb{C})$ and $\mathfrak{a} \in J_L(\mathfrak{m})$, then $\sigma\mathfrak{a} \in J_{\sigma L}(\mathfrak{m})$ and

$$\sigma N_{L|M}(\mathfrak{a}) = N_{\sigma L|M}(\sigma\mathfrak{a}).$$

Note that $\sigma\mathfrak{a} \in J_L(\mathfrak{m})$ and $\sigma P_M(\mathfrak{m}) \subseteq P_M(\mathfrak{m})$ because $\sigma\mathfrak{m} = \mathfrak{m}$. Hence

$$\sigma H \subseteq N_{\sigma L|M}(J_{\sigma L}(\mathfrak{m})) \cdot P_M(\mathfrak{m}).$$

Since $G_{\sigma L|M} \cong G_{L|M}$, these two groups have the same index in $J_M(\mathfrak{m})$ by class field theory, so they must already be equal. As σ was chosen arbitrary, we have

$$L|K \text{ Galois} \quad \Leftrightarrow \quad \sigma L = L \quad \Leftrightarrow \quad \sigma H = H$$

by class field theory.

(b): $G_{L|M}$ is contained in the centre of $G_{L|K}$ if and only if $G_{L|M}$ is fixed by conjugation. Since $G_{L|M}$ is an abelian extension, this action factors through $G_{M|K}$, so it suffices to show that

$$(\sigma\mathfrak{p},\ L|M) = \sigma(\mathfrak{p},\ L|M)\sigma^{-1}$$

for every $\sigma \in G_{M|K} = G_{L|K}/G_{L|M}$ and every prime $\mathfrak{p} \in J_M(\mathfrak{m})$. However,

$$\sigma(\mathfrak{p},\ L|M)\sigma^{-1} = \sigma\varphi_{\mathfrak{p}}\sigma^{-1} = \varphi_{\sigma\mathfrak{p}} = (\sigma\mathfrak{p},\ L|M)$$

where $\varphi_{\mathfrak{p}}$ and $\varphi_{\sigma\mathfrak{p}}$ denote the Frobenius at $\mathfrak{p}$ and $\sigma\mathfrak{p}$, respectively. □

The same, entirely group-theoretic, considerations as in the local case bestow the following useful Corollary on us.

(4.17) Corollary. Let $M|K$ be a cyclic extension of number fields and $L|M$ a finite abelian extension. Let $\mathfrak{m}$ be a modulus of definition for $L|M$ fixed by $G_{M|K}$ and $H \subseteq J_M(\mathfrak{m})$ the subgroup corresponding to L. Then $L|K$ is an abelian extension if and only if

(a) $G_{M|K} \cdot H \subseteq H$ and

(b) $G_{M|K}$ acts trivially on $J_M(\mathfrak{m})/H$.

The next ingredient we are going to need is the interrelation of the global (ideal-theoretic) Artin symbol and the local norm residue symbol. For that purpose recall that the conductor $\mathfrak{f}$ of an abelian extension $L|K$ can be written as

$$\mathfrak{f} = \prod_{\mathfrak{p}} \mathfrak{f}_{\mathfrak{p}},$$

where for every prime $\mathfrak{p}$ the local conductor $\mathfrak{f}_{\mathfrak{p}}$ is defined as the least power $\mathfrak{p}^n$ such that the group of principal units $U_{K_{\mathfrak{p}}}^{(n)}$ is contained in the local norm group $N_{L_{\mathfrak{P}}|K_{\mathfrak{p}}}(L_{\mathfrak{P}}^{\times})$.

(4.18) Lemma (cf. [Ble03, p. 75])**.** Let $L|K$ a finite abelian extension of number fields, $\mathfrak{p}$ a prime of K and $\mathfrak{P} \mid \mathfrak{p}$ a prime of L. Let $\mathfrak{f} = \prod_{k=0}^{r} \mathfrak{p}_k^{s_k}$ be the conductor of $L|K$ and assume $\mathfrak{p}_0 = \mathfrak{p}$. Let further $\pi \in \mathcal{O}_K$ be an element such that

$$v_{\mathfrak{p}_j}(\pi) = \begin{cases} 1 & \text{if } j = 0, \\ 0 & \text{if } 0 < j \leq r \end{cases}$$

and $\alpha \in \mathcal{O}_K \setminus \{0\}$. If $\xi \in \mathcal{O}_K$ is a solution to

$$\begin{aligned} \xi &\equiv \pi^e \mod \mathfrak{p}^{s_j} \quad \text{for } 0 < j \leq r, \\ \xi &\equiv \frac{\pi^e}{\alpha} \mod \mathfrak{p}_0^{s_0}, \end{aligned}$$

where $e = v_{\mathfrak{p}}(\alpha)$, then

$$(\alpha, L_{\mathfrak{P}}|K_{\mathfrak{p}}) = (\xi \prod_{\substack{\mathfrak{q}|\pi \\ \mathfrak{q}\neq\mathfrak{p}}} \mathfrak{q}^{-ev_{\mathfrak{q}}(\pi)},\ L|K).$$

Proof. Using the embedding

$$n_{\mathfrak{p}} \colon K_{\mathfrak{p}}^{\times} \to I_K, \quad x \mapsto (x_w)_w, \quad \text{where} \quad x_w = \begin{cases} x & \text{if } w = \mathfrak{p}, \\ 1 & \text{elsewise,} \end{cases}$$

we have $(n_p(\alpha), L|K) = (\alpha, L_{\mathfrak{P}}|K_{\mathfrak{p}})$, where the left hand side denotes the idèle-theoretic norm residue symbol and the right hand side the local norm residue symbol. Moreover, if $a \in I_K$ is an idèle such that $n_{\mathfrak{p}}(\alpha) \equiv a \mod N_{L|K}(C_L) \cdot K^{\times}$ and the conductor $\mathfrak{f}$ is coprime to the content $c(a) = \prod_{\mathfrak{q}} \mathfrak{q}^{v_{\mathfrak{q}}(a_{\mathfrak{q}})}$ of $a = (a_{\mathfrak{q}})_{\mathfrak{q}}$, then

$$(n_{\mathfrak{p}}(\alpha),\ L|K) = (c(a),\ L|K).$$

Thus, we can first replace $n_{\mathfrak{p}}(\alpha)$ by $\frac{1}{\pi^e} \cdot n_{\mathfrak{p}}(\alpha)$ and subsequently replace the latter by $(x_w)_w$, where

$$x_w = \begin{cases} \xi^{-1} & \text{if } w \mid \mathfrak{f}, \\ \pi^{-e} & \text{otherwise,} \end{cases}$$

because we may multiply by elements of $U_{\mathfrak{p}_k}^{(s_k)}$ in every component $\mathfrak{p}_k$ for $k \in \{0, ..., r\}$. Piecing everything together we get

$$\begin{aligned} (\alpha,\ L_{\mathfrak{P}}|K_{\mathfrak{p}}) = (n_{\mathfrak{p}}(\alpha),\ L|K) &= \big((x_w)_w,\ L|K\big) = \big((\xi x_w)_w,\ L|K\big) \\ &= (c((\xi x_w)_w)),\ L|K) \end{aligned}$$

and $c((\xi x_w)_w) = \xi \mathcal{O}_K \cdot \pi^{-e} \mathcal{O}_K \cdot \mathfrak{p}^e$. □

4.3 Weakly ramified and non-abelian extensions of degree $l^2 p$

We will now describe how to find global extensions $L|\mathbb{Q}$ of degree $l^2 p$, where l, p are odd primes satisfying $l \mid (p-1)$, that are non-abelian, weakly ramified, have cyclic l-Sylow group and full decomposition group at p. Interested in performing computations, we restrict ourselves to the case of $l^2 \nmid (p-1)$ modelling $l = 3$ and $p = 7$. This method was also implemented in MAGMA by the author.

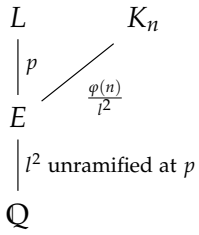
(4.19) Definition. Let $L|K$ be a finite Galois extension, $\mathfrak{p}$ an ideal of K, and $\mathfrak{P}|\mathfrak{p}$ an ideal of L. If $L_{\mathfrak{P}}|K_{\mathfrak{p}}$ is weakly ramified in the sense of Definition (3.16), we say that $L|K$ is ***weakly ramified at*** $\mathfrak{p}$. If $L|K$ is weakly ramified at all primes $\mathfrak{p}$ of K, then $L|K$ is called ***weakly ramified***.

Note that this definition does not depend on the choice of $\mathfrak{P} \mid \mathfrak{p}$, since if $\mathfrak{P}' \mid \mathfrak{p}$ is another choice, we have $\mathfrak{P}' = \tau\mathfrak{P}$ for some $\tau \in G_{L|K}$ and

$$G_{\mathfrak{P},s} \to G_{\tau\mathfrak{P},s}, \quad \sigma \mapsto \tau\sigma\tau^{-1}$$

is an isomorphism for all $s \geq -1$.

Let $L|\mathbb{Q}$ be a Galois extension as described above and E its unique subfield satisfying $[E : \mathbb{Q}] = l^2$. We know from Lemma (3.26) that the condition $l^2 \nmid (p-1)$ forces $E|\mathbb{Q}$ to be unramified at p, hence E is a subfield of some cyclotomic field $K_n = \mathbb{Q}(\xi_n)$ for an n not divisible by p and such that $p \mid \varphi(n)$, where φ denotes the Euler φ-function. We therefore have a diagram of the following shape.



We now first describe how to find such a field E that fits our purposes. Let $n \in \mathbb{N}$ be an integer such that $l^2 \mid \varphi(n)$ holds, $K_n = \mathbb{Q}(\xi_n)$ as before, and $E \subseteq K_n$ a subfield satisfying $[E : \mathbb{Q}] = l^2$.
Recall that the residue degree f_p of $K_n \mid \mathbb{Q}$ at p equals the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$, which we denote by $\operatorname{ord} p$. If we require $\operatorname{ord} p^{\varphi(n)/l^2} \geq l^2$, we therefore obtain the following inequalities for the respective decomposition groups

$$\begin{aligned} l^2 \geq |D_p(E|\mathbb{Q})| &= \left|D_p(K_n|\mathbb{Q})/D_p(K_n|E)\right| = \frac{f_p}{|D_p(K_n|\mathbb{Q}) \cap G_{K_n|E}|} \\ &\geq \frac{f_p}{\gcd(f_p, \frac{\varphi(n)}{l^2})} = \frac{\operatorname{ord} p}{\gcd(\operatorname{ord} p, \frac{\varphi(n)}{l^2})} = \operatorname{ord} p^{\frac{\varphi(n)}{l^2}} \geq l^2 \end{aligned}$$

forcing $D_p(E|\mathbb{Q}) = G_{E|\mathbb{Q}}$ as desired. It remains to show there always exists such an integer n. This is done by the the following elementary Lemma based on a Lemma by Van der Waerden (cf. [Lan95, Ch. X, 2, Lemma 1]).

(4.20) Lemma. Let l, p be odd primes such that $l \mid (p-1)$, but $l^2 \nmid (p-1)$. Then there is a prime q enjoying the following properties:

(a) $q \neq p$,

(b) $q \equiv 1 \mod l^2$,

(c) the order of $p^{(q-1)/l^2}$ in $(\mathbb{Z}/q\mathbb{Z})^\times$ equals l^2.

Proof. Firstly, observe that for every $n \geq 1$

$$\ker\left\{(\mathbb{Z}/l^{n+1}\mathbb{Z})^\times \to (\mathbb{Z}/l^n\mathbb{Z})^\times\right\}$$

is the unique subgroup of order l, hence

$$p^l \equiv 1 \mod l^{n+1} \quad \Leftrightarrow \quad p \equiv 1 \mod l^n.$$

Our assumptions therefore ensure

$$p^l - 1 \equiv 0 \mod l^2, \qquad p^l - 1 \not\equiv 0 \mod l^3.$$

Now consider the integer

$$T = \frac{p^{l^2}-1}{p^l-1} = (p^l-1)^{l-1} + l(p^l-1)^{l-2} + \ldots + l(l-1)(p^l-1) + l.$$

We have $T \equiv 0 \mod l$, but $T \equiv l \mod l^2$. As $T > l$, there has to be a prime divisor ξ of T such that $\xi \neq l$. Suppose ξ is also a divisor of $p^l - 1$, then $\xi \mid l$, whence $l = \xi$. This shows that the order of p in $(\mathbb{Z}/\xi\mathbb{Z})^\times$ is l^2 and it suffices to show that there is such a prime divisor ξ accessory satisfying $\frac{\xi-1}{l^2} \in (\mathbb{Z}/l^2\mathbb{Z})^\times$, which is the same as stating that $l^3 \nmid (\xi - 1)$.

Let $T = l \cdot \prod q_i^{\nu_i}$ be the prime decomposition of T. We have

$$T \equiv l(l-1)(p^l-1) + l \mod l^4 \quad \Leftrightarrow \quad \prod q_i^{\nu_i} \equiv (l-1)p^l + 1 \mod l^3.$$

The equivalences

$$(l-1)p^l + 1 \equiv 1 \mod l^3 \quad \Leftrightarrow \quad (l-1)p^l \equiv 0 \mod l^3 \quad \Leftrightarrow \quad p^l \equiv 0 \mod l^3$$

show that we must have $\prod q_i^{\nu_i} \not\equiv 1 \mod l^3$, hence $q_i \not\equiv 1 \mod l^3$ for at least one i. □

Let z be a prime as provided by Lemma (4.20) and E the unique subfield of $\mathbb{Q}(\xi_z)$ of degree $[E : \mathbb{Q}] = l^2$. Consider the embedding problem

$$\begin{array}{ccccccccc} & & & & & & \Gamma & & \\ & & & & & & \downarrow \varphi & & \\ 1 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & G & \xrightarrow{j} & G_{E|\mathbb{Q}} & \longrightarrow & 1, \end{array}$$

where G is a non-abelian subgroup of order l^2p. The exact sequence at the bottom splits by the Theorem of Schur-Zassenhaus [Mac94, Ch. IV, Thm. 10.5] as $\mathbb{Z}/l^2\mathbb{Z}$ and $G_{E|\mathbb{Q}}$ have coprime group orders, hence Theorem (4.14) ensures the solvability of this embedding problem. That is, if $\mathcal{L}$ is the set of $l-1$ extension fields defining a non-abelian weakly ramified extension of $\mathbb{Q}_p$ as described in Proposition (3.29), there are extension fields $L_1, \ldots, L_{l-1}$ of E such that the set of completions of the L_i at some prime

of L_i lying above p is exactly $\mathcal{L}$.

Computing candidates for L_i

Let L be one of these L_i and $\mathfrak{f}$ the conductor of $L|E$. Since p is inert in $E|\mathbb{Q}$ and $L|E$ is weakly ramified at p, we have $v_p(\mathfrak{f}) = 2$. Thus, $\mathfrak{f} \mid qp^2$ for some integer $q \in \mathbb{Z}$ coprime to z and L corresponds to a subgroup H of the ray class group $\mathrm{cl}_E(qp^2)$. Let $H \subseteq \mathrm{cl}_E(qp^2)$ be an arbitrary subgroup and $E(H)$ the corresponding class field, then

(a) $(\mathrm{cl}_E(qp^2) : H) = p$ if and only if $[E(H) : E] = p$,

(b) H is stable by $G_{E|\mathbb{Q}}$ if and only if $E(H)|\mathbb{Q}$ is Galois by Lemma (4.16),

(c) $I_{G_{E|\mathbb{Q}}} \mathrm{cl}_E(qp^2) \not\subseteq H$ if and only if $E(H)|\mathbb{Q}$ is non-abelian by Lemma (4.17),

(d) $v_p(\mathfrak{f}) = 2$, where $\mathfrak{f}$ denotes the conductor of $E(H)|E$, if and only if $E(H)|\mathbb{Q}$ is weakly ramified by Lemma (3.19).

Note that an extension $E(H)|E$ satisfying condition (d) automatically has full decomposition group at $\mathfrak{p} \mid p$, because $p \mid \mathfrak{f}$ implies that p (totally) ramifies in $E(H)|E$.

Our set of global realisations is therefore in bijection with subgroups enjoying these properties (a) - (d), where q ranges over the integers.

Determing the completion at $\mathfrak{p}$

We can easily decide which local field of $\mathcal{L}$ we get by the completion $E(H)_\mathfrak{p}$, because according to our local considerations in the previous chapter (see Remark (3.30)), every field $F \in \mathcal{L}$ is uniquely determined by

$$1 + pN(X^p - rX)^\perp \subseteq N_{F|E_p},$$

where $r \in \mathbb{F}_p^\times \setminus \{1\}$ is of order l and $N(X^p - rX)^\perp$ is a set of lifts from $\mathbb{F}_{p^{l^2}}$ to $E_p^\times$ of the orthogonal complement of the set of roots of the polynomial $X^p - rX$ in $\mathbb{F}_{p^{l^2}}$ with respect to the trace form. Note that

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \quad \text{and} \quad \mathbb{F}_{p^{l^2}} = \mathcal{O}_E/p\mathcal{O}_E,$$

so the set $N(X^p - rX)^\perp$ can be chosen to consist of elements in $E^\times$. We therefore need to check whether

$$(x, E(H)_\mathfrak{p}|E_p) = 1$$

for all elements x of a $\mathbb{F}_p$-basis of $N(X^p - rX)^\perp$. Choose a solution ξ of

$$\xi \equiv 1 \mod q\mathcal{O}_E \quad \text{and} \quad \xi \equiv \frac{1}{x} \mod p^2\mathcal{O}_E,$$

then, by Lemma (4.18) from the previous section, we have

$$(\xi\mathcal{O}_E, E(H)|E) = (x, E(H)_\mathfrak{p}|E_p),$$

and hence

$$(x, E(H)_\mathfrak{p}|E_p) = 1 \quad \Leftrightarrow \quad \xi\mathcal{O}_E \in H.$$

Summarising these thoughts, the method is therefore as follows: Compute subgroups $H \subseteq \mathrm{cl}_E(qp^2)$ satisfying the conditions (a)-(d) stated above for, if necessary, gradually increasing q, while collecting those subgroups having pairwise different completions at $\mathfrak{p} \mid p$ until you have a set of $l-1$ such subgroups.

(4.21) Remark. The method described works well for odd primes l, p such that $l \mid (p-1)$ and $l^2 \nmid (p-1)$, only limited by computational power. If $l = 3$ and $p = 7$, then the set $\mathcal{L}$ consists of two distinct local fields F_1 and F_2. Performing computations in MAGMA using the method described above with $E = \mathbb{Q}(\zeta_{37})$, one finds that the number of suitable subgroups $H \subseteq \mathrm{cl}_E(qp^2)$ such that $E(H)$ takes F_i as completion is distributed as follows:

	F_1	F_2
$1 \leq q \leq 20$	1	-
$1 \leq q \leq 40$	8	1
$100 \leq q \leq 120$	10	4

When considering a pair of primes l, p satisfying $l^2 \mid (p-1)$ the general method should also work. However, the proof of Lemma (4.20) fails in this case, making the approach only a heuristic one. Of course, one would not get a complete set of representatives for all weakly ramified and non-abelian extensions of $\mathbb{Q}_p$ with cyclic l-Sylow group here but only of those extensions having ramification degree p.

An open question

When considering the table given above in Remark (4.21) one might wonder why one of the two possible local fields appears much more often as completion at $\mathfrak{p}|p$ for small q or whether this finding is just coincidental, caused by the method of computation. This question seems to be closely linked to the question of how the norm group of $E(qp^2)_\mathfrak{p}|E_p$, where $E(qp^2)$ denotes the ray class field of qp^2, can be explicitely described, because each F_i was characterised by its norm group and if, for example, $q = 2$, then p has full decomposition group in $E(qp^2)|E$ and as soon as

$$N_{E(qp^2)|E_p}(E(qp^2)^\times) \subseteq N_{F_i|E_p}(F_i^\times), \qquad (*)$$

we get at least one field $E(H) \subseteq E(qp^2)$ taking F_i as completion above p. Twisting by a suitable cocycle of $H^1(\mathrm{cl}_E(qp^2), \mathbb{Z}/l^2\mathbb{Z})$ as in Lemma (4.4) should now give any other such field contained in $E(qp^2)$. It is therefore an interesting question the author has not been able to answer yet, whether one can find a condition on q (depending on E) ensuring that $(*)$ holds.

5 Bibliography

Bibliography

[BBH17] Werner Bley, David Burns, and Carl Hahn. On Refined Metric and Hermitian Structures in Arithmetic, I: Galois-Gauss Sums and Weak Ramification. Preprint, 2017.

[Ble03] Werner Bley. Numerical evidence for a conjectural generalization of hilbert's theorem 132. *LMS J.Comput.Math.*, 6:68–88, 2003.

[Bos09] Siegfried Bosch. *Algebra*. Springer, Berlin, Heidelberg, 7th edition, 2009.

[CR87] Charles W. Curtis and Irving Reiner. *Methods of Representation Theory - with Applications to Finite Groups and Orders, Vol. II*, volume 2 of *Pure and applied mathematics. A Wiley-Interscience Series of Texts, Monographs & Tracts*. John Wiley & Sons, Inc., 1987.

[Ere91a] Boas Erez. A survey of recent work on the square root of the inverse different. *Asterisque*, (198-199-200):133–152, 1991. Journees Arithmetiques de Luminy 17-21 Juillet 1989.

[Ere91b] Boas Erez. The Galois structure of the square root of the inverse different. *Math. Z.*, 208:239–255, 1991.

[Frö85] A. Fröhlich. Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants. *Journal für die reine und angewandte Mathematik*, 360:84–123, 1985.

[Hal63] M. Hall. *The theory of groups*. Macmillan, 1963.

[IP64] I. Martin Isaacs and D. S. Passman. Groups with representations of bounded degree. *Canad. J. Math.*, 16:299–309, 1964.

[Isa76] I. Martin Isaacs. *Character Theory of Finite Groups*, volume 69 of *Pure and applied mathematics, a series of monographs and textbooks*. Academic Press, Inc., 1976.

[Iwa86] Kenkichi Iwasawa. *Local Class Field Theory*. Oxford Mathematical Monographs. Oxford University Press, 1986.

[Lan95] S. Lang. *Algebraic number theory*. Springer, 2nd edition, 1995.

[Mac94] Saunders Mac Lane. *Homology*, volume 114 of *Grundlehren der mathematischen Wissenschaften*. Springer, 4th edition, 1994.

[Neu73] Jürgen Neukirch. Über das Einbettungsproblem der algebraischen Zahlentheorie. *Inventiones math.*, 21:59–116, 1973.

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer, 1992.

[Neu11] Jürgen Neukirch. *Klassenkörpertheorie*. Springer, 2011. Neu herausgegeben von Alexander Schmidt.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*. Grundlehren der mathematischen Wissenschaften. Springer, second edition, 2008.

[Poi67] G. Poitou. *Cohomologie Galoisienne des Modules finis*. Dunod, 1967.

[Ros09] Harvey E. Rose. *A Course on Finite Groups*. Springer, 2009.

[Ser79] Jean-Pierre Serre. *Local Fields*. Number 69 in Graduate Texts in Mathematics. Springer, 1979. Translated from the French by Martin Jay Greenberg.

[Swa68] Richard Swan. *Algebraic K-Theory*. Number 76 in Lecture Notes in Mathematics. Springer, 1968.

[Tay81] Martin J. Taylor. On Fröhlich's conjecture for rings of integers of tame extensions. *Inventiones math.*, 63(1):41–79, 1981.

[VC16] Stephane Vinatier and Luca Caputo. Galois module structure of the square root of the inverse different in even degree tame extensions of number fields. *Journal of Algebra*, 468:103–154, 2016.

[Vin01] Stephane Vinatier. Structure galoisienne dans les extesions faiblement ramifes de $\mathbb{Q}$. *J. Number Theory*, 91:126–152, 2001.

[Vin03] Stephane Vinatier. Sur la racine caree de la codifferente. *J. Theor. Nombres Bordeaux*, 15:393–410, 2003.

I declare that this thesis has been composed solely by myself and that I have not used any other resources than those indicated.

Munich, 15th May 2018