The Capitulation Problem in Class Field Theory

Dissertation
zur Erlangung des mathematisch-naturwissenschaftlichen Doktorgrades
"Doctor rerum naturalium"
der Georg-August-Universität Göttingen

vorgelegt von
Tobias Bembom

aus Nienburg, 27.02.2012

Referent: Prof. Dr. Preda Mihailescu
Koreferent: Prof. Dr. Valentin Blomer
Tag der mündlichen Prüfung: 02.04.2012

To Hubert, Anna, Oliver, Kerstin

Acknowledgments

It is a pleasure to thank those who made this thesis possible. I owe deepest gratitude to my supervisor Preda Mihailescu, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject. His creativity and insistence have been an enormous help and without him this thesis would not have been possible. Additionally, I am indebted to my second supervisor and referee Valentin Blomer for his efforts and general remarks. I would also like to thank my former colleagues Matthias Wulkau, Julian Wolff, Arne Buchholz, Tyge Tiessen, and Sören Kleine, for all their help, support and interest. Particular gratitude goes to Christopher Ambrose for reading my thesis, giving me valuable hints, and being a good friend. Last but not least, I want to thank my family, my friends, and especially my girlfriend, who always supported me during the dissertation process.

Contents

1 Introduction **3**

1.1 Description of the Capitulation Problem and its Historical Background 3

1.2 Overview and Organization of the Thesis 6

1.3 Basic Notations and Results in Class Field Theory 11

2 Galois Cohomology and Furtwängler's Theorem for Unramified Cyclic Extensions **20**

2.1 $\mathcal{H}^0(G, \mathcal{O}_L^*) \cong A(L)^G/\imath_{L/K}(A(K))$ 21

2.2 Iwasawa's Theorem 23

2.3 Hilbert's Theorem 94 and Furtwängler's Theorem 24

2.4 Chevalley's Theorem and Capitulation in Ramified Cyclic Extensions 28

2.5 Number Fields with Cyclic Class Groups 32

2.6 $\mathbb{Z}[s]$-Cycles and an Upper Bound for the Rank of $A(L)$ 35

2.7 Exact and Non-Exact $\mathbb{Z}[s]$-Cycles 39

2.8 Decomposition of $A(L)$ into a Product of $\mathbb{Z}[s]$-Cycles and its Effect on Capitulation 42

3 On the Structure of the Capitulation Kernel in Unramified Cyclic Extensions **52**

3.1 Unramified Cyclic p-Extensions of Higher Degree and the Deep Cohomology 53

3.2 Numerical Data for Capitulation in Unramified Cyclic Extensions of Degree 9 60

4 Growth of Ideal Classes in Extensions with F-Property **62**

4.1 Preliminary Results on Finite Abelian p-Groups and a Classification of the Growth of Ideal Classes 63

4.2 Stable Growth of Ideal Classes 66

4.3 Tame Growth of Ideal Classes 68

4.4 Semi-Stable Growth of Ideal Classes 71
4.5 Wild Growth of Ideal Classes 72

5 G-Action on Ideal Classes 79
5.1 Preliminary Results 80
5.2 Decomposition of $A(K)$ via Idempotents and Lifting of Idempotents 83
5.3 Suzuki's Theorem on α-Components 87
5.4 Capitulation in CM-Fields 95
5.5 Interlude on Representation Theory and α-Components 97
5.6 Capitulation for the Case that $A(K)$ is $\mathbb{Z}_p[G]$-Cyclic 105
5.7 Decomposition of $A(K)$ into a Direct Product of $\mathbb{Z}_p[G]$-Cycles 110
5.8 Some Results on the Genus Field 114
5.9 The Automorphisms of $G(H^{(2)}(K)/K)$ Acting on $A(K)$ 116

6 Capitulation in Extensions of Imaginary Quadratic Fields 120
6.1 Structure of Class Groups of Extensions of Imaginary Quadratic Fields 121
6.2 Heuristics on Class Groups of Unramified Cyclic Extensions of Imaginary Quadratic Fields 123
6.3 Database for Capitulation in Degree 5-and-7-Extensions 128
6.4 Main Theorem on Capitulation in Extensions of Prime Degree 133

7 The Capitulation Problem in $\mathbb{Z}_p$-Extensions 146

Appendix 150

A List of Notations 150

B Source Codes Used in MAGMA 152

Bibliography 154

Curriculum Vitae 157

Chapter 1

Introduction

1.1 Description of the Capitulation Problem and its Historical Background

The original capitulation problem in class field theory is more than one century old. It was Hilbert, who did pioneering work on the capitulation problem. In his celebrated Zahlbericht of 1897, he proved Hilbert's Theorem 94 which can be seen as the foundation of this subject. In what follows, we shortly describe the problem. For further details on Hilbert's Theorem, we refer to [22]. A comprehensive overview of the topic yields Miyake, see [4]. For an extension L/K of number fields with groups of fractional ideals $\mathfrak{J}_K$ and $\mathfrak{J}_L$, respectively, we define the *lift of ideals* in K to L as follows:

$$\imath_{L/K} : \mathfrak{J}_K \to \mathfrak{J}_L, \ I \mapsto I \cdot \mathcal{O}_L.$$

This is obviously an injective group homomorphism, which canonically induces the lift of ideal classes:

$$\bar{\imath}_{L/K} : Cl(K) \to Cl(L), \ [I] \mapsto [I \cdot \mathcal{O}_L],$$

where I is an ideal in K and $[I]$ is the ideal class generated by I. Hilbert's Theorem 94 states that in an unramfied cyclic extension L/K, there are non-principal ideals in K, which become principal when lifted to L. In the 1930s Scholz coined the expression that such ideals *capitulate* in L. Accordingly, the capitulation kernel of L/K is defined as

$$ker(\bar{\imath}_{L/K} : Cl(K) \to Cl(L)) = P_K(L).$$

More precisely, Hilbert showed that the degree of L/K divides the order of the capitulation kernel. At that time, however, one could only prove this

result for unramified cyclic extensions but not more generally for unramified abelian extensions. Meanwhile, in 1906 Hilbert's student Furtwängler paved the way for class field theory by proving the existence of a Hilbert class field for any given number field K. It is the maximal uramified abelian extension of K and has the property that its Galois group over K is isomorphic to the ideal class group of K. For further details on the explicit construction of such a Hilbert class field, we refer to Furtwängler's original work, see [1]. An outline of the history of class field theory can be found in [26]. In 1932, Furtwängler proved the Principal Ideal Theorem which asserts that the class group of a given number field capitulates completely in its Hilbert class field. His proof is based on a theorem due to Artin of 1930 in which he proved that the capitulation problem is equivalent to finding the kernel of the transfer of certain groups. Thus, he reduced the capitulation problem to a purely group theoretic challenge. Having established the Principal Ideal Theorem, the question remains which ideal classes of K capitulate in a field which lies between K and its Hilbert class field. In 1932, Furtwängler's student Taussky analyzed under which conditions a number field K, with ideal class group of the form C_p^n, has a basis such that each basis element capitulates in an unramified cyclic extension of K of degree p. The original work can be found in [39]. Taussky and Scholz were the first who explicitly computed the capitulation kernel of unramified cyclic degree-3-extensions of several imaginary quadratic fields. Their work dates back to 1934 and can be studied in [21]. In 1958, Tannaka and Terada proved that for a cyclic extension K/k with Galois group G, the G-invariant ideal classes in K capitulate in the genus field of K/k, i.e. in the maximal extension of K which is unramified over K and abelian over k. For more details, we refer to [30]. Heider and Schmithals extended the ideas of Taussky and Scholz in 1982. They yielded a general criterion for capitulation in unramified cyclic extensions of prime degree and used this to delineate a procedure that explicitly computes the capitulation kernel. Verifying the conditions for the above criterion, however, is difficult as well, cf. [25]. In 1989, Iwasawa constructed a family of real quadratic fields in which the ideal class already capitulates in an extension strictly contained in the Hilbert class field. For additional insight, we commend [24]. Afterward, this approach has been generalized by Cremona and Odoni, see [28]. In 1991, the capitulation problem culminated in Suzuki's Theorem who proved that for any unramified abelian extension L/K, the order of the capitulation kernel is divided by the degree of L over K. This result essentially comprises all information we have with regard to the capitulation problem, nowadays. Gonzalez-Aviles considered the capitulation problem in arbitrary Galois extensions and yielded various generalizations of the existing results for unramified abelian extensions. His paper dates back

to 2007 and can be found in [27]. In 2009, Daniel Mayer et alii launched the so-called principalization project, which can be found on the website given in [36]. Amongst others, this site contains a list of capitulation kernels for unramified cyclic degree-3-extensions of both real and imaginary quadratic fields, thus extending the numerical data computed by Scholz, Taussky, Heider, and Schmithals.

Naturally, several interesting questions emerge in this context:

1) What is the exact order of the capitulation kernel of a given unramified abelian extension?

2) Suzuki's Theorem only yields a statement on the cardinality of the capitulation kernel of an extension L/K but no information on the structure of it. Under which circumstances, for instance, can we embed the Galois group of L/K in the capitulation kernel of L/K?

3) Let K be a number field with class group being isomorphic to $C_p \times C_p$, for example. Then there exist $p+1$ unramified cyclic extensions of K of degree p. Are the various capitulation kernels of these extensions somehow correlated? Do the capitulation kernels tend to be pairwise distinct for example?

Amongst others, we will investigate these questions in this thesis, putting particular emphasis on the second and third question.

1.2 Overview and Organization of the Thesis

In the following section, we first give a very concise overview of the topics we discuss in this thesis. In particular, we indicate which parts are predominantly a reproduction of known results and which parts contain a high percentage of own contributions to the subject. Afterward, we yield a more precise outline of the thesis and summarize the contents of the various chapters.

After an introduction on the capitulation problem, we gather certain properties of unramified cyclic extensions. In doing so, we establish known results as Furtwängler's Theorem and extend them by own contributions which can be found in the preliminary section and in the last two sections of Chapter 2. In view of the second question from above, Chapter 3 revisits Hilbert's work on the capitulation problem and yields additional information on the structure of a capitulation kernel by generalizing his approach. Subsequently, we compare the ideal classes of unramified cyclic extensions in Chapter 4. In particular, we derive a strict relationship between the orders of those ideal classes and show why this is of importance with respect to capitulation. In this context, we begin with ideas on the growth of ideal classes due to Professor Mihailescu. Later, this work is extended and generalized in various aspects. In Chapter 5, we assume an additional group action on the class group of a given number field. This can be used to obtain further results on the structure of a capitulation kernel. Chapter 6 comprises one of the main results of the thesis. It deals with capitulation in extensions of imaginary quadratic fields and the correlations between the various capitulation kernels of a number of unramified cyclic extensions of a given imaginary quadratic base field. (See the third question from above). In this connection, we also introduce some heuristics on the class groups of unramified cyclic extensions of imaginary quadratic fields. Most of the results in this chapter are due to the author. The last chapter deals with capitulation in $\mathbb{Z}_p$-extensions and also yields some new insights.

We now proceed with a more precise summary of the contents of this thesis:

Chapter I. This preliminary chapter describes the capitulation problem in class field theory. We outline the historical progress in this field and give an overview of natural questions arising in this context. Subsequently, we introduce the basic results in class field theory and present the notations used in the sequel.

Chapter II. In this chapter, we illuminate various properties of an unramified cyclic extension L/K with Galois group G and rings of integers $\mathcal{O}_K$, $\mathcal{O}_L$, respectively. We establish an explicit relation between the G-invariant ideal classes in L and $\mathcal{O}_K^*/N_{L/K}(\mathcal{O}_L^*)$. This connection is not mentioned anywhere in the literature. We then follow ideas of Iwasawa to show that the first Galois cohomology group of the G-module $\mathcal{O}_L^*$ is isomorphic to the capitulation kernel of L/K. Applying the above results, we obtain a particularly short and modern proof of Furtwängler's Theorem, which is essentially a version of Hilbert's Theorem 90 for ideal classes. More generally, we say that cyclic extensions in which Hilbert 90 for ideal classes holds satisfy the *Furtwängler-property* or short *F-property*. Proving a theorem due to Chevalley, we demonstrate that extensions in which at most one prime ramifies have the F-property. In light of that theorem, we also discuss capitulation in ramified cyclic extensions, investigating which further factors influence capitulation in this case. Afterward, we conclude several interesting properties arising from the F-property. We show that a number field with cyclic class group has a Hilbert class field with trivial class group. Moreover, we analyze the structure of the class group $A(L)$ of L in dependence on the class group of K, determine an upper bound for the rank of $A(L)$, and finally decompose $A(L)$ into a product of certain cyclic $\mathbb{Z}[G]$-submodules. Striving for a connection between such a decomposition and capitulation, we introduce the notation of exact and non-exact $\mathbb{Z}[G]$-submodules of $A(L)$ and prove that non-exact $\mathbb{Z}[G]$-modules give rise to non-capitulating ideal classes in L/K. The theoretical results are supplemented by various numerical examples which we computed on MAGMA.

Chapter III. Here, we want to show which factors determine the structure of the capitulation kernel of an unramified cyclic p-extension L/K with Galois group G. In doing so, we first disclose the underlying concept of Galois cohomology with regard to capitulation and explicitly show how elements in $\mathcal{O}_K^*/N_{L/K}(\mathcal{O}_L^*)$ give rise to capitulating ideal classes in L/K. In this context, we revisit Hilbert's ideas that led to Hilbert's Theorem 94, see [22], and present various generalizations of Hilbert's original ideas. Amongst others, we give a sufficient condition under which G and $\mathcal{O}_K^*/N_{L/K}(\mathcal{O}_L^*)$ can be embedded in the capitulation kernel. Numerical examples, however, show that this is not the case in general. Hence, we introduce the so-called *deep cohomology*, which yields a more subtle picture of the interplay between the according Galois cohomology and the capitulation kernel. Appealing to the developed theory of the deep cohomology, we give a concrete formula for the rank of a capitulation kernel. Afterward, we extend the results by evaluating some numerical data of capitulation in unramified cyclic extensions of degree

9 with regard to the evolved theory.

Chapter IV. This chapter deals with the growth of ideal classes in a given cyclic extension L/K of prime degree p, satisfying the F-property as defined in Chapter 2. (We can then generalize the results to cyclic p-extensions simply by splitting them into extensions of degree p). More precisely, we discuss questions of the following type: Let b be an ideal class of L and a an ideal class in K with $N_{L/K}(b) = a$. How are the orders of b and a correlated? We will prove that under certain conditions, we have that

$$ord(b) \quad = \quad p \cdot ord(\imath_{L/K}(N_{L/K}(b))). \tag{1.1}$$

Obviously, the growth of ideal classes is closely connected with capitulation. Indeed, if equation (1.1) holds, the ideal class a capitulates in L if and only if a and b are of the same order. For a more sophisticated approach, we distinguish between four different types of growth: *stable growth*, *tame growth*, *semi-stable growth*, and *wild growth*. We then show that (1.1) is satisfied in the first three cases provided that a can be extended to a minimal generating system of $N_{L/K}(A(L))$. Subsequently, we discuss wild growth in further depth. We show that the exponent of $ker N_{L/K}$ can be arbitrarily large. In doing so, we construct a family of finite p-groups G such that G contains an abelian subgroup of index p and such that the exponent of the commutator group G' is unbounded as G ranges of the constructed family of p-groups. A theorem due to Ozaki, then reveals that for each such group G, there exists an unramified cyclic extension L/K of degree p with $Gal(H(L)/K)$ being isomorphic to G, which eventually yields the desired result. In the remainder of this chapter, we give numerous concrete examples for the various types of growth.

Chapter V. In order to obtain more information on the structure of a capitulation kernel, we additionally assume some Galois action on the class group of a given number field K. More precisely, we suppose that K contains a subfield k such that K/k is Galois with Galois group G. Throughout this chapter, we assume that a fixed prime p does not divide the order of G. We begin our analysis by showing how G acts on the p-class group $A(K)$ of K and on the Galois group of the p-Hilbert class field $H(K)$ of K over K, illustrating how this action affects the capitulation problem. We then use idempotents in $\mathbb{Z}_p[G]$ to decompose the class group of K and thus the Hilbert class field of K into so-called α-components $A(K)_\alpha$ and $H(K)_\alpha$, respectively, corresponding to certain idempotents α in $\mathbb{Z}_p[G]$. In this context, we draw particular attention to irreducible α-components, i.e. to those components which correspond to primitive idempotents. We show under which circum-

stances Suzuki's Theorem extends to a component wise version. More precisely, assuming that L is an intermediate field of K and a given α-component $H(K)_\alpha$, we investigate under which conditions the degree of L over K divides the order of the capitulation kernel of L/K on the given component $A(K)_\alpha$, i.e. the order of $P_K(L) \cap A(K)_\alpha$. The theoretic results are then extended by several numerical examples in which we decompose the class group of a given number field K into α-components and compute the capitulation kernels on the various components of the class group of K. In light of the above results, we also shortly deal with capitulation in CM-fields, where the developed theory can be applied more specifically. We then insert several results in p-adic analysis and representation theory in order to prove that $\mathbb{Q}_p[G]$ and $\mathbb{F}_p[G]$ have the same number of primitive idempotents supposing that G is abelian. Appealing to this result, we conclude that p-maximal elements in irreducible α-components of the class group of K are invertible in some sense. In the case that the class group of K is $\mathbb{Z}_p[G]$-cyclic, we derive that all p-maximal elements in a given irreducible α-component are of the same order. We then use this property to prove that under certain conditions, all ideal classes in K of order equal or less than p^l capitulate in an intermediate field of $H(K)/K$ whose Galois group over K is isomorphic to $A(K)/A(K)^{p^l}$.
In order to abandon the assumption that the class group of K is $\mathbb{Z}_p[G]$-cyclic, we apply the developed results to prove that the class group of K can be decomposed into a direct product of cyclic $\mathbb{Z}_p[G]$-submodules. All previous results then extend to cyclic $\mathbb{Z}_p[G]$-submodules of $A(K)$ lying within a given irreducible component. Having established such a decomposition of the class group of K, we show that $KH(k)$ is the p-genus field of K/k, i.e. the maximal unramified p-extension of K which is abelian over k. We conclude this chapter with a generalization of the G-action on $A(K)$. We replace it by the action of the automorphism group of the Galois group of the second Hilbert class field of K over K. Assuming that this automorphism group is not a p-group, we evolve a similar machinery as above and use this with respect to capitulation.

Chapter VI. This chapter deals with capitulation in extensions of an imaginary quadratic field K. For a given unramified cyclic extension L/K of degree p, we prove that the kernel of the norm of ideal classes $N_{L/K}$ is non-trivial and of even rank. Generalizing a paper due to Wittmann, we introduce a substantiated heuristic on the structure of $ker N_{L/K}$, taking the above property into account. Subsequently, we compare our heuristics with the given numerical data, noticing that the heuristics are in good accordance with the computed data.
Whereas there was only a database for capitulation in extensions of imagi-

nary quadratic fields of degree 2 and 3, we first extend the numerical data to extensions of degree 5 and 7. In this regard, we draw our attention to questions of the following type: For example, let K be as above with class group being isomorphic to $C_p \times C_p$, where $p > 3$ is a prime. Then there exist $p+1$ unramified cyclic extensions of K of degree p. How are the capitulation kernels of these intermediate fields correlated, are there any noticeable patterns? Evaluating the numerical data, we observed the following surprising phenomenon: Either the capitulation kernels of all these intermediate fields are pairwise distinct (1-1-capitulation), or there exists a non-trivial ideal class in K that capitulates in at least p fields of these intermediate fields (p-capitulation). We proceed with a proof of the main theorem of this chapter stating that K has 1-1-capitulation or p-capitulation if K satisfies certain assumptions and if $p > 3$. In view of the developed results and heuristics of Section 6.1 and 6.2, we notice that the assumptions we make in the above theorem are satisfied with high likelihood. The proof of the theorem is divided into several lemmata and propositions. Amongst others, we apply the theory of the transfer of groups and some of its group theoretical properties. Summing up all results we need to prove, the proof comprises approximately ten pages.

Chapter VII. The final chapter deals with capitulation in $\mathbb{Z}_p$-extensions. More precisely, let K be a number field and K_∞ be a $\mathbb{Z}_p$-extension of K. For an intermediate field K_n of K_∞/K, we let H_n be the Hilbert class field of K_n and H_∞ be the composite of the H_n's. For an intermediate field L of H_∞/K_∞, which is Galois over K, we set $L_n = L \cap H_n$. We then show that $(X_n = ker(\imath_{L_n/K_n}))_n$ is a projective limit with respect to the norm map and apply Iwasawa Theory to obtain a statement on the cardinality of the X_n's.

1.3 Basic Notations and Results in Class Field Theory

In this section, we want to state the basic results in class field theory. For a comprehensive and exhaustive treatise on class field theory, we refer to [2] and [3], where the proofs of the results mentioned here can be found. Moreover, we introduce the notation that we will use throughout the thesis. We start with

Theorem 1.3.1. *Let K be an algebraic number field with ideal class group $Cl(K)$. Then there exists a unique field extension $H(K)/K$ such that:*

(i) $H(K)$ is the maximal unramified abelian extension of K;
(ii) $Cl(K) \cong Gal(H(K)/K)$.

$H(K)$ is called the Hilbert class field of K.

Proof. See Chapter 13 of [3] and in particular Corollary 13.3.5. □

Remark: 1) For clarification, we need to say a word on the ramification of an infinite prime $\mathfrak{p}_\infty$ in K in a given Galois extension L/K. Both Lorenz and Neukirch define the ramification index $e_{\mathfrak{p}_\infty}$ to be one and set

$$f_{\mathfrak{p}_\infty} = [L_{\mathfrak{P}_\infty} : K_{\mathfrak{p}_\infty}],$$

where $\mathfrak{P}_\infty$ is a prime in L lying above $\mathfrak{p}_\infty$. Using these definitions, the Hilbert class field $H(K)$ of K is the maximal abelian extension such that all finite primes in K are unramified and all infinite primes in K split completely in $H(K)$. With a slight abuse of notation, we will henceforth say that an infinite prime $\mathfrak{p}_\infty$ in K ramifies in an extension L if $f_{\mathfrak{p}_\infty} = 2$. We can then use the definition of $H(K)$ as used in the above theorem.

2) The isomorphism in (ii) is induced by the Artin symbol of $H(K)/K$. In what follows, we shortly explain it. For further details and proofs, see Chapter 7 of [3]. Let L/K be an unramified abelian extension and $\mathfrak{P}$ be a prime ideal in L lying above the prime ideal $\mathfrak{p}$ in K. Let

$$D_{\mathfrak{P}|\mathfrak{p}} = \{\sigma \in Gal(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

be the decomposition group of $\mathfrak{P}|\mathfrak{p}$. Let $\mathcal{O}_K$ and $\mathcal{O}_L$ denote the ring of integers of K and L, respectively. One can show that the canonical map

$$D_{\mathfrak{P}|\mathfrak{p}} \to Gal((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$$

is surjective and also injective since L/K is assumed to be unramified. Elementary Galois theory also yields that $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$ is a cyclic field extension whose Galois group is generated by the Frobenius homomorphism, which sends all elements of $\mathcal{O}_L/\mathfrak{P}$ to the power of $|\mathcal{O}_K/\mathfrak{p}|$. Let $Frob_{\mathfrak{P}|\mathfrak{p}}$ be the automorphism in $D_{\mathfrak{P}|\mathfrak{p}}$ that corresponds to the Frobenius homomorphism. As L/K is abelian, one can show that $Frob_{\mathfrak{P}|\mathfrak{p}} = Frob_{\mathfrak{P}'|\mathfrak{p}}$, for all primes $\mathfrak{P}, \mathfrak{P}'$ lying above $\mathfrak{p}$. Thus, we may simply write $Frob_{\mathfrak{p}}$. One can then show:

$$Cl(K) \cong Gal(H(K)/K),\ [\mathfrak{p}] \mapsto Frob_{\mathfrak{p}}.$$

Here $\mathfrak{p}$ is a prime ideal in K and $[\mathfrak{p}]$ denotes the ideal class generated by $\mathfrak{p}$. In the rest of the thesis, we set $\varphi_K([\mathfrak{p}]) := \left(\frac{H(K)/K}{[\mathfrak{p}]}\right) := Frob_{\mathfrak{p}}$, i.e. when we say φ_K is the Artin symbol of K, we mean more precisely the Artin symbol of $H(K)/K$.

Let L/K be an extension of number fields. Then we define the norm map of ideals as

$$N_{L/K} : \mathfrak{J}_L \to \mathfrak{J}_K,\ N_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f_{\mathfrak{P}|\mathfrak{p}}},$$

where $\mathfrak{P}$ is a prime ideal in L that lies above the prime ideal $\mathfrak{p}$ in K and $f_{\mathfrak{P}|\mathfrak{p}}$ denotes the inertia degree of $\mathfrak{P}|\mathfrak{p}$. This group homomorphism induces a norm map on ideal classes:

$$\bar{N}_{L/K} : Cl(L) \to Cl(K),\ [I] \mapsto [N_{L/K}(I)],$$

where I is an ideal in L. Basically, we are only interested in the lift and the norm map of ideal classes. For the ease of notation, we will thus henceforth write $\imath_{L/K}$ instead of $\bar{\imath}_{L/K}$ and $N_{L/K}$ instead of $\bar{N}_{L/K}$. We then have

Proposition 1.3.2. *Notations being like above, it follows that*

(i) $N_{L/K}(\imath_{L/K}(a)) = a^{[L:K]},\ \forall\ a \in Cl(K)$.
In particular, if $([L:K], ord(a)) = 1$, *then* $ord(a) = ord(\imath_{L/K}(a))$.

(ii) Let L/K be Galois with Galois group G. Then, $\forall\ b \in Cl(L)$:

$$\prod_{\sigma \in G} b^{\sigma} = \imath_{L/K}(N_{L/K}(b)).$$

Proof. See page 197, Theorem 1.6 (ii), (iv), of [2]. □

Remark: The previous proposition allows us to focus on p-parts of $Cl(K)$ and on unramified abelian p-extension of K, where p is some fixed prime. *For*

some fixed prime p, we henceforth set $A(K) = Cl(K)_p$, the p-Sylow subgroup of $Cl(K)$. Moreover, let $H(K) = H(K)_p$ denote the p-Hilbert class field of K, i.e. the maximal unramified abelian p-extension of K.

Definition: Let A be a finite abelian p-group. Then:

(i) $rk(A)$ denotes the $p - rk(A)$ of A, i.e. $rk(A) = dim_{\mathbb{F}_p}(A/A^p)$.

(ii) $S_l(A)$ denotes the l-socle of A, i.e.

$$S_l(A) = \{a \in A : \ ord(a) \leq p^l\}, \ \forall \ 1 \leq p^l \leq exp(A).$$

(iii) Supposing that A is a G-module for some group G, the G-invariant elements in A are denoted by A^G.

Proposition 1.3.3. *Let L/K be an unramified abelian extension. Then:*

(i) $Gal(H(K)/L) \cong N_{L/K}(A(L))$;

(ii) $Gal(H(L)/H(K)) \cong ker N_{L/K}$.

Proof. Using the basic properties of the Artin symbol (cf. Corollaries 7.1.1 and 7.1.3 of [3]), one can verify that the following diagram commutes:

$$\begin{array}{ccc} A(L) & \longrightarrow & Gal(H(L)/L) \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle res_{|H(K)}} \\ A(K) & \longrightarrow & Gal(H(K)/K) \end{array}$$

Here the horizontal maps are isomorphisms given by the Artin symbol of $H(K)/K$ and $H(L)/L$, respectively. Furthermore, $res_{|H(K)}$ denotes the restriction of $Gal(H(L)/L)$ to $H(K)$. This readily proves the statements (i) and (ii). □

Now suppose that L/K is an abelian extension such that $H(K) \cap L = K$, then $N_{L/K} : A(L) \to A(K)$ is surjective. Indeed, we have

Proposition 1.3.4. *Let L/K be an abelian extension such that $H(K) \cap L = K$. Then the following diagram commutes:*

$$\begin{array}{ccc} A(L) & \longrightarrow & Gal(H(L)/L) \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle res_{|H(K)}} \\ A(K) & \longrightarrow & Gal(H(K)/K) \end{array}$$

Again, the horizontal maps are isomorphisms given by the Artin symbol of $H(K)/K$ and $H(L)/L$, respectively.

In particular, $N_{L/K} : A(L) \to A(K)$ is surjective, which implies that $ker N_{L/K}$ is isomorphic to $G(H(L)/H(K)L)$. It follows that $|ker N_{L/K}| = [H(L) : H(K)]/[L : K]$.

Proof. See Theorem 5, page 400, of [8]. □

The two propositions from above show that the group theoretic equivalent to the norm map is the restriction map. This poses the natural question what the group theoretical equivalent to the lift of ideal classes is. When L/K is unramified and abelian, a celebrated theorem due to Artin yields the answer. Before we state it, we need the definition of the *transfer of groups*. We have

Definition: Let G be a finite group and H be a subgroup of G. Let R be a system of representatives of left cosets of H in G. For some $\sigma \in G$, we may write for each $\rho \in R$:

$$\sigma\rho = \rho'\sigma_\rho, \text{ for some } \sigma_\rho \in H \text{ and } \rho' \in R.$$

Then we define the transfer of G to H in the following way:

$$Ver_{G\to H} : G/G' \to H/H', \ (\sigma \ mod \ G') \mapsto \prod_{\rho\in R} \sigma_\rho \ mod \ H'.$$

Here G' and H' denote the respective commutator subgroups. The notation Ver comes from the German word *Verlagerung*. This map yields a well-defined group homomorphism, cf. [37].

We are now prepared to state

Theorem 1.3.5 (Artin)**.** *Let L/K be an unramified abelian extension. Then the following diagram is commutative:*

$$\begin{array}{ccc} A(L) & \longrightarrow & Gal(H(L)/L) \\ \uparrow{\scriptstyle \imath_{L/K}} & & \uparrow{\scriptstyle Ver_{G(H(L)/K)\to G(H(L)/L)}} \\ A(K) & \longrightarrow & Gal(H(K)/K) \end{array}$$

The horizontal maps are isomorphisms given by the Artin symbol of $H(K)/K$ and $H(L)/L$, respectively. Also, note that $G(H(L)/H(K))$ is the commutator subgroup of $G(H(L)/K)$.

Proof. Cf. page 285, of [3]. □

Remark: This result reduces the capitulation problem to a purely group theoretical problem. Many major contributions to the capitulation problem have been made by using group theory and analyzing the kernel of the transfer. Also in our treatise, group theory and the transfer of groups will play a decisive role.

Proposition 1.3.6. *Let E/K be a Galois extension with Galois group G and let $\mathfrak{J}_K$, $\mathfrak{J}_E$ denote the corresponding groups of fractional ideals. Then*

$$(\mathfrak{J}_E^G : \mathfrak{J}_K) = \prod_{\mathfrak{p}} e_{\mathfrak{p}},$$

where $\mathfrak{J}_E^G$ are the G-invariant ideals in E, $\mathfrak{p}$ runs through the set of finite primes in K and $e_{\mathfrak{p}}$ denotes the ramification index of $\mathfrak{p}$ in E/K. Moreover, we identify $\mathfrak{J}_K$ with $\imath_{E/K}(\mathfrak{J}_K)$.

Proof. See Remark 6.8.1, page 109, of [3]. □

Theorem 1.3.7 (Chebotarev's Density Theorem)**.** *Let L/K be a Galois extension of number fields with Galois group G. For each $\sigma \in G$, we may consider the set $S_{L/K}(\sigma)$ of all primes $\mathfrak{p}$ in K being unramified in L such that there exists a prime $\mathfrak{P}|\mathfrak{p}$ in L with*

$$\sigma = \left(\frac{L/K}{\mathfrak{P}}\right).$$

Let $[\sigma]$ denote the conjugacy class of $\sigma \in G$. Then $S_{L/K}(\sigma)$ has the Dirichlet density

$$d(S_{L/K}(\sigma)) = \frac{|[\sigma]|}{|G|}.$$

In particular, each $\sigma \in G$ is Frobenius automorphism for $\mathfrak{P}$ for infinitely many primes $\mathfrak{P}$ in L.

Proof. See Theorem 13.4.6, page 290, of [3]. □

Theorem 1.3.8. *Let L/K and K'/K be extensions lying in the algebraic closure $\bar{K}$ of K and $L' = LK'$. Suppose that L/K is unramified. Then L'/K' is also unramified.*

Proof. See Theorem 7.2, page 160, of [2]. □

We now introduce some basic concepts of Galois cohomology. A theorem by Iwasawa will show that there is a direct link between Galois cohomology and the capitulation problem.

Let G be a finite group and A be a G-module, denoted multiplicatively. Then

$$A^G = \{x \in A : x^\sigma = x, \ \forall \ \sigma \in G\}$$

is the fix module of A by G. Also we define the norm of $x \in A$ as

$$N_G(x) = \prod_{\sigma \in G} x^\sigma.$$

Clearly, $N_G(A) \subset A^G$ and we define

$$\mathcal{H}^0(G, A) = A^G / N_G(A).$$

We call $\mathcal{H}^0(G, A)$ the 0-th cohomology group of G with coefficients in A. Next, we define the first cohomology group: A map $\sigma \mapsto a_\sigma$ from G to A satisfying the property that $a_{\sigma\tau} = a_\sigma^\tau a_\tau$, $\forall$ σ,$\tau \in G$, is called a cocycle of G to A. Let $C^1(G, A)$ denote the set of cocycles of G to A, which form a group in the obvious way.
In addition, for each $a \in A$, we have a map $\sigma \mapsto a^{\sigma-1}$ from G to A. It is called a coboundary of G in A. The group of such couboundaries is denoted by $B^1(G, A)$, which is clearly a subgroup of $C^1(G, A)$. We then define

$$\mathcal{H}^1(G, A) = C^1(G, A)/B^1(G, A),$$

which we call the first cohomology group of G in A. Last but not least, we define $\mathcal{H}^{-1}(G, A)$. To this end, we set

$$I_G(A) =< \{a^{\sigma-1} : \ a \in A, \ \sigma \in G\} >,$$

the subgroup of A which is generated by all elements of the form $a^{\sigma-1}$. One easily verifies that $I_G(A)$ is a submodule of the G-module A. Then we set

$$\mathcal{H}^{-1}(G, A) = ker N_G / I_G(A).$$

The following theorem connects $\mathcal{H}^{-1}(G, A)$ and $\mathcal{H}^1(G, A)$ supposing that G is cyclic. We have

Theorem 1.3.9. *Let G be a cyclic group and A be a G-module. Then*

$$\mathcal{H}^1(G, A) \cong \mathcal{H}^{-1}(G, A).$$

Proof. See page 152, Theorem 8.1.9, of [3]. □

Definition: Let G be a cyclic group. For a G-module A, we call

$$h(G, A) = \frac{|\mathcal{H}^0(G, A)|}{|\mathcal{H}^1(G, A)|}$$

the *Herbrand quotient* of A provided that $\mathcal{H}^0$ and $\mathcal{H}^1$ are finite groups.

Theorem 1.3.10. *Let L/K be a cyclic Galois extension with Galois group G and groups of units $\mathcal{O}_K^*$, $\mathcal{O}_L^*$, respectively. Then*

$$|\mathcal{H}^1(G, \mathcal{O}_L^*)| = [L : K] \cdot |\mathcal{H}^0(G, \mathcal{O}_L^*)|.$$

Proof. See Theorem 8.3.4, page 160, of [3]. Then the proof follows for $S = S_\infty$. □

Theorem 1.3.11 (Hassescher Normensatz)**.** *Let L/K be a cyclic field extension. An element $x \in K^*$ is a norm if and only if it is norm of each completion $L_{\mathfrak{P}}/K_{\mathfrak{p}}$, $\mathfrak{P}|\mathfrak{p}$.*

Proof. See Corollary 4.5, page 401, of [2]. □

Proposition 1.3.12. *Let L/K be a cyclic unramified extension of local fields. Then:*

$$\mathcal{H}^0(Gal(L/K), \mathcal{O}_L^*) = \{1\}.$$

Proof. See Corollary 1.2, page 335, of [2]. □

Corollary 1.3.13. *Let L/K be a cyclic unramified field extension. Then $\mathcal{O}_K^* \subset N_{L/K}(L^*)$.*

Proof. The proof follows immediately from Theorem 1.3.11 and Proposition 1.3.12, observing that L/K being unramified implies that $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is unramified as well. □

Theorem 1.3.14 (Tannaka-Terada)**.** *Let k/k_0 be a cyclic extension (not necessarily unramified) and K be the genus field of k/k_0, i.e. the maximal unramified extension of k that is abelian over k_0. Then the ideals of k belonging to a $Gal(k/k_0)$-invariant ideal class of k become principal ideals in K.*

Proof. See Corollary 4, page 310, of [4]. □

In [4], Miyake shows that the above statement does not hold in general, when k/k_0 is just abelian. So the assumption that k/k_0 is cyclic is essential here. But at least, we have the following result due to Hisako Furuya:

Theorem 1.3.15. *Let $K/\mathbb{Q}$ be an abelian extension with Galois group G. Then all G-invariant ideals in K capitulate in the genus field of $K/\mathbb{Q}$.*

Proof. See [31]. □

At this point, we remark that one always has to distinguish between ideals and ideal classes. For instance, the above theorem does not yield that all G-invariant ideal classes capitulate in the genus field of $K/\mathbb{Q}$.

By Artin's theorem, the capitulation problem can be transferred to a purely group theoretical problem. The transition to group theory allows one to interpret capitulation kernels as transfer kernels. More precisely: Let G be a finite group, then a finite abelian group X is a *transfer kernel* for G if there exists an exact sequence of multiplicatively written groups

$$1 \to A \hookrightarrow H \to G \to 1$$

with A finite abelian such that X is isomorphic to the kernel of the transfer homomorphism $H/[H,H] \to A$. We have

Theorem 1.3.16 (Suzuki)**.** *If G is a finite abelian group, then the finite additive group X is a transfer kernel for G if and only if $|G|X = 0$ and $|G|$ divides $|X|$.*

Proof. The proof is originally due to Hiroshi Suzuki. Another proof can be found in [5], page 220 et seq.. □

We can apply the above theorem in the following context: Let L/K be an unramified abelian extension. Furthermore, we set $H = Gal(H(L)/K)$, $A = Gal(H(L)/L)$, and $G = Gal(L/K)$. It then follows that

$$1 \to A \hookrightarrow H \to G \to 1$$

is an exact sequence. By Artin's Theorem, we obtain that $Ver_{H\to A}$ is a transfer kernel for G and hence $[L:K]$ divides the order of the capitulation kernel of L/K. As a special case of Suzuki's Theorem, we obtain

Theorem 1.3.17 (Principal Ideal Theorem)**.** *Let K be an algebraic number field with ideal class group $Cl(K)$ and Hilbert class field $H(K)$. Then $Cl(K)$ capitulates completely in $H(K)$.*

In Chapter 5, we will need some basic knowledge of Representation Theory, Kummer Theory, and p-adic analysis. All relevant results will be outlined in the beginning of the respective section. Chapter 7 requires some basic insight into Iwasawa Theory. All necessary results will be given in the introduction of that chapter.

Chapter 2

Galois Cohomology and Furtwängler's Theorem for Unramified Cyclic Extensions

This chapter deals with cyclic p-extensions L/K, where p is some fixed prime. We set $G = Gal(L/K)$ generated by some $\sigma \in G$ and define $s = \sigma - 1$. We then introduce some basic ideas of Galois cohomology and show how the 0-th and first cohomology groups $\mathcal{H}^0(G, \mathcal{O}_L^*)$ and $\mathcal{H}^1(G, \mathcal{O}_L^*)$ are closely linked with the capitulation kernel of L/K. To this end, we establish a relation between $\mathcal{H}^0(G, \mathcal{O}_L^*)$ and the G-invariant ideal classes of L, the proof of which seems original. Afterward, we follow the ideas of Iwasawa and show that $\mathcal{H}^1(G, \mathcal{O}_L^*)$ is isomorphic to the capitulation kernel $P_K(L)$ if L/K is unramified. We then use these tools to obtain a rather short and modern proof of a theorem due to Furtwängler, which is essentially a version of Hilbert 90 for ideal classes for the case that L/K is unramified. We also state and prove Chevalley's Theorem which is a generalization of Furtwängler's Theorem to ramified cyclic extensions. In this context, we also shortly address the capitulation problem in the case that L/K is ramified, and discuss which additional factors influence the cardinality of the capitulation kernel. Having established this result, we say that a cyclic field extension L/K as above satisfies the Furtwängler-property (or short F-property) if $ker N_{L/K} = A(L)^s$. Subsequently, we draw several interesting conclusions arising from the F-property: We show that a number field K with cyclic ideal class group $A(K)$ has a Hilbert class field tower of length 1, i.e. the Hilbert class field $H(K)$ of K has trivial ideal class group. Moreover, we analyze the structure of $A(L)^s$, give an upper bound for the rank of $A(L)^s$ and $A(L)$, and decompose $A(L)^s$ into a direct product of cyclic $\mathbb{Z}[s]$-submodules of $A(L)$, which we will call $\mathbb{Z}[s]$-cycles. In this context, we introduce the concept of exact and non-exact

$\mathbb{Z}[s]$-cycles and show that non-exact $\mathbb{Z}[s]$-cycles give rise to non-capitulating ideal classes in $A(K)$. Thus, we link the capitulation problem with the problem of verifying if certain $\mathbb{Z}[s]$-cycles are exact or not. Throughout this chapter, we apply the computer algebra system MAGMA to compute several concrete examples of unramified cyclic extensions and its capitulation kernels. We also illustrate that most of the results in this chapter cannot be generalized to non-cyclic abelian unramified extensions.

2.1 $\mathcal{H}^0(G, \mathcal{O}_L^*) \cong A(L)^G / \imath_{L/K}(A(K))$

In this section, we want to establish a correlation between the 0-th Galois cohomology group $\mathcal{H}^0(G, \mathcal{O}_L^*)$ and the G-invariant ideal classes in L, where L/K is an unramified cyclic extension with Galois group G. The result that we prove is interesting in its own right, but it will also contribute to a particularly easy and modern proof of a theorem due to Furtwängler.

We begin with an easy proposition. It is basically a version of Hilbert 90 for ideals. We have

Proposition 2.1.1. *Let L/K be an unramified cyclic extension with Galois group G generated by some $\sigma \in G$, and $I \in \mathcal{J}_L$ an ideal with $N_{L/K}(I) = (1)$. Then there is an ideal $J \in \mathcal{J}_L$ with*

$$I = J^{\sigma-1}.$$

Moreover, J is uniquely determined up to lifts of $\mathcal{J}_K$.

Proof. Let $I = \prod_i^k \mathcal{P}_i^{\theta_i}$, where $\theta_i \in \mathbb{Z}[Gal(L/K)/\mathcal{D}_{\mathcal{P}_i|P_i}]$ and $\mathcal{P}_i$ prime ideals in L lying above distinct prime ideals P_i in K. Obviously, $N_{L/K}(I) = (1)$ implies that $N_{L/K}(\mathcal{P}_i^{\theta_i}) = (1)$, $\forall\ 1 \leq i \leq k$. Thus, it is sufficient to prove the proposition for $k = 1$. Let $\mathcal{P} = \mathcal{P}_1$, $P_1 = P$ with $\mathcal{P}_1|P_1$, and $\theta_1 = \theta = \sum_{j=0}^{l} \lambda_j \sigma^j$, where l is the order of σ in $Gal(L/K)/\mathcal{D}_{\mathcal{P}|P}$. Since $N_{L/K}(\mathcal{P}) = N_{L/K}(\mathcal{P}^\sigma)$, it follows that $N_{L/K}(\mathcal{P}^\theta) = P^{f_{\mathcal{P}|P} \sum_{j=0}^{l} \lambda_j}$, where $f_{\mathcal{P}|P}$ denotes the residue degree of $\mathcal{P}|P$. As $N_{L/K}(I) = (1)$, we obtain that $\sum_{j=0}^{l} \lambda_j = 0$. Henceforth, let $J := \mathcal{P}^{\sum_{j=0}^{l} \mu_j \sigma^j}$, $\mu_j \in \mathbb{Z}$, and assume that $I = J^{\sigma-1}$. We now show how to choose the μ_j's such that $I = J^{\sigma-1}$ holds. We have

$$J^{\sigma-1} = \mathcal{P}^{(\mu_l - \mu_0) + (\mu_0 - \mu_1)\sigma + \cdots + (\mu_{l-1} - \mu_l)\sigma^l}.$$

By the assumption that $I = J^{\sigma-1}$, it follows that

$$\begin{aligned} \mu_l - \mu_0 &= \lambda_0 \\ \mu_0 - \mu_1 &= \lambda_1 \\ &\cdots \\ \mu_{l-1} - \mu_l &= \lambda_l. \end{aligned}$$

This system of equation is obviously solvable if and only if $\sum_{j=0}^{l} \lambda_j = 0$. In this case, the $\mu_j's$ are unique up to a constant in $\mathbb{Z}$. This implies that J is uniquely determined modulo lifts of $\mathcal{J}_K$ as L/K is unramified (cf. Proposition 1.3.6). This finishes the proof. □

Theorem 2.1.2. *Let L/K be a cyclic unramified extension with Galois group G and notations from above. Then we have:*

$$\mathcal{H}^0(G, \mathcal{O}_L^*) \cong A(L)^G/\imath_{L/K}(A(K)). \tag{2.1}$$

Proof. In what follows, we explicitly state a group isomorphism between the above groups: Let $e \in \mathcal{O}_K^*$. By Corollary 1.3.13, there is an $x \in L^*$ with $N_{L/K}(x) = e$. Since $N_{L/K}((x)) = (e) = (1)$, the previous proposition yields that there is an ideal $I \in \mathcal{J}_L$ with $(x) = I^{\sigma-1}$, where σ is a generator of G. Then we map e to $[I]$, where $[I]$ denotes the ideal class generated by I. As $(x) = I^{\sigma-1}$, it follows that $[I] = [I]^\sigma$ in $A(L)$. This yields a map

$$\Psi : \mathcal{H}^0(G, \mathcal{O}_L^*) \to A(L)^G/\imath_{L/K}(A(K)),$$

$$e \mapsto [I] \ mod \ \imath_{L/K}(A(K)).$$

We will show that it is a well-defined group isomorphism:
1. Ψ is well-defined: Let e_1, $e_2 \in \mathcal{O}_K^*$ with $e_1 \equiv e_2 \ mod \ (N_{L/K}(\mathcal{O}_L^*))$. Let $x_1, x_2 \in L^*$ with $N_{L/K}(x_1) = e_1$, $N_{L/K}(x_2) = e_2$. By assumption, we obtain that $N_{L/K}(x_1/x_2) = N_{L/K}(x)$, for some $x \in \mathcal{O}_L^*$, yielding $N_{L/K}(x_1/(x_2x)) = 1$. Since L/K is cyclic, Hilbert's Theorem 90 implies that there is an $y \in L^*$ with $x_1/(x_2x) = y^{\sigma-1}$. It follows that $(x_1) = (x_2)(y)^{\sigma-1}$, observing that $(x) = 1$ due to $x \in \mathcal{O}_L^*$. Now let $(x_1) = I_1^{\sigma-1}$ and $(x_2) = I_2^{\sigma-1}$, with I_1, $I_2 \in \mathcal{J}_L$. Hence, $I_1^{\sigma-1} = I_2^{\sigma-1}(y)^{\sigma-1}$. Proposition 1.3.6 then yields that $I_1 \equiv I_2(y) \ mod \ \imath_{L/K}(\mathfrak{J}_K)$, implying that $[I_1] \equiv [I_2] \ mod \ \imath_{L/K}(A(K))$.

2. Ψ is a group homomorphism: Let e_1, $e_2 \in \mathcal{O}_K^*$, and $x_1, x_2 \in L^*$ with $N_{L/K}(x_1) = e_1$, $N_{L/K}(x_2) = e_2$. Moreover, let $(x_1) = I_1^{\sigma-1}$ and $(x_2) = I_2^{\sigma-1}$, with I_1, $I_2 \in \mathcal{J}_L$. Now we can conclude that $N_{L/K}(x_1x_2) = e_1e_2$, and hence $(x_1x_2) = (I_1I_2)^{\sigma-1}$. It follows that $\Psi(e_1e_2) = [I_1][I_2] = \Psi(e_1)\Psi(e_2)$.

3. Ψ is bijective: Let $e \in \mathcal{O}_K^*$ with $N_{L/K}(x) = e$, $(x) = J^{\sigma-1}$, and $J \in \mathfrak{J}_K$. Hence, $J^{\sigma-1} = (1)$, which implies that $x \in \mathcal{O}_L^*$ due to $(x) = (1)$. It follows that $e \in N_{L/K}(\mathcal{O}_L^*)$ and hence Ψ is injective.
Now let $J \in \mathcal{J}_L$ with $[J]^\sigma = [J]$. Then there is an $x \in L^*$ with $J^\sigma = J(x)$, i.e. $(x) = J^{\sigma-1}$. This implies that $N_{L_K}(x) = e$, for some $e \in \mathcal{O}_K^*$. Finally, $\Psi(e) = [J]\ mod\ \imath_{L/K}(A(K))$, i.e. Ψ is surjective. This finishes the proof. $\square$

Remark: The above theorem does not hold in general if L/K is unramified and just abelian:

Example: Let $K = \mathbb{Q}(\alpha)$ with $\alpha^2 + 3896 = 0$. Then MAGMA yields:
1. $A(K) =< a_1, a_2 > \cong C_3 \times C_3$.
2. $A(H(K))$ is non-trivial.
Since K is imaginary quadratic, it follows that $\mathcal{H}^0(Gal(H(K)/K)) = \{1\}$. Moreover, $\imath_{H(K)/K}(A(K)) = \{1\}$ by the Principal Ideal Theorem. Let G denote the Galois group of $H^{(2)}(K)/K$. Then G has the commutator subgroup $G' = Gal(H^{(2)}(K)/H(K))$. Section 2.5 then, however, implies that $G' \cap Z(G) \neq \{1\}$ and hence $A(H(K))^{G(H(K)/K)} \neq \{1\}$.

2.2 Iwasawa's Theorem

In what follows, we derive Iwasawa's Theorem. It yields a direct link between the first cohomology group $\mathcal{H}^1(Gal(L/K), \mathcal{O}_L^*)$ and the capitulation kernel of L/K. In the following, we basically follow the ideas of Iwasawa, cf. [14]. We have

Theorem 2.2.1 (Iwasawa)**.** *Let L/K be an unramified cyclic extension with Galois group G and let $\mathcal{O}_L^*$ denote the group of units of $\mathcal{O}_L$. Then*

$$P_K(L) \cong \mathcal{H}^{-1}(G, \mathcal{O}_L^*). \tag{2.2}$$

Proof. Let $\sigma \in G$ be a generator of G and set $\mathcal{C} = \{x \in \mathcal{O}_L^* |\ N_{L/K}(x) = 1\}$. Then we obtain that

$$\mathcal{H}^{-1}(G, \mathcal{O}_L^*) = \mathcal{C}/(\mathcal{O}_L^*)^{\sigma-1}.$$

Now let $x \in \mathcal{C}$. By Hilbert 90, it follows that there exists some $y \in L^*$ such that $y^{\sigma-1} = x$. Since $x \in \mathcal{O}_L^*$, it follows that $(y)^\sigma = (y)$. Let $\mathcal{P}_K$ and $\mathcal{P}_L$ denote the principal ideals of K and L, respectively. Then one easily verifies that the above map yields a well-defined group isomorphism

$$\Psi : \mathcal{C}/(\mathcal{O}_L^*)^{\sigma-1} \to \mathcal{P}_L^G/\mathcal{P}_K.$$

Also, we can conclude that $\mathcal{P}_L^G/\mathcal{P}_K \cong P_K(L)$. Indeed, let $J = (\alpha) \in \mathcal{P}_L^G$. By Proposition 1.3.6, it follows that there is a unique $I \in \mathcal{J}_K$ such that $\imath_{L/K}(I) = J = (\alpha)$. This yields the isomorphisms

$$\mathcal{P}_L^G/\mathcal{P}_K \cong P_K(L) \cong \mathcal{H}^{-1}(G, \mathcal{O}_L^*),$$

and thus the desired statement. □

Remark: Iwasawa's Theorem is actually even more general. For a given Galois extension L/K with Galois group G, it asserts that

$$\mathcal{P}_L^G/\mathcal{P}_K \cong \mathcal{H}^1(G, \mathcal{O}_L^*).$$

However, the isomorphism $\mathcal{P}_L^G/\mathcal{P}_K \cong P_K(L)$ only holds when L/K is unramified. And

$$\mathcal{H}^1(G, \mathcal{O}_L^*) \cong \mathcal{H}^{-1}(G, \mathcal{O}_L^*)$$

only holds when L/K is cyclic.

2.3 Hilbert's Theorem 94 and Furtwängler's Theorem

In this section, we make use of the results of the Sections 2.1 and 2.2 to prove Hilbert's Theorem 94 and Furtwängler's Theorem. Hilbert's Theorem 94 is essentially the cornerstone of the capitulation problem. It says that the capitulation kernel $P_K(L)$ is non-trivial in the case that L/K is an unramified cyclic extension. Furtwängler's Theorem is the key ingredient to prove the existence of Hilbert class fields. It is basically a version of Hilbert 90 for ideal classes. We begin with a result that comprises Hilbert's Theorem 94 as it not only shows that $P_K(L)$ is non-trivial, but also yields a concrete formula for the cardinality of the capitulation kernel. We have

Theorem 2.3.1. *Let L/K be an unramified cyclic extension with Galois group G. Then*

$$|P_K(L)| \;=\; [L:K] \cdot |\mathcal{H}^0(G, \mathcal{O}_L^*)|. \tag{2.3}$$

Proof. In light of Iwasawa's Theorem, we obtain that $|P_K(L)| = |\mathcal{H}^1(G, \mathcal{O}_L^*)|$. Since L/K is cyclic, Herbrand's Theorem yields that

$$|\mathcal{H}^1(G, \mathcal{O}_L^*)| = [L:K] \cdot |\mathcal{H}^0(G, \mathcal{O}_L^*)|.$$

Combing these results, we obtain the desired statement. □

This poses the natural question if equation (2.3) also holds for a non-cyclic unramified abelian extension L/K. The following example illustrates that this is not the case in general.

Example: Consider the imaginary quadratic number field

$$K = \mathbb{Q}(\sqrt{-8867 \cdot 73681}).$$

MAGMA yields that $A(K)_3 \cong C_3 \times C_3 \times C_3 \times C_3$. Theorem 2, page 747, of [19], says that there exist at least 81 subfields L_j, $1 \leq j \leq 81$, of $H(K)_3$ such that $[H(K)_3 : L_j] = 9$ and $A(K)_3$ capitulates completely in L_j. On the other hand, Dirichlet's Unit Theorem yields that $\mathcal{H}^0(Gal(L_j/K), \mathcal{O}_{L_j}^*)$ is trivial as K is imaginary quadratic. It follows that

$$|P_K(L_j)| = 81 \neq 9 = [L_j : K] \cdot |\mathcal{H}^0(Gal(L_j/K), \mathcal{O}_{L_j}^*)|.$$

In the remainder of this section, we want to deduce Furtwängler's Theorem. This theorem seems to be rather unknown but is very important for the entire future chapters. While it was quite easy to establish Hilbert 90 for ideals, Hilbert 90 for ideal classes is a rather deep-seated theorem. We have

Theorem 2.3.2 (Furtwängler)**.** *Let L/K be a cyclic unramified field extension with Galois group G generated by some $\sigma \in G$. Then*

$$ker N_{L/K} = A(L)^{\sigma-1}.$$

Proof. Combining the results of (2.1) and (2.3), we derive that

$$|P_K(L)| = [L : K] \cdot \frac{|A(L)^G|}{|\imath_{L/K}(A(K))|}.$$

Since $|\imath_{L/K}(A(K))| = |A(K)|/|P_K(L)|$, it follows that

$$[H(K) : K] = |A(K)| = [L : K] \cdot |A(L)^G|,$$

i.e. $|A(L)^G| = [H(K) : L]$. Likewise, we know that $ker N_{L/K}$ is isomorphic to $Gal(H(L)/H(K))$ by Proposition 1.3.3 and thus

$$|ker N_{L/K}| = [H(L) : H(K)].$$

Due to the isomorphism $A(L)/A(L)^G \cong A(L)^{\sigma-1}$, it follows that $|A(L)^{\sigma-1}| = [H(L) : H(K)]$ and hence $ker N_{L/K} = A(L)^{\sigma-1}$. □

Corollary 2.3.3. *Notations being like above, it follows that*

$$|A(L)^G| = [H(K) : L].$$

Proof. See the proof of the above theorem. □

Remark: However, $A(L)^G$ and $Gal(H(K)/L))$ are in general not isomorphic:

Example: Consider the imaginary quadratic number field

$$K = \mathbb{Q}(\alpha) \text{ with } \alpha^2 + 11651 = 0.$$

Using MAGMA, we obtain that: 1. $A(K) =< a_1, a_2 > \cong C_3 \times C_9$;
2. We define $L = H(K)^{<a_2>}$ and obtain $A(L) \cong C_3 \times C_9 \times C_{27}$;
3. $P_K(L) =< a_2^3 >$ which implies that $\imath_{L/K}(A(K)) = A(L)^{G(L/K)} \cong C_3 \times C_3$;
On the contrary, $N_{L/K}(A(L)) \cong C_9$.

Definition: We say a cyclic extension L/K, with Galois group G generated by some $\sigma \in G$, satisfies the *Furtwängler-property* (or short F-property) if

$$ker N_{L/K} = A(L)^{\sigma-1}.$$

As we have seen, if L/K is unramified and cyclic, then L/K has the F-property. Moreover, Chevalley's Theorem (see next section) shows that it also holds in the case that L/K is cyclic and only one prime in K ramifies in L.

Remark: 1) One can also use Iwasawa's Theorem and Furtwängler's Theorem to prove Herbrand's Theorem, i.e. the various proofs are somewhat circular.

2) Note that the Hilbert class field $H(K)$ of K is the genus field of L/K, i.e. it is the maximal unramified abelian extension of L which is abelian over K. The theorem of Tannaka-Terada then implies that $A(L)^G \subset P_L(H(K))$, where $P_L(H(K))$ denotes the capitulation kernel of $H(K)/L$. In view of that, the result of (2.1) shows that $\mathcal{H}^0(Gal(L/K), \mathcal{O}_L^*)$ yields interesting information on the structure of $P_L(H(K))$. Moreover, observe that $[H(K) : L] = |A(L)^G|$ divides $|P_L(H(K))|$ (verifying the theorem due to Suzuki in that case).

One natural question that emerges is whether a version of Furtwängler's theorem is also true for an unramified abelian field extensions L/K which is not cyclic. Again it makes sense to consider ideals first and ideal classes

afterward. We start with the definition of an augmentation ideal and a basic result on it:

For the ring homomorphism

$$\phi : \mathbb{Z}[G(L/K)] \to \mathbb{Z}, \sum_{\sigma \in G(L/K)} \lambda_\sigma \sigma \mapsto \sum_{\sigma \in G(L/K)} \lambda_\sigma$$

we define the augmentation ideal $Aug(G(L/K))$ to be the kernel of ϕ. We have the following useful result:

Proposition 2.3.4. *Let G be a finite group generated by a system $\{\sigma_1, ..., \sigma_n\}$. Then*

$$Aug(G) = \mathbb{Z}(\sigma_1 - 1) + ... + \mathbb{Z}(\sigma_n - 1).$$

Proof. The proof is elementary and straightforward. □

We are now prepared to state and prove the next

Proposition 2.3.5. *Let L/K be an abelian field extension with Galois group $G =< \sigma_1, ..., \sigma_n >$ and $I \in \mathfrak{J}_L$ be an ideal with $N_{L/K}(I) = (1)$. Then there exist ideals $I_1, ..., I_n \in \mathfrak{J}_L$ such that*

$$I = I_1^{\sigma_1 - 1} \cdot I_2^{\sigma_2 - 1} \cdot \ldots \cdot I_n^{\sigma_n - 1}.$$

Proof. Let $I = \prod_{i=1}^n \mathfrak{P}_i^{\theta_i}$, where $\mathfrak{P}_i$ are primes in L lying above distinct primes P_i in K and for some $\theta_i = \sum_{\sigma \in G(L/K)} \lambda_{\sigma,i}\sigma$. Since $N_{L/K}(I) = (1)$, it follows, $\forall\ i = 1, .., n$:

$$1 = P_i^{\sum_{\sigma \in G(L/K)} \lambda_{\sigma,i}}, \text{ and hence}$$

$$\sum_{\sigma \in G(L/K)} \lambda_{\sigma,i} = 0.$$

By the previous proposition, we obtain for all $i = 1, .., n$:

$$\theta_i = \sum_{\sigma \in G(L/K)} \lambda_{\sigma,i}\sigma \in \mathbb{Z}(\sigma_1 - 1) + ... + \mathbb{Z}(\sigma_n - 1).$$

Rearranging the terms, we can conclude that there exist ideals $I_1, ..., I_n \in \mathfrak{J}_L$ such that

$$I = I_1^{\sigma_1 - 1} \cdot I_2^{\sigma_2 - 1} \cdot \ldots \cdot I_n^{\sigma_n - 1}.$$

□

A version of the above proposition for ideal classes does not hold, however, as the following example shows: Let K be a number field such that the Galois group $Gal(H(K)/K) =< \sigma_1, \sigma_2 > \cong C_p \times C_p$ and such that $A(H(K))$ is non-trivial. By Proposition 1.3.3, we know that $kerN_{H(K)/K} \cong A(H(K))$. Assume that

$$kerN_{H(K)/K} = A(H(K))^{\sigma_1 - 1} \cdot A(H(K))^{\sigma_2 - 1}.$$

Since $A(H(K))^{(\sigma_i - 1)^{p^l}} = \{1\}$, for $i = 1, 2$, and sufficiently large l, one easily verifies that $A(H(K))$ must be trivial then, a contradiction to the assumption. This example illustrates that there is no generalization of Furtwängler's Theorem to the abelian case whatsoever. Moreover, we learn that

$$|N_{H(K)/K}(A(H(K)))| = \{1\} \neq |A(H(K))^{G(H(K)/K)}|.$$

The first equality is obvious and the second inequality follows easily: Indeed, let $H^{(2)}(K)$ be the Hilbert class field of $H(K)$ and $G = Gal(H^{(2)}(K)/K)$. Then $\{1\} \neq G' = Gal(H^{(2)}(K)/H(K))$. By Theorem 2.5.5, it follows that $Z(G) \cap G' \neq \{1\}$ and hence the statement.

2.4 Chevalley's Theorem and Capitulation in Ramified Cyclic Extensions

Henceforth, we want to allow arbitrary cyclic extensions of number fields, i.e. we do not necessarily assume that the given field extension is unramified anymore. The main theorem in this context is Chevalley's Theorem.

From now on, let L/K be a general cyclic extension with $G = Gal(L/K)$ generated by some $\sigma \in G$. Let $\mathcal{J}_L^G$ be the group of G-invariant ideals in L, and $[\mathcal{J}_L^G]$ be the image of $\mathcal{J}_L^G$ in $\mathcal{J}_L/\mathcal{P}_L$, where $\mathcal{P}_L$ are the principal ideals in L. Accordingly, $\mathcal{P}_L^G$ denotes the G-invariant principal ideals.
Let $e_0(L/K) = \prod_{\mathfrak{p}} e_{\mathfrak{p}}$, where $\mathfrak{p}$ runs through the set of finite primes in K and $e_{\mathfrak{p}}$ denotes the ramification index of $\mathfrak{p}$. Also, we set $e_\infty(L/K) = \prod_{\mathfrak{p}_\infty} f_{\mathfrak{p}_\infty}$, where $\mathfrak{P}_\infty$ runs through the set of infinite primes in L lying above $\mathfrak{p}_\infty$ in K and where $f_{\mathfrak{p}_\infty} := [L_{\mathfrak{P}_\infty} : K_{\mathfrak{p}_\infty}]$ for $\mathfrak{P}_\infty | \mathfrak{p}_\infty$. Finally, we define

$$e(L/K) = e_0(L/K) e_\infty(L/K).$$

Using the results of the previous sections, we obtain the following three results:

$$A(L)^G/[\mathcal{J}_L^G] \;\cong\; (\mathcal{O}_K^* \cap N_{L/K}(L^*))/N_{L/K}(\mathcal{O}_L^*) \tag{2.4}$$

$$\mathcal{H}^1(G, \mathcal{O}_L^*) \;\cong\; \mathcal{P}_L^G/\mathcal{P}_K \tag{2.5}$$

$$\frac{|\mathcal{H}^0(G, \mathcal{O}_L^*)|}{|\mathcal{H}^1(G, \mathcal{O}_L^*)|} = \frac{e_\infty(L/K)}{[L:K]} \tag{2.6}$$

Statement (2.4) follows directly from the proof of Theorem 2.1.2.
The isomorphism (2.5) is an immediate consequence of the proof of Iwasawa's Theorem of Section 2.2.
For result (2.6), see Herbrand's Theorem and apply it to $S = S_\infty$.

Now we are ready to state the main theorem of this section. We have

Theorem 2.4.1 (Chevalley)**.** *Let L/K be a cyclic extension with Galois group G generated by some $\sigma \in G$. As before, let $A(L)^G$ denote the G-invariant ideal classes in $A(L)$. Then*

$$|A(L)^G| = \frac{|A(K)|e(L/K)}{[L:K](\mathcal{O}_K^* : N_{L/K}(L^*) \cap \mathcal{O}_K^*)}.$$

Proof. The proof is quite straightforward. Essentially, we only have to slightly modify the arguments we used for the unramified case. We will make use of the above results, Iwasawa's Theorem and Herbrand's Theorem. Combining them, we eventually obtain the above statement. By virtue of (2.4), it follows that

$$|A(L)^G/[\mathcal{J}_L^G]| \;=\; \frac{|\mathcal{H}^0(G, \mathcal{O}_L^*)|}{(\mathcal{O}_K^* : N_{L/K}(L^*) \cap \mathcal{O}_K^*)}. \tag{2.7}$$

In view of (2.6), we conclude that

$$|A(L)^G| \;=\; \frac{|\mathcal{H}^1(G, \mathcal{O}_L^*)| \cdot e_\infty(L/K) \cdot |[\mathcal{J}_L^G]|}{[L:K] \cdot (\mathcal{O}_K^* : N_{L/K}(L^*) \cap \mathcal{O}_K^*)}. \tag{2.8}$$

Moreover, we have that

$$[\mathcal{J}_L^G] \cong \mathcal{J}_L^G \mathcal{P}_L/\mathcal{P}_L \cong \mathcal{J}_L^G/\mathcal{P}_L^G.$$

Thus, Proposition 1.3.6 yields that

$$\begin{aligned} |\mathcal{H}^1(G, \mathcal{O}_L^*)| \cdot |[\mathcal{J}_L^G]| &= |\mathcal{P}_L^G/\mathcal{P}_K| \cdot |\mathcal{J}_L^G/\mathcal{P}_L^G| \\ &= |\mathcal{J}_L^G/\mathcal{J}_K| \cdot |\mathcal{J}_K/\mathcal{P}_K| \\ &= e_0(L/K)|A(K)|. \end{aligned}$$

Plugging this into equation (2.8), it finally follows that

$$|A(L)^G| = \frac{|A(K)|e(L/K)}{[L:K]\cdot(\mathcal{O}_K^* : N_{L/K}(L^*)\cap\mathcal{O}_K^*)}.$$

This finishes the proof. □

In the remainder of this section, we want to address the capitulation problem for ramified cyclic extensions. In particular, we will analyze which further factors influence the cardinality of the capitulation kernel. Let L/K be as before, $\mathfrak{p}\in K$ be a finite prime, and $\mathfrak{P}|\mathfrak{p}$ be a prime in L lying above $\mathfrak{p}$. Then we define

$$I_{\mathfrak{p}} := \prod_{\tau \ mod \ G_{\mathfrak{P}}} \tau(\mathfrak{P}),$$

where $G_{\mathfrak{P}}$ is the decomposition group of $\mathfrak{P}|\mathfrak{p}$ and $\tau\in G$. Observe that $I_{\mathfrak{p}}$ is independent of the choice for $\mathfrak{P}$. Let us set

$$\lambda(L/K) := \prod_{\mathfrak{p}}(e_{\mathfrak{p}}, ord(I_{\mathfrak{p}})),$$

where $\mathfrak{p}$ runs through the set of finite primes in K, $(e_{\mathfrak{p}}, ord(I_{\mathfrak{p}}))$ denotes the greatest common divisor of $e_{\mathfrak{p}}$ and $ord(I_{\mathfrak{p}})$, and $ord(I_{\mathfrak{p}})$ denotes the order of $I_{\mathfrak{p}}$ in $\mathcal{J}_L/\mathcal{P}_L$. We have

Lemma 2.4.2. *Notations being like above, it follows that*

$$|[\mathcal{J}_L^G]/\imath_{L/K}(A(K))| \ = \ \lambda(L/K). \tag{2.9}$$

Proof. Observe that

$$\begin{aligned}[\mathcal{J}_L^G]/\imath_{L/K}(A(K)) &\cong \mathcal{J}_L^G\mathcal{P}_L/\mathcal{J}_K\mathcal{P}_L \\ &\cong (\mathcal{J}_L^G/\mathcal{J}_L^G\cap\mathcal{P}_L)/(\mathcal{J}_K/\mathcal{J}_K\cap\mathcal{P}_L).\end{aligned}$$

Obviously, for all unramified primes $\mathfrak{p}$ in K, we have that $I_{\mathfrak{p}}\in\mathcal{J}_K$. Thus, we can focus on the ramified primes as possible generators of $[\mathcal{J}_L^G]/\imath_{L/K}(A(K))$. Let $\mathfrak{p}$ be a ramified prime in K and say that n is the order of $I_{\mathfrak{p}}$ in $\mathcal{J}_L/\mathcal{P}_L$. Then $I_{\mathfrak{p}}^{e_{\mathfrak{p}}}$ has the order $n/(n,e_{\mathfrak{p}})$ in $\mathcal{J}_L/\mathcal{P}_L$. Combining these arguments shows that

$$\begin{aligned}|[\mathcal{J}_L^G]/\imath_{L/K}(A(K))| &= \prod_{\mathfrak{p}}\frac{ord(I_{\mathfrak{p}})}{ord(I_{\mathfrak{p}})/(ord(I_{\mathfrak{p}}),e_{\mathfrak{p}})} \\ &= \prod_{\mathfrak{p}}(ord(I_{\mathfrak{p}}),e_{\mathfrak{p}}).\end{aligned}$$

□

Corollary 2.4.3. *With the notations as above, we conclude that*

$$|P_K(L)| = \frac{\lambda(L/K)[L:K]|\mathcal{H}^0(G,\mathcal{O}_L^*)|}{e(L/K)} \leq \frac{[L:K]|\mathcal{H}^0(G,\mathcal{O}_L^*)|}{e_\infty(L/K)}.$$

Proof. Due to the equations (2.7) and (2.9), it follows that

$$|\imath_{L/K}(A(K))| = \frac{|A(L)^G|(\mathcal{O}_K^* : N_{L/K}(L^*) \cap \mathcal{O}_K^*)}{\lambda(L/K) \cdot |\mathcal{H}^0(G,\mathcal{O}_L^*)|}.$$

By the previous theorem, we thus obtain

$$\begin{aligned} |P_K(L)| &= \frac{|A(K)|}{|\imath_{L/K}(A(K))|} \\ &= \frac{\lambda(L/K) \cdot |A(K)| \cdot |\mathcal{H}^0(G,\mathcal{O}_L^*)| \cdot [L:K] \cdot (\mathcal{O}_K^* : N_{L/K}(L^*) \cap \mathcal{O}_K^*)}{(\mathcal{O}_K^* : N_{L/K}(L^*) \cap \mathcal{O}_K^*) \cdot |A(K)| \cdot e(L/K)} \\ &= \frac{\lambda(L/K)[L:K]|\mathcal{H}^0(G,\mathcal{O}_L^*)|}{e(L/K)}. \end{aligned}$$

□

Henceforth, assume that $G = Gal(L/K) =< \sigma >$ and $H(K) \cap L = K$. By Proposition 1.3.4, this assumption implies that $|ker N_{L/K}| = [H(L) : H(K)]/[L : K]$, where $N_{L/K} : A(L) \to A(K)$ is the usual norm map. We can now use the above results to compare $ker N_{L/K}$ with $A(L)^{\sigma-1}$. Since $A(L)^{\sigma-1} \cong A(L)/A(L)^G$, we can derive that

$$|A(L)^{\sigma-1}| = \frac{|A(L)|[L:K](\mathcal{O}_K^* : N_{L/K}(L^*) \cap \mathcal{O}_K^*)}{|A(K)|e(L/K)}.$$

Hence,

$$\begin{aligned} |ker N_{L/K}/A(L)^{\sigma-1}| &= \frac{|A(K)| \cdot e(L/K) \cdot |A(L)|}{|A(K)| \cdot |A(L)| \cdot [L:K] \cdot (\mathcal{O}_K^* : N_{L/K}(L^*) \cap \mathcal{O}_K^*)} \\ &= \frac{e(L/K)}{[L:K](\mathcal{O}_K^* : N_{L/K}(L^*) \cap \mathcal{O}_K^*)}. \end{aligned}$$

We gather the information in

Corollary 2.4.4. *Assume that L/K is a cyclic Galois extension as above such that $H(K) \cap L = K$. Then:*

$$|ker N_{L/K}/A(L)^{\sigma-1}| = \frac{e(L/K)}{[L:K](\mathcal{O}_K^* : N_{L/K}(L^*) \cap \mathcal{O}_K^*)}.$$

Corollary 2.4.5. *Let L/K be a cyclic Galois extension as above. Assume that there is exactly one prime in K that ramifies in L and that this prime is totally ramified. Then:*

(i) $ker N_{L/K} = A(L)^{\sigma-1}$

(ii) $(\mathcal{O}_K^* : N_{L/K}(L^*) \cap \mathcal{O}_K^*) = 1$

(iii) $\mathcal{H}^0(Gal(L/K), \mathcal{O}_L^*) \cong A(L)^{Gal(L/K)}/\imath_{L/K}(A(K))$

Proof. The proof follows from the previous corollary and the fact that $H(K) \cap L = K$ as L/K has a totally ramified prime. □

Remark: 1) Using the notation of the previous section, the extension L/K as in the above corollary satisfies the F-property.

2) For instance, let $L = \mathbb{Q}(\zeta_{p^n})$, where ζ_{p^n} is a primitive p^n-th root of unity (p an odd prime), and $K = \mathbb{Q}$. Then L/K satisfies the F-property.

2.5 Number Fields with Cyclic Class Groups

In what follows, we intend to show that $A(H(K)) = \{1\}$ if $H(K)/K$ is cyclic, i.e. in this case K has a Hilbert class field tower of length 1. We give three different proofs of that as they are all interesting in their own rights. Furthermore, the theory used in these proofs will be of relevance in the future thesis. The first proof uses the results of Section 2.3 and the others apply group theory. Especially, the group theory developed in the two latter proofs plays a major role in the further treatise. We have

Proposition 2.5.1. *Let K be a number field such that $A(K)$ is cyclic. Then $A(H(K)) = \{1\}$.*

Proof. 1. Let $G = Gal(H(K)/K) =< \sigma >$. Appealing to Proposition 1.3.3, we obtain that $A(H(K)) = ker N_{H(K)/K}$. By Furtwängler's Theorem, it thus follows that $A(H(K)) = A(H(K))^{\sigma-1}$. Let $a \in A(H(K))$ and $a = a_1^{\sigma-1}$ for some $a_1 \in A(H(K))$. Now we choose an $a_2 \in A(H(K))$ with $a_1 = a_2^{\sigma-1}$. Iterating this procedure, we obtain for $k \geq 0$ an a_k such that $a = a_k^{(\sigma-1)^k}$. If we choose $k = p^l$ for $l > 0$ sufficiently large, we see that $a = 1$ and thus $A(H(K)) = \{1\}$. □

For the next two proofs of the above proposition we need an interlude on group theory. We begin with the following

Definition: If G is a group, its *Frattini subgroup* $\Phi(G)$ is defined as the intersection of all the maximal subgroups of G. (Since G is finite in our case, G certainly contains a maximal subgroup).

Definition: An element $x \in G$ is called a *nongenerator* if it can be omitted from any generating system: If $G =< x, Y >$, then $G =< Y >$.

Theorem 2.5.2. *For every group G, the Frattini subgroup $\Phi(G)$ is the set of all nongenerators.*

Proof. See Theorem 5.47, page 123, of [9]. □

Theorem 2.5.3. *Let G be a finite Group. Then:*

(i) (Frattini,1885) $\Phi(G)$ is nilpotent.

(ii) If G is a finite p-group, then $\Phi(G) = G'G^p$, where G^p is the subgroup of G generated by all p-th powers.

(iii) If G is a finite p-group, then $G/\Phi(G)$ is a vector space over $\mathbb{F}_p$.

Proof. See Theorem 5.48, page 123, of [9]. □

Definition: A *minimal generating set* of a group G is a generating set X such that no proper subset of X is a generating set of G.

Theorem 2.5.4 (Burnside's Basis Theorem, 1912)**.** *: If G is a finite p-group, then any two minimal generating sets have the same cardinality, namely $dim(G/\Phi(G))$. Moreover, every $x \notin \Phi(G)$ can be extended to a minimal system of generators.*

Proof. See Theorem 5.50, page 124, of [9]. □

Burnside's Basis Theorem yields another way of proving the above proposition. We have

Proof. 2. Recall that K is a number field such that $A(K)$ is cyclic. Let $H^{(2)}(K)$ be the second Hilbert class field of K and set $G = G(H^{(2)}(K)/K)$. By class field theory, the commutator group G' of G is then given by $G' = Gal(H^{(2)}(K)/H(K))$. Since

$$G(H^{(2)}(K))/K)/Gal(H^{(2)}(K)/H(K)) \cong Gal(H(K)/K)$$

is cyclic, $G/\Phi(G) = G/(G'G^p)$ is cyclic a fortiori. By Burnside's Basis Theorem, it follows that G is cyclic as well and hence $H^{(2)}(K)/K$ is an unramified abelian extension. By class field theory, it follows that $H^{(2)}(K) = H(K)$ and hence $A(H(K)) = \{1\}$. □

The last proof uses the theory of central series and nilpotent groups. We start with a fundamental result on finite p-groups (cf. 5.51, page 118, of [9]):

Theorem 2.5.5. *Let G be a finite p-group and $H \subset G$ be a non-trivial normal subgroup. Then*

$$H \cap Z(G) \neq \{1\},$$

where $Z(G)$ denotes the center of G.

Proof. First, we define the *upper central series* of G by induction:

$$\zeta^0(G) = 1,\ \zeta^{i+1}(G)/\zeta^i(G) = Z(G/\zeta^i(G)),\ \text{i.e.}$$

if $h_i :\ G \to G/\zeta^i(G)$ is the natural map, then $\zeta^{i+1}(G)$ is the inverse image of the center. Obviously, $\zeta^1(G) = Z(G)$. Moreover, we can conclude that

$$\zeta^{i+1}(G) = \{z \in G|\ zgz^{-1}g^{-1} \in \zeta^i(G),\ \forall\ g \in G\}.$$

It is well-known that finite p-groups are nilpotent, i.e. there exists some $c \geq 1$ such that

$$\{1\} = \zeta^0(G) \subset \zeta^1(G) \subset ... \subset \zeta^c(G) = G.$$

Furthermore, one verifies that

$$[\zeta^i(G), G] \subset \zeta^{i-1}(G).$$

This follows immediately from the definition. Due to $\zeta^c(G) = G$, there is a minimal $1 \leq m \leq c$ such that $\zeta^m(G) \cap H \neq \{1\}$. Since H is a normal subgroup of G, it follows that

$$(\zeta^m(G) \cap [H, G]) \subset ([\zeta^m(G), G] \cap H) \subset (\zeta^{m-1}(G) \cap (H)) = \{1\}.$$

Hence, $\{1\} \neq \zeta^m(G) \cap H \subset Z(G) \cap H$. This finishes the proof. □

We conclude this section with the third proof. We have

Proof. 3. Let $H^{(2)}(K)$ be the second Hilbert class field of K and set $G = G(H^{(2)}(K)/K)$. By the previous section, we can deduce that

$$|A(H(K))^{G(H(K)/K)}| = |N_{H(K)/K}(A(H(K)))| = 1.$$

Moreover,

$$A(H(K))^{G(H(K)/K)} \cong Gal(H^{(2)}(K)/H(K)) \cap Z(G).$$

It follows that $Gal(H^{(2)}(K)/H(K)) \cap Z(G) = \{1\}$. The previous theorem then yields that $G' = \{1\}$ and hence $A(H(K)) = \{1\}$. □

2.6 $\mathbb{Z}[s]$-Cycles and an Upper Bound for the Rank of $A(L)$

In this section, let L/K be a cyclic extension of prime degree p and we assume that it satisfies the F-property, i.e. $kerN_{L/K} = A(L)^{\sigma-1}$, where σ is a generator of $G = G(L/K)$. Before we begin with the next theorem, we state and prove the following basic results:

Lemma 2.6.1. *Let R be a commutative ring, $x \in R$ nilpotent, and $u \in R^*$ a unit in R. Then: $x + u \in R^*$.*

Proof. First, we show that $1 + x \in R^*$: Setting $x^n = 0$, it follows that

$$\frac{(-x)^n - 1}{-x - 1} = (-x)^{n-1} + (-x)^{n-2} + ... + 1, \text{ i.e.}$$

$$((1 + x)((-x)^{n-1} + (-x)^{n-2} + ... + 1) = 1.$$

Thus, $1 + x$ is a unit in R. We conclude that $x + u = u(u^{-1}x + 1)$. Since $u^{-1}x$ is nilpotent and $u \in R^*$, the claim follows with the arguments from above. □

Proposition 2.6.2. *Let L/K be a cyclic extension of degree p, satisfying the F-property. Let $\sigma \in G(L/K)$ be a generator of $G = G(L/K)$ and $s = \sigma - 1$. Suppose that $exp(A(L)^s) = p^l$, for some $l \in \mathbb{N}$, and let $a \in A(L)$. Setting $R = \mathbb{Z}[s]/(s^{p^l})$, it follows that $A(L)^s$ is an R-module and*

(i) $a^{s^p} = a^{psu}$, for some unit $u \in R^*$.

(ii) $p \cdot ord(a^{s^p}) = ord(a^s)$.

(iii) $\imath_{L/K}(N_{L/K}(a)) = a^{1+\sigma+...+\sigma^{p-1}} = a^{pu'+s^{p-1}}$, $u' \in R^*$.

Proof. We have

$$\begin{aligned} 0 &= \sigma^p - 1 \\ &= (s+1)^p - 1 \\ &= \sum_{k=1}^{p} \binom{p}{k} s^k \\ &= s^p + ps \sum_{k=1}^{p-1} \frac{1}{p} \binom{p}{k} s^{k-1}. \end{aligned}$$

This reveals that $A(L)^{s^{p^l}} = \{1\}$, where $p^l = exp(A(L)^s)$. Hence, we can regard $A(L)$ as an $\mathbb{Z}[s]/(s^{p^l})$-module, where (s^{p^l}) is the ideal in $\mathbb{Z}[s]$ generated by s^{p^l}. Now we can apply the previous lemma for the case that $R = \mathbb{Z}[s]/(s^{p^l})$, which implies that s is nilpotent in R. We then obtain that $\sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k} s^{k-1}$ is a unit in R, which yields the first statement. The second statement follows immediately as u is a unit in R and s^{p^l} is nilpotent in R.

(iii) Let $0 \leq k, m \leq n$ and let us define that $\binom{m}{k} = 0$ if $m < k$. Then

$$\sum_{m=0}^{n} \binom{m}{k} = \binom{n+1}{k+1}.$$

It then follows that

$$\begin{aligned} 1 + \sigma + ... + \sigma^{p-1} &= 1 + (s+1) + (s+1)^2 + ... + (s+1)^{p-1} \\ &= p + \sum_{k=1}^{p-1} \binom{k}{1} s + \sum_{k=2}^{p-1} \binom{k}{2} s^2 + ... + \sum_{k=p-1}^{p-1} \binom{k}{p-1} s^{p-1} \\ &= p + \sum_{j=1}^{p-1} \binom{p}{j+1} s^j \end{aligned}$$

For $j \leq p-2$, then obviously $\binom{p}{j+1} \in p\,\mathbb{Z}[s]$. The rest follows from the previous lemma. □

Assuming the notation as above, let $\mathbb{Z}[T]$ denote the ring of polynomials with variable T and integer coefficients. For a non-trivial ideal class $a \in A(L)$, we define the $\mathbb{Z}[s]$-*cycle of* a as

$$a^{\mathbb{Z}[s]} = \{a^{f(s)} : \ f \in \mathbb{Z}[T]\}.$$

In this context, we also define

$$r(a) = max\{n \in \mathbb{N} : \ a^{s^n} \neq 1\},$$

which we call the *length* of a. We are now prepared to state and prove the following

Theorem 2.6.3. *Notations being like above, let* $r = rk(a^{s\,\mathbb{Z}[s]})$. *Then*

$$a^{s\,\mathbb{Z}[s]} \cong < a^s > \times < a^{s^2} > \times ... \times < a^{s^r} >,$$

i.e. $\{a^s, a^{s^2}, ..., a^{s^r}\}$ *forms a* $\mathbb{Z}$*-basis of* $a^{s\,\mathbb{Z}[s]}$.
In particular, if $ord(a^s) > p$, *then* $r = p - 1$.

Proof. Without loss of generalization, we may assume that $r(a) > 1$. (In the following, r and $r(a)$ are not be confused). By the previous proposition, we then have that $ord(a^{s^p}) = ord(a^{ps})$. Hence $r(a) \leq p - 1$ if $ord(a^s) = p$. Let us prove the above statement by induction on the order of a^s:
Induction start: $ord(a^s) = p$: Assume that

$$a^{k_1 s} \cdot a^{k_2 s^2} \cdot ... \cdot a^{k_r s^r} = 1,$$

where $k_1, ..., k_r \in \mathbb{Z}$. Taking both sides of the equation to the s^{r-1}, we obtain that $a^{k_1 s^r} = 1$ and hence $k_1 \equiv 0\ mod\ p$. Continuing in this fashion, we readily see that $k_i \equiv 0\ mod\ p$, $\forall\ 1 \leq i \leq r$. This proves the statement.
Induction hypothesis: The statement holds in the case that $ord(a^s) = p^{k-1}$, for some $k > 1$.
Induction step: $ord(a^s) = p^k$, for $k > 1$. Note that if $ord(a^s) > p$, then $a^{s^p} \neq 1$ and hence $r = p - 1$. Let us now assume the equation as above, i.e.

$$a^{k_1 s} \cdot a^{k_2 s^2} \cdot ... \cdot a^{k_l s^r} \quad = \quad 1. \tag{2.10}$$

Let $1 \leq t \leq p - 1$ be maximal such that $ord(a^s) = ord(a^{s^t})$. Taking both sides of the equation to the power p, we obtain that

$$a^{pk_1 s} \cdot a^{pk_2 s^2} \cdot ... \cdot a^{pk_r s^r} = 1,$$

observing that $ord(a^{ps}) = p^{k-1}$. By induction hypothesis, it follows that $k_i = p^{k-1} k_i'$, for $1 \leq i \leq t$, and $k_i' \in \mathbb{Z}$. Also, $k_i = p^{k-2} k_i'$, for $t+1 \leq i \leq p-1$ and $k_i' \in \mathbb{Z}$. It follows that $ord(a^{k_i s^i}) \leq p$, $\forall\ 1 \leq i \leq r$. Equation (2.10) can be written as

$$a^{p^{k-1} k_1' s} \cdot ... \cdot a^{p^{k-1} k_t' s^t} \cdot a^{p^{k-2} k_{t+1}' s^{t+1}} ... \cdot a^{p^{k-2} k_r' s^r} = 1.$$

Taking both sides of the equation to the power of s^{p-1}, one easily verifies that $a^{p^{k-2} k_{t+1}' s^{t+1}} = 1$ and thus $k_{t+1}' \equiv 0\ mod\ p$. Repeating this procedure with s^{p-2} and so on, one can eventually conclude that $k_i' \equiv 0\ mod\ p$. This proves the induction step and hence the proof. □

Another important implication of the F-property is that we obtain an upper bound for the rank of $A(L)$. We have the following:

Proposition 2.6.4. *In the situation as before, let L/K be more generally a cyclic p-extension (i.e. not necessarily of degree p), still satisfying the F-property. We set $A(K)' = N_{L/K}(A(L))$, and $r = rk(A(K)')$. Assume that $A(K)' =< a_1, ..., a_r >$ and let $B' :=< b_1, ..., b_r > \subset A(L)$ with $N_{L/K}(b_j) = a_j$, $\forall\ 1 \leq j \leq r$. Then B' generates $A(L)$ as an $\mathbb{Z}[s]$-module.*

Proof. Let $A(L) = B$. Then we have

$$(B' \cdot B^s)/B^s \cong B'/(B' \cap B^s) \cong A(K)' \cong B/B^s.$$

Slightly modifying the arguments in the case where $[L : K] = p$, one still obtains that $B^{s^{p^l}} = \{1\}$, for sufficiently large $l \in \mathbb{N}$. It thus follows that

$$B \subset B' \cdot B^s \subset B' \cdot B'^s \cdot B'^{s^2} \subset ... \subset B'^{\mathbb{Z}[s]}.$$

This completes the proof. □

Remark: Essentially, the above statement is a special case of Nakayama's Lemma. See page 126, of [11]. Apply it for $V = A(L)$ and $\mathfrak{o} = \mathbb{Z}_p[[T]]$, where T is identified with s.

Corollary 2.6.5. *Let L/K and $A(K)'$ be as in the previous proposition. Then:*

(i) $rk(A(L)) \leq [L : K] \cdot rk(A(K)')$;

(ii) $rk(A(L)^s) \leq ([L : K] - 1) \cdot rk(A(K)')$.

Proof. The proof follows immediately from the previous proposition and Proposition 2.6.2. □

The above theorem poses the following natural question: Let L/K be cyclic of degree p, satisfying the F-property. Let $\sigma \in G(L/K)$ be a generator of $G(L/K)$, $s = \sigma - 1$. Also, assume that $b_1, ..., b_r$ is a system in $A(L)$ such that $\overline{b_1}, ..., \overline{b_r}$ form a basis of $A(L)/A(L)^s$, where $\overline{b_i}$, $i = 1, ..., r$, denote the images of b_i in $A(L)/A(L)^s$. Now we define $\lambda(b_i) = rk(b_i^{\mathbb{Z}[s]})$.
Question: Can we choose the b_i's such that

$$\sum_{i=1}^{r} \lambda(b_i) = rk(A(L)) \ ?$$

Answer: In general, this is not possible as the following example shows. In particular, we cannot decompose $A(L)$ into a direct product of $\mathbb{Z}[s]$-cycles.

Example: Let $K = \mathbb{Q}(\alpha)$ with $\alpha^2 + 3299 = 0$. Then MAGMA yields:

1. $A(K) =< a_1, a_2 > \cong C_3 \times C_9$;
2. $A(L) =< b_1, b_2, b_3 > \cong C_3 \times C_3 \times C_9$;

Now let $L = H(K)^{<a_1, a_2^3>}$. Then L/K is an unramified cyclic extension of degree 3 and $N_{L/K}(A(L)) \cong < a_1, a_2^3 > \cong C_3 \times C_3$. Set $G = Gal(L/K) =< \sigma >$, $s = \sigma - 1$. MAGMA yields that

3. $P_K(L) =< a_1 >$. It follows that $A(L)^G = \imath_{L/K}(< a_2 >) \cong C_9$ and $A(L)^s \cong C_3 \times C_3$.

Without loss of generality, we may assume that $N_{L/K}(b_1) = 1$, $N_{L/K}(b_2) = a_1$, $N_{L/K}(b_3) = a_2^3$ with $b_3 = \imath_{L/K}(a_2)$. Then b_2, b_3 form a basis for $A(L)/A(L)^s$ with

$$\lambda(b_2) + \lambda(b_3) = 3 + 1 = 4 > 3 = rk(A(L)).$$

Observe that $\lambda(b_3) = 1$ since b_3 is G-invariant and $\lambda(b_2) = 3$ since $A(L)^s =< b_2^s, b_2^{s^2} >$ and $b_2 \notin A(L)^s$. One may easily verify that it is impossible to find b_2', b_3' forming a basis of $A(L)/A(L)^s$ with $\lambda(b_2') + \lambda(b_3') = 3$.

2.7 Exact and Non-Exact $\mathbb{Z}[s]$-Cycles

In the following discussion, we intend to yield more information on the structure of the ideal class groups in cyclic extensions with F-property. Henceforth, let L/K be a cyclic Galois extension of degree p satisfying the F-property. Also, let $G = Gal(L/K)$, generated by some $\sigma \in G$, and $s = \sigma - 1$. Suppose now that a is a non-trivial ideal class in K of order p^l, for some $l \in \mathbb{N}$, and $b \in A(L)$ with $N_{L/K}(b) = a$. We then define $B = b^{\mathbb{Z}[s]} \subset A(L)$. In this section, we will focus on analyzing the structure of $\mathbb{Z}[s]$-cycles. In the subsequent section, we will also discuss how the $\mathbb{Z}[s]$-cycles can be used to form a generating set of $A(L)$, which is minimal in some sense. It is worth mentioning that the F-property does not need to hold on $\mathbb{Z}[s]$-cycles, i.e. in general we do not have $B \cap A(L)^s = B^s$. Let us assume that $B \cap A(L)^s \neq B^s$. Then there exists an integer $k \in \mathbb{Z}$ such that $b^k \in A(L)^s \setminus B^s$. It follows that $b^k = c^s$, for some $c \in A(L) \setminus B$. Due to $c^{s^p} = c^{pus}$, for some unit $u \in \mathbb{Z}[s]/(s^{p^l})$ (l sufficiently large), we obtain that

$$b^{pk} = c^{ps} = c^{u'(s^p)} \in B^s,$$

where u' is some unit $\mathbb{Z}[s]$. Thus, we can derive that $|B \cap A(L)^s|/|B^s| \leq p$. We introduce the following

Definition: Notations being like above, we say that the $\mathbb{Z}[s]$-cycle B is *exact* if $B \cap A(L)^s = B^s$ and *not exact* otherwise.

Remark: Let $B^G = B \cap A(L)^G$. Then $|B^G| = ord(N_{L/K}(b))$ if B is exact. If B is not exact, then $|B^G| = p \cdot ord(N_{L/K}(b))$. This follows easily due the above arguments and the isomorphism $B/B^G \cong B^s$. Another important remark is that $exp(B^s) > p$ may be possible as we will see in Chapter 4.

We begin our investigations with the following

Lemma 2.7.1. *Notations being like above (B exact or non-exact), let $r = rk(B^s)$ and $N = \imath_{L/K} \circ N_{L/K}$ the algebraic norm. Assume that there exist integers $k_i \in \mathbb{Z}$, $0 \leq i \leq r-1$, such that*

$$b^{k_0 + k_1 s + ... + k_{r-1} s^{r-1}} = 1,$$

where $b^{k_i s^i} \neq 1$, for at least one $0 \leq i \leq r-1$. It then follows that $exp(B^s) > p$ and

$$1 \neq b^{k_0} = b^{k_t s^t} \in B^G, \text{ for some } 0 \leq t \leq r-1.$$

Moreover, $ord(b) = p \cdot ord(N(B))$ and $ord(b) = p \cdot ord(a)$.

Proof. Assume that $b^{k_0 + k_1 s + ... + k_{r-1} s^{r-1}} = 1$. Taking this equation to the s, we obtain that

$$b^{k_0 s + k_1 s^2 + ... + k_{r-1} s^r} = 1.$$

By Theorem 2.6.3, we know that $\{b^s, ..., b^{s^r}\}$ is a $\mathbb{Z}$-basis of B^s. This implies that b^{k_0} is non-trivial and that $b^{k_i s^{i+1}} = 1$, $\forall\ 0 \leq i \leq r-1$. In particular, $b^{k_0} \in B^G \cap B^s$, yielding that $ord(b^{k_0}) = p$. Hence, there exists exactly one $t \in \{1, ..., r-1\}$ such that $b^{k_t s^t} \cap B^G \neq \{1\}$ and $< b^{k_0} >=< b^{k_t s^t} >$. This implies that $exp(B^s) > p$ since otherwise $rk(B^s) = t < r$. Hence, $r = p-1$. As $< b^{k_0} >=< b^{k_t s^t} >$ and $t < r$, it follows that $ord(b^{s^{p-1}}) \leq ord(b)/p^2$. Recall that $N(b) = b^{pu + s^{p-1}}$, for some unit $u \in \mathbb{Z}_p[s]/(s^l)$ and sufficiently large l. Combining these arguments, we deduce that $p \cdot ord(N(B)) = ord(b)$. As $< b > \cap B^s \neq \{1\}$ the rest follows. □

For a better overview, we will analyze the case where B is exact and where B is not exact separately. We begin with the exact case. We have

Proposition 2.7.2. *Notations being like above, assume that B is exact, $a \in A(K)$ of order p^l, for some $l > 0$, and $b \in A(L)$ with $N_{L/K}(b) = a$ and $ord(b) = p^m$. We define $B = b^{\mathbb{Z}[s]}$, $r = rk(B^s)$, and $n = exp(< b > \cap B^G)$. Also, we set $\mathcal{B}_{r-1} = \{b, b^s, ..., b^{s^{r-1}}\}$ and $B_{r-1} =< \mathcal{B}_{r-1} >$. We then differentiate between the following cases:*

Case 1. If $rk(B) = 1$, *then* $B \cong C_{p^{l+1}}$.

Case 2. If $ord(a) = ord(b)$, *then* $rk(B) > 1$ *and* $\mathcal{B}_{r-1} \cup < b^{s^r} >$ *forms a basis of* B. *Hence,*

$$B \cong C_{p^m} \times C_{p^{m-n}} \times ... \times C_{p^{m-n}} \times C_{p^{m-n-1}} \times ... \times C_{p^{m-n-1}}.$$

Case 3. Suppose that $rk(B) > 1$ *and* $ord(b) > ord(a)$.
Case 3.1. Assume that $ord(b) = p \cdot ord(N(b))$ *and hence* $ord(b) = p \cdot ord(a)$.
Case 3.1.1. Assume case 3.1 with $n = 0$*: The system* $\mathcal{B}_{r-1}$ *can be extended to a basis of* B *and thus*

$$B \cong C_{p^m} \times C_{p^m} \times ... \times C_{p^m} \times C_{p^{m-1}} \times ... \times C_{p^{m-1}} \times C_{p^{m-2}}.$$

Case 3.1.2. Assume case 3.1 with $n > 0$.
Case 3.1.2.1. Assume case 3.1.2 and that $\mathcal{B}_{r-1}$ *is a basis for* B_{r-1}. *Then*

$$B \cong C_{p^m} \times C_{p^{m-n}} \times ... \times C_{p^{m-n}} \times C_{p^{m-n-1}}.$$

Case 3.1.2.2. Assume case 3.1.2 and that $\mathcal{B}_{r-1}$ *is not a basis for* B_{r-1}. *It then follows that*

$$B^s \cong \underbrace{C_{p^{m-n}} \times ... \times C_{p^{m-n}}}_{r_0-times} \times \underbrace{C_{p^{m-n-1}} \times ... \times C_{p^{m-n-1}}}_{r_1-times},$$

with $1 \leq r_0 \leq r-1$, $r = r_0 + r_1$, *and*

$$B \cong C_{p^m} \times \underbrace{C_{p^{m-n}} \times ... \times C_{p^{m-n}}}_{(r_0-1)-times} \times \underbrace{C_{p^{m-n-1}} \times ... \times C_{p^{m-n-1}}}_{(r_1+1)-times}.$$

Case 3.2. Assume that $ord(b) > p \cdot ord(N(b))$*: Then the system* $\mathcal{B}_{r-1}$ *can be extended to a basis of* B *and thus*

$$B \cong C_{p^m} \times C_{p^m} \times ... \times C_{p^m} \times C_{p^{m-1}} \times ... \times C_{p^{m-1}} \times C_{p^{l-1}}.$$

Additionally, $n \leq 1$ *in this case.*

Proof. Case 1 is evident.
Case 2. Since $ord(a) = ord(b)$, it follows that $< b > \cap < b^s, ..., b^{s^r} >= \{1\}$.

The rest follows due to $B^s \cap B^G \cong C_p$.
Case 3.1.1. By the previous lemma, the system $\mathcal{B}_{r-1}$ is a basis of B_{r-1} and can be extended to a basis of B. Indeed, there exists an b^{xs}, $x \in \mathbb{Z}[s]$, such that $B^s =< b^s, ..., b^{s^{r-1}}, b^{xs} >$ and $b^{p^{m-2}xs} = b^{p^{m-1}}$. Then $\{b, b^s, ..., b^{s^{r-1}}, b^{xs-p}\}$ is a basis of B. The rest follows since $S_1(< b^{s^r} >)$ cannot be G-invariant since otherwise $\mathcal{B}_{r-1}$ would not be a basis of B_{r-1}.
Case 3.1.2.1. With the same notation and arguments as above, the system $\{b, b^s, ..., b^{s^{r-1}}, b^{xs-p}\}$ is a basis of B. The rest follows since $S_1(< b^{s^r} >)$ must be G-invariant in this case.
Case 3.1.2.2. The statement follows readily from the fact that $1 \neq b^{k_0} = b^{k_t s^t} \in B^G$, for some $0 \leq t \leq r-1$, by the previous lemma.
Case 3.2. By the previous lemma, $\mathcal{B}_{r-1}$ is a basis of B_{r-1} and can be extended to a basis of B as above. Also observe that $exp(B^s \cap < b >) = p^{m-l}$ as B is exact. Finally, $n \leq 1$ due to $ord(b) > p \cdot ord(N(b))$. □

Remark: The case where B is not exact is rather analogous: The first two cases from the above proposition stay the same.
In all other cases where $\mathcal{B}_{r-1}$ can be extended to a basis of B, we only have to raise the exponent of the last direct factor by p. This follows from the remark before the definition of the exactness of $\mathbb{Z}[s]$-cycles.
In case 3.1.2.2, we have to replace $r_0 - 1$ by r_0 and $r_1 + 1$ by r_1.

2.8 Decomposition of $A(L)$ into a Product of $\mathbb{Z}[s]$-Cycles and its Effect on Capitulation

Henceforth, let L/K be a cyclic extension of degree p satisfying the F-property, i.e. $kerN_{L/K} = A(L)^s$. Let $G = Gal(L/K) =< \sigma >$, where $\sigma \in G$ is a generator of G, and we set $s = \sigma - 1$. In the previous section, we have focused our investigations on a $\mathbb{Z}[s]$-cycle B. Now one may ask how can we deduce the structure of $A(L)$ from the structure of the various $\mathbb{Z}[s]$-cycles? The upcoming analysis will answer this question. For this purpose, we intend to decompose the ideal class group $A(L)$ into a product of $\mathbb{Z}[s]$-cycles. As we have seen in the end of Section 2.6, this product cannot necessarily chosen to be direct. However, one can choose $\mathbb{Z}[s]$-cycles $B_1, ..., B_n$ such that $A(L) = B_1 \cdots B_n$ and $kerN_{L/K} = \prod_{j=1}^{n} B_j^s$, where $\prod$ is a direct product here. We introduce the so-called *method of contraction* and explicitly show how to obtain such a system $(B_1, ..., B_n)$. Subsequently, we explain why this does not necessarily imply that $A(L)$ is a direct product of these B_i's. Led by this observation, we revisit the concept of exact and non-exact $\mathbb{Z}[s]$-cycles

and show that there is no capitulation in non-exact cycles. Thus, we link the problem of the decomposition of $A(L)$ into a product of $\mathbb{Z}[s]$-cycles with the problem of capitulation. Finally, we obtain sufficient conditions under which $A(L)$ can be decomposed into a direct product of $\mathbb{Z}[s]$-cycles. One general remark: Henceforth, $\prod$ does not necessarily denote a direct product, unless stated explicitly.

Let $b \in A(L)$ such that b^s is non-trivial, $B = b^{\mathbb{Z}[s]}$, and $r := r(b)$, i.e. $r \in \mathbb{N}$ such that $b^{s^r} \neq 1$ and $b^{s^{r+1}} = 1$. Let $c \in B^s$ of the form

$$c = \prod_{j=1}^{r} b^{k_j s^j},$$

where $k_j \in \mathbb{Z}$. Due to the relation $b^{ps} = b^{u(s^p - s^{p-1})}$, for some $u \in \mathbb{Z}[s]$, we may assume that in the above equation $k_j = 0$ or $p \nmid k_j$ holds, $\forall\ 1 \leq j \leq r$. Indeed, if $k_j = pk'_j$, for some $1 \leq j \leq r$ and $k'_j \in \mathbb{Z}$, we may have

$$b^{pk'_j s^{k_j}} = b^{k'_j s^{k_j - 1}(u(s^p - s^{p-1}))} \in B^{s^{k_j + p - 2}}.$$

If $p \geq 3$, we can now assume that $k_j = 0$. If $p = 2$, we can iterate this procedure until $p \nmid k_j$.

Definition: As usual, we denote by $A(L)^G$ the G-invariant ideal classes in $A(L)$, i.e. $A(L)^G = \{a \in A(L) : a^\sigma = a\}$. For a subgroup A of $A(L)$, we then define $A^G = A \cap A(L)^G$.

The following proposition will prove useful:

Proposition 2.8.1. *Notations being like above, assume that*

$$c = \prod_{j=1}^{r} b^{k_j s^j} = 1,\ k_j \in \mathbb{Z},$$

where $k_j = 0$ or $p \nmid k_j$ holds, $\forall\ 1 \leq j \leq r$. Then

$$k_j = 0,\ \forall\ 1 \leq j \leq r.$$

Proof. If $ord(b^s) \leq p$, then $r \leq p - 1$ and the statement follows from Proposition 2.6.3. Now let us assume that $ord(b^s) > p$, which implies that $B^s =< b^s, ..., b^{s^{p-1}} >$ and $rk(B^s) = p - 1$. Let $t \in \{1, ..., p-1\}$ such that $S_1(< b^{s^t} >) \subset A(L)^G$. Recall that t is uniquely determined and observe that all elements in $\{b^s, ..., b^{s^t}\}$ are of order $ord(b^s)$, all elements in

$\{b^{s^{t+1}}, ..., b^{s^{t+p-1}}\}$ are of order $ord(b^s)/p$, and so on. Due to $k_j = 0$ or $p \nmid k_j$, it follows that $\prod_{j=1}^{r} b^{k_j s^j} = 1$ if and only if $\prod_{j=1}^{t} b^{k_j s^j} = 1$, $\prod_{j=t+1}^{t+p-1} b^{k_j s^j} = 1$, and so on. Since all products have at most $(p-1)$ factors, Proposition 2.6.3 yields that $b^{k_j s^j} = 1$, $\forall\ 1 \leq j \leq r$. □

Corollary 2.8.2. *Notations being like above, assume that* $1 \neq c \in B^s \cap B^G$. *Then*

$$< c >=< b^{s^r} > .$$

Proof. Assume that $c = \prod_{j=1}^{r} b^{k_j s^j}$, with $k_j = 0$ or $p \nmid k_j$, for all $1 \leq j \leq r$. Then

$$1 = c^s = \prod_{j=2}^{r} b^{k_{j-1} s^j}.$$

By the above proposition, it follows that $k_1 = ... = k_{r-1} = 0$ and $p \nmid k_r$ due to $c \neq 1$. This proves the claim. □

After having generalized Proposition 2.6.3, the next results will explicitly show how to find a $\mathbb{Z}[s]$-basis for $A(L)^s$. We have

Proposition 2.8.3. *Notations being like above, one can choose a* $\mathbb{Z}[s]$*-basis* $\{\tilde{b}_1, ..., \tilde{b}_n\}$ *of* $A(L)$ *with corresponding* $\mathbb{Z}[s]$*-cycles* $\tilde{B}_i = \tilde{b}_i^{\mathbb{Z}[s]}$ *such that*

$$\tilde{B}_1^s \times ... \times \tilde{B}_n^s = ker N_{L/K}. \tag{2.11}$$

Proof. Let $\{a_1, ..., a_n\}$ be a basis of $N_{L/K}(A(L)) =: A(K)'$ and $b_i \in A(L)$ such that $N_{L/K}(b_i) = a_i$, $\forall\ 1 \leq i \leq n$. Also set $B_i = b_i^{\mathbb{Z}[s]}$, $\forall\ 1 \leq i \leq n$. By Furtwängler's Theorem, we certainly have that

$$ker N_{L/K} = B_1^s \cdot B_2^s \cdots B_n^s.$$

However, the above product does not need to be direct as we have seen. Hence, we will apply the *method of contraction*:
For all $1 \leq i \leq n$, let $r_i = r(b_i) =: l(b_i)$ be the length of the flag of b_i as defined before. Assume that there exist $k_{i,j} \in \mathbb{Z}$, not all being zero, such that

$$\prod_{i=1}^{n} \prod_{j=1}^{r_i} b_i^{k_{i,j} s^j} = 1, \tag{2.12}$$

where, $\forall\ 1 \leq i \leq n$, $1 \leq j \leq r_i$, we have that $k_{i,j} = 0$ or $p \nmid k_{i,j}$.
For all $1 \leq i \leq n$, we let $t_i = min\{j \in \{1, ..., r_i\} : k_{i,j} \neq 0\}$. (Without loss

of generality, we may assume that, $\forall\ 1 \leq i \leq n$, there exists an j such that $k_{i,j} \neq 0$. Otherwise, the index i only runs through a subset of $\{1, ..., n\}$ and things are fine as well).
Let $max_{i\in\{1,...,n\}}\{r_i - t_i\} = r_l - t_l$, for some $1 \leq l \leq n$. Also, let $I \subset \{1, ..., n\}$ such that for all $i \in I$, we have $r_i - t_i = r_l - t_l$. Taking equation (2.12) to the $s^{r_l - t_l}$, we then obtain

$$\prod_{i\in I} b_i^{k'_i s^{r_i}} = 1,$$

where $k'_i := k_{i,t_i}$.
Now let $m \in I$ such that $r_m = min_{i\in I}\{r_i\}$. Then, we may write

$$\prod_{i\in I}(b_i^{k'_i s^{r_i - r_m}})^{r_m} = 1, \text{ and set}$$

$$\tilde{b}_m = \prod_{i\in I} b_i^{k'_i s^{r_i - r_m}}.$$

First assume that r_m is a strict minimum, i.e. $r_m < r_i$, $\forall\ i \in I$, $i \neq m$. Then, $< N_{L/K}(\tilde{b}_m) >=< a_m >$ and $l(\tilde{b}_m) < l(b_m)$ due to $\tilde{b}_m^{s^{r_m}} = 1$. If r_m is not a strict minimum, then choose $m \in I$ such that r_m is minimal and $ord(a_m)$ is maximal among those $i \in I$ with $r_i = r_m$. It then follows that $\{a_1, ..., a_{m-1}, N_{L/K}(\tilde{b}_m), a_{m+1}, ..., a_n\}$ is a basis for $A(K)'$. In both cases, we have found a new system $\{b_1, ..., b_{m-1}, \tilde{b}_m, b_{m+1}, ..., b_n\}$ in $A(L)$ such that $\{N_{L/K}(b_1), ..., N_{L/K}(b_{m-1}), N_{L/K}(\tilde{b}_m), N_{L/K}(b_{m+1}), ..., N_{L/K}(b_n)\}$ is a basis for $A(K)'$ and such that

$$l(\tilde{b}_m) + \sum_{i=1,\ i\neq m}^{n} l(b_i) < \sum_{i=1}^{n} l(b_i). \tag{2.13}$$

That means, we have reduced the total length of the b_i's. Since this procedure must terminate, the above *method of contraction*, finally yields $\mathbb{Z}[s]$-cycles $\tilde{B}_1, ..., \tilde{B}_n$ such that

$$ker N_{L/K} = \prod_{j=1}^{n} \tilde{B}_j^s, \text{ where } \prod \text{ is a direct product.}$$

□

Remark: (1) The above proof is constructive, i.e. the method of contraction finally leads to a desired family of $\mathbb{Z}[s]$-cycles satisfying the condition as in the above proposition.

(2) Let $B_i = b_i^{\mathbb{Z}[s]}$ and $\tilde{B}_i = \tilde{b}_i^{\mathbb{Z}[s]}$, $1 \leq i \leq n$, such that $ker N_{L/K} = \prod_{i=1}^{n} B_i^s =$

$\prod_{i=1}^{n} \tilde{B}_i^s$, where $\prod$ denotes the direct product. Then one easily verifies that $\sum_{i=1}^{n} l(b_i) = \sum_{i=1}^{n} l(\tilde{b}_i)$.

Henceforth, assume that $B_1 = b_1^{\mathbb{Z}[s]}, ..., B_n = b_n^{\mathbb{Z}[s]}$ are given as in equation (2.11) with $\{N_{L/K}(b_i)\}_{1 \leq i \leq n}$ forming a basis of $N_{L/K}(A(K))$. We will then refer to such a system $\{B_1, ..., B_n\}$ as being in *standard form.*

Corollary 2.8.4. *Let $(B_1, ..., B_n)$ be in standard form. Then*

$$A(L)^G = \prod_{i=1}^{n} B_i^G.$$

Proof. Let $c \in A(L)^G$, $c = \prod_{i=1}^{n} b_i^{x_i}$, for some $x_i \in \mathbb{Z}[s]$. It then follows that $1 = c^s = \prod_{i=1}^{n} b_i^{x_i s}$. Since $ker N_{L/K} = B_1^s \times ... \times B_n^s$ by assumption, we obtain that $b_i^{x_i s} = 1$ and thus $b_i^{x_i} \in B_i \cap A(L)^G$, $\forall\ 1 \leq i \leq n$. □

Corollary 2.8.5. *Let $(B_1, ..., B_n)$ be in standard form. Assume that*

$$1 = \prod_{i=1}^{n} b_i^{x_i}, \text{ for some } x_i \in \mathbb{Z}[s].$$

Then: $b_i^{x_i} \in B_i^G, \forall\ \leq i \leq n.$

Proof. The proof follows immediately from the proof of the above corollary. □

Let $(B_1, ...B_n)$ be in standard form and set

$$z = |\{1 \leq j \leq n : B_j \text{ is not exact}\}|.$$

Also, we define

$$\mathcal{C} = \{(b_1^{x_1}, ..., b_n^{x_n}) :\ x_i \in \mathbb{Z}[s]\ (1 \leq i \leq n),\ \prod_{i=1}^{n} b_i^{x_i} = 1\} \subset \prod_{i=1}^{n} B_i,$$

where the second $\prod$ denotes a Cartesian product.
By the previous corollary, we obtain that

$$\mathcal{C} \subset \prod_{i=1}^{n} (B_i^G \cap ker N_{L/K}) \subset \prod_{i=1}^{n} S_1(B_i).$$

(Again, $\prod$ denotes the Cartesian product in both cases).

Proposition 2.8.6. *Notations being like above, it follows that*

$$rk(\mathcal{C}) = z.$$

Proof. Without loss of generality, we may assume that $B_1, ..., B_z$ are not exact and $B_{z+1}, ..., B_n$ are exact. For all $1 \leq i \leq z$, let $b_i^{p^{k_i}} \in ker N_{L/K} \setminus B_i^s$ for some $k_i \in \mathbb{Z}$. By Furtwängler's Theorem, it follows that

$$b_i^{p^{k_i}+w_{i,i}s} \cdot \prod_{j=1,\ j\neq i}^{n} b_j^{w_{i,j}s} = 1,$$

for some $w_{i,j} \in \mathbb{Z}[s]$, $1 \leq i \leq z$, $1 \leq j \leq n$. Observe that $b_j^{w_{i,j}s} \in A(L)^G$, for all $j \neq i$, and hence $b_j^{w_{i,j}s} \in < b_j^{s^{r_j}} >$. Let us say $b_j^{w_{i,j}s} = b_j^{l_{i,j}s^{r_j}}$, for some $0 \leq l_{i,j} < p$.
For all $1 \leq i \leq z$, we now define

$$y_i = (b_1^{x_{i,1}}, ..., b_n^{x_{i,n}}), \text{ where}$$

$$x_{i,j} = \begin{cases} l_{i,j}s^{r_j} & \text{if } j \neq i, \\ p^{k_i} + w_{i,i}s & \text{if } j = i. \end{cases}$$

It follows that $y_1, ..., y_z \in \mathcal{C}$ and one easily verifies that

$$rk(< y_1, ..., y_z >) = z.$$

Now it is only left to show that $< y_1, ..., y_z >$ even forms a basis of $\mathcal{C}$: Let $y \in \mathcal{C}$, $y = (b_1^{v_1}, ..., b_n^{v_n})$, for some $v_j \in \mathbb{Z}[s]$, $1 \leq j \leq n$. By renumbering the b_i's, we may assume that there is an $l \in \mathbb{N}$ such that $v_j = sv'_j$ ($v'_j \in \mathbb{Z}[s]$) for all $j > l$ and $v_j \notin s\mathbb{Z}[s]$ for all $j \leq l$. Since $B_{z+1}, ..., B_n$ are exact, it follows that $l \leq z$ and that $B_1, ..., B_l$ are not exact. Thus, for all $1 \leq j \leq l$, $b_j^{v_j} = b_j^{p^{k_j}+v'_j s}$ for some $v'_j s \in \mathbb{Z}[s]$. All in all, we obtain that

$$y = (b_1^{p^{k_1}+v'_1 s}, ..., b_l^{p^{k_l}+v'_l s}, b_{l+1}^{v'_{l+1}s}, ..., b_n^{v'_n s}).$$

Since $B_1, ..., B_n$ are in standard form, one easily obtains that $y \in < y_1, ..., y_z >$. This finishes the proof. □

The next result shows: *In non-exact $\mathbb{Z}[s]$-cycles we have no capitulation.* More precisely, we have

Proposition 2.8.7. *Let $b \in A(L)$ with $1 \neq N_{L/K}(b) = a \in A(K)$ and $B = b^{\mathbb{Z}[s]}$. Assume that B is not exact, then $ord(a) = ord(\iota_{L/K}(a))$.*

Proof. It is sufficient to show that $S_1(< a >)$ does not capitulate in L. Since B is not exact, there exists an $1 \neq b^{p^k} \in ker N_{L/K} \setminus B^s$ for some $k \in \mathbb{N}$. Observe that $b^{p^{k-1}} \notin ker N_{L/K}$ due to $|(B \cap ker N_{L/K})/B^s| = p$. It follows that $N_{L/K}(b^{p^{k-1}}) = S_1(a)$, where $S_1(a)$ is a generator of $S_1(< a >)$. Now assume that $S_1(a)$ capitulates in L. Due to $1 = \imath_{L/K}(S_1(a)) = (b^{p^{k-1}})^{pu+s^{p-1}}$, for some unit $u \in \mathbb{Z}[s]$, it then follows that $b^{p^k} \in B^s$, which is a contradiction to the initial assumption. □

This leads us to the following

Corollary 2.8.8. *Notations being like above, suppose that $S_1(A(K)')$ capitulates completely in L. Then there exist $\mathbb{Z}[s]$-cycles $B_1, ..., B_n$ such that $A(L)$ is a direct product of $B_1, ..., B_n$, i.e.*

$$A(L) = \prod_{j=1}^{n} B_j.$$

Proof. The proof follows immediately from the above discussion and the previous proposition. Any system $(B_1, ..., B_n)$ being in standard form yields a decomposition of $A(L)$ into a direct product of $\mathbb{Z}[s]$-cycles. □

Let $(B_1, ..., B_n)$ be a system of $\mathbb{Z}[s]$-cycles in standard form, i.e. $ker N_{L/K} = \prod_{j=1}^{n} B_j^s$, where $\prod$ denotes the direct product. (Again, $B_j = b_j^{\mathbb{Z}[s]}$, $\forall\ 1 \leq j \leq n$). As we have seen in earlier examples, this does not necessarily imply that $A(L)$ is a direct product of the B_i's. The reason for this are the non-exact cycles. This poses the question if one can reduce the number of non-exact $\mathbb{Z}[s]$-cycles by some clever modifications without violating the standard form assumption. In the following, we will show under which prerequisites this is possible and we will explicitly show how to do this. We will restrict ourselves to the case where $exp(ker N_{L/K}) \leq p$:

Let us assume that B_1 is not exact, say $b_1^{p^{l_1}} \in ker N_{L/K} \setminus B_1^s$. Due to $exp(ker N_{L/K}) \leq p$ by assumption, it follows that $B_1 =< b_1 > \times B_1^s$. Also, $|B_1^G| = p \cdot ord(a_1)$ and hence $< b_1 >^G =< b_1 >$ (which implies that $B_1^s = 1$) or $< b_1 >^G =< b_1^p >$. In either way, we have that $B_1^G =< b_1 >^G \cdot < b_1^{s^{r_1}} >$, where $r_1 = l(b_1)$ is the length of b_1 as before. By Furtwängler's Theorem and the fact that $\mathcal{C}_{(B_1,...,B_n)} \subset \prod_{j=1}^{n} ker N_{L/K} \cap B_j^G$, we then obtain that

$$b_1^{p^{l_1}} = \prod_{j=1}^{n} b_1^{k_j s^{r_j}},$$

where $0 \leq k_j < p$, $\forall\ 1 \leq j \leq n$. In the following, we will differentiate two cases. In the first case, $k_1 \neq 0$ and in the second case $k_1 = 0$.

Case 1: Assume that $k_1 \neq 0$ and that $0 < r_1 < r_j$, $\forall\ 2 \leq j \leq n$, with $k_j \neq 0$. Then we set

$$\tilde{b}_1 = \prod_{j=1}^{n} b_j^{k_j s^{r_j - r_1}}.$$

As $r_1 < r_j$, for all $2 \leq j \leq n$ with $k_j \neq 0$, and as $p \nmid k_1$, it follows that $< N_{L/K}(\tilde{b}_1) >=< a_1 >$. Moreover, $l(\tilde{b}_1) = r_1$. Also note that $S_1(< b_1 >) = S_1(< \tilde{b}_1 >)$ since $ord(b_1) > p$. Thus, $< \tilde{b}_1^{p^{l_1}} >=< \tilde{b}_1^{s^{r_1}} >$, which implies that $\tilde{B}_1 = \tilde{b}_1^{\mathbb{Z}[s]}$ is exact now. Furthermore, $l(\tilde{b}_1) + \sum_{j \geq 2}^{n} l(b_j)$ is still minimal, implying that $(\tilde{B}_1, B_2, ..., B_n)$ is in standard form with

$$rk(\mathcal{C}_{(\tilde{B}_1, B_2, ..., B_n)}) < rk(\mathcal{C}_{(B_1, ..., B_n)}).$$

Case 2: Assume that $k_1 = 0$ and that there exist $l_j > 0$ such that $< b_j^{s^{r_j}} >=< b_j^{p^{l_j}} >$, $\forall\ 2 \leq j \leq n$, with $k_j \neq 0$. (If B_j is exact and $ker N_{L/K} \cap < b_j > \neq 1$, one easily verifies that this is always the case). If $l_1 < l_j$ for all j as above, we then set

$$\tilde{b}_1 = \prod_{j=1}^{n} b_j^{k'_j p^{l_j - l_1}},$$

where $0 \leq k'_j < p$, $\forall\ 1 \leq j \leq n$, satisfying $\tilde{b}_1^{p^{l_1}} = 1$. We then obtain that $ord(\tilde{b}_1) = p^{l_1} = ord(b_1)/p$ and $< \tilde{b}_1 > \cap ker N_{L/K} = 1$, which implies that $\tilde{B}_1 = \tilde{b}_1^{\mathbb{Z}[s]}$ is exact now. Observe that $ord(N_{L/K}(b_j^{k'_j p^{l_j - l_1}})) = p^{l_1}$, $\forall\ 1 \leq j \leq n$, with $k'_j \neq 0$. Hence, $< N_{L/K}(\tilde{b}_1), a_2, ..., a_n >$ is a basis of $A(K)'$. Due to $exp(ker N_{L/K}) \leq p$ and $l_1 < l_j$, we obtain that $l(\tilde{b}_1) = l(b_1)$. With the same arguments as in the first case, we can thus derive that $(\tilde{B}_1, B_2, ..., B_n)$ is in standard form with $rk(\mathcal{C}_{(\tilde{B}_1, B_2, ..., B_n)}) < rk(\mathcal{C}_{(B_1, ..., B_n)})$.

Remark: One can show that the two methods above are essentially the only ways to lower the $rk(\mathcal{C})$ for a given system $(B_1, ..., B_n)$ in standard form. The proof is rather arduous and is omitted here, though. Examples show that the two previous methods work no longer in general, when we relax the assumption that $exp(ker N_{L/K}) \leq p$. It makes sense now to introduce the following

Definition: Let $(B_1, ..., B_n)$ be a system of $\mathbb{Z}[s]$-cycles in $A(L)$ with $A(L) = \prod_{j=1}^{n} B_j$. (This product is not necessarily direct). Then we say the system

$(B_1, ..., B_n)$ is in *minimized standard form* if it is in standard form and the number of non-exact cycles is minimal among all systems of $\mathbb{Z}[s]$-cycles being in standard form. Let z be the number of non-exact cycles of a system $(B_1, ..., B_n)$ in minimized standard form. Then we set $min(L/K) := z$.

Remark: Let $(B_1, ..., B_n)$ be in minimized standard form. The previous results then imply that $\mathcal{C}_{(B_1,...,B_n)}$ is of minimal rank among all systems of $\mathbb{Z}[s]$-cycles being in standard form.

Now we are in the position to state and prove the main result of this section. We have

Theorem 2.8.9. *Notations being like above, let $\{a_1, ..., a_n\}$ be a basis of $A(K)'$ and $b_i \in A(L)$ with $N_{L/K}(b_i) = a_i$, $\forall\ 1 \leq i \leq n$. We set $B_i = b_i^{\mathbb{Z}[s]}$, $\forall\ 1 \leq i \leq n$, and assume that $(B_1, ..., B_n)$ is in standard form. Let us say $B_1, ..., B_k$ are non-exact cycles and $B_{k+1}, ..., B_n$ are exact cycles, for some $1 \leq k \leq n$. We then obtain that*

$$a)\ P_K(L) \cap < a_{k+1}, ..., a_n >= \prod_{j=k+1}^{n} (< a_j > \cap P_K(L));$$

$$b)\ \prod_{j=1}^{k} (< a_j > \cap P_K(L)) = \{1\};$$

Now additionally assume that $(B_1, ..., B_n)$ is in minimized standard form, i.e. $min(L/K) = k$, and that $exp(B_i^s) \leq p$, $\forall\ 1 \leq i \leq k$. Then

$$c)\ P_K(L) \cap < a_1, ..., a_k >= \{1\}$$

In particular, $min(L/K) \leq rk(A(K)') - rk(P_K(L) \cap A(K)')$.

Proof. (a) Is straightforward and left to the reader.
(b) follows from a previous proposition.
(c) Let us suppose that there is some $1 \neq a \in P_K(L)$ with

$$a = \prod_{j=1}^{k} S_1(a_j)^{k_j},$$

where $S_1(a_j)$ is a generator of $S_1(< a_j >)$, $0 \leq k_j < p$ $(1 \leq j \leq k)$. Without loss of generality, we may assume that $k_j = 0$ or $k_j = 1$, $\forall\ 1 \leq j \leq k$, by replacing a_j by $a_j^{k_j}$ if $k_j = 0$. Let $I \subset \{1, ..., k\}$ such that $k_j \neq 0$, i.e. $k_j = 1$

for all $j \in I$. As $a \in P_K(L)$, it follows that $1 = \prod_{j\in I} \imath_{L/K}(S_1(a_j))$. Let $N_{L/K}(b_j^{p^{m_j}}) = S_1(a_j)$, for some $m_j \in \mathbb{Z}$ and all $j \in I$. Due to $exp(B_i^s) \leq p$, for all $1 \leq i \leq k$ by assumption, we can derive that

$$\prod_{j\in I}(b_j^{p^{m_j}})^{p+s^{p-1}} = 1 \quad (*)$$

Suppose that I is not empty, which implies that $|I| \geq 2$, since $S_1(< a_j >)$ does not capitulate in L, $\forall\ 1 \leq j \leq k$, and hence $(b_j^{p^{m_j}})^{p+s^{p-1}} \neq 1$, for all $j \in I$. Then let $m := min_{j\in I}\{m_j\}$ and let $1 \leq l \leq k$ be such that $m_l = m$ and $r_l = l(b_l)$ is maximal among all indices j satisfying $m_j = m$. Then, we set

$$\tilde{b}_l = \prod_{j\in I} b_j^{p^{m_j-m_l}}.$$

Observe that $ord(N_{L/K}(b_j^{p^{m_j-m_l}})) = p^{m_l+1} = ord(a_l)$, for all $j \in I$. Hence, $\{a_1, ..., a_{l-1}, N_{L/K}(\tilde{b}_l), a_{l+1}, ..., a_n\}$ is a basis of $A(K)'$. For all $j \in I$ with $m_j > m_l$, we have that $l(b_j^{p^{m_j-m_l}}) = 0$ due to $exp(B_j^s) \leq p$. For all $j \in I$ with $m_j = m_l$, we have that $r_l \geq r_j$. Thus, we obtain that $l(\tilde{b}_l) = l(b_l)$.
Using equation (*), it also follows that

$$\tilde{b}_l^{p^{m_l+1}} = \prod_{j\in I} b_j^{-p^{m_j}s^{p-1}}.$$

If $m_l > 0$, then obviously $\tilde{b}_l^{p^{m_l+1}} = 1$ and $\tilde{B}_l$ is exact. Assume now that $m_l = 0$ and let $I' \subset I$ such that $m_j = 0$ for all $j \in I'$. Then the above equation reads

$$\tilde{b}_l^p = \prod_{j\in I'} b_j^{-s^{p-1}} \in \tilde{B}_l^s,$$

implying that $\tilde{B}_l$ is exact. In both cases, we obtain a contradiction to the assumption that $(B_1, ..., B_n)$ is minimized and hence I must be empty. This proves the claim. □

Remark: In (c), the assumption that $exp(B_i^s) \leq p$, $\forall\ 1 \leq i \leq k$, seems essential. If $exp(B_i^s) > p$, for some $1 \leq i \leq k$, then $\tilde{B}_l$ from above is not necessarily exact anymore and the standard form assumption may be violated.

Chapter 3

On the Structure of the Capitulation Kernel in Unramified Cyclic Extensions

In this chapter, we want to investigate the structure of the capitulation kernel in unramified cyclic p-extensions of higher degree. Henceforth, let L/K be an unramified cyclic extension of degree p^n, where p is an odd prime and $n \in \mathbb{N}$. Let σ be a generator of the Galois group $G = Gal(L/K)$. For the ease of notation, we set $\mathcal{O}_L^* = E(L)$ and $\mathcal{O}_K^* = E(K)$. Also, we let μ_K and μ_L denote the group of roots of unity in K and L, respectively. For simplicity, we assume that L only contains the trivial roots of unity ± 1. Most of the following arguments, however, still hold when $\mu_L \neq \{\pm 1\}$. So far, the results of Chapter 2 only yield a statement about the cardinality of the capitulation kernel, namely

$$|P_K(L)| = [L : K] \cdot |\mathcal{H}^0(G, E(L))|.$$

This, however, neither yields any information on the structure of the capitulation kernel $P_K(L)$ nor does it explain how elements in $\mathcal{H}^0(G, E(L))$ give rise to capitulating ideals in L/K. On account of that, we illuminate the underlying concept of Galois cohomology with respect to capitulation and revisit Hilbert's ideas that led to Hilbert's Theorem 94 (see [22]). Subsequently, we push this approach further and present various generalizations of Hilbert's original ideas. In particular, we give sufficient conditions under which the Galois group $G(L/K)$ and the 0-th cohomology group $\mathcal{H}^0(G, E(L))$ can be embedded in the capitulation kernel $P_K(L)$. Guided by MAGMA, we then consider various examples where the above does not hold. In view of that, we generalize our approach and denominate further factors that influence the structure of the capitulation kernel. To this end, we introduce

the so-called *deep cohomology*, which contributes to a more subtle picture of $\mathcal{H}^{-1}(G, E(L))$. Due to the enormous complexity, we will then restrict ourselves to extensions of degree p^2. In this case, the rank of the capitulation kernel already yields the precise structure of $P_K(L)$. We conclude the first section with a result that gives us a concrete formula for the rank of $P_K(L)$. In the second section, we supplement the theoretic results of the first section by giving some numerical data of concrete unramified cyclic extensions L/K of degree 9 and their capitulation kernels $P_K(L)$. We then compare the theoretic results of Section 1 with the developed database of Section 2.

3.1 Unramified Cyclic p-Extensions of Higher Degree and the Deep Cohomology

Let r_1 be the number of real embeddings of K, r_2 be the number of pairs of complex embeddings of K, and set $r = r_1 + r_2$. By Dirichlet's Unit Theorem, we obtain that $rk(E(K)) = r - 1$. (Here $rk(E(K))$ denotes the $\mathbb{Z}$-rank of the $\mathbb{Z}$-torsion-free part $E(K)/\mu_K$). Let $e_2, ..., e_r \in E(K)$ be a $\mathbb{Z}$-basis of $E(K)/\mu_K$. Since $\mu_L = \{\pm 1\}$ by assumption, it follows that the e_i's are p-maximal in $E(L)$, i.e. $e_i \notin E(L)^p$, $\forall\ 2 \leq i \leq r$. Indeed, suppose that $e_2 = x^p$ for some $x \in E(L) \setminus E(K)$. Then $x^{\sigma-1} \neq 1$ and $x^{p(\sigma-1)} = 1$, i.e. $x^{\sigma-1}$ is a non-trivial p-th root of unity, which contradicts the assumption that $\mu_L = \{\pm 1\}$. Thus, the system $\{e_2, ..., e_r\}$ can be extended to a $\mathbb{Z}$-basis of $E(L)/\mu_L$. (From now on, we will neglect μ_L and we will only refer to $E(L)/\mu_L$ as $E(L)$. We certainly may do this as p is odd). Now let L_1 be the unique intermediate field of L/K of degree p^{n-1} over K with $\mathcal{O}_{L_1}^*$ being denoted by $E(L_1)$. Let $\{\epsilon_1, ..., \epsilon_\nu\} \subset E(L)$, $\nu \in \mathbb{N}$ such that its images form an $\mathbb{F}_p$-vector-space basis of $E(L)/(E(L_1)E(L)^{(s,p)})$, where $s = \sigma - 1$ and $E(L)^{(s,p)} = E(L)^s E(L)^p$.
Claim: $\nu = r$.
Proof: Note that the infinite places of K split completely in L due to $K \subset L \subset H(K)$. Dirichlet's Unit Theorem thus yields that

$$rk(E(L)) \;=\; p^n r - 1 = r - 1 + r(p^n - 1). \tag{3.1}$$

For all $1 \leq i \leq \nu$, we also have that $rk(< \epsilon_i^s, ..., \epsilon_i^{sp^{n-1}} >) = p^n - 1$. This follows from elementary computations, using that $\epsilon_i \notin E(L_1)E(L)^{(s,p)}$. (Also recall the results of Proposition 2.6.2). Furthermore, note that $\epsilon_i^{sp^{n-1}} \in (< \epsilon_i, ..., \epsilon_i^{sp^{n-2}} > \cdot N_{L/K}(\epsilon_i))$. Combining the above arguments, one easily verifies that $< \epsilon_i >_{\mathbb{Z}[s]}$ *mod* $E(K)$ can be generated by a minimal number of $p^n - 1$ generators in $E(L)/E(K)$. By equation (3.1), we can then conclude

that $\nu = r$, i.e. we have

$$rk(< e_2, ..., e_r > \cdot < \epsilon_1, ..., \epsilon_r >_{\mathbb{Z}[s]}) = rk(E(L)).$$

Let us define $E(L)' =< e_2, ..., e_r > \cdot < \epsilon_1, ..., \epsilon_r >_{\mathbb{Z}[s]}$. By the theory on finitely generated free $\mathbb{Z}$-modules, we know that $E(L)'$ is of finite index in $E(L)$. However, the equality of the ranks of $E(L)'$ and $E(L)$ does not necessarily imply $E(L)' = E(L)$. However, in the case that $[L : K] = p$, we always have this equality since $E(L)^p \subset E(K)E(L)^s$. Henceforth, we will first analyze the case where $E(L) = E(L)'$ and later on the more general case where $E(L) \neq E(L)'$.

So let us first assume that

$$E(L) =< e_2, ..., e_r > \cdot < \epsilon_1, ..., \epsilon_r >_{\mathbb{Z}[s]} . \tag{3.2}$$

Let $t = rk(N_{L/K}(< \epsilon_1, ..., \epsilon_r >))$ and thus $t \leq r - 1$. Hence, there exist $\delta_i \in < \epsilon_1, ..., \epsilon_r >$, $1 \leq i \leq r - t$, such that $N_{L/K}(\delta_i) = 1$ and $\delta_i \notin E(L)^s$. It follows that $\mathcal{H}^{-1}(G, E(L))$ is not trivial and hence the capitulation kernel $P_K(L)$ not either. This recovers Hilbert's Theorem 94.
Let us now define

$$\delta_i = \prod_{j=1}^{r} \epsilon_j^{k_{i,j}},$$

where $k_{i,j} \in \mathbb{Z}$ and $1 \leq i \leq r - t$. Since $\mu_K = \{\pm 1\}$ by assumption, we may assume that $0 \leq k_{i,j} < p$. As $rk(< \delta_1, ..., \delta_{r-t} >) = r - t$, it then follows that $< \delta_1, ..., \delta_{r-t} >$ can be extended to a minimal system of generators of $< \epsilon_1, ..., \epsilon_r >$. Without loss of generality, we may thus assume that $\epsilon_i = \delta_i$, $\forall\ 1 \leq i \leq r - t$. By a suitable basis transformation of $\{e_2, ..., e_r\} \subset E(K)$, we may also assume, $\forall\ i = r - t + 1, ..., r$:

$$N_{L/K}(\epsilon_i) = e_i^{q_i},$$

where $1 \leq q_i \leq p^n$ and q_i is a p-th power.
We then define

$$\delta_i = \frac{\epsilon_i^{p^n/q_i}}{e_i},\ \forall\ r - t + 1 \leq i \leq r.$$

It then follows that $\delta_i \in ker N_{L/K}$, $\forall\ 1 \leq i \leq r$, and $|\mathcal{H}^0(G, E(L))| = \prod_{i=2}^{r} q_i$, where $q_i = p^n$, $\forall\ 2 \leq i \leq r - t$. (Note, however, that it may be possible that $\delta_i \in E(L)^s$, for some $r - t + 1 \leq i \leq r$). The above calculations show very well how non-trivial elements in $\mathcal{H}^0(G, E(L))$ yield non-trivial elements in $\mathcal{H}^{-1}(G, E(L))$, thus giving rise to capitulating ideal classes. The next proposition shows that the whole capitulation kernel is described by the above δ_i. More precisely, we have

Proposition 3.1.1. *Assume the situation as above, in particular $E(L)$ is given as in equation (3.2). Then we obtain that*

$$\mathcal{H}^{-1}(G, E(L)) =< \overline{\delta}_i >_{1\leq i\leq r},$$

where $\overline{\delta}_i$ denotes the image of δ_i in $E(L)/E(L)^s$, $\forall\ 1 \leq i \leq r$.

Proof. Let $x \in E(L)$ with $N_{L/K}(x) = 1$. By equation (3.2), there exist $k_j, l_i \in \mathbb{Z}$ such that

$$x \equiv \prod_{j=2}^{r} e_j^{k_j} \prod_{i=1}^{r} \epsilon_i^{l_i}\ mod\ E(L)^{\sigma-1}.$$

Since $\epsilon_i = \delta_i$, $\forall\ 1 \leq i \leq r-t$, and $e_i = \delta_i^{-1}\epsilon_i^{p^n/q_i}$, $\forall\ i = r-t+1, ..., r$, it follows that

$$x \equiv \prod_{j=2}^{r-t} e_j^{k_j} \prod_{i=r-t+1}^{r} \epsilon_i^{l_i}(\epsilon_i^{p^n/q_i})^{k_i}\ mod\ \ < \delta_i >_{1\leq i\leq r} \cdot E(L)^{\sigma-1}.$$

Due to $N_{L/K}(x) = 1$, we obtain that

$$N_{L/K}(\prod_{j=2}^{r-t} e_j^{-k_j}) = N_{L/K}(\prod_{i=r-t+1}^{r} \epsilon_i^{l_i}(\epsilon_i^{p^n/q_i})^{k_i}).$$

As $< e_1, ..., e_{r-t} > \cap N_{L/K}(< \epsilon_{r-t+1}, ..., \epsilon_r >) = 1$ and

$$rk(N_{L/K}(< \epsilon_{r-t+1}, ..., \epsilon_r >)) = r - t,$$

we can conclude that

$$\prod_{i=r-t+1}^{r} \epsilon_i^{l_i}(\epsilon_i^{p^n/q_i})^{k_i} = 1,\ \text{and}$$

$$\prod_{j=2}^{r-t} e_j^{k_j} = 1.$$

It follows that $x \in < \delta_i >_{1\leq i\leq r} \cdot E(L)^{\sigma-1}$ and hence the claim. □

Now we want to use the above proposition in order to give an upper bound for the rank of $\mathcal{H}^{-1}(G, E(L))$. For this purpose, we need to bound the rank of $< \overline{\delta}_i >_{1\leq i\leq r}$ in $E(L)/E(L)^s$. Let us have a look at the $\delta_i = \epsilon_i^{p^n/q_i}/e_i$ with

$i > r - t$. If $q_i = 1$, for some $i > r - t$, then $N_{L/K}(\epsilon_i) = e_i$ and hence $\delta_i = \epsilon_i^{p^n}/e_i \in E(L)^s$. Indeed,

$$\begin{aligned} \epsilon_i^{p^n}/e_i &= \prod_{k=0}^{p^n-1} \epsilon_i/\epsilon_i^{\sigma^k} \\ &= \prod_{k=0}^{p^n-1} (\epsilon_i^{\sigma^k-1})^{-1} \in E(L)^{\sigma-1}. \end{aligned}$$

We may now proceed with the next

Corollary 3.1.2. *Notations being like above, we have that*

$$rk(\mathcal{H}^{-1}(G, E(L))) = rk(\mathcal{H}^0(G, E(L))) + 1.$$

Moreover, there exist subgroups G_1, G_2 of $\mathcal{H}^{-1}(G, E(L))$ with $G_1 \cong G$ and $G_2 \cong \mathcal{H}^0(G, E(L))$ such that

$$\mathcal{H}^{-1}(G, E(L)) \cong G_1 \times G_2.$$

Proof. Let $m = rk(H^0(G, E(L)))$. By the above arguments and the previous proposition, we then easily obtain that $rk(\mathcal{H}^{-1}(G, E(L))) \leq m+1$. Without loss of generality, we may assume that $\delta_i \in E(L)^{\sigma-1}$, $\forall\ m+2 \leq i \leq r$, and that $< \overline{\delta}_1, ..., \overline{\delta}_{m+1} >= \mathcal{H}^{-1}(G, E(L))$. Observe that $ord(\overline{\delta}_i) \leq q_i, \forall\, r-t+1 \leq i \leq r$, due to

$$\delta_i^{q_i} = \epsilon_i^{p^n}/e_i^{q_i} = \epsilon_i^{p^n}/N_{L/K}(\epsilon_i) \in E(L)^{\sigma-1}.$$

As $ord(\overline{\delta}_i) \leq p^n$, $\forall\ 1 \leq i \leq r - t$, and $p^n \cdot |\mathcal{H}^0(G, E(L))| = |\mathcal{H}^{-1}(G, E(L))|$, we obtain that $ord(\overline{\delta}_i) = p^n$, $\forall\ 1 \leq i \leq r - t$, and that $ord(\overline{\delta}_i) = q_i$, $\forall\ r - t + 1 \leq i \leq r$. This finishes the proof. □

The following two examples show that the Galois group G of an unramified cyclic extension L/K cannot be embedded in the capitulation kernel $P_K(L)$ in general. We have

Example 1. Let $K = \mathbb{Q}(\alpha)$ be an imaginary quadratic number field with $\alpha^2 = 3299$. Then MAGMA yields that $A(K) =< a_1, a_2 > \cong C_3 \times C_9$. Let $L = H(K)^{<a_1>}$. Hence, L/K is cyclic of degree 9. By [21], it follows that $P_K(L) =< a_1, a_2^3 > \cong C_3 \times C_3$.

Example 2. Let $K = \mathbb{Q}(\alpha)$ be an imaginary quadratic number field with $65\alpha^2 + 168 = 0$. Then MAGMA yields that $A(K) =< a_1, a_2, a_3, a_4 > \cong$

$C_2 \times C_2 \times C_2 \times C_4$. Let $L = H(K)^{<a_1,a_2,a_3>}$. Then L/K is a cyclic extension of degree 4. MAGMA states that $P_K(L) =< a_1, a_2, a_3a_4^2 > \cong C_2 \times C_2 \times C_2$.

The above examples demonstrate that the assumption as in equation (3.2) is not always satisfied. In the following, we want to investigate the more general case where $E(L)' \neq E(L)$. In this case, the structure of the capitulation kernel depends on further parameters as we will see below. Due to the complexity, we will restrict ourselves to the case where $[L : K] = p^2$. In order to determine the structure of the capitulation kernel, it is then sufficient to determine the rank of $\mathcal{H}^{-1}(G, E(L))$. We start our analysis with

Proposition 3.1.3. *Let $K \subset L_1 \subset L \subset H(K)$ with $[L : L_1] = [L_1 : K] = p$ and $r - 1 = rk(E(K))$ be as before. Let $\{\epsilon_1, ..., \epsilon_r\} \subset E(L)$ be a system with $dim_{\mathbb{F}_p}(< \overline{\epsilon}_1, ..., \overline{\epsilon}_r >) = r$ in $E(L)/(E(L_1)E(L)^{(s,p)})$. Then*

$$E(L) = E(L_1) \cdot < \epsilon_1, ..., \epsilon_r >_{\mathbb{Z}[s]} .$$

Proof. First observe that $rk(E(L_1)) = pr - 1$. Moreover, one verifies that the system $\{\epsilon_1, ..., \epsilon_1^{s^{p-2}}, ..., \epsilon_r, ..., \epsilon_r^{s^{p-2}}\}$ is independent over $E(L_1)E(L)^{(\sigma^p-1,p)}$. Further elementary computations then reveal the claim, noting that $E(L)^p \subset E(L_1)E(L)^s$. □

Definition: Notations being like above, we define the *deep cohomology of* L/L_1 as

$$\overline{\mathcal{H}}^0(L/L_1) = E(L_1)/(E(K)E(L_1)^{(s,p)}N_{L/L_1}(E(L))).$$

Remark: 1) Obviously, $\overline{\mathcal{H}}^0(L/L_1)$ is isomorphic to a subgroup of the 0-th cohomology group $\mathcal{H}^0(Gal(L/L_1), E(L))$.

2) Let $\gamma \in E(L_1)$. Then $\gamma \in E(K)E(L_1)^{(s,p)} \Leftrightarrow \gamma \in E(K)E(L)^{(s,p)}$. This is an elementary computation.

Proposition 3.1.4. *Notations being like above, we have that*

$$dim_{\mathbb{F}_p}(E(L)/(E(K)E(L)^{(s,p)})) = r + dim_{\mathbb{F}_p}(\overline{\mathcal{H}}^0(L/L_1)).$$

Proof. Let $< \epsilon_1, ..., \epsilon_r > \subset E(L)$ be as in the previous proposition. Then:

$$rk(< e_2, ..., e_r > \cdot < \epsilon_1, ..., \epsilon_r >_{\mathbb{Z}[s]}) = rk(E(L)) = p^2r - 1.$$

It follows that

$$< e_2^p, ..., e_r^p > \cdot < N_{L/L_1}(\epsilon_i), ..., N_{L/L_1}(\epsilon_i)^{s^{p-2}} >_{1 \leq i \leq r}$$

has the same rank as $E(L_1)$, namely $pr-1$. In particular, $N_{L/L_1}(\epsilon_i) \neq 1$, for all $1 \leq i \leq r$. It follows that $N_{L/L_1}(E(K) \cdot < \epsilon_1, ..., \epsilon_r >_{\mathbb{Z}[s]}) = N_{L/L_1}(E(L))$, observing that $E(L) = E(L_1) \cdot < \epsilon_1, ..., \epsilon_r >_{\mathbb{Z}[s]}$ by Proposition 3.1.3. Let $I \subset \{1, ..., r\}$ such that $N_{L/L_1}(\epsilon_j) \in E(L_1)^p$ for all $j \in I$ and $N_{L/L_1}(\epsilon_j) \notin E(L_1)^p$, for all $j \in \{1, ..., r\} \setminus I$. For all $j \in I$, we choose some p-maximal $\gamma_j \in E(L_1)$ such that $N_{L/L_1}(\epsilon_j) = \gamma_j^p$ and for all $j \notin I$, we choose some p-maximal $\gamma_j \in E(L_1)$ such that $N_{L/L_1}(\epsilon_j) = \gamma_j$. Let $\overline{\gamma}_j$ be the image of γ_j in $E(L)/(E(K)E(L)^{(s,p)})$, for all $1 \leq j \leq r$. Then the previous arguments reveal that

$$< \overline{\epsilon}_1, ..., \overline{\epsilon}_r > \cdot < \overline{\gamma}_j >_{j \in I} = E(L)/(E(K)E(L)^{(s,p)}).$$

More precisely, we have that $< \overline{\epsilon}_1, ..., \overline{\epsilon}_r >$ and $< \overline{\gamma}_j >_{j \in I}$ are disjoint since otherwise we would get a contradiction to the fact that $dim_{\mathbb{F}_p}(< \overline{\epsilon}_1, ..., \overline{\epsilon}_r >) = r$ in $E(L)/(E(L_1)E(L)^{(s,p)})$. (Note: In the proof $\overline{\epsilon}_i$ denotes the image of ϵ_i in both $E(L_1)E(L)^{(s,p)}$ and $E(K)E(L)^{(s,p)}$). By Remark 2) before this proposition, the claim now follows. □

Let $\{\epsilon_1, ..., \epsilon_r\}$ be as above and $t = rk(N_{L/K}(< \epsilon_1, ..., \epsilon_r >))$. As before, we may assume that $< \epsilon_1, ..., \epsilon_{r-t} > \subset ker N_{L/K}$ and set $\delta_i = \epsilon_i$ for all $1 \leq i \leq r-t$. By a suitable basis transformation of $\{e_2, ..., e_r\} \subset E(K)$, we may also assume for all $i = r-t+1, ..., r$:

$$N_{L/K}(\epsilon_i) = e_i^{q_i},$$

where $1 \leq q_i \leq p^2$ and q_i is a p-th power.
We then define

$$\delta_i = \epsilon_i^{p^2/q_i}/e_i, \ \forall \ i = r-t+1, ..., r.$$

It then follows that $\delta_i \in ker N_{L/K}$, for all $1 \leq i \leq r$. The above proposition shows that the system $(\overline{\delta}_i)_{1 \leq i \leq r}$ does not necessarily generate $\mathcal{H}^{-1}(G, E(L))$ anymore. Indeed, the γ_j, $j \in I$, may also give rise to capitulating ideal classes:
Let $j \in I$. If $\gamma_j \in ker N_{L/K}$, then we define $\beta_j = \gamma_j$. If $\gamma_j \notin ker N_{L/K}$, we obtain that $N_{L/K}(\gamma_j) = N_{L/K}(\epsilon_j) = e_j^{q_j}$. Then we define $\beta_j = \gamma_j^{p^2/q_j}/e_j$. Note: If $q_j = p$, then $\delta_j \equiv \beta_j \ mod \ E(L)^s$. We are now prepared to state the next

Proposition 3.1.5. *Notations being like above, let $J'' \subset \{1, ..., r\}$ such that for all $j \in J''$, we have that $N_{L/L_1}(\epsilon_j) = \gamma_j^p$ and $N_{L_1/K}(\gamma_j) = e_j$. It then follows that*

$$\mathcal{H}^{-1}(G, E(L)) =< \overline{\delta}_i >_{1 \leq i \leq r} \cdot < \overline{\beta}_j >_{j \in I} \cdot < \overline{\epsilon_j/\gamma_j} >_{j \in J''},$$

where for $x \in E(L)$, $\overline{x}$ denotes the image of x in $E(L)/E(L)^{\sigma-1}$.

Proof. The proof follows from Proposition 3.1.3 and by a slight modification of the proof of Proposition 3.1.1. The details can be verified in a straightforward way. □

In order to determine the structure of the capitulation kernel precisely, we still need some further information on the structure of $\mathcal{H}^0(G, E(L))$ and on $\mathcal{H}^0(Gal(L_1, K), E(L_1))$. For instance, if $N_{L/K}(\epsilon_j) = e_j^p$, for some $j \in \mathbb{N}$, then we cannot say if $N_{L/L_1}(\epsilon_j)$ is in $E(L_1)^p$ or not. The following proposition describes the rank of $\mathcal{H}^{-1}(G, E(L))$ more exactly. For the ease of notation, we set for an arbitrary Galois extension M/F: $\mathcal{H}^i(Gal(M/F), E(M)) = \mathcal{H}^i(M/F)$, $i = -1, 0, 1$. Also, we define

$$d = |\{\epsilon_j,\ r - t + 1 \leq j \leq r :\ N_{L/L_1}(\epsilon_j) = \gamma_j^p,\ N_{L_1/K}(\gamma_j) = e_j\}|.$$

The subsequent proposition comprises all of the previous results and yields a concrete formula for the cardinality of the capitulation kernel $P_K(L)$. We have

Proposition 3.1.6. *Notations being like, it follows that*

$$rk(\mathcal{H}^{-1}(L/K)) = rk(\mathcal{H}^0(L/K)) + rk(\overline{\mathcal{H}}^0(L/L_1)) + 1 - d.$$

Proof. For $1 \leq i \leq r$, let ϵ_i and δ_i be defined as above. Also, let β_j, $j \in I$, and $t = rk(N_{L/K}(< \epsilon_1, ..., \epsilon_r >))$ be as before. By construction, we have that $\epsilon_i \in ker N_{L/K}$, for all $1 \leq i \leq r-t$, and hence that $rk(< \overline{\delta}_1, ..., \overline{\delta}_{r-t} >) = r-t$ in $E(L)/E(L)^s$. Let $J \subset \{r - t + 1, ..., r\}$ such that for all $j \in J$, we have that $N_{L/K}(\epsilon_j) = e_j^{p^2}$ and thus $\delta_j = \epsilon_j/e_j$. In particular, $N_{L/L_1}(\epsilon_j) = \gamma_j^p$, which yields $\beta_j = \gamma_j/e_j \in ker N_{L/K}$ with $\delta_j \beta_j^{-1} \notin E(L)^s$ by the choice of ϵ_j. It then follows that in $E(L)/E(L)^s$:

$$rk(< \overline{\delta}_1, ..., \overline{\delta}_{r-t} > \cdot < \overline{\delta}_j, \overline{\beta}_j >_{j \in J}) = r - t + |J| + rk(< \overline{\beta}_j >_{j \in J}).$$

Observe that $rk(< \overline{\beta}_j >_{j \in J})$ equals $rk(< \overline{\gamma}_j >_{j \in J})$ in $\overline{\mathcal{H}}^0(L/L_1)$. Let $J' \subset \{r - t + 1, ..., r\} \setminus J$ such that for all $j \in J'$, we have that $N_{L/K}(\epsilon_j) = e_j^p$.

Note that obviously $\delta_i \in E(L)^s$ for all $i \in \{r-t+1, ..., r\} \setminus \{J \cup J'\}$, i.e. for all δ_i with $N_{L/K}(\delta_i) = e_i$. Now let $j \in J'$ and hence $N_{L/K}(\epsilon_j) = e_j^p$. If $N_{L/L_1}(\epsilon_j) \in E(L_1)^p$, then $N_{L/L_1}(\epsilon_j) = \gamma_j^p$. By construction of ϵ_j, it follows that $\epsilon_j/\gamma_j \in ker N_{L/K} \setminus E(L)^s$. Since $N_{L_1/K}(\gamma_j) = e_j$, it follows that $\gamma_j^p/e_j \in E(L_1)^s$. Due to $\epsilon_j^p/e_j \equiv \gamma_j^p/e_j \; mod \; E(L)^s$, this implies that also $\delta_j = \epsilon_j^p/e_j \in E(L)^s$.
Again let $j \in J'$, $N_{L/K}(\epsilon_j) = e_j^p$, and now suppose that $N_{L/L_1}(\epsilon_j) \notin E(L_1)^p$. Then, $N_{L/L_1}(\epsilon_j) = \gamma_j$ and $N_{L_1/K}(\gamma_j) = e_j^p$. It follows that

$$\gamma_j/e_j \in ker N_{L_1/K} \setminus E(L_1)^s.$$

A moment of reflection also shows that $\gamma_j/e_j \in ker N_{L/K} \setminus E(L)^s$. Since, $\epsilon_j^p/e_j = (\epsilon^p/\gamma_j)(\gamma_j/e_j) \equiv \gamma_j/e_j \; mod \; E(L)^s$, it follows that $\overline{\delta}_j = \overline{\gamma_j/e_j}$.
All in all, we have that

$$rk(\mathcal{H}^{-1}(L/K)) = rk(\mathcal{H}^0(L/K)) + 1 + rk(< \overline{\gamma_j} >_{j \in J}),$$

where $\overline{\gamma_j}$ denotes the image of γ_j in $\overline{\mathcal{H}}^0(L/L_1)$. As $rk(< \overline{\gamma_j} >_{j \in J}) = rk(\overline{\mathcal{H}}^0(L/L_1)) - d$, we finally obtain the claim by the previous proposition. □

Remark: 1) The proof yields that $d \leq rk(\overline{\mathcal{H}^0}(L/L_1))$. Hence,

$$rk(\mathcal{H}^{-1}(L/K)) \geq rk(\mathcal{H}^0) + 1.$$

2) By the proof of Corollary 3.1.2, we obtain that both $\mathcal{H}^0(L/K)$ and $Gal(L/K)$ can be embedded in the capitulation kernel $P_K(L)$ in the case that $d = rk(\overline{\mathcal{H}^0}(L/L_1))$.

In the next section, we compile some computational data concerning the structure of the capitulation kernel in unramified cyclic extension of degree 9.

3.2 Numerical Data for Capitulation in Unramified Cyclic Extensions of Degree 9

In this section, we supplement the theoretic results of the previous section by computing the capitulation kernels of various unramified cyclic extensions L/K of degree 9, assuming that the base field K is imaginary quadratic. In particular, we are interested in the question whether such a capitulation kernel is isomorphic to C_9 or isomorphic to $C_3 \times C_3$, or equivalently in the question if the Galois group $Gal(L/K)$ can be embedded in the capitulation

kernel. The previous section has shown that this is not the case in general, but one may ask how likely it is that $Gal(L/K)$ is isomorphic to $P_K(L)$. (Observe that $|P_K(L)| = 9$ by the results of Chapter 2). In the following list, we consider imaginary quadratic fields with $A(K) \cong C_3 \times C_9$, i.e. with the easiest non-cyclic class groups having a cyclic subgroup of order 9. Let $A(K) =< a_1, a_2 >$ with $ord(a_1) = 3$ and $ord(a_2) = 9$. We then obtain four subfields $L_1, ..., L_4$ of $H(K)/K$ with $[L_i : K] = 9$. Let the ordering be as follows:
$L_1 = H(K)^{<a_1>}$, $L_2 = H(K)^{<a_1 a_2^3>}$, $L_3 = H(K)^{<a_1^2 a_2^3>}$, and $L_4 = H(K)^{<a_2^3>}$. It follows that $Gal(L_i/K) \cong C_9$, for $i = 1, 2, 3$, and $Gal(L_4/K) \cong C_3 \times C_3$. In the subsequent list, the capitulation type is given in the form $(P_K(L_i))_{i=1,...,4}$ and $S_1 = S_1(A(K))$ will denote the 1-socle of $A(K)$. We have:

Nr.	Discriminant	Capitulation Type
1	-3299	(S_1,S_1,S_1,S_1)
2	-5703	$(a_1a_2,\ a_2,\ a_1a_2,\ S_1)$
3	-10015	(S_1,S_1,S_1,S_1)
4	-11561	(S_1,S_1,S_1,S_1)
5	-17728	(S_1,S_1,S_1,S_1)
6	-19427	$(a_2,\ a_1a_2,\ a_1^2a_2,\ S_1)$
7	-19919	(S_1,S_1,S_1,S_1)
8	-27635	$(a_2,\ a_1^2a_2,\ a_1a_2,\ S_1)$
9	-27656	(S_1,S_1,S_1,S_1)
10	-31983	(S_1,S_1,S_1,S_1)
11	-33879	(S_1,S_1,S_1,S_1)
12	-34603	(S_1,S_1,S_1,S_1)
13	-35331	(S_1,S_1,S_1,S_1)
14	-38296	$(a_1a_2,a_1^2a_2,a_2,S_1)$
15	-43763	(S_1,S_1,S_1,S_1)
16	-48039	(S_1,S_1,S_1,S_1)
17	-56132	$(a_2,a_1a_2,a_1^2a_2,S_1)$
18	-57336	$(a_1^2a_2,a_2,a_2,S_1)$
19	-64571	$(a_2,a_1a_2,a_1^2a_2,S_1)$
20	-62527	(S_1,S_1,S_1,S_1)

The above table comprises $20 \cdot 3 = 60$ different unramified cyclic extensions of degree 9. In 39 cases, we have that $P_K(L) \cong C_3 \times C_3$, i.e. in roughly 2/3 of the cases. This underlines that the assertion of equation (3.2) is not only wrong in general, but it is violated with rather high frequency.

Chapter 4

Growth of Ideal Classes in Extensions with F-Property

After Furtwängler had proved the Principal Ideal Theorem in 1932, he posed the following question: Let K be a number field and let $H^{(i+1)}(K)$ denote the Hilbert class field of $H^{(i)}(K)$, for $i \geq 0$. Then Furtwängler asked if this tower of Hilbert class fields eventually terminates? In the case that $H^{(k+1)}(K) = H^{(k)}(K)$, for some $k \in \mathbb{N}$, one says that K has a class field tower of length k. In 1964, Golod and Shafarevich, however, proved that the Hilbert class field tower of a number field can also be infinite, see [29]. Whereas the above question implicitly deals with the growth of ideal classes of successive Hilbert class fields, we henceforth want to study the growth of ideal classes in a given unramified cyclic extension of prime degree.
In what follows, let L/K be an extension of degree p and let $A(K)'$ denote the image of $A(L)$ arising from the norm map $N_{L/K}$. In this chapter, we want to compare the ideal classes of K and L. In particular, we are interested in the following question: Let a and b be ideal classes in K and L, respectively, with $N_{L/K}(b) = a$. How is the order of b related with the order of a? If L/K satisfies the F-property, then the index of $A(K)'$ in $A(K)$ is p or trivial. Thus, $A(K)'$ is a good approximation for the ideal class of K. Since the norm maps the ideal class of L onto $A(K)'$, it follows that $A(K)'$ is contained in $A(L)$ in some sense. Hence, it makes sense to speak of the *growth of ideal classes*. Once we have examined the growth of ideal classes in extension of degree p, we can generalize the results to p-extensions, simply by splitting them into extensions of degree p.
It is quite evident that the analysis of such a growth is inextricably linked with the capitulation problem. Indeed, let b be a non-trivial ideal class in L with $N_{L/K}(b) = a$ as above. We will then show that under certain conditions

the following relation holds:

$$ord(b) \;=\; p \cdot ord(\imath_{L/K}(N_{L/K}(b))). \tag{4.1}$$

It then follows that a capitulates in L if and only if $ord(b) = ord(a)$.
For a more sophisticated investigation, we distinguish between four different types of growth: stable growth, tame growth, semi-stable growth, and wild growth. We then show that equation (4.1) holds for the first three types in the case that a can be extended to a minimal system of generators of $A(K)'$. In the last section, we show that in general there is no bound for the growth of ideal classes. More precisely, we demonstrate that $exp(ker N_{L/K})$ can be arbitrarily large. To this end, we construct a family of finite p-groups G such that G contains an abelian normal subgroup of index p and such that $exp(G')$ is arbitrarily large. A theorem due to Ozaki then tells us that there exist unramified cyclic extensions L/K of degree p with $Gal(H(L)/K) \cong G$, thus showing that $G' \cong ker N_{L/K}$ is unbounded as G ranges of the constructed family of p-groups. Supported by MAGMA, we supplement these theoretic results by giving concrete examples for the various types of growth.

4.1 Preliminary Results on Finite Abelian p-Groups and a Classification of the Growth of Ideal Classes

In this section, we first state and prove some basic results on finite abelian p-groups. Subsequently, we classify the different types of the growth of ideal classes. From now on, let p be prime, A be a finite abelian p-group of rank r, denoted multiplicatively, and $\{a_1, ..., a_n\}$ a system of generators of A. Then we say $\{a_1, ..., a_n\}$ is a *minimal system of generators* of A if $n = r$. Moreover, we say a minimal system of generators $\{a_1, ..., a_r\}$ is a *basis* of A if every $a \in A$ has a unique representation of the form $a = \prod_{i=1}^{r} a_i^{k_i}$ with $0 \leq k_i < ord(a_i)$. We say $a \in A$ is *p-maximal* if $a \notin A^p$. Finally, we define the *subexponent* of A as $subexp(A) = min\{p^k,\ k \in \mathbb{N} :\ rk(A^{p^k}) < rk(A)\}$.
We start with some basic results on finite abelian p-groups and minimal systems of generators. We have

Proposition 4.1.1. *Let A be a finite abelian p-group and $\{a_1, ..., a_r\}$ be a minimal system of generators of A. Then $a_i \notin A^p$, for all $i = 1, ..., r$.*

Proof. Suppose $a_1 = a^p$, for some $a \in A$. Since $\{a_1, ..., a_r\}$ is a system of

generators, we have:

$$a = a^{k_1 p} \prod_{i=2}^{r} a_i^{k_i},$$

for some $k_i \in \mathbb{N}$, and thus

$$a^{1-k_1 p} = \prod_{i=2}^{r} a_i^{k_i}.$$

It follows that $< a^{1-k_1 p} >=< a > \subset span(a_2^{k_2}, ..., a_2^{k_r})$ and thus a_1 lies in $span(a_2^{k_2}, ..., a_2^{k_r})$, which yields a contradiction to $\{a_1, ..., a_r\}$ being a minimal system. □

Proposition 4.1.2. *Let A be a finite abelian p-group and $a \in A \setminus A^p$. Then a can be extended to a minimal system of generators of A.*

Proof. Let $\{a_1, ..., a_r\}$ be a basis of A. Then we have a unique representation for a of the form $a = \prod_{i=1}^{r} a_i^{k_i}$ with $0 \leq k_i < ord(a_i)$. Since $a \in A \setminus A^p$, we can assume that p does not divide k_1 without loss of generality. This implies that $< a_1 >=< a_1^{k_1} >$ and hence $\{a, a_2, ..., a_r\}$ forms a minimal system of generators of A. □

Proposition 4.1.3. *Let A be a finite abelian p-group of rank r and $\{a_1, ..., a_r\}$ be a system of elements in A. Then $\{a_1, ..., a_r\}$ is a minimal system of generators of A if and only if the system $\{a_1 A^p, ..., a_r A^p\}$ forms a basis of the $\mathbb{F}_p$-vector-space A/A^p.*

Proof. First, we assume that $\{a_1, ..., a_r\}$ is a minimal system of generators of A and that $\{a_1 A^p, ..., a_r A^p\}$ does not form a basis of A/A^p. Without loss of generality, we may then assume that there exist $0 \leq k_i < p$, $i = 2, ..., r$, with $a_1 A^p = \prod_{i=2}^{r} a_i^{k_i} A^p$ which implies that $a_1 = \prod_{i=2}^{r} a_i^{k_i} a^p$ for some $a \in A$. It follows that $\{a_1, ..., a_r\} = \{a^p, a_2, ..., a_r\}$. This, however, yields a contradiction to Proposition 4.1.1.
Now let us assume that $\{a_1 A^p, ..., a_r A^p\}$ forms a basis of A/A^p. It is then sufficient to show that $A' :=< a_1, ..., a_r >$ equals A. Let $a \in A$. By assumption, there exist $k_i \in \mathbb{Z}$ $(1 \leq i \leq r)$ and some $b \in A$ such that

$$a = \prod_{i=1}^{r} a_i^{k_i} b^p.$$

Iterating this procedure, it follows for sufficiently large $l > 0$:

$$a \in A' \cdot A'^{p} \cdots A'^{p^l} \subset A'.$$

Hence, $A \subset A'$, which completes the proof. □

We proceed with further elementary observations on the structure of finite abelian groups. We have

Lemma 4.1.4. *Let A be a finite abelian p-group, denoted multiplicatively, and $a \in A$. Then*

$$rk(A/ < a >) = rk(A) - 1 \text{ if } a \notin A^p \text{ and}$$

$$rk(A/ < a >) = rk(A) \text{ if } a \in A^p.$$

Proof. The proof follows immediately from the previous assertions. □

Proposition 4.1.5. *Let A be a finite abelian p-group of rank s, $A' \subset A$ a subgroup of rank $0 < r \leq s$, and $rk(A/A') = s-l$, for some $l \in \mathbb{N}$. Then there is a system $\{a'_1, ..., a'_l\} \subset A'$ which can be extended to a minimal generating system of A.*

Proof. Assume that there is a system $\{a'_1, ..., a'_k\} \subset A'$ $(k \geq 0)$, which can be extended to a minimal generating system of A and that k is maximal with this property. Then A has a minimal generating system of the form $\{a'_1, ..., a'_k, a_{k+1}, ..., a_s\}$ and A' has a minimal generating system of the form $\{a'_1, ..., a'_k, a'_{k+1}, ..., a'_r\}$. (By the previous proposition, $\{a'_1, ..., a'_k\}$ can a fortiori be extended to a minimal generating system of A'). We define $A_{k+1} =< a_{k+1}, ..., a_s >$, $A'_{k+1} =< a'_{k+1}, ..., a'_r >$, and $\bar{A} =< a'_1, ..., a'_k >$. It then follows that

$$A/A' \cong A_{k+1}\bar{A}/A'_{k+1}\bar{A}.$$

Clearly, $k \leq l$. Assume that $k < l$. Since $rk(A/A') = s - l < s - k$, it thus follows that

$$rk(A_{k+1}) = s - k > rk(A_{k+1}\bar{A}/A'_{k+1}\bar{A}).$$

A moment of reflection shows that this implies that there exists a non-trivial $a' \in A'_{k+1}$ with $a \notin A^p$. Hence, $\{a'_1, ..., a'_k, a'\}$ can be extended to a minimal generating system of A, which yields a contradiction to the assumption that k was maximal. Thus, $k = l$. □

For the further analysis of the growth of ideal classes, we introduce the following classification. (In the course of the discussion, the denominations become more comprehensible). We have

Definition: Let L/K be a Galois extension of degree p satisfying the F-property. Let $G = Gal(L/K)$ generated by some $\sigma \in G$ and $s = \sigma - 1$. We define $A(K)' = N_{L/K}(A(L))$ and set $N = N_{L/K}$. Then we say L/K has

(a) *stable growth* if $rk(A(K)') = rk(A(L))$ and $subexp(A(K)') > p$;

(b) *tame growth* if $subexp(A(K)') > p$ and $A(L)$ has a basis of the form $\{b_1, .., b_r, b_{r+1}, .., b_t\}$ with $N(b_j) = 1,\ \forall\ r+1 \leq j \leq t$, and $\{N(b_1), ..., N(b_r)\}$ forms a minimal system of generators of $A(K)'$;

(c) *semi-stable growth* if $A(L)^{s^{p-1}} = \{1\}$;

(d) *wild growth*, otherwise.

Remark: We will treat the cases (a) and (b) in greater generality and we do not need the F-property there. In the later chapters, however, we are mainly interested in the case where L/K is unramified and so we have chosen the above setting. Henceforth, we will analyze the growth of ideal classes in the various cases listed above beginning with stable and tame growth.

4.2 Stable Growth of Ideal Classes

We start with the investigation of stable growth. The analysis of stable growth essentially goes back to Preda Mihailescu. The following theorem discusses stable growth in a more general context. We have

Theorem 4.2.1. *Let A and B be finite abelian p-groups, denoted additively, with $subexp(A) > p$. Let $N : B \to A$ and $\imath : A \to B$ be group homomorphisms such that:*
(i) N is surjective;
(ii) $rk(A) = rk(B)$;
(iii) $N(\imath(a)) = pa$, for all $a \in A$.
Then $\imath(A) = pB$ and $ord(b) = p \cdot ord(\imath(Nb))$, for all non-trivial $b \in B$.

Proof. The maps N and $\imath$ induce maps $\bar{N} : B/pB \to A/pA$ and $\bar{\imath} : A/pA \to B/pB$. By (i) we obtain that $\bar{N}$ is surjective and by (ii) it follows that $\bar{N}$ is also injective and hence $\bar{N}$ is a group isomorphism. Moreover, we can conclude that the map $\bar{N} \circ \bar{\imath}$: $A/pA \to A/pA$ is the trivial map due to (iii). It follows that $\imath(A) \subset pB$.

Now let $\{b'_1, ..., b'_r\}$ be a minimal system of generators of B. Hence, the images $\overline{b'_i}$ of b'_i in B/pB form an $\mathbb{F}_p$-basis of B/pB. Let $a_i = N(b'_i)$ for $i = 1, ..., r$. Let $\overline{a_i}$ denote the images of a_i in A/pA. Since $\bar{N}$ is a group isomorphism, we obtain that the system $\{\bar{a_i}\}_{1 \leq i \leq r}$ forms an $\mathbb{F}_p$-basis of A/pA. Thus, $\{a_1, ..., a_r\}$ is a minimal system of generators of A by Proposition 4.1.3. Now let $a'_i = \imath(a_i)$. Then $\{a'_1, ..., a'_r\}$ forms a minimal system of $\imath(A)$ as $\imath$ is rank preserving due to (iii) and $subexp(A) > p$. For all $1 \leq i \leq r$, let $b_i \in B$ with $p^{e_i} b_i = a'_i$ and $e_i \geq 0$ maximal among all possible choices of b_i. A moment of reflection shows that $\{b_1 \cdot pB, ..., b_r \cdot pB\}$ forms an $\mathbb{F}_p$-basis of B/pB since $\{a_1 \cdot pA, ..., a_r \cdot pA\}$ forms an $\mathbb{F}_p$-basis of A/pA. Hence, $\{b_1, ..., b_r\}$ is a minimal system of generators of B by Proposition 4.1.3. Furthermore, $\imath(A) \subset pB$ implies that $e_i \geq 1$, for all $1 \leq i \leq r$. As $\{b'_1, ..., b'_r\}$ is a minimal system of generators, there is a matrix $E \in Mat(r, \mathbb{Z})$ with $\vec{b} = E \cdot \vec{b'}$, where $\vec{b} = (b_1, ..., b_r)^T$ and $\vec{b'} = (b'_1, ..., b'_r)^T$. ($M^T$ denotes the transponent matrix of a matrix M). (Accordingly, $\vec{a} = (a_1, ..., a_r)^T$ and $\vec{a'} = (a'_1, ..., a'_r)^T$). Let $\mathbf{Diag}(p^{e_i})$ denote the $r \times r$ diagonal matrix with entries $p^{e_1}, ..., p^{e_r}$. It then follows that

$$\imath(\vec{a}) = \vec{a'} = \mathbf{Diag}(p^{e_i})\vec{b} = \mathbf{Diag}(p^{e_i})E \cdot \vec{b'}.$$

Also, the group homomorphism $N : B \to A$ acts component wise on vectors in the Cartesian product B^r and hence

$$N(\vec{b}) = N(E \cdot \vec{b'}) = E \cdot N(\vec{b'}) = E \cdot \vec{a}.$$

Combining the two above results and denoting the unit matrix by I, we obtain that

$$\begin{aligned} N(\vec{a'}) &= p\vec{a} = pI \cdot \vec{a} = N(\mathbf{Diag}(p^{e_i})\vec{b}) = \mathbf{Diag}(p^{e_i}) \cdot N(\vec{b}) \\ &= \mathbf{Diag}(p^{e_i}) \cdot E\vec{a}. \end{aligned}$$

It follows that

$$\vec{a} = \mathbf{Diag}(p^{e_i - 1}) \cdot E\vec{a} + \vec{x},$$

where $\vec{x} = (x_1, ..., x_r)$ with $x_i \in A$ and $ord(x_i) = p$, for all $1 \leq i \leq r$. Since $subexp(A) > p$, it follows that $x_i \in pA$. Now let $E\vec{a} =: \vec{\alpha} = \{\alpha_1, ..., \alpha_r\}$. As $\{a_1, ..., a_r\}$ is a minimal system of generators, we obtain that $\mathbf{Diag}(p^{e_i - 1}) \cdot \vec{\alpha} + \vec{x}$ is also a minimal generating system of A. Proposition 4.1.3 thus yields that $e_i = 1$, for all $1 \leq i \leq r$. Indeed, if $e_k \geq 2$ for some k, then $a_k \in pA$ due to $subexp(A) > p$. This proves that $\imath(A) = pB$.
Now we want to show that $ord(b) = p \cdot ord(\imath(Nb))$ holds for all non-trivial $b \in B$. If $b \in pB = \imath(A)$, $b \neq 1$, then there is an $a \in A$ with $\imath(a) = b$. It follows that $N(b) = N(\imath(a)) = pa$ and hence $\imath((N(b))) = \imath(pa) = p\imath(a) = pb$. This implies that $ord(b) = p \cdot ord(\imath(N(b)))$. Now let $b \in B \setminus pB$. First,

we show that $\imath(N(b)) \neq 1$. Indeed, since $b \notin pB$, Proposition 4.1.2 yields that we can extend b to a minimal system of generators of B. As $\bar{N}$ is an isomorphism, we obtain that $a := N(b) \notin pA$. As $a \notin pA$, we can also extend a to a minimal system of generators of A. Since $\imath$ is rank preserving, it follows that $\imath(a) = \imath(N(b)) \neq 1$. Due to $pb \in \imath(A)$ and $\imath(N(b)) \neq 1$, we can now conclude that

$$\begin{aligned} ord(b)/p &= ord(pb) = p \cdot ord(\imath(N(pb))) = p \cdot ord(p(\imath(N(b)))) \\ &= ord(\imath(N(b))) \end{aligned}$$

This yields the claim. □

Corollary 4.2.2. *Let L/K be an extension of degree p and $A(K)'$ as before. Assume that $subexp(A(K)') > p$ and that $rk(A(K)') = rk(A(L))$. Then $\imath_{L/K}(A(K)') = A(L)^p$ and*

$$ord(b) = p \cdot ord(\imath_{L/K}(N_{L/K}(b))),\ \forall\ b \in A(L),\ b \neq 1.$$

Proof. The proof follows immediately from the previous theorem. (Note that $A(K)$ and $A(L)$ are denoted multiplicatively and not additively as in the theorem above). □

Remark: Sören Kleine has shown that one can also relax the assumption that $subexp(A(K)') > p$ by replacing it with the assumption that $rk(A(L)^p) = rk(A(K)'^p)$.

4.3 Tame Growth of Ideal Classes

One natural question is to what extent can we generalize the results of the previous section in the case that $rk(A(K)') < rk(A(L))$. As in Section 4.2, we begin with some more general observations. We have the following

Theorem 4.3.1. *Let A and B be finite abelian p-groups, denoted additively, with $subexp(A) > p$. Moreover, let $N : B \to A$ and $\imath : A \to B$ be group homomorphisms such that:*
(i) N is surjective;
(ii) $N(\imath(a)) = pa$, for all $a \in A$;
(iii) $r = rk(A) < rk(B) = t$;

Also assume that there is a basis $\{b_1, .., b_r, b_{r+1}, .., b_t\}$ of B with $N(b_j) = 1$,

$r+1 \leq j \leq t$, *such that* $\{a_1 = N(b_1), ..., a_r = N(b_r)\} \subset A$ *forms a minimal system of generators of* A. *Then*

$$ord(b_j) \leq p \cdot ord(\imath(N(b_j))),\ \forall\ 1 \leq j \leq r.$$

Proof. Again, the maps N and $\imath$ induce maps $\bar{N} : B/pB \to A/pA$ and $\bar{\imath} : A/pA \to B/pB$. By assumption, it follows that $ker\bar{N} =< b_{r+1}, .., b_t > \cdot pB$. Also, (ii) yields that the map $\bar{N} \circ \bar{\imath}$: $A/pA \to A/pA$ is the trivial map. Thus, $\imath(A) \subset < b_{r+1}, .., b_t > \cdot pB$. Let $a_i' = \imath(a_i)$ for some $1 \leq i \leq r$. For the ease of notation, let us say that $i = 1$ without loss of generality. Then there are $k_1, .., k_t \in \mathbb{Z}$ such that

$$a_1' = k_1 p b_1 + ... + k_r p b_r + k_{r+1} b_{r+1} + ... + k_t b_t.$$

We claim that p does not divide k_1.
Proof: For the following, we set $\vec{a} = (a_1, ..., a_r)^T$. Since $N(b_j) = 1$, $\forall\ j = r+1, .., t$, and $N(b_j) = a_j$, $\forall\ 1 \leq j \leq r$, it follows that

$$pa_1 = N(a_1') = (k_1 p, ..., k_r p) \cdot \vec{a}.$$

Consequently, there is an $x \in A$ with $ord(x) = p$ such that

$$a_1 = (k_1, ..., k_r) \cdot \vec{a} + x.$$

Since $subexp(A) > p$, we obtain that $x \in pA$. Now assume that $p | k_1$. Then $a_1 \in (k_2, .., k_r) \cdot (a_2, .., a_r)^T + pA$. This, however, yields a contradiction since $rk(< a_1 \cdot pA, .., a_r \cdot pA >) = rk(A) = r$. Thus, the claim follows.
On the other hand, we have that

$$\begin{aligned} ord(\imath(N(b_1))) &= ord(a_1') \\ &= max\{ord(k_1 p b_1), .., ord(k_r p b_r), ord(k_{r+1} b_{r+1}), .., ord(k_t b_t)\} \end{aligned}$$

As $\{b_1, .., b_t\}$ is a basis of B and p does not divide k_1, we can conclude that

$$ord(\imath(N(b_1))) \geq ord(k_1 p b_1) = ord(b_1)/p, \text{ and hence}$$

$$ord(b_1) \leq p \cdot ord(\imath(N(b_1))).$$

This proves the theorem. □

In what follows, we apply the above result for the case of a field extension L/K of degree p. The previous theorem yields

Corollary 4.3.2. *Let L/K be an extension of degree p and $A(K)'$ as before with $subexp(A(K)') > p$. Let $rk(A(L)) = t > r = rk(A(K)')$. Assume that $\{b_1, .., b_r, b_{r+1}, .., b_t\}$ is a basis of $A(L)$ with $N_{L/K}(b_j) = 1$, $r+1 \leq j \leq t$, such that $\{N_{L/K}(b_j) = a_j\}_{1 \leq j \leq r}$ forms a minimal system of generators of $A(K)'$. Then*

$$ord(b_j) \leq p \cdot ord(\imath_{L/K}(N_{L/K}(b_j))), \ \forall \ 1 \leq j \leq r.$$

If L/K is cyclic and has the F-property, then equality holds in the above statement.

Proof. The proof of the inequality follows immediately from the previous theorem, noting that $A(K)$ and $A(L)$ are multiplicative groups. Now suppose that L/K is cyclic and has the F-property. Let $b_j \in A(L)$ be as above, for some $1 \leq j \leq r$. Obviously, $ord(b_j) > p$ by assumption. Assume that $ord(b_j) = ord(\imath_{L/K}(N_{L/K}(b_j)))$. Then $< b_j > \cap ker N_{L/K} = \{1\}$. By Section 2.5, we also have that $exp(ker N_{L/K}) = p$. As $ord(b_j) > p$, it follows that $< b_j > \cap A(L)^G \neq \{1\}$. This yields the desired contradiction. □

Remark: Again one can relax the assumption $subexp(A(K)') > p$ by replacing it by the assumption that $rk(< b_1, .., b_r >^p) = rk(< a_1, .., a_r >^p)$. The details are omitted here.

We conclude this section with an example where

$$ord(b_j) < p \cdot ord(\imath_{L/K}(N(b_j))), \text{ for some } 1 \leq j \leq r,$$

i.e. the case that $ord(b_j) = ord(\imath_{L/K}(N(b_j)))$ may occur as the following example shows. (Observe, however, that $subexp(A(K)') = p$).

Example: Consider the imaginary quadratic field

$$K = \mathbb{Q}(\alpha) \text{ with } \alpha^2 + 3896 = 0.$$

Then MAGMA yields:
(i) $A(K) =< a_1, a_2 > \cong C_3 \times C_3$, for some $a_1, a_2 \in A(K)$.
(ii) We define $L = H(K)^{<a_2>}$, which implies that $N_{L/K}(A(L)) =< a_2 > \cong C_3$. Using MAGMA, we obtain: $A(L) \cong C_3 \times C_3 \times C_3$.
(iii) $P_K(L) \cap N_{L/K}(A(L)) = \{1\}$.
Since $N_{L/K}$ is surjective, there is an ideal class $b \in A(L)$ with $N_{L/K}(b) = a_2$ and one observes that b can be extended to a basis $< b, b_2, b_3 >$ of $A(L)$ with $< b_2, b_3 >= ker N_{L/K}$, i.e. the assumptions of the previous theorem are satisfied apart from $subexp(A(K)') > p$. By (iii), it follows that

$$ord(b) = ord(\imath_{L/K}(N_{L/K}(b)).$$

Later in this chapter, we show that even $ord(b_j) \leq p \cdot ord(\imath_{L/K}(N_{L/K}(b_j)))$ does not hold if we relax the assumption of the previous theorem. In Section 4.5, we will even show that there are no general bounds for the exponent of $ker N_{L/K}$.

4.4 Semi-Stable Growth of Ideal Classes

Henceforth, we want to study semi-stable growth. Whereas L/K was an arbitrary extension of degree p in the previous corollary, we now assume that L/K is a cyclic extension of degree p, satisfying the F-property. Let $\sigma \in G(L/K)$ be a generator of $G = G(L/K)$ and $s = \sigma - 1$. We assume that L/K has semi-stable growth, i.e. $A(L)^{s^{p-1}} = \{1\}$. Suppose that $exp(A(L)^s) = p^l$, for some $l \in \mathbb{N}$, and let b be a non-trivial ideal class in L. Recall Proposition 2.6.2 (iii): Setting $R = \mathbb{Z}[s]/(s^{p^l})$, it follows that $A(L)^s$ is an R-module and due to $A(L)^{s^{p-1}} = \{1\}$, we can derive that

$$\imath_{L/K}(N_{L/K}(b)) = b^{1+\sigma+\ldots+\sigma^{p-1}} = b^{pu'},\ u' \in R^*.$$

In particular, $p \cdot ord(\imath_{L/K}(N_{L/K}(b))) = ord(b)$, for all non-trivial $b \in A(L)$.

Heuristics: If p tends to infinity, the likelihood of $A(L)^{s^{p-1}}$ being trivial should go to 1, i.e. if p is large, then L/K has semi-stable growth with a rather high probability. (Also see Chapter 6). In this case, equation (4.1) applies.

We now want to generalize the above definition to an unramified abelian p-extension L/K. We say that L/K has semi-stable growth if there exists a tower $K \subset L_1 \subset L_2 \subset \ldots \subset L_k = L$ such that $[L_{i+1} : L_i] = p$ and L_{i+1}/L_i is semi-stable, $\forall\ 1 \leq i \leq k-1$. We then have

Proposition 4.4.1. *Let L/K be an unramified abelian extension with semi-stable growth. Then*

$$\imath_{L/K}(N_{L/K}(b)) = b^{[L:K]},\ \forall\ b \in A(L).$$

Proof. Let $p^n = [L : K]$. Then, we may prove the proposition by induction on n. For $n = 1$, we have already established the result. Now let $n > 1$ and $K \subset L' \subset L$ with $[L' : K] = p^{n-1}$. Let $b \in A(L)$ with $N_{L/L'}(b) = b'$ and

$N_{L/K}(b) = a$. Using the induction hypothesis for L'/K, it follows that

$$\begin{aligned} \imath_{L/K}(N_{L/K}(b)) &= \imath_{L/L'} \circ \imath_{L'/K}(N_{L'/K}(b')) \\ &= \imath_{L/L'}(b'^{[L':K]}) \\ &= \imath_{L/L'}(N_{L/L'}(b))^{[L':K]} \\ &= b^{p[L':K]} \\ &= b^{[L:K]}. \end{aligned}$$

□

4.5 Wild Growth of Ideal Classes

In Section 2.6, we have shown that $rk(A(L)) \leq p \cdot rk(A(K))$, where L/K is a cyclic extension of prime degree satisfying the F-property. Hence, one may be inclined to think that the exponent of $A(L)$ is also somehow bounded by the exponent of $A(K)$. For instance, we first conjectured that $exp(kerN_{L/K}) \leq p^{rk(A(K))}$. This, however, turned out to be wrong. One can even show that the exponent of $kerN_{L/K}$ is unbounded and thus the exponent of $A(L)$ as well. Before we begin to show that the exponent of $kerN_{L/K}$ can be arbitrarily large, we state two very useful results due to Yahagi and Ozaki. These results link the field theoretic situation with the group theoretic situation. More precisely, we have

Theorem 4.5.1 (Yahagi)**.** *Let G be a finite abelian p-group. Then there exists a number field K with maximal unramified p-extension M such that $Gal(M/K)^{ab} \cong G$.*

Proof. See [13]. □

An immediate consequence is

Corollary 4.5.2. *Let G be a finite abelian p-group. Then there exists a number field K such that the p-part of its ideal class group is isomorphic to G.*

Theorem 4.5.3 (Ozaki)**.** *Let G be a finite p-group. Then there exists a number field K with maximal unramified p-extension M such that $Gal(M/K) \cong G$.*

Proof. See [12]. □

Before we apply Ozaki's Theorem to show that $exp(kerN_{L/K})$ can be arbitrarily large, we derive the following group theoretic version of Furtwängler's Theorem. We have

Corollary 4.5.4. *Let G be a finite p-group with abelian normal subgroup H such that G/H is cyclic. Let $\sigma \in G$ such that $< \bar{\sigma} >= G/H$, where $\bar{\sigma}$ denotes the image of σ in G/H. Since H is abelian, $\bar{\sigma}$ acts on H by $h^{\bar{\sigma}-1} = \sigma h \sigma^{-1} h^{-1}$, for $h \in H$, and*

$$G' = H^{\sigma-1}.$$

In this case, we will say that $H \subset G$ satisfies the F-property.

Proof. The proof follows immediately by Ozaki's Theorem and the theorem due to Furtwängler. □

One can now use the above corollary to prove the classical Principal Genus Theorem. We have

Theorem 4.5.5 (Principal Genus Theorem)**.** *Let L/K be a cyclic extension with Galois group $G =< \sigma >$, for some $\sigma \in G$. Let M be the genus field of L/K, i.e. the maximal abelian extension of K which is unramified over L. Then*

$$Gal(H(L)/M) = Gal(H(L)/K)' = Gal(H(L)/L)^{\sigma-1}.$$

Proof. By the previous corollary, we obtain that $Gal(H(L)/L)^{\sigma-1}$ is the commutator group of $Gal(H(L)/K)$. One easily verifies that $H(L)^{Gal(H(L)/K)'}$ is the maximal subfield of $H(L)/L$ which is abelian over K. It follows that $H(L)^{Gal(H(L)/K)'} = M$ and thus $Gal(H(L)/K)' = Gal(H(L)/M)$. □

Remark: By the theorem of Tannaka-Terada, we obtain that the G-invariant ideal classes of $A(L)$ capitulate in $H(L)^{Gal(H(L)/L)^{\sigma-1}}$.

In what follows we apply Ozaki's Theorem to show that the $exp(kerN_{L/K})$ is unbounded. To this end, we construct a group with the following properties:

1. G is a finite p-group with abelian normal subgroup H of index p in G.
2. $exp(G')$ is arbitrarily large.

Suppose G is a group with the above properties. By Ozaki's Theorem, it follows that there exists a number field K with maximal unramified p-extension M such that $Gal(M/K) \cong G$. Now we define $L = M^H$, yielding that L/K is an unramified abelian extension of degree p. Since L/K is unramified, we

obtain that $H(L) \subset M$. One the other hand, $Gal(M/L) = H$ is abelian, showing that $H(L) = M$ and hence $G \cong Gal(H(L)/K)$. As usual, we can derive that $G' = Gal(H(L)/H(K)) \cong kerN_{L/K}$. By construction of G, it follows that $exp(kerN_{L/K})$ is arbitrarily large. Thus, it is sufficient to show that there are finite p-groups satisfying the above properties.

One can show that a subgroup of a p-group of index p is normal. Indeed, we have

Proposition 4.5.6. *Let G be a finite p-group and H be a subgroup of index p. Then H is a maximal subgroup and hence a normal subgroup of G.*

Proof. Since H is of index p, H is maximal by Lagrange's theorem. The second statement follows from Theorem 4.6, page 75, of [9]. □

For the ease of notation, we make the following definition: Let G be a group and g_1, $g_2 \in G$. Then $[g_1, g_2] := g_1 g_2 g_1^{-1} g_2^{-1}$ and $g_2^{g_1} := g_1 g_2 g_1^{-1}$.

We now start with the construction of 2-groups with the above properties:

One can easily show that the dihedral groups D_{2n} with $n = 2^k$, for some $k \geq 2$, satisfy the above properties:

$$D_{2n} =< s, t|\ s^n = 1,\ t^2 = 1 \text{ and } tst = s^{-1} > .$$

It is well-known that D_{2n} is a group of order $2n = 2^{k+1}$ and that it is non-abelian for $n \geq 3$. One can also verify that
1. The commutator subgroup $G' = [G, G]$ is of order 2^{k-1}.
2. G contains a normal cyclic subgroup $H =< s >\cong C_{2^k}$ of index 2 in D_{2n}, which contains G'.
3. $G' \cong C_{2^{k-1}}$, i.e. $exp(G')$ is unbounded as k tends to infinity.
4. $G/G' \cong C_2 \times C_2$.
5. $H \subset G$ satisfies the F-property.

For $p = 3$, the group becomes more complicated. Consider the finitely presented 3-group

$$G_n =< a, b, c|\ a^3, b^{3^{n+1}}, c^{3^n}, [a, b] = c, [a, c] = b^{3^n-3}c^{-3}, bc = cb > .$$

One can verify: 1. $ord(G_n) = 3^{1+n+1+n} = 3^{2(n+1)}$.
2. $H_n :=< b, c >$ is an abelian normal subgroup of index 3 in G_n, i.e. $H_n \cong C_{3^{n+1}} \times C_{3^n}$.
3. $G_n' \cong C_{3^n} \times C_{3^n}$.

4. $G_n/G_n' \cong C_3 \times C_3$.

For a general prime p, we can generalize the above construction. We set $k_j = \binom{p}{j}$ and define the finitely presented groups

$$\begin{aligned} G_n =< a_0, a_1, ..., a_{p-1} \quad | \quad & a_0^p = 1,\ a_1^{p^{n+1}} = 1,\ a_i^{p^n} = 1,\ \forall\ 2 \leq i \leq p-1, \\ & [a_i, a_j] = 1,\ \forall\ i, j \neq 0, \\ & a_1^{a_0-1} = a_2,\ a_1^{(a_0-1)^2} = a_3, ...,\ a_1^{(a_0-1)^{p-2}} = a_{p-1}, \\ & a_{p-1}^{a_0-1} = a_1^{p^n-k_1} \cdot ... \cdot a_{p-1}^{p^n-k_{p-1}} > . \end{aligned}$$

Remark: Setting $a_{p-1}^{a_0-1} = a_1^{p^n-k_1} \cdot \cdots \cdot a_{p-1}^{p^n-k_{p-1}}$ yields that

$$a_{p-1}^{(a_0-1)^2} = a_1^{(a_0-1)^p} = a_1^{-\sum_{i=1}^{p-1}\binom{p}{i}(a_0-1)^i}.$$

Hence, the choice for $a_{p-1}^{a_0-1}$ is not arbitrary but well thought about.

One can verify that: 1. $ord(G_n) = p^{1+n+1+(p-2)n} = p^{n(p-1)+2}$.
2. $H_n :=< a_1, ..., a_{p-1} >$ is an abelian normal subgroup of index p in G_n, i.e. $H_n \cong C_{p^{n+1}} \times C_{p^n} \times ... \times C_{p^n}$.
3. $G_n' \cong C_{p^n} \times ... \times C_{p^n}$ with $ord(G_n') = (p-1)p^n$.
4. $G_n/G_n' \cong C_p \times C_p$.

The statements in the above example can be verified by arduous calculations or for the specific cases by MAGMA.
These examples show that the growth of ideal classes is unbounded! For a better understanding, we want to state a few examples illustrating the different types of growth. Due to the theorem of Ozaki, we may either look at the group theoretic or field theoretic case. When introducing the upcoming examples, we think of identifications as follows: Let $K \subset L \subset H(K) \subset H(L)$ be the usual tower of an unramified cyclic extension L/K with Hilbert class fields $H(L)$ and $H(K)$, respectively. Then we identify:

1. $G \approx Gal(H(L)/K)$.
2. $H \approx Gal(H(L)/L)$.
3. $G' = [G, G] \approx Gal(H(L)/H(K))$.
4. $G/G' \approx Gal(H(K)/K)$.
5. $G/H \approx Gal(L/K)$.

Example 1: Consider the following finitely presented group

$$G =< a, b, c |\ a^3, b^{81}, c^{27}, aba^{-1} = bc, aca^{-1}c^{-1} = b^{24}c^{24}, bc = cb > .$$

MAGMA yields the following facts: 1. $ord(G) = 3^8$.
2. G contains an abelian normal subgroup $H \cong C_{81} \times C_{27}$.
3. The commutator subgroup of G is given by $G' \cong C_{27} \times C_{27}$ and is contained in H.
4. $H \subset G$ satisfies the F-property.

Now we set $N : H \to H/G'$ to be the canonical projection and $\imath : H/G' \to H$ to be the transfer of G to H. By Miyake, we obtain that $N(\imath(a)) = a^3$, for all $a \in H/G'$. Hence, the assumptions (i)-(iii) of Theorem 4.3.1 hold, but $subexp(H/G') = 3$ and $kerN = G' \cong C_{27} \times C_{27}$, i.e. $exp(kerN) = 27$.

Example 2: Consider the following finitely presented group:

$$G =< a, b|\ a^3, b^{81}, b(aba^{-1}) = (aba^{-1})b, (a^2ba^{-2})^3 = b^{24}(aba^{-1})^{24} > .$$

Then MAGMA yields that: 1. $ord(G) = 3^9$.
2. G contains an abelian normal subgroup $H \cong C_{81} \times C_{27} \times C_3$.
3. The commutator subgroup of G is given by $G' \cong C_{27} \times C_{27}$ and is contained in H.
4. $G/G' \cong C_3 \times C_9$.
Hence, there exists a number field K with $A(K) =< a_1, a_2 > \cong C_3 \times C_9$ and $L = H(K)^{<a_2>}$ such that $A(L) \cong H$.

We point out that Ozaki's Theorem and the above identifications also enable us to create different types of capitulation. For instance, in the above example one verifies that $\imath_{L/K}(a_2^3) \neq 1$. Indeed, for $Gal(L/K) =< \tau >$, we have that $ord(\imath_{L/K}(a_2^3)) = ord(N(b^3) = b^{3+3\tau+24+24\tau}) = 3$. Hence, there is no capitulation in $A(K)' = N_{L/K}(A(K))$. A few modifications of the above group, however, give us a different type of capitulation.

Example 3: Consider the following finitely presented group

$$G =< a, b|\ a^3, b^{81}, b(aba^{-1}) = (aba^{-1})b, (a^2ba^{-2})^3 = b^{-3}(aba^{-1})^{-3} > .$$

Then MAGMA yields that: 1. $ord(G) = 3^{10}$.
2. G contains an abelian normal subgroup $H \cong C_{81} \times C_{81} \times C_3$.
3. The commutator subgroup of G is given by $G' \cong C_{81} \times C_{27}$ and is contained in H.
4. $G/G' \cong C_3 \times C_9$.
By Ozaki's Theorem, there exists a number field K with $A(K) =< a_1, a_2 > \cong C_3 \times C_9$ and $L = H(K)^{<a_2>}$ such that $A(L) \cong H$. Moreover, for $Gal(L/K) =< \tau >$, we have that $\imath_{L/K}(a_2^3) = N(b^3) = b^{3+3\tau-3-3\tau} = 1$. Thus, we have capitulation in $A(K)' = N_{L/K}(A(K))$.

We proceed with some concrete examples of the growth of ideal classes in an unramified cyclic extension L/K of degree p. We will restrict ourselves to the case where K is an imaginary quadratic number field and where $p = 2$ or $p = 3$.

Example 4: Consider the imaginary quadratic number field

$$K = \mathbb{Q}(\alpha) \text{ with } \alpha^2 + 11651 = 0.$$

Then MAGMA yields: 1. $A(K) =< a_1, a_2 >\cong C_3 \times C_9$, for some $a_1, a_2 \in A(K)$.
2. We define $L = H(K)^{<a_2>}$, i.e. $A(K)' = N_{L/K}(A(L)) =< a_2 >$. We obtain $A(L) \cong C_3 \times C_9 \times C_{27}$.
3. $P_K(L) =< a_2^3 >\cong C_3$.
4. $kerN_{L/K} \cong C_9 \times C_9$ and hence $exp(kerN_{L/K}) > 3$.

Example 5: Consider the imaginary quadratic number field

$$K = \mathbb{Q}(\alpha) \text{ with } \alpha^2 + 9748 = 0.$$

Then MAGMA yields: 1. $A(K) =< a_1, a_2 >\cong C_3 \times C_3$, for some $a_1, a_2 \in A(K)$.
2. We define $L := H(K)^{<a_2>}$, i.e. $A(K)' := N_{L/K}(A(L)) =< a_2 >$. We obtain that $A(L) \cong C_9 \times C_{27}$.
3. $kerN_{L/K} \cong C_9 \times C_9$ and hence $exp(kerN_{L/K}) > 3$.

Example 6: Consider the imaginary quadratic number field

$$K = \mathbb{Q}(\alpha) \text{ with } 93\alpha^2 + 865 = 0.$$

Then MAGMA yields: 1. $A(K) =< a_1, a_2, a_3, a_4 >\cong C_2 \times C_2 \times C_2 \times C_2$, for some $a_1, a_2, a_3, a_4 \in A(K)$.
2. We define $L = H(K)^{<a_2, a_1a_3, a_4>}$, i.e. $N_{L/K}(A(L)) =< a_2, a_1a_3, a_4 >$. We obtain that $A(L) \cong C_2 \times C_4 \times C_{32}$.
3. $kerN_{L/K} \cong C_2 \times C_{16}$ and hence $exp(kerN_{L/K}) = 2^4$.

It is worth mentioning that in all of the above examples the author's initial conjecture that $exp(kerN_{L/K}) \leq p^{rk(A(K))}$ is true. Laborious calculations on MAGMA, however, showed that the cases where $exp(kerN_{L/K}) > p^{rk(A(K))}$, are extremely seldom but they do exist! We give the following

Example 7: Consider the imaginary quadratic number field

$$K = \mathbb{Q}(\alpha) \text{ with } 113\alpha^2 + 111 = 0.$$

Then MAGMA yields: 1. $A(K) =< a_1, a_2 > \cong C_2 \times C_2$, for some $a_1, a_2 \in A(K)$.
2. We define $L = H(K)^{<a_2>}$, i.e. $N_{L/K}(A(L)) =< a_2 >$. We obtain that $A(L) \cong C_{16}$.
3. $kerN_{L/K} \cong C_8$ and hence $exp(kerN_{L/K}) = 2^3 > 2^{rk(A(K))} = 4$. We even have that $exp(kerN_{L/K}) = 2^3 > |A(K)|$.

We have seen that the prerequisites for wild growth are rather restrictive, which also explains why wild growth is quite a rare phenomenon.

Chapter 5

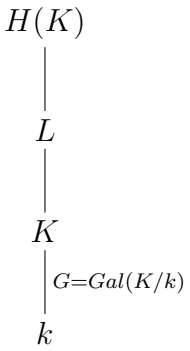
G-Action on Ideal Classes

In the following chapter, we let K/k be a Galois extension with Galois group $G = Gal(K/k)$. *Throughout this chapter, we assume that the prime p does not divide the order of G.*
In the introductory Section 5.1, we yield some preliminary results concerning the action of G on $A(K)$ and on $Gal(H(K)/K)$, respectively, and consider the action of G in the context of the capitulation problem.
In Section 5.2, we use the idempotents in $\mathbb{Z}_p[G]$ to decompose the ideal class group of K into a direct product of so-called α-components of the form $A(K)^\alpha$, where α runs through a subset of idempotents in $\mathbb{Z}_p[G]$. Accordingly, this decomposition gives rise to a decomposition of $H(K)$ into α-components $H(K)_\alpha$. For an intermediate field L of $H(K)/K$, which is Galois over k, we then sort of lift the idempotents in $\mathbb{Z}_p[G]$ to idempotents in $\mathbb{Z}_p[Gal(L/k)]$, which in turn yields a decomposition of the ideal class group of L and of $H(L)$, respectively.
In Section 5.3, we show under which conditions Suzuki's Theorem extends to a component wise version of Suzuki's Theorem. In other words, assuming that L is contained in an α-component $H(K)_\alpha$, we show under which prerequisites the degree of L over K divides the order of the capitulation kernel restricted to the α-component $A(K)_\alpha$. Supported by MAGMA, we give several concrete examples of a decomposition of $A(K)$ into α-components and also compute the capitulation kernels on the various α-components.
In view of the developed theory, Section 5.4 proceeds with a discussion of the capitulation problem in CM-fields, where we would like to draw the reader's attention to Proposition 5.4.1.
In Section 5.5, we insert an interlude on representation theory and particularly consider irreducible α-components, i.e. those components which correspond to primitive idempotents. Using p-adic analysis, we prove that $\mathbb{Q}_p[G]$ and $\mathbb{F}_p[G]$ have the same number of primitive idempotents provided that G

is abelian. As a main proposition of this section, we conclude from the above result that p-maximal elements in irreducible α-components of $A(K)$ are invertible in some sense.
In Section 5.6, we use this property to show that under certain conditions the l-socle of $A(K)$ capitulates completely in the l-socle of $H(K)$, where the l-socle of $A(K)$ contains all ideal classes in K of order equal or less than p^l and the l-socle of $H(K)$ is the intermediate field of $H(K)/K$ whose Galois group over K is isomorphic to the l-socle of $A(K)$. Moreover, we show that all p-maximal ideal classes in an irreducible α-component of $A(K)$ have the same order, provided that $A(K)$ is $\mathbb{Z}_p[G]$-cyclic.
In Section 5.7, we prove that $A(K)$ can be decomposed in a direct product of $\mathbb{Z}_p[G]$-cycles, thus getting rid of the assumption of Section 5.6 that $A(K)$ is $\mathbb{Z}_p[G]$-cyclic.
In Section 5.8, we apply the results of Section 5.7 to show that the p-genus field of K/k is $KH(k)$, i.e. $KH(k)$ is the maximal unramified p-extension of K, which is abelian over k. (Here, $H(k)$ is the p-Hilbert class field of k and K/k is abelian).
In Section 5.9, we generalize the developed theory of the previous sections by replacing the action of G on $A(K)$ by the action of the automorphism group of the Galois group $(Gal(H^{(2)}/K))$ on $A(K)$. Assuming that the automorphism group of $(Gal(H^{(2)}/K))$ is not a p-group, we show that it gives rise to a non-trivial action on $A(K)$, which then in turn can be used with respect to capitulation.

5.1 Preliminary Results

In what follows, let K/k be a Galois extension with Galois group $G = Gal(K/k)$ and L be an intermediate field of $H(K)/K$. The situation is shown in the following diagram:



We first verify that $H(K)/k$ is a Galois extension. We have

Proposition 5.1.1. *Let K/k be a Galois extension and $H(K)$ be the Hilbert class field of K. Then $H(K)/k$ is Galois.*

Proof. Let $\sigma : H(K) \to \sigma(H(K))$ be a ring homomorphism fixing k. Since $H(K)/K$ is Galois, it follows that $\sigma(K) = K$. Furthermore, one easily verifies that $Gal(\sigma(H(K))/K) = \sigma Gal(H(K)/K)\sigma^{-1}$ and hence $Gal(H(K)/K) \cong Gal(\sigma(H(K))/K)$. A moment of reflection also shows that $\sigma(H(K))/K$ is unramified. Since $H(K)$ is the maximal unramified field extension of K, we obtain that $\sigma(H(K)) \subset H(K)$. Applying the above arguments to σ^{-1}, shows that $\sigma(H(K)) = H(K)$. By Galois theory, it follows that $H(K)/k$ is Galois. □

Let us say that $exp(Gal(H(K)/K)) = p^n$, for some $n \in \mathbb{N}$. For $1 \leq l \leq n$, we then define the *l-socle* of $H(K)$ as the unique intermediate field of $H(K)/K$ with Galois group being isomorphic to $Gal(H(K)/K)/Gal(H(K)/K)^{p^l}$. Using the same arguments as above, we obtain

Proposition 5.1.2. *Let K/k be a Galois extension and $S_l(H(K))$, $1 \leq l \leq n$, denote the l-socle of $H(K)$. Then $S_l(H(K))/k$ is Galois.*

Let K/k be as above with Galois group $Gal(K/k) = G$. Then G obviously acts on the ideal class group $A(K)$ of K in the following way: Let $\sigma \in G$ and $a \in A(K)$. Then we set $a^\sigma := \sigma(a)$. One easily verifies that $A(K)$ becomes a G-module in this way. Note: For $a \in A(K)$, σ, $\tau \in G$, we have that $a^{\sigma\tau} = \sigma\tau(a) = \sigma(a^\tau) = (a^\tau)^\sigma$.
Since $A(K) \cong Gal(H(K)/K)$ by the Artin isomorphism $\varphi_{H(K)/K} = \varphi = (\frac{H(K)/K}{})$, the G-action on $A(K)$ is transferred to $Gal(H(K)/K)$: Let $\tau \in Gal(H(K)/K)$ and $\sigma \in G$. Then we define

$$\tau^\sigma := \varphi((\varphi^{-1}(\tau))^\sigma).$$

A moment of reflection shows that $Gal(H(K)/K)$ thus becomes a G-module. Another way of transporting the G-action on $A(K)$ to $Gal(H(K)/K)$ is the following: Let $\tau \in Gal(H(K)/K)$ and $\sigma \in G$. Since K/k and $H(K)/k$ are Galois, we may lift σ to an automorphism $\tilde{\sigma} \in Gal(H(K)/k)$, i.e. $\tilde{\sigma}_{|K} = \sigma$. Then we define

$$\tau^\sigma := \tilde{\sigma}\tau\tilde{\sigma}^{-1}.$$

In order to show that this defines a G-action on $Gal(H(K)/K)$, we must check that the above definition is well-defined, i.e. it is independent of the choice of the lift of σ: Let σ_1 and σ_2 be lifts of σ to $Gal(H(K)/k)$. Then

$\sigma_1 = \sigma_2 h$, for some $h \in Gal(H(K)/K)$. Since $H(K)/K$ is abelian, it follows that $h\tau = \tau h$ and hence

$$\begin{aligned} \sigma_1 \tau \sigma_1^{-1} &= \sigma_2 h \tau (\sigma_2 h)^{-1} \\ &= \sigma_2 h \tau h^{-1} \sigma_2^{-1} \\ &= \sigma_2 \tau \sigma_2^{-1}. \end{aligned}$$

As one might have expected, the two above definitions of a G-action on $Gal(H(K)/K)$ are the same:

Proposition 5.1.3. *In the situation as above, let $\tau = \varphi(a) \in Gal(H(K)/K)$, for some $a \in A(K)$, $\sigma \in G$, and $\tilde{\sigma} \in Gal(H(K)/k)$ be a lift of σ. Then*

$$\varphi \sigma \varphi^{-1}(\tau) = \tilde{\sigma} \tau \tilde{\sigma}^{-1}.$$

Proof. We have that

$$\begin{aligned} \varphi \sigma \varphi^{-1}(\tau) &= \left(\frac{H(K)/K}{\tilde{\sigma}(a)} \right) \\ &= \left(\frac{\tilde{\sigma}(H(K))/\tilde{\sigma}(K)}{\tilde{\sigma}(a)} \right) \\ &= \tilde{\sigma} \left(\frac{H(K)/K}{a} \right) \tilde{\sigma}^{-1}. \end{aligned}$$

□

Let $\sigma \in G$ and $\tilde{\sigma} \in Gal(H(K)/k)$ be a lift of σ. For an intermediate field L of $H(K)/K$, we then define

$$L^\sigma = \tilde{\sigma}(L).$$

This definition is well-defined. Indeed, let σ_1 and σ_2 be lifts of σ to the Galois group $Gal(H(K)/k)$. Then $Gal(H(K)/\sigma_i(L)) = \sigma_i Gal(H(K)/L)\sigma_i^{-1}$, for $i = 1, 2$. By the above arguments, we obtain that

$$\sigma_1 Gal(H(K)/L)\sigma_1^{-1} = \sigma_2 Gal(H(K)/L)\sigma_2^{-1}, \text{ and hence}$$

$$\sigma_1(L) = \sigma_2(L).$$

These observations lead us to the next

Proposition 5.1.4. *Let $H(K)/L/K/k$ be as above and $\sigma \in G$. Let I be a fractional ideal in K and $a = [I]$ be an ideal class in K represented by I. Assume that a capitulates in L. Then a^σ capitulates in L^σ.*
In particular, $P_K(L) \cong P_K(L^\sigma)$.

Proof. Let $I\mathcal{O}_L = x\mathcal{O}_L$ for some $x \in L^*$. Then

$$\begin{aligned} I^\sigma \mathcal{O}_{L^\sigma} &= (I\mathcal{O}_L)^{\tilde{\sigma}} \\ &= (x\mathcal{O}_L)^{\tilde{\sigma}} \\ &= x^{\tilde{\sigma}}\mathcal{O}_{L^\sigma}. \end{aligned}$$

The second statement is evident. □

Corollary 5.1.5. *If L/k is Galois, then $L = L^\sigma$ and thus $P_K(L)$ is a G-module.*

Proof. Elementary. □

5.2 Decomposition of $A(K)$ via Idempotents and Lifting of Idempotents

As before, let K/k be a Galois extension with Galois group $Gal(K/k) = G$ and $p \nmid |G|$. The goal of this section is the decomposition of $A(K)$ via idempotents. For a supplementary insight, we refer to [6]. For the following discussion, let $\alpha \in \mathbb{Z}_p[G]$ be an idempotent. Such an element certainly exists if $p \nmid |G|$ as $|G|$ has an inverse in $\mathbb{Z}_p$ in this case. For instance, one readily verifies that $\beta = (1/|G|)\sum_{\sigma\in G}\sigma$ is a central idempotent in $\mathbb{Z}_p[G]$. This yields the decomposition

$$\mathbb{Z}_p[G] = \alpha\mathbb{Z}_p[G] \oplus (1-\alpha)\mathbb{Z}_p[G].$$

Since $A(K)$ is a finite p-abelian G-module, it is also a $\mathbb{Z}_p[G]$-module and we obtain the decomposition

$$A(K) = A(K)_\alpha \times A(K)_{1-\alpha}, \text{ where}$$

$$A(K)_\alpha = A(K)^\alpha = \{a^\alpha |\ a \in A(K)\} \text{ and } A(K)_{1-\alpha} \text{ accordingly.}$$

Indeed, let $a^\alpha = b^{1-\alpha}$, for some ideal classes $a, b \in A(K)$. Taking the term on both sides of the equation to the α, it follows that

$$a^\alpha = b^{\alpha(1-\alpha)} = 1.$$

The rest is evident. We remark that we will use both the notation $A(K)_\alpha$ and $A(K)^\alpha$, meaning the same object.
Furthermore, observe that $A(K)_\alpha$ and $A(K)_{1-\alpha}$ are subgroups of $A(K)$. If α is central in $\mathbb{Z}_p[G]$ they are also $\mathbb{Z}_p[G]$-modules.

For the upcoming discussion, the following theorem proves useful:

Theorem 5.2.1 (Schur-Zassenhaus)**.** *Let $\mathcal{G}$ be a finite group and H be a normal subgroup of $\mathcal{G}$ such that $(|H|, |\mathcal{G}/H|) = 1$. Then H has a complement in $\mathcal{G}$. In particular, $\mathcal{G}$ is a semi-direct product of H and $\mathcal{G}/H$.*

Proof. See Theorem 7.41, page 190, of [9]. □

Let $H^{(2)}(K)$ denote the p-Hilbert class field of $H(K)$. As $p \nmid |G|$, the above theorem then implies that there is a subgroup $\mathcal{H} \cong Gal(K/k)$ of $Gal(H^{(2)}(K)/k)$ such that

$$Gal(H^{(2)}(K)/k) = Gal(H^{(2)}(K)/K) \ltimes \mathcal{H}.$$

Obviously, the restriction of $H^{(2)}(K)$ to K satisfies that $res_{H^{(2)}(K)/K}(\mathcal{H}) = Gal(K/k)$. Thus, we obtain the isomorphism

$$res_{H^{(2)}(K)/K} : \mathcal{H} \to Gal(K/k),\ \sigma \mapsto \sigma_{|K}.$$

Then we define the group homomorphism

$$s_{H^{(2)}(K)/K} : Gal(K/k) \to Gal(H^{(2)}(K)/k),\ s_{H^{(2)}(K)/K}(\tau) := res^{-1}_{H^{(2)}(K)/K}(\tau).$$

It follows that $s_{H^{(2)}(K)/K} \circ res_{H^{(2)}(K)/K} = id_{\mathcal{H}}$. Now let M be an intermediate field of $H^{(2)}(K)/K$ which is Galois over k. Then the restriction of $H^{(2)}(K)$ to M yields that

$$Gal(M/k) = Gal(M/K) \ltimes res_{H^{(2)}(K)/M}(\mathcal{H}),$$

$$res_{M/K} : Gal(M/k) \to Gal(K/k),\ \sigma \mapsto \sigma_{/K},\ \text{and}$$
$$s_{M/K} : Gal(K/k) \to Gal(M/k),\ s_{M/K}(\tau) := res^{-1}_{M/K}(\tau).$$

One easily verifies that $s_{H^{(2)}(K)/M} \circ s_{M/K} = s_{H^{(2)}(K)/K}$ and likewise that $res_{M/K} \circ res_{H^{(2)}(K)/M} = res_{H^{(2)}(K)/K}$, where $s_{H^{(2)}(K)/M}$ is defined in the canonical way. On account of that, we may lift the idempotent α from K to M and $H^{(2)}(K)$. More precisely, we have

$$\tilde{\alpha} = s_{M/K}(\alpha) \in \mathbb{Z}_p[s_{M/K}(G)] \subset \mathbb{Z}_p[G(M/k)],$$

$$\tilde{\tilde{\alpha}} = s_{H^{(2)}(K)/K}(\alpha) \in \mathbb{Z}_p[s_{H^{(2)}(K)/K}(G)] \subset \mathbb{Z}_p[G(H^{(2)}(K)/k)].$$

Clearly, $s_{H^{(2)}(K)/M}(\tilde{\alpha}) = \tilde{\tilde{\alpha}}$, $res_{H^{(2)}(K)/M}(\tilde{\tilde{\alpha}}) = \tilde{\alpha}$, and $res_{M/K}(\tilde{\alpha}) = \alpha$. If α is central in $\mathbb{Z}_p[G]$, then $\tilde{\alpha}$ and $\tilde{\tilde{\alpha}}$ are central idempotents in $\mathbb{Z}_p[s_{M/K}(G)]$ and $\mathbb{Z}_p[s_{H^{(2)}(K)/K}(G)]$, respectively. Henceforth, we simply write α instead of $\tilde{\alpha}$ and $\tilde{\tilde{\alpha}}$, respectively, as long as this does not cause any confusion.

Let $\alpha \in \mathbb{Z}_p[G]$ be an idempotent as before and L be an intermediate field of $H(K)/K$ which is Galois over k. By the previous arguments, we may lift α to an idempotent $\tilde{\alpha} \in \mathbb{Z}_p[Gal(L/k)]$, i.e. $res_{|K}(\tilde{\alpha}) = \alpha$. Observe that the choice of $\tilde{\alpha}$ is not unique, however. We obtain a decomposition of $A(L)$ into

$$A(L) = A(L)_{\tilde{\alpha}} \times A(L)_{1-\tilde{\alpha}}, \text{ where}$$

$$A(L)_{\tilde{\alpha}} = \{a^{\tilde{\alpha}} |\ a \in A(L)\} \text{ and } A(L)_{1-\tilde{\alpha}} \text{ accordingly.}$$

Moreover, we have

Proposition 5.2.2. *In the situation as before, we obtain that*

$$\imath_{L/K}(A(K)_\alpha) \subset A(L)_{\tilde{\alpha}}.$$

Proof. Let I be a fractional ideal in K and $a = [I]$ the ideal class group in K represented by I. Let $\sigma \in Gal(K/k)$ and $\tilde{\sigma}$ an extension to L. Then

$$\begin{aligned} \imath_{L/K}([I]^\sigma) &= \imath_{L/K}([I^\sigma]) \\ &= [I^\sigma \mathcal{O}_L] \\ &= [(I\mathcal{O}_L)]^{\tilde{\sigma}} \\ &= \imath_{L/K}([I])^{\tilde{\sigma}}. \end{aligned}$$

Since α is a $\mathbb{Z}_p$-linear combination of elements in $Gal(K/k)$, the claim follows. □

We may use the decomposition of $A(K)$ and $A(L)$ via idempotents to learn more about the capitulation kernel. For this purpose, we define

$$P_K(L)_\alpha = P_K(L) \cap A(K)_\alpha.$$

The above introduced machinery now allows us to restrict the search for capitulating ideal classes to $A(K)_\alpha$ and $A(K)_{1-\alpha}$. More precisely, we obtain

Proposition 5.2.3. *In the situation as above, we have that*

$$P_K(L) = P_K(L)_\alpha \times P_K(L)_{1-\alpha}.$$

Proof. Obviously, $P_K(L)_\alpha \cap P_K(L)_{1-\alpha} = \{1\}$. Now let

$$a = a^\alpha a^{1-\alpha} \in P_K(L).$$

It follows that

$$1 = \imath_{L/K}(a) = \imath_{L/K}(a)^\alpha \imath_{L/K}(a)^{1-\alpha}.$$

As $\imath_{L/K}(A(L))^\alpha \cap \imath_{L/K}(A(L))^{1-\alpha} = \{1\}$, we obtain that

$$\imath_{L/K}(a^\alpha) = \imath_{L/K}(a^{1-\alpha}) = 1.$$

□

We can find an even finer decomposition of $A(K)$: Let X be the set of non-trivial central idempotents in $\mathbb{Z}_p[G]$ and $|X| = 2r$, for some $r \in \mathbb{N}$. Let X^r be the set of non-ordered r-tuples of elements in X and

$$Y = \{(\alpha_1, ..., \alpha_r) \in X^r : \alpha_i \neq \alpha_j,\ \alpha_i\alpha_j \neq 0,\ \forall\ 1 \leq i, j \leq r\}.$$

Since the product of central idempotents is again an idempotent, we obtain the decomposition

$$A(K) = \prod_{(\alpha_1,...,\alpha_r)\in Y} A(K)^{\alpha_1 \cdot \ldots \cdot \alpha_r},\ \text{where}$$

$\prod$ denotes the Cartesian product and $A(K)^{\alpha_1 \cdot \ldots \cdot \alpha_r} = \{a^{\alpha_1 \cdot \ldots \cdot \alpha_r} |\ a \in A(K)\}$. The above proposition thus yields

Corollary 5.2.4. *In the situation as above, we have that*

$$P_K(L) = \prod_{(\alpha_1,...,\alpha_r)\in Y} P_K(L)_{\alpha_1 \cdot \ldots \cdot \alpha_r},\ \textit{where}$$

$\prod$ *denotes the Cartesian product and* $P_K(L)_{\alpha_1 \cdot \ldots \cdot \alpha_r} = P_K(L) \cap A(K)^{\alpha_1 \cdot \ldots \cdot \alpha_r}$.

This is a useful simplification when determining the capitulation kernel $P_K(L)$ as we obtain $P_K(L)$ by calculating the various $P_K(L)_{\alpha_1 \cdot \ldots \cdot \alpha_r}$ and afterward forming the Cartesian product of the various components.

5.3 Suzuki's Theorem on α-Components

By Suzuki's Theorem, we obtain that for an unramified abelian extension L/K the order of the capitulation kernel $P_K(L)$ is divided by the degree of L over K. We are now interested in the question under which conditions Suzuki's Theorem extends to a component wise version of Suzuki's Theorem, i.e. under which prerequisites do we have that $[L : K]$ divides the order of $P_K(L)_\alpha$, where α is an idempotent in $\mathbb{Z}_p[G]$ and $L \subset H(K)_\alpha$? (For a definition of $H(K)_\alpha$ see below). In this context, we also investigate under which conditions the F-property as defined in Chapter 2 holds component wise. Supported by MAGMA, we give several concrete examples of a decomposition of $A(K)$ into α-components and also compute the capitulation kernels on the various α-components.

Let $H(K)/L/K/k$ be as in the previous section, i.e. L/k and K/k are Galois extensions. Let $\alpha \in \mathbb{Z}_p[G]$ be an idempotent and $\tilde{\alpha} \in \mathbb{Z}_p[G(L/k)]$ be a lift of α. Throughout this section, we write for a Galois group of an extension M/F from now on $G(M/F)$ instead of $Gal(M/F)$. Finally, we let φ_K and φ_L be the Artin symbols of K and L, respectively. Then we define

$$H(K)_\alpha = H(K)^{\varphi_K(A(K)_{1-\alpha})},$$

$$H(K)_{1-\alpha} = H(K)^{\varphi_K(A(K)_\alpha)}.$$

Obviously, $H(K) = H(K)_\alpha H(K)_{1-\alpha}$ and $H(K)_\alpha \cap H(K)_{1-\alpha} = K$. Moreover, it follows that $G(H(K)_\alpha/K) \cong A(K)_\alpha$ and $G(H(K)_{1-\alpha}/K) \cong A(K)_{1-\alpha}$. Accordingly, we may define the fields

$$H(L)_{\tilde{\alpha}} = H(L)^{\varphi_L(A(L)_{1-\tilde{\alpha}})},$$

$$H(L)_{1-\tilde{\alpha}} = H(L)^{\varphi_L(A(L)_{\tilde{\alpha}})},$$

satisfying the according properties as $H(K)_\alpha$ and $H(K)_{1-\alpha}$.
We have

Proposition 5.3.1. *Let $H(K)/L/K/k$ be as before. Then $H(K)_\alpha \subset H(L)_{\tilde{\alpha}}$.*

Proof. We have

$$H(L)_{\tilde{\alpha}} = H(L)^{G(H(L)/L)^{1-\tilde{\alpha}}}, \text{ and}$$
$$H(K)_\alpha = H(K)^{G(H(K)/K)^{1-\alpha}}.$$

Now let $z \in H(K)_\alpha$, i.e. $z \in H(K)$ and $\varphi(z) = z$, for all $\varphi \in G(H(K)/K)^{(1-\alpha)}$. Let $\Psi \in G(H(L)/L)^{(1-\tilde{\alpha})}$. *Claim*: $\Psi_{|H(K)} \in G(H(K)/L)^{(1-\alpha)}$.

Proof: For $x \in \mathbb{Z}_p[G(L/k)]$, $x = \sum_{\sigma \in G(L/k)} \lambda_\sigma \sigma$, $\lambda_\sigma \in \mathbb{Z}_p$, we define $x_{|K} := \sum_{\sigma \in G(L/k)} \lambda_\sigma \sigma_{|K}$. Then

$$\Psi^x = \prod_\sigma (\Psi^{\lambda_\sigma})^\sigma = \prod_\sigma \tilde{\sigma} \Psi^{\lambda_\sigma} \tilde{\sigma}^{-1},$$

where $\tilde{\sigma}$ is a lift of $\sigma \in G(L/k)$ to $G(H(L)/k)$. It follows that

$$\Psi^x_{|H(K)} = \prod_\sigma \tilde{\sigma}_{|H(K)} \circ (\Psi_{|H(K)})^{\lambda_\sigma} \circ \tilde{\sigma}^{-1}_{|H(K)}.$$

Since $\tilde{\sigma}$ is a lift of $\sigma \in G(L/k)$ to $G(H(L)/k)$, we obtain that $\tilde{\sigma}_{|H(K)}$ is a lift of σ to $G(H(K)/k)$. Thus,

$$\Psi^x_{|H(K)} = (\Psi_{|H(K)})^{x_{|K}}.$$

Since $\tilde{\alpha}_{|K} = \alpha$, the proof of the claim follows, implying that $\Psi(z) = z$. This proves the proposition. □

All in all, we obtain the following tower of number fields: $k \subset K \subset L \subset H(K)_\alpha \subset H(L)_{\tilde{\alpha}}$.

The next proposition yields additional structural information. We have

Proposition 5.3.2. *Let $k \subset K \subset L \subset H(K)_\alpha \subset H(L)_{\tilde{\alpha}}$ be as before and L/k Galois. Then*

1. $H(K)_\alpha = H(L)_{\tilde{\alpha}} \cap H(K)$.
2. $ker(N_{L/K} : A(L)_{\tilde{\alpha}} \to A(K)_\alpha) \cong G(H(L)/H(K))_{\tilde{\alpha}} \cong G(H(L)_{\tilde{\alpha}}/H(K)_\alpha)$.
3. $im(N_{L/K} : A(L)_{\tilde{\alpha}} \to A(K)_\alpha) \cong G(H(K)_\alpha/L)$.

Proof. 1. "$\supset$": Let $x \in H(K)$ with $\tau(x) = x$, for all $\tau \in G(H(L)/L)_{1-\tilde{\alpha}}$, implying that $\sigma(x) = x$, for all $\sigma \in G(H(K)/L)_{1-\alpha}$, since $H(K)/k$ Galois. Due to $L \subset H(K)_\alpha$, it follows, for all $\rho \in G(H(K)/K)_{1-\alpha}$ and all $y \in L$ that $\rho(y) = y$ and thus $G(H(K)/K)_{1-\alpha} \subset G(H(K)/L)$. Hence, $G(H(K)/K)_{1-\alpha} \subset G(H(K)/L)_{1-\alpha}$. This implies that $x \in H(K) \cap H(L)_{\tilde{\alpha}}$ lies in $H(K)_\alpha$.
"$\subset$": Elementary.
2. We have that

$$\begin{aligned} ker(N_{L/K} : A(L)_{\tilde{\alpha}} \to A(K)_\alpha) &\cong G(H(L)/L)_{\tilde{\alpha}} \cap G(H(L)/H(K) \\ &= G(H(L)/L)_{\tilde{\alpha}} \cap G(H(L)/H(K))_{\tilde{\alpha}} \\ &= G(H(L)/H(K))_{\tilde{\alpha}}. \end{aligned}$$

For the second isomorphism in the proposition, we consider the isomorphism

$$\Psi := res_{H(L)/H(L)_{\tilde{\alpha}}} : \ G(H(L)/L)_{\tilde{\alpha}} \to G(H(L)_{\tilde{\alpha}}/L).$$

In particular, $\Psi(G((H(L)/H(K))_{\tilde{\alpha}}) = G(H(L)_{\tilde{\alpha}}/H(L)_{\tilde{\alpha}} \cap H(K))$. Since $H(L)_{\tilde{\alpha}} \cap H(K) = H(K)_{\alpha}$, we finally obtain the claim.
3. With the same arguments as before, we can conclude that

$$\begin{aligned} im(N_{L/K} : A(L)_{\alpha} \to A(K)_{\alpha}) &\cong G(H(L)/L)_{\tilde{\alpha}}/G(H(L)/H(K))_{\tilde{\alpha}} \\ &\cong G(H(K)/L)_{\alpha}, \end{aligned}$$

which yields the third statement of the proposition. □

In order to apply transfer theory to the capitulation problem on α-components, we need $H(L)_{\tilde{\alpha}}/K$ to be Galois. This is certainly the case if $\tilde{\alpha}$ is central in $\mathbb{Z}_p[G(L/k)]$. Indeed, we have the following

Proposition 5.3.3. *In the situation as before, assume that $\tilde{\alpha}$ is a central idempotent in $\mathbb{Z}_p[G(L/k)]$. Then $H(L)_{\tilde{\alpha}}/k$ is Galois.*

Proof. Let $\varphi = \varphi_L$ be the Artin symbol of L. By definition, we have that $H(L)_{\tilde{\alpha}} = H(L)^{\varphi(A(L)_{1-\tilde{\alpha}})}$. Also $H(L)/k$ is Galois since L/k is Galois by assumption. Hence, it is sufficient to show that $\varphi(A(L)_{1-\tilde{\alpha}})$ is a normal subgroup of $G(H(L)/k)$. Let $\sigma \in G(L/k)$, $\tilde{\sigma} \in G(H(L)/k)$ be an extension of σ, and $\tau \in \varphi(A(L)_{1-\tilde{\alpha}})$ with $\tau = \varphi(a^{1-\tilde{\alpha}})$ for some $a \in A(L)$. In the initial section of this chapter, we have shown how $G(L/k)$ acts on $G(H(L)/L)$ and that the action is independent of the choice for the extension of elements in $G(L/k)$. Since $\tilde{\alpha}$ is central in $\mathbb{Z}_p[G(L/k)]$, we thus obtain that

$$\begin{aligned} \tilde{\sigma}\tau\tilde{\sigma}^{-1} &= \tilde{\sigma}\varphi(a^{1-\tilde{\alpha}})\tilde{\sigma}^{-1} \\ &= (\varphi(a)^{1-\tilde{\alpha}})^{\sigma} \\ &= \varphi(a)^{\sigma(1-\tilde{\alpha})} \\ &= \varphi(a)^{(1-\tilde{\alpha})\sigma} \\ &= (\varphi(a)^{\sigma})^{1-\tilde{\alpha}} \\ &= \varphi(a^{\sigma})^{1-\tilde{\alpha}} \in \varphi(A(L)_{1-\tilde{\alpha}}). \end{aligned}$$

This completes the proof. □

In particular, we obtain that $H(K)_{\alpha}/k$ is Galois if $\alpha \in \mathbb{Z}_p[G]$ is central. Before we start the machinery of transfer theory, we need to show

Proposition 5.3.4. *Let $H(L)_{\tilde{\alpha}} \supset H(K)_{\alpha} \supset L \supset K$ be as before and assume that $\tilde{\alpha}$ is a central idempotent in $\mathbb{Z}_p[G(L/k)]$. It then follows that $H(K)_{\alpha}$ is the maximal intermediate field of $H(L)_{\tilde{\alpha}}/K$ which is abelian over K. In particular,*

$$G(H(L)_{\tilde{\alpha}}/K)' = G(H(L)_{\tilde{\alpha}}/H(K)_{\alpha}),$$

where $G(H(L)_{\tilde{\alpha}}/K)'$ denotes the commutator subgroup of $G(H(L)_{\tilde{\alpha}}/K)$.

Proof. Since $H(L)_{\tilde{\alpha}}/K$ is unramified, the statement follows from the fact that $H(L)_{\tilde{\alpha}} \cap H(K) = H(K)_{\alpha}$. □

This implies the next

Proposition 5.3.5. *We have the following commutative diagram:*

$$\begin{array}{ccc} A(L)_{\tilde{\alpha}} & \longrightarrow & G(H(L)_{\tilde{\alpha}}/L) \\ \uparrow{\scriptstyle \imath_{L/K}} & & \uparrow{\scriptstyle Ver} \\ A(K)_{\alpha} & \longrightarrow & G(H(K)_{\alpha}/K) \end{array}$$

The horizontal isomorphisms are induced by the Artin symbols of K and L. The transfer map Ver is more precisely given by

$$Ver : G(H(L)_{\tilde{\alpha}}/K)/(G(H(L)_{\tilde{\alpha}}/K))' \to G(H(L)_{\tilde{\alpha}}/H(K)_{\alpha}).$$

Proof. By the previous proposition, it follows that the above transfer is well-defined. It is quite straight forward to prove that the diagram is commutative. (For details, see Theorem 3.13, of [6]). □

Now we are prepared to prove the main result of this section:

Theorem 5.3.6. *Let α be a central idempotent in $\mathbb{Z}_p[G]$ and $\tilde{\alpha}$ be a lift of α which is central in $\mathbb{Z}_p[G(L/k)]$. Furthermore, let $H(L)_{\tilde{\alpha}} \supset H(K)_{\alpha} \supset L \supset K$ be as before. Then $[L : K]$ divides $|P_K(L)_{\alpha}|$.*

Proof. By the above proposition, it follows that

$$P_K(L)_{\alpha} \cong ker(Ver_{G(H(L)_{\tilde{\alpha}}/K)/(G(H(L)_{\tilde{\alpha}}/K))' \to G(H(L)_{\tilde{\alpha}}/H(K)_{\alpha})}).$$

Moreover, we have the exact sequence

$$1 \to G(H(L)_{\tilde{\alpha}}/L) \to G(H(L)_{\tilde{\alpha}}/K) \to G(L/K) \to 1.$$

Hence, $P_K(L)$ is isomorphic to a transfer kernel for $G(L/K)$. (For the definition of a transfer kernel, revisit the introduction). By Suzuki's Theorem, the claim follows. □

Corollary 5.3.7. *Let α be a central idempotent in $\mathbb{Z}_p[G]$ and assume that α can be lifted to a central idempotent in $\mathbb{Z}_p[G(H(K)_\alpha/k)]$. Then $A(K)_\alpha$ capitulates completely in $H(K)_\alpha$.*

Since additionally $G(H(K)_\alpha/K) \cong A(K)_\alpha$, $H(K)_\alpha$ can thus be seen as a Hilbert class field for the α-component $A(K)_\alpha$.

Definition: In the above situation, we call $H(K)_\alpha$ the *canonic α-component* and $H(K)_{1-\alpha}$ the *canonic $(1-\alpha)$-component* of $H(K)/K$.

Henceforth, we resume the situation where $H(L)_{\tilde{\alpha}} \supset H(K)_\alpha \supset L \supset K \supset k$ with L/k Galois. Now we want to discuss the case where α is central in $\mathbb{Z}_p[G]$, but $\tilde{\alpha}$ is not central in $\mathbb{Z}_p[G(L/k)]$. In this case $H(L)_{\tilde{\alpha}}$ is not necessarily Galois over K. However, for the special case that L/K is a quadratic extension, the above statements are still valid, i.e. we have

Corollary 5.3.8. *Let $H(K)_\alpha \supset L \supset K \supset k$ be as before with L/k Galois, and $[L:K] = 2$. Then $[L:K]$ divides the order of $P_K(L)_\alpha$.*

Proof. Let σ be a generator of $G(L/K)$. It is sufficient to show that $A(L)_{\tilde{\alpha}}$ is $G(L/K)$-invariant. The rest is analogous to the preceding proof. For an ideal class $a^{\tilde{\alpha}} \in A(L)_{\tilde{\alpha}}$, we obviously have that

$$\imath_{L/K}(N_{L/K}(a^{\tilde{\alpha}})) = (a^{\tilde{\alpha}})^{1+\sigma} \in A(L)_{\tilde{\alpha}}.$$

It follows that $(a^{\tilde{\alpha}})^\sigma \in A(L)_{\tilde{\alpha}}$, implying that $A(L)_{\tilde{\alpha}}$ is $G(L/K)$-invariant. $\square$

For the other cases, we define $H(L)'_{\tilde{\alpha}}$ to be the maximal subfield of $H(L)_{\tilde{\alpha}}/K$ which is Galois over K. Since α is central in $\mathbb{Z}_p[G]$, it follows that $H(K)_\alpha/K$ is Galois and hence $H(L)'_{\tilde{\alpha}} \supset H(K)_\alpha$. We can recover the following

Proposition 5.3.9. *Let $H(L)_{\tilde{\alpha}} \supset H(K)_\alpha \supset L \supset K$ be as before. Let α be a central idempotent in $\mathbb{Z}_p[G]$ and $\tilde{\alpha}$ be a lift of α in $\mathbb{Z}_p[G(L/k)]$ (not necessarily central). Then*

$$|P_K(L)_\alpha| \geq \frac{[L:K]}{[H(L)_{\tilde{\alpha}} : H(L)'_{\tilde{\alpha}}]}.$$

Proof. By the proof of a previous proposition, we know that $H(K)_\alpha$ is the maximal abelian subfield of $H(L)_{\tilde{\alpha}}/K$. Hence, $H(K)_\alpha$ is a fortiori the maximal abelian subfield of $H(L)'_{\tilde{\alpha}}/K$. Furthermore, the diagram as in Proposition 5.3.5, with $H(L)_{\tilde{\alpha}}$ replaced by $H(L)'_{\tilde{\alpha}}$, is still commutative. The only difference is that the Artin symbol $\varphi_L = \varphi$ induces a homomorphism

$$\Psi = \varphi_{|H(L)'_{\tilde{\alpha}}} : \; G(H(L)/L)_{\tilde{\alpha}} \to G(H(L)'_{\tilde{\alpha}}/L),$$

which is not necessarily injective anymore. But we have that $|ker\Psi| \leq [H(L)_{\tilde{\alpha}} : H(L)'_{\tilde{\alpha}}]$. Hence,

$$|P_K(L)_\alpha| \geq \frac{[L:K]}{[H(L)_{\tilde{\alpha}} : H(L)'_{\tilde{\alpha}}]}.$$

□

In a nutshell, we have shown that Suzuki's Theorem can also be extended to subfields L of $H(K)_\alpha/K$ provided that L/k is Galois and that the lift $\tilde{\alpha}$ of α to L is central in $\mathbb{Z}_p[G(L/k)]$. The assumption that L/k is Galois is essential as it guarantees that idempotents in $\mathbb{Z}_p[G]$ can be lifted to idempotents in $\mathbb{Z}_p[G(L/k)]$. Moreover, we have seen that if $\tilde{\alpha}$ is not central we obtain weaker results than in the central case.

Now we want to give a concrete example of a non-trivial decomposition of $A(K)$ into α-components. We have

Example: Let K be the splitting field of $X^3 + 4X + 14$ over $\mathbb{Q}$. Then $K/\mathbb{Q}$ is a Galois extension of degree 6. Supported by MAGMA, we obtain that:
1. K contains the quadratic number field $k = \mathbb{Q}(\beta)$ with $\beta^2 = -5548$.
2. K/k is Galois with $G := G(K/k) \cong C_3$.
3. $\mathbb{F}_2[G] = \alpha\mathbb{F}_2[G] \oplus (1-\alpha)\mathbb{F}_2[G]$, for some idempotent α in $\mathbb{F}_2[G]$. We have that $dim_{\mathbb{F}_2}(\alpha\mathbb{F}_2[G]) = 1$ and $dim_{\mathbb{F}_2}((1-\alpha)\mathbb{F}_2[G]) = 2$.
4. $A(K) =< a_1, a_2, a_3 > \cong C_2 \times C_2 \times C_4$.
5. $< a_1a_2a_3 >$ is the only G-invariant subgroup of $A(K)$ which is isomorphic to C_4. One verifies that $A(K)$ has 4 subgroups being isomorphic to C_4. Since $|G| = 3$, the Orbit Stabilizer Theorem yields that the 3 subgroups which are isomorphic to C_4 and different from $< a_1a_2a_3 >$ are conjugates with respect to G. Hence,

$$a_3^{\mathbb{Z}_2[G]} \supset < a_3, a_1a_3, a_2a_3 > = A(K),$$

i.e. $A(K)$ is $\mathbb{Z}_2[G]$-cyclic. This implies that $A(K)_\alpha \cong C_4$ and $A(K)_{1-\alpha} \cong C_2 \times C_2$. But we do not know the generators of $A(K)_\alpha$ and $A(K)_{1-\alpha}$ yet.
6. Since $< a_1a_2a_3 >$ is the only G-invariant subgroup of $A(K)$ which is isomorphic to C_4, it follows that $H(K)_{1-\alpha} = H(K)^{\varphi_K(<a_1a_2a_3>)}$.
7. $H(K)_\alpha = H(K)^{\varphi_K(<a_1,a_2>)}$. Indeed, $< a_1, a_2 >$ is the only G-invariant subgroup of $A(K)$ which is isomorphic to $C_2 \times C_2$. The rest follows from the above theory.
8. We finally obtain that $A(K)_\alpha =< a_1a_2a_3 >$ and $A(K)_{1-\alpha} =< a_1, a_2 >$.
9. $P_K(H(K)_\alpha) = A(K)$ and $P_K(H(K)_{1-\alpha}) =< a_1, a_2, a_3^2 > \cong C_2 \times C_2 \times C_2$.

This example demonstrates that $A(K)_\alpha$ capitulates in $H(K)_\alpha$ and $A(K)_{1-\alpha}$

capitulates in $H(K)_{1-\alpha}$. Moreover, we see that also ideal classes from $A(K)_{1-\alpha}$ can capitulate in $H(K)_\alpha$. In our example, even all ideals in K capitulate in $H(K)_\alpha$. In $H(K)_{1-\alpha}$ only the socle of $A(K)$ capitulates, though.
We also learn that the decomposition of the kernel $P_K(L) = P_K(L)_\alpha \times P_K(L)_{1-\alpha}$ does not hold in general if L/k is not Galois: For instance, let $L = H(K)^{\varphi_K(<a_1,a_1a_2a_3>)}$. MAGMA yields that L/k is not Galois and that $P_K(L) =< a_1, a_2a_3^2 >$, i.e. $P_K(L)_\alpha =< a_1 > \cong C_2$ and $P_K(L)_{1-\alpha} = \{1\}$. This is not astonishing as we cannot lift α to $G(L/k)$.

It also should be mentioned that the decomposition of $A(K)$ into α-components may be trivial, i.e. we may have the case that $A(K)_\alpha$ is trivial and hence $A(K)_{1-\alpha} = A(K)$. If K is a quadratic number field for example, this is always the case. Indeed, let $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_K$ lying above some prime $p \in \mathbb{Z}$ and σ be a generator of $G(K/\mathbb{Q})$. If $\mathfrak{P}$ is inert, it follows that $[\mathfrak{P}] = 1$ due to $p\mathcal{O}_K = \mathfrak{P}$. Now assume that $\mathfrak{P}|p$ is not inert. Then

$$p\mathcal{O}_K = \mathfrak{P}\mathfrak{P}^\sigma.$$

Since $p\mathcal{O}_K$ is principal, it follows that $[\mathfrak{P}]^\sigma = [\mathfrak{P}]^{-1}$. For $\alpha = (1+\sigma)/2$, Chebotarev's Density Theorem then yields that $A(K)_\alpha = \{1\}$.

We have already seen that the generalization of Suzuki's Theorem to α-components is not necessarily exact, i.e. for an intermediate field L of $H(K)_\alpha/K$, it does not necessarily follow that $[L : K] = |P_K(L)_\alpha|$. Even if $A(K)$ is assumed to be $\mathbb{Z}_p[G]$-cyclic, Suzuki's Theorem is not exact on α-components in general. We have

Example: Let K be the splitting field of $x^3 + 6x - 23$ over $\mathbb{Q}$. Supported by MAGMA, we obtain:
1. K contains a quadratic subfield $k = \mathbb{Q}(\beta)$ with $\beta^2 + 15147 = 0$ and K/k is Galois of degree 3. Let us say $G = G(K/k)$.
2. $\mathbb{Z}_2[G] = \alpha\mathbb{Z}_2[G] \oplus (1-\alpha)\mathbb{Z}_2[G]$, where $\alpha \in \mathbb{Z}_2[G]$ is an idempotent with $rk_{\mathbb{Z}_2}(\alpha\mathbb{Z}_2[G]) = 2$ and $rk_{\mathbb{Z}_2}((1-\alpha)\mathbb{Z}_2[G]) = 1$.
3. $A(K) =< a_1, a_2, a_3 > \cong C_2 \times C_4 \times C_4$. Again, it is not at all obvious how the decomposition of $A(K)$ looks like and MAGMA is not able to yield the decomposition of $A(K)$ into $A(K)_\alpha$ and $A(K)_{1-\alpha}$ directly. However, we can use the fact that $A(K)_\alpha$ and $A(K)_{1-\alpha}$ are G-invariant since G is abelian.
4. $< a_2, a_3 >$ is the only G-invariant subgroup of $A(K)$ which is isomorphic to $C_4 \times C_4$. This implies that $< a_2^2, a_3^2 > \cong C_2 \times C_2$ is also G-invariant. Moreover, MAGMA yields that $< a_2, a_3 >$ has no G-invariant subgroups which are isomorphic to $C_2 \times C_4$. A moment of reflection thus reveals that $< a_2, a_3 >$ has no G-invariant subgroups being isomorphic to C_2. Hence, all elements in $< a_2, a_3 >$ of order 4 generate $< a_2, a_3 >$ over $\mathbb{Z}_2[G]$. Fur-

thermore, we see that $A(K)$ has no G-invariant subgroups being isomorphic to C_4. Indeed, suppose that $< a_1 a_2^k a_3^l >$ is such a subgroup for suitable $k, l \in \mathbb{N}$. Then a fortiori, $< a_1^2 a_2^{2k} a_3^{2l} >=< a_2^{2k} a_3^{2l} > \cong C_2$ is a G-invariant subgroup of $< a_2, a_3 >$ of order 2, which yields a contradiction. Since $A(K)_\alpha$ and $A(K)_{1-\alpha}$ are G-invariant, it necessarily follows that $A(K)_\alpha =< a_2, a_3 >$. Also, we obtain that $A(K)_{1-\alpha} \cong C_2$. Since $A(K)_\alpha \cap A(K)_{1-\alpha}$ are disjoint, it follows that $A(K)_{1-\alpha} =< a_1 a_2^{2k} a_3^{2l} >$, for some suitable $k, l \in \mathbb{N}$. Obviously, $< a_1 a_2^{2k} a_3^{2l}, a_2^2, a_3 >=< a_1, a_2^2, a_3 >$, i.e. $L = H(K)^{\varphi_K(<a_1, a_2^2, a_3>)}$ lies in $H(K)_\alpha$ with $[L : K] = 2$.
5. $P_K(L) =< a_2^2, a_3^2 > \cong C_2 \times C_2$.
This shows that Suzuki is not necessarily exact on α-components even if the component is $\mathbb{Z}_p[G]$-cyclic.

In the remainder of this section, we want to analyze under which conditions the F-property as defined in Chapter 2 is satisfied on α-components. More precisely: Let L be an intermediate field of $H(K)/K$ which is cyclic over K and Galois over k. Let α be a central idempotent in $\mathbb{Z}_p[G(K/k)]$ and $\tilde{\alpha}$ be a lift of α to L. (We subsequently simply write α instead of $\tilde{\alpha}$). Suppose that $\sigma \in G(L/K)$ is a generator of $G(L/K)$ and set $s = \sigma - 1$. Under which circumstances, do we have that

$$ker(N_{L/K} : A(L)_\alpha \to A(K)_\alpha) = (A(L)_\alpha)^s \ ?$$

Let $a \in kerN_{L/K} \cap A(L)_\alpha$. By Furtwängler's Theorem, there exists an $a_1 \in A(L)$ with

$$\begin{aligned} a &= a_1^s \\ &= (a_1^s)^\alpha (a_1^s)^{1-\alpha} \\ &= a_1^{\alpha s} a_1^{(1-\alpha)s}. \end{aligned}$$

As $a \in A(L)_\alpha$, it follows that

$$\begin{aligned} a &= a^\alpha \\ &= a_1^{\alpha s} \\ &= (a_1^s)^\alpha \in (A(L)^s)^\alpha. \end{aligned}$$

The problem now is that σ and α do not necessarily commute since the lift of the central idempotent $\alpha \in \mathbb{Z}_p[G(K/k)]$ to L does not need to be central in $\mathbb{Z}_p[G(L/k)]$. In order to make sure that the F-property holds component wise, it is reasonable to require that α is lifted to a central idempotent in $\mathbb{Z}_p[G(L/k)]$. In this case we obtain

Proposition 5.3.10. *Let α be a central idempotent in $\mathbb{Z}_p[G(K/k)]$ and L be an intermediate field of $H(K)/K$ which is cyclic over K and Galois over k. Let $\sigma \in G(L/K)$ be a generator of $G(L/K)$ and $s = \sigma - 1$. Assume that α is lifted to a central idempotent in $\mathbb{Z}_p[G(L/k)]$. Then:*

(i) $ker(N_{L/K} : A(L)_\alpha \to A(K)_\alpha) = (A(L)_\alpha)^s$.

(ii) $|A(L)_\alpha^{G(L/K)}| = [H(K)_\alpha : L]$.

(iii) $|P_K(L)_\alpha| \geq [L : K]$.

Proof. (i) By the above computations and by the assumption that α commutes with σ, the above statement readily follows.
(ii) Consider the group homomorphism

$$A(L)_\alpha \to ker(N_{L/K} : A(L)_\alpha \to A(K)_\alpha),\ a \mapsto a^s.$$

By (i), the above homomorphism is surjective with kernel $A(L)_\alpha^{G(L/K)}$. By the isomorphism theorem and previous arguments, it follows that
$|A(L)_\alpha^{G(L/K)}| = |G(H(L)_\alpha/L)|/|G(H(L)_\alpha/H(K)/\alpha)| = [H(K)_\alpha : L]$.
The third statement of the proposition follows due to

$$|im(\imath_{L/K} : A(K)_\alpha \to A(L)_\alpha)| \leq |A(L)_\alpha^{G(L/K)}| = [H(K)_\alpha : L],\ \text{i.e.}$$

$$|P_K(L)_\alpha| \geq [[H(K)_\alpha : K]/[H(K)_\alpha : L] = [L : K].$$

□

5.4 Capitulation in CM-Fields

The results of the previous section suggest that Suzuki's Theorem does not extend to α-components in general. The crucial problem was that the lifted elements of $G(K/k)$ to $G(L/k)$ do not not necessarily commute with elements in $G(L/K)$. On the contrary, we will see that the generalization of Suzuki's Theorem holds for so-called CM-fields at least on $A(K)^+$. If K contains a primitive p-th root of unity, we show that a subgroup of $A(K)^-$ of the same rank as $A(K)^+$ capitulates in $H(K)^+$. (For the definitions of $A(K)^+$ and $H(K)^+$ see below).
We recall that a CM-field is a totally imaginary quadratic extension of a totally real field. For instance, $\mathbb{Q}(\zeta_n)$ is a CM-field, where ζ_n is a primitive n-th root of unity. Indeed, it contains the real number field $\mathbb{Q}(\zeta_n)^+ := \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ and we obtain $\mathbb{Q}(\zeta_n)$ by adjoining the square root of $\zeta_n^2 + \zeta_n^{-2} - 2$. These fields are called CM-fields since the complex multiplication in $\mathbb{C}$ can be transferred to such fields in a well-defined way: Let K be a CM-field and

Φ be an embedding of K into $\mathbb{C}$. For $x \in K$, we then define $\bar{x} = \Phi^{-1}(\overline{\Phi(x)})$. From the properties of CM-fields, one easily derives that the above definition is well-defined, i.e. $\overline{\Phi(K)} \subset \Phi^{-1}$ and the definition is independent of the chosen embedding. Let K^+ be the totally real subfield of K and $G(K/K^+) = \{1, J\}$, where J is the complex multiplication on K. Henceforth, let p be an odd prime and $A(K) = Cl(K)_p$. Then we define $\alpha = \frac{1+J}{2}$ and obtain the decomposition

$$A(K) = A(K)_\alpha \times A(K)_{1-\alpha}.$$

For the ease of notation, we will set $A(K)_\alpha = A^+$ and $A(K)_{1-\alpha} = A^-$. As before, the decomposition of $A(K)$ yields a decomposition of $H(K)$ into

$$H(K) = H(K)^+ \cdot H(K)^-,$$

where $H(K)^+ = H(K)^{\varphi(A^-)}$ and $H(K)^- = H(K)^{\varphi(A^+)}$, with φ being the Artin symbol of K as usual. It follows that $H(K)^+$ is also a CM-field. Indeed, let $H(K^+)$ be the p-Hilbert class field of K^+. Since K^+ is totally real, $H(K^+)$ is also totally real. As $A(K^+) \cong A(K)^+$, one also verifies that $H(K)^+ = KH(K^+)$. It follows that $H(K^+)$ lies in $H(K)^+$ with $[H(K)^+ : H(K^+)] = 2$. Since K is totally imaginary, we obtain that $H(K)^+$ is totally imaginary and hence $H(K)^+$ is a CM-field. Furthermore, we have that $A(K)^+$ capitulates completely in $H(K)^+$ since $H(K)^+ = KH(K^+)$ and $A(K^+)$ capitulates in $H(K^+)$.

This poses the question whether there also exist ideal classes in $A(K)^-$ which capitulate in $H(K)^+$. If K contains a primitive p-th root of unity, we have the following surprising

Proposition 5.4.1. *Let K be a CM-field containing a primitive p-th root of unity. Then $A(K)^-$ contains a subgroup C with $rk(C) = rk(A^+)$ such that all ideal classes of C capitulate in $H(K)^+$.*

Proof. Let $r = rk(A(K)^+)$ and L be the 1-socle of $H(K)^+/K$, i.e. L is the maximal intermediate field of $H(K)^+/K$ such that $rk(Gal(L/K)) = rk(Gal(H(K)^+/K))$ and $exp(Gal(L/K)) = p$. Since K contains a primitive p-th root of unity by assumption, L/K is a Kummer extension, i.e. $L = K(b_1^{1/p}, ..., b_r^{1/p})$, for some $b_i \in K^*$, $1 \leq i \leq r$. The following lemma proves useful now:

Lemma 5.4.2. *Assume the situation as above. If $K(b^{1/p^n})/K$ is unramified, for some $b \in K^*$ and $n \in \mathbb{N}$, then $b\mathcal{O}(K) = I^n$ for some ideal I of K.*

Proof. Let $K_1 = K(b^{1/p^n})$. As K contains a primitive p-th root of unity, the principal ideal $b^{1/p^n}\mathcal{O}(K_1)$ is invariant under the action of $G(K_1/K)$. Since K_1/K is unramified, Proposition 1.3.6 implies that $b^{1/p^n}\mathcal{O}(K_1) = I\mathcal{O}(K_1)$, for some ideal I of K, and hence $b\mathcal{O}(K_1) = I^n\mathcal{O}(K_1)$. As the embedding of ideals of K into K_1 is injective, it follows that $b\mathcal{O}(K) = I^n$. □

Back to the proof of the proposition: Let $b = b_i$, for some $1 \leq i \leq r$, and $K_1 = K(b^{1/p})$. By the proof of the previous lemma, we can conclude that $I\mathcal{O}(K_1) = b^{1/p}\mathcal{O}(K_1)$, for some ideal I in K. Now let $B =< b_1, ..., b_r >$ be the Kummer radical of L/K.
Claim: Then $B = B^-$.
Proof: Let $W_K =< \zeta_p >$ be the group of p-th roots of unity and consider the Kummer pairing

$$< , >:\ G(L/K) \times B \to W_K,\ < \sigma, b > \mapsto \frac{\sigma(b^{1/p})}{b^{1/p}}.$$

Since $W_K \subset (\mathcal{O}(K)^*)^-$ and as the Kummer pairing is bilinear, we obtain that $< G(L/K), B^+ >= 1$ and hence the map $< , >:\ G(L/K) \times B^- \to W_K$ is non-degenerate. It follows that $G(L/K) \cong B^-$ and thus $B = B^-$.
As we have already shown that $I\mathcal{O}(K_1) = b^{1/p}\mathcal{O}(K_1)$, it is now sufficient to show that I is not principal in K. Suppose that $I = (x)$ for some $x \in K^*$. Then $b = x^p\epsilon$ for some $\epsilon \in \mathcal{O}(K)^*$. Observe that $\epsilon/\overline{\epsilon}$ is a root of unity as it is of absolute value 1. As $b \in B^-$, it follows that $b = (x^p)^-\zeta_p^k$, for some $k \in \mathbb{N}$. If $\zeta_p^k = 1$, then $K_1 = K(x) = K$, which yields a contradiction. Otherwise, it follows that $K_1 = K(\zeta_{p^2})$, which is a contradiction to K/K_1 being unramified. We have now shown that, for all $1 \leq i \leq r$, there exists a non-principal ideal I_i in K that capitulates in $K(b_i^{1/p})$ and hence in L. It is now left to show that $rk([I_1], ..., [I_r]) = r$. This, however, follows easily from the fact that $K(b_1^{1/p}, ..., b_r^{1/p})/K$ has a Galois group of rank r and that $B = B^-$. This proves the claim. □

5.5 Interlude on Representation Theory and α-Components

In what follows, we introduce some basic facts on the representation theory of finite groups and use these results to decompose $\mathbb{Z}_p[G]$ into irreducible submodules, which give rise to so-called irreducible α-components of $A(K)$. For further details on representation theory, we refer to [7], [16]. Using p-adic analysis, we then prove that $\mathbb{Q}_p[G]$ and $\mathbb{F}_p[G]$ have the same number

of primitive idempotents provided that G is abelian. As a main proposition of this section, we use the above result to prove that p-maximal elements in irreducible α-components are invertible in some sense. This property can then be applied to the capitulation problem. We begin with

Proposition 5.5.1. *Let G be a finite group and p be a prime not dividing $|G|$. Then*

$$\mathbb{Z}_p[G] = \alpha_1\mathbb{Z}_p[G] \oplus ... \oplus \alpha_r\mathbb{Z}_p[G],$$

where α_i, $1 \leq i \leq r$ ($r \in \mathbb{N}$), are the primitive orthogonal idempotents in $\mathbb{Z}_p[G]$.

Proof. See Corollary 2.5, page 17, of [6]. □

Theorem 5.5.2 (Maschke)**.** *Let G be a finite group and $\mathbb{F}$ be a field. Then the group ring $\mathbb{F}[G]$ is semi-simple (i.e. $\mathbb{F}[G]$ can be decomposed as a direct sum of irreducible $\mathbb{F}[G]$-modules) if and only if $\mathbb{F}$ has characteristic 0 or characteristic coprime to $|G|$.*

Proof. See Theorem 5.1, page 221, of [17]. □

Proposition 5.5.3. *Let R be a semi-simple ring and M be an R-module. Then M is irreducible if and only if M is indecomposable.*

Proof. See Corollary 2.13, of [16]. □

Proposition 5.5.4. *Let R be a ring and $\alpha \in R$ be an idempotent. Then α is primitive if and only if $R\alpha$ is indecomposable as an R-module.*

Proof. See Lemma 3.8, of [16]. □

Proposition 5.5.5. *Let G be a finite group and $\mathbb{F}$ be a field with characteristic 0 or characteristic coprime to $|G|$. Furthermore, let $\chi_1, ..., \chi_s : G \to \mathbb{F}$ be the irreducible characters of G. Then the elements*

$$1_{\chi_i} = \frac{\chi_i(1)}{|G|} \sum_{\sigma \in G} \chi_i(\sigma^{-1})\sigma, \quad 1 \leq i \leq s,$$

form a complementary set of central primitive idempotents in $\mathbb{F}[G]$. (And these are all central primitive idempotents).

Proof. See Proposition 6.1, of [16]. □

Instead of considering a decomposition of $\mathbb{Z}_p[G]$, we may also analyze the decomposition of $\mathbb{Z}_p[G]/p\mathbb{Z}_p[G] \cong \mathbb{F}_p[G]$. Obviously, idempotents in $\mathbb{Z}_p[G]$ yield idempotents in $\mathbb{F}_p[G]$. On the other hand, the image of primitive idempotents in $\mathbb{Z}_p[G]$ does not necessarily have to be primitive in $\mathbb{F}_p[G]$. Thus, we introduce the following

Definition: Let G be a finite group and p be a prime not dividing $|G|$. Then we say $\mathbb{Z}_p[G]$ has *good reduction* if all primitive idempotents in $\mathbb{Z}_p[G]$ induce primitive idempotents in $\mathbb{F}_p[G]$.

In what follows, we prove that $\mathbb{Z}_p[G]$ has good reduction if G is abelian:
By Maschke's Theorem, $\mathbb{Q}_p[G]$ and $\mathbb{F}_p[G]$ are semi-simple. Hence, they have a finite number of irreducible submodules. Since G is abelian and $p \nmid |G|$, it follows that the number of primitive idempotents in $\mathbb{Z}_p[G]$ equals the number of primitive idempotents in $\mathbb{Q}_p[G]$. Thus, it is sufficient to verify the following

Theorem 5.5.6. *Let G be a finite abelian group of order n with $p \nmid n$. Then $\mathbb{Q}_p[G]$ and $\mathbb{F}_p[G]$ have the same number of irreducible submodules.*

Proof. Before we begin with the actual proof, we need some further background in p-adic analysis:

Proposition 5.5.7. *Let $K/\mathbb{Q}_p$ be a finite field extension with ramification index e and $f = [K : \mathbb{Q}_p]/e$. Furthermore, let k be the residue field of K. Then*

$$[k : \mathbb{F}_p] = f.$$

Proof. See Proposition 5.4.6, page 162, of [18]. □

Proposition 5.5.8. *Let $f(X) \in \mathbb{Z}_p[X]$ be a monic polynomial whose reduction modulo p is irreducible in $\mathbb{F}_p[X]$. Then $f(X)$ is irreducible over $\mathbb{Q}_p$.*

Proof. See Corollary 5.3.8, page 155, of [18]. □

We now resume the proof of the above theorem. Let ζ denote a primitive n-th root of unity in the algebraic closure of $\mathbb{Q}_p$ and $\tilde{\zeta}$ be a primitive n-th root of unity in the algebraic closure of $\mathbb{F}_p$. Then we define $K = \mathbb{Q}_p(\zeta)$ and $\mathbb{F}_q = \mathbb{F}_p(\tilde{\zeta})$, where q is a power of p. By the above proposition, it follows that $K/\mathbb{Q}_p$ and $\mathbb{F}_q/\mathbb{F}_p$ are cyclic Galois extensions of the same degree. Since $p \nmid n$

by assumption, it follows that K is an unramified extension of $\mathbb{Q}_p$. Let k be the residue field of K and $\mathcal{P}$ be the maximal ideal of K. Then Proposition 5.5.7 yields that $[k : \mathbb{F}_p] = [K : \mathbb{Q}_p]$, i.e. $k = \mathbb{F}_q$. Thus, we may assume that

$$\zeta \ mod \ \mathcal{P} = \tilde{\zeta}.$$

Since G is of order n, representation theory then yields that $K[G]$ and $\mathbb{F}_q[G]$ can be decomposed into n one dimensional irreducible submodules. As ρ runs through the set of characters of G over K and $\tilde{\rho}$ runs through the set of characters of G over $\mathbb{F}_q$, we thus obtain n primitive idempotents of the form

$$1_\rho = \frac{1}{n} \sum_{\sigma \in G} \rho(\sigma)\sigma^{-1} \in K[G],$$

$$1_{\bar{\rho}} = \frac{1}{n} \sum_{\sigma \in G} \bar{\rho}(\sigma)\sigma^{-1} \in \mathbb{F}_q[G],$$

which are in 1-1 correspondence.
Now let $H = Gal(K/\mathbb{Q}_p)$ and X be the set of primitive idempotents in $K[G]$. Then H defines an equivalence relation on X in the following way: Let 1_ρ and $1_{\rho'}$ be two primitive idempotents in X. Then we say

$$1_\rho \sim 1_{\rho'} \quad \Leftrightarrow \exists \ \nu \in H : \ \nu(1_\rho) = 1_{\rho'}.$$

This yields indeed an equivalence relation on X. The proof is straightforward. Now let $\alpha \in \mathbb{Q}_p[G]$ be a primitive idempotent, i.e. $\alpha\mathbb{Q}_p[G]$ is irreducible. Then $\alpha K[G]$ has a decomposition into irreducible submodules of $K[G]$, which are generated by elements of X. Let $1_\rho \in K[G]$ be a primitive idempotent lying in $\alpha K[G]$. Since $\alpha \in \mathbb{Q}_p[G]$, it follows that $\alpha K[G]$ is invariant by all $\nu \in H$. It follows that

$$\tilde{\alpha} := \frac{1}{|H|} \sum_{\nu \in H} \nu(1_\rho) \in \mathbb{Q}_p[G].$$

Indeed, $\tilde{\alpha}$ is an idempotent lying in $\mathbb{Q}_p[G]$ as it is the algebraic trace of 1_ρ. Since $\alpha \in \mathbb{Q}_p[G]$ is primitive, one verifies that

$$\alpha\mathbb{Q}_p[G] = \tilde{\alpha}\mathbb{Q}_p[G] \text{ and thus } \alpha K[G] = \tilde{\alpha}K[G].$$

Let X_ρ be the equivalence class represented by 1_ρ. Obviously, then

$$\alpha K[G] = \frac{1}{|H|} \sum_{\nu \in H} \nu(1_\rho)K[G] = \sum_{1_\tau \in X_\rho} 1_\tau K[G] =: K[G]_{X_\rho}.$$

This shows that the primitive idempotents in $\mathbb{Q}_p[G]$ are in 1-1 correspondence to the $K[G]_{X_\rho}$, where X_ρ runs through the equivalence classes of X. Certainly, we have the according 1-1 correspondence for the primitive idempotents in $\mathbb{F}_p[G]$. Due to $Gal(K/\mathbb{Q}_p) \cong Gal(\mathbb{F}_q/\mathbb{F}_p)$, it follows that X and the set of primitive idempotents in $\mathbb{F}_p[G]$ have the same number of equivalence classes. Combining these arguments, we obtain that $\mathbb{F}_p[G]$ and $\mathbb{Q}_p[G]$ have the same number of primitive idempotents. This proves the theorem. □

This yields the desired result, namely

Corollary 5.5.9. *Let G be a finite abelian group of order n with $p \nmid n$. Then $\mathbb{Z}_p[G]$ has good reduction.*

Corollary 5.5.10. *Let G be a finite abelian group of order n with $p \nmid n$. Then, we have a 1-1-correspondence between the idempotents in $\mathbb{Q}_p[G]$ and $\mathbb{F}_p[G]$. In particular, $\mathbb{Q}_p[G]$ has only finitely many idempotents.*

Proof. The proof follows immediately from the proof of the above theorem. Indeed, all idempotents in $\mathbb{Q}_p[G]$ are a sum of primitive idempotents in $\mathbb{Q}_p[G]$. Moreover, the algebraic trace is additive. Thus, the claim follows. □

We would also like to give an alternative proof in the case where G is cyclic. The alternative proof is worth mentioning as it emphasizes the role of the Hensel lifting and as it uses elementary tools only. Before we start with the actual proof, we recall

Lemma 5.5.11 (Hensel)**.** *Let $f(X)$ be a primitive polynomial in $\mathbb{Z}_p[X]$, i.e. $f(X) \not\equiv 0 \ mod\ (p)$. Assume that $f(X)$ modulo (p) has a decomposition*

$$f(X) \equiv \bar{g}(X)\bar{h}(X) \ mod\ (p)$$

into coprime polynomials $\bar{g}, \bar{h} \in \mathbb{F}_p[X]$, then $f(X)$ has a decomposition

$$f(X) = g(X)h(X)$$

into polynomials $g, h \in \mathbb{Z}_p[X]$ with $deg(g) = deg(\bar{g})$ and

$$g(X) \equiv \bar{g}(X) \ mod\ (p) \quad and\ h(X) \equiv \bar{h}(X) \ mod\ (p).$$

Proof. See Lemma 4.6, page 135, of [2]. □

Proof. We now want to give the alternative proof. We assume that G is cyclic of order n and that $\sigma \in G$ is a generator of G. It then follows that

$$\mathbb{Z}_p[G] \cong \mathbb{Z}_p[X]/((1+X)^n - 1),\ \sigma \mapsto X+1,$$

$$\mathbb{F}_p[G] \cong \mathbb{F}_p[X]/((1+X)^n - 1),\ \sigma \mapsto X+1.$$

In the following, we want to show that for every idempotent $\tilde{\alpha} \in \mathbb{F}_p[G]$ there exists an idempotent $\alpha \in \mathbb{Z}_p[G]$ with $\tilde{\alpha} = \alpha\ mod\ (p)$.
Let $\bar{f}(X) \in \mathbb{F}_p[X]$ correspond to a non-trivial idempotent $\tilde{\alpha}$ in $\mathbb{F}_p[G]$, i.e.

$$\bar{f}(\bar{f}-1) \equiv 0\ mod\ ((1+X)^n - 1).$$

Then there exists an $\bar{g} \in \mathbb{F}_p[X]$ such that

$$\bar{f}(\bar{f}-1) = \bar{g}((1+X)^n - 1).$$

Now we define the polynomial $s(X) = g(X)((1+X)^n - 1) \in \mathbb{Z}_p[X]$, where $g(X) \in \mathbb{Z}_p[X]$ with $\bar{g}(X) = g(X)\ mod\ (p)$. Obviously, $\bar{s} = \bar{g}((1+X)^n - 1)$, where $\bar{\cdot}$ denotes the reduction modulo (p). Observe that $s(X) \notin p\mathbb{Z}_p[X]$. Otherwise, $\bar{f}(\bar{f}-1) = 0$ in $\mathbb{F}_p[X]$. This implies that $\bar{f} = 1$ or $\bar{f} = 0$, yielding the contradiction that $\bar{f}$ was assumed to be non-trivial. Moreover, $\bar{f}$ and $\bar{f} - 1$ are certainly coprime in $\mathbb{F}_p[X]$. By Hensel's Lemma, it follows that $\bar{f}$ and $\bar{f} - 1$ can be lifted to polynomials $f(X), \tilde{f}(X) \in \mathbb{Z}_p[X]$ such that $s(X) = f(X)\tilde{f}(X)$. We need to show that we can choose $\tilde{f} = f - 1$. For doing so, we revisit the proof of Hensel's Lemma, following the proof of [2], page 135, with according notation:
In the proof, we have that $\bar{h} = \bar{g} - 1$ and hence $h_0 = g_0 - 1$. Thus, we may set $a = 1$ and $b = -1$. Following the proof, we see that it is sufficient to solve the congruence

$$g_0 f_n - (g_0 - 1)f_n \equiv f_n\ mod\ (\pi).$$

(See page 136, first congruence for $a = 1$, $b = -1$, and $\bar{h} = \bar{g} - 1$). Let $f_n(X) = -q(X)g_0(X) - p_n(X)$ with $q(X), p_n(X) \in \mathbb{Z}_p[X]$ with $deg(p_n) < deg(g_0)$. (Observe that $q(X) \in \mathbb{Z}_p[X]$ since the leading coefficient of g_0 is a unit). It follows that

$$g_0 p_n(X) + (g_0 - 1)p_n(X) \equiv f_n(X)\ mod\ (\pi).$$

Since $p_n(X) = q_n(X)$, for all $n \in \mathbb{N}$, it follows that $h = g - 1$.
Resuming the previous context and notation, we obtain that we can indeed set $\tilde{f} = f - 1$. It follows that there exists a polynomial $f(X) \in \mathbb{Z}_p[X]$ such that

$$f(f-1) = s = g(X)((1+X)^n - 1),\ \text{and thus}$$

$$f(f-1) \equiv 0 \; mod \; ((1+X)^n - 1).$$

Hence, f is an idempotent in $\mathbb{Z}_p[X]/((1+X)^n - 1)$, yielding an idempotent in $\mathbb{Z}_p[G]$. This shows that we can lift idempotents of $\mathbb{F}_p[G]$ to idempotents of $\mathbb{Z}_p[G]$. Henceforth, let ϕ denote the reduction modulo (p), A be the set of idempotents in $\mathbb{Z}_p[G]$, and B be the set of idempotents in $\mathbb{F}_p[G]$. Since ϕ certainly maps idempotents in $\mathbb{Z}_p[G]$ to idempotents in $\mathbb{F}_p[G]$, it follows that

$$\phi_{|A} : A \to B$$

is surjective by the above arguments.
Claim: $\phi_{|A}$ is also injective .
Proof: Assume that $\alpha, \beta \in \mathbb{Z}_p[G]$ are distinct idempotents with $\phi(\alpha) = \phi(\beta)$. It follows that $\phi(\alpha - \beta) = 0$, i.e. $\alpha - \beta \in p\mathbb{Z}_p[G]$. Let us say $\alpha - \beta = p^k x$, for some $x \in \mathbb{Z}_p[G] \setminus p\mathbb{Z}_p[G]$, $k \in \mathbb{Z}_{>0}$. (As $\alpha - \beta \neq 0$ by assumption, we can certainly write $\alpha - \beta$ like that). It follows that

$$\begin{aligned} p^{3k}x^3 &= (\alpha - \beta)^3 \\ &= \alpha^3 - 3\alpha^2\beta + 3\alpha\beta^2 - \beta^3 \\ &= \alpha - 3\alpha\beta + 3\alpha\beta - \beta \\ &= \alpha - \beta \\ &= p^k x. \end{aligned}$$

It follows that $x = p^{2k}x^3 \in p\mathbb{Z}_p[G]$, which contradicts the choice of x. Hence, $\phi(\alpha) = \phi(\beta)$, α, β idempotents, implies that $\alpha = \beta$. This proves the claim.
It is left to show that primitive idempotents in $\mathbb{Z}_p[G]$ are mapped to primitive idempotents in $\mathbb{F}_p[G]$:
Let α be a primitive idempotent in $\mathbb{Z}_p[G]$ and assume that

$$\phi(\alpha) = \tilde{\alpha}_1 + \tilde{\alpha}_2,$$

where $\tilde{\alpha}_1, \tilde{\alpha}_2$ are orthogonal idempotents in $\mathbb{F}_p[G]$. Since $\phi_{|A}$ is bijective, there exist unique idempotents α_1, α_2 in $\mathbb{Z}_p[G]$ with $\phi(\alpha_i) = \tilde{\alpha}_i$, $i = 1, 2$. Since $\phi(\alpha_1\alpha_2) = 0$ and $\alpha_1\alpha_2$ idempotent, it also follows that $\alpha_1\alpha_2 = 0$. As ϕ is injective, we can conclude that $\alpha = \alpha_1 + \alpha_2$. This yields the desired contradiction as α was supposed to be primitive. □

After this interlude on representation theory, we now want apply the developed results to the capitulation problem. By Proposition 5.5.5, we have that

$$\mathbb{Z}_p[G] = \alpha_1\mathbb{Z}_p[G] \oplus ... \oplus \alpha_r\mathbb{Z}_p[G], \tag{5.1}$$

where the α_i are primitive orthogonal idempotents in $\mathbb{Z}_p[G]$, for all $1 \leq i \leq r$. Let $\tilde{\alpha}_i \in \mathbb{F}_p[G]$, $1 \leq i \leq r$, denote the image of α_i in $\mathbb{F}_p[G]$. It follows that

$$\mathbb{F}_p[G] = \tilde{\alpha}_1\mathbb{F}_p[G] \oplus ... \oplus \tilde{\alpha}_r\mathbb{F}_p[G],$$

where the $\tilde{\alpha}_i$, $1 \leq i \leq r$, are central orthogonal idempotents in $\mathbb{F}_p[G]$ as G is abelian. Moreover, the $\tilde{\alpha}_i$'s are primitive since $\mathbb{Z}_p[G]$ has good reduction. By Maschke's Theorem, we know that $\mathbb{F}_p[G]$ is semi-simple. Also, $\tilde{\alpha}_i\mathbb{F}_p[G]$, $1 \leq i \leq r$, is an indecomposable $\mathbb{F}_p[G]$-module since the $\tilde{\alpha}_i$'s are primitive. As $\mathbb{F}_p[G]$ is semi-simple, it even follows that $\tilde{\alpha}_i\mathbb{F}_p[G]$ is an irreducible $\mathbb{F}_p[G]$-module. (See Proposition 5.5.4). Observe that

$$\tilde{\alpha}_i\mathbb{F}_p[G] \cong \alpha_i\mathbb{Z}_p[G]/(\alpha_i\mathbb{Z}_p[G] \cap p\mathbb{Z}_p[G]),\ 1 \leq i \leq r.$$

It follows that $\alpha_i\mathbb{Z}_p[G]/(\alpha_i\mathbb{Z}_p[G] \cap p\mathbb{Z}_p[G])$, $1 \leq i \leq r$, is an irreducible $\mathbb{Z}_p[G]$-module. Thus, we have shown

Proposition 5.5.12. *Let G be a finite abelian group of order n with $p \nmid n$. Let $\mathbb{Z}_p[G]$ be decomposed as in (5.1). Then $\alpha_i\mathbb{Z}_p[G]/(\alpha_i\mathbb{Z}_p[G] \cap p\mathbb{Z}_p[G])$ is an irreducible $\mathbb{Z}_p[G]$-module, for all $1 \leq i \leq r$.*

Remark: Observe that $\alpha_i\mathbb{Z}_p[G] \cap p\mathbb{Z}_p[G] = p\alpha_i\mathbb{Z}_p[G]$, for all $1 \leq i \leq r$.
Proof: "$\supset$" is obvious.
$\subset$: Let $\alpha_i x = py$ with $x, y \in \mathbb{Z}_p[G]$, for some $1 \leq i \leq r$. It follows that $py = p\alpha_i y \in p\alpha_i\mathbb{Z}_p[G]$.

Definition: Let $\mathbb{Z}_p[G]$ be decomposed as in (5.1). Then we call the α-components $A(K)_{\alpha_i}$ irreducible α-components as they correspond to primitive idempotents. Accordingly, we speak of irreducible α-components $H(K)_{\alpha_i}$.

The above proposition shows that p-maximal elements in an irreducible component $\alpha\,\mathbb{Z}_p[G]$ are invertible in a certain sense. More precisely, we have

Corollary 5.5.13. *In the situation as above, let $\alpha = \alpha_i$, for some $1 \leq i \leq r$, and let $\alpha x \in \alpha\mathbb{Z}_p[G] \setminus p\alpha\mathbb{Z}_p[G]$. Then there exists an $y \in \mathbb{Z}_p[G]$ such that $\alpha x \alpha y = \alpha x y \equiv \alpha\ mod\ (p\alpha\mathbb{Z}_p[G])$.*

Proof. The proof follows immediately from the fact that $\alpha\mathbb{Z}_p[G]/p\alpha\mathbb{Z}_p[G]$ is an irreducible $\mathbb{Z}_p[G]$-module. □

Corollary 5.5.14. *In the situation as above, let* $\alpha x \in \alpha\mathbb{Z}_p[G] \setminus p\alpha\mathbb{Z}_p[G]$. *Then for all* $a \in A(K)$,

$$ord(a^{\alpha}) = ord(a^{\alpha x}).$$

Proof. Since $\alpha x \notin p\alpha\mathbb{Z}_p[G]$, there exists an $y \in \mathbb{Z}_p[G]$ such that $\alpha x \alpha y = \alpha + p\alpha z$, for some $z \in \mathbb{Z}_p[G]$. It follows that

$$ord(a^{\alpha}) \geq ord(a^{\alpha x}) \geq ord(a^{\alpha x \alpha y}) = ord(a^{\alpha + p\alpha z}) = ord(a^{\alpha}).$$

Hence, the above inequalities are all equalities and the claim follows. □

5.6 Capitulation for the Case that $A(K)$ is $\mathbb{Z}_p[G]$-Cyclic

As before, let K/k be an abelian extension with Galois group $G = Gal(K/k)$ and we suppose that the prime p does not divide the order of G. In this section, we additionally assume that $A(K)$ is $\mathbb{Z}_p[G]$-cyclic, i.e. $A(K) = a^{\mathbb{Z}_p[G]}$, for some ideal class a in K. By virtue of Corollary 5.5.13, we then obtain particularly strong results for the structure of $A(K)$ and the capitulation kernel. For instance, we show that under certain conditions the l-socle of $A(K)$ capitulates completely in the l-socle of $H(K)$, where $1 \leq p^l \leq exp(A(K))$. Moreover, we explicitly state the $\mathbb{Z}_p[G]$-annihilator of $A(K)$. We conclude this section with an analysis of the special case that the irreducible components of $A(K)$ are cyclic.

Let $S_l(Gal(H(K)/K))$ be the l-socle of $Gal(H(K)/K)$, where $1 \leq p^l \leq exp(Gal(H(K)/K))$. Recall that

$$S_l(Gal(H(K)/K)) = \{\sigma \in Gal(H(K)/K) |\ ord(\sigma) \leq p^l\}.$$

Then we define $S_l(H(K))$ to be the unique intermediate field of $H(K)/K$ with Galois group over K being isomorphic to $S_l(Gal(H(K)/K))$. In the same way we may define the l-socle of $H(K)_{\alpha}$ to be the unique subfield $S_l(H(K)_{\alpha})$ of $H(K)_{\alpha}/K$ with $Gal(S_l(H(K)_{\alpha})/K) \cong S_l(Gal(H(K)_{\alpha}/K))$. We may now apply the machinery that we developed in the previous section. We have

Theorem 5.6.1. *Notations being like above, let* $H(K)_{\alpha}$ *be a fixed irreducible* α*-component of* $H(K)$. *Assume that* $G = Gal(K/k)$ *is abelian with* $p \nmid |G|$ *and that* α *has a central lift to the* l*-socle* $S_l(H(K)_{\alpha})$, $1 \leq p^l \leq exp(A(K)_{\alpha})$, *denoted by* $\tilde{\alpha}$. *Let* $\mathbb{Z}_p[G]$ *be decomposed as in (5.1) and assume that* $A(K)_{\alpha}$ *is* $\mathbb{Z}_p[G]$*-cyclic. Then the* k*-socle of* $A(K)_{\alpha}$ *capitulates completely in the* k*-socle of* $H(K)_{\alpha}$, $\forall\ 1 \leq k \leq l$.

Proof. For the ease of notation, we set $A_\alpha = A(K)_\alpha$. We prove the theorem by induction on $1 \leq p^k \leq p^l$. As $\tilde{\alpha}$ is a central lift to $S_l(H(K)_\alpha)$ by assumption, it follows that Suzuki's Theorem holds for each subfield of $S_l(H(K)_\alpha)/K$ which is Galois over k. In particular, it holds for all k-socles $S_k(H(K)_\alpha)$ of $H(K)_\alpha$ with $k \leq l$. This implies that for each $1 \leq p^k \leq p^l$, there is an ideal class $b_k \in S_k(A_\alpha)$ with $ord(b_k) = p^k$ such that b_k capitulates in $S_k(H(K)_\alpha)$. Let $a \in A_\alpha$ such that $A_\alpha = a^{\alpha\mathbb{Z}_p[G]}$. Let $a_k = a^{p^m}$ such that $m \in \mathbb{N}$ and $ord(a^{p^m\alpha}) = p^k$. By the last corollary, it then follows that $S_k(A_\alpha) = a_k^{\alpha\mathbb{Z}_p[G]}$. Since $ord(b_k) = p^k$, it follows that $b_k = a_k^{\alpha x}$, where $\alpha x \in \alpha\mathbb{Z}_p[G] \setminus p\alpha\mathbb{Z}_p[G]$. Now let $1 \neq a_k^{\alpha y} \in S_k(A_\alpha)$. Since $\alpha x \notin p\alpha\mathbb{Z}_p[G]$, there exists an $y' \in \mathbb{Z}_p[G]$ such that $\alpha x \alpha y' = \alpha + p\alpha y''$, for some $y'' \in \mathbb{Z}_p[G]$, and hence $\alpha x \alpha y' y = \alpha y + p\alpha y'' y$. Since $b_k = a_k^{\alpha x}$ capitulates in $S_k(H(K)_\alpha)$, it easily follows that $a_k^{\alpha x \alpha y' y} = a_k^{\alpha y + p\alpha y'' y}$ also capitulates in $S_k(H(K)_\alpha)$ as $S_k(H(K)_\alpha)$ is Galois over k. By induction hypothesis, we may assume that $a_k^{p\alpha y'' y}$ capitulates due to $ord(a_k^{p\alpha y'' y}) < ord(a_k^{\alpha y}) \leq p^k$. (By the previous arguments, the induction start for $k = 1$ obviously holds). All in all, we obtain that $a_k^{\alpha y}$ capitulates in $S_k(H(K)_\alpha)$. As $S_k(A_\alpha)$ is $\mathbb{Z}_p[G]$-cyclic, the claim follows. □

Corollary 5.6.2. *In the situation as in the above theorem, it follows that all p-maximal elements in A_α, i.e. all elements which do not lie in A_α^p, have the same order.*

Proof. Obviously, all p-maximal elements in A_α are of the form $a^{\alpha x}$ with $\alpha x \in \alpha\mathbb{Z}_p[G] \setminus p\alpha\mathbb{Z}_p[G]$. Corollary 5.5.14 then yields that $ord(a^\alpha) = ord(a^{\alpha x})$. □

We continue this section by explicitly stating the $\mathbb{Z}_p[G]$-annihilator of $A(K)$ provided that $A(K)$ is $\mathbb{Z}_p[G]$-cyclic. We have

Theorem 5.6.3. *Let us assume that $A(K)$ is $\mathbb{Z}_p[G]$-cyclic and let $A(K)$ be decomposed as in (5.1). Let $n_i = exp(A(K)_{\alpha_i})$, $\forall\ 1 \leq i \leq r$. Let $S_1 \subset \{1, ..., r\}$ such that for all $i \in S_1$, we have that $A(K)_{\alpha_i} = \{1\}$. We define $\alpha = \sum_{i \in S_1} \alpha_i$ and $S_2 = \{1, ..., r\} \setminus S_1$. Then*

$$Ann_{\mathbb{Z}_p[G]}(A(K)) = \alpha\mathbb{Z}_p[G] \oplus_{i \in S_2} p^{n_i}\alpha_i\mathbb{Z}_p[G].$$

Proof. Since the α_i's are orthogonal to each other, α is certainly an idempotent and $\alpha\mathbb{Z}_p[G] = \sum_{i \in S_1} \alpha_i\mathbb{Z}_p[G]$. Moreover, for all $i \in S_2$ we have that $A(K)_{\alpha_i} \neq \{1\}$ and by the previous corollary it follows that the annihilator is given by $Ann_{\mathbb{Z}_p[G]}(A(K)_{\alpha_i}) = p^{n_i}\mathbb{Z}_p[G]$. As the α_i's are orthogonal to each other, the claim follows. □

In view of Theorem 5.6.1, the following question emerges: What can we say when L/k is Galois, but L is not contained in an α-component $H(K)_\alpha$? In this context, it makes sense to introduce the following

Definition: Let K/k be as before and let $A(K)$ be decomposed as in (5.1). Let L be an intermediate field of $H(K)/K$ and set $L_i = L \cap H(K)_{\alpha_i}$, $\forall\ 1 \leq i \leq r$. Then we say L is *faithful* with respect to $(\alpha_1, ..., \alpha_r)$ if

$$L \ = \ \prod_{i=1}^{r} L_i. \tag{5.2}$$

Remark: One can easily construct group theoretic examples where the above property does not hold. If L is not faithful w.r.t. $(\alpha_1, ..., \alpha_r)$, then it becomes very difficult to extract information for the capitulation problem from the decomposition of $A(K)$ into α-components.

Proposition 5.6.4. *Notations being like above, let L be an intermediate field of $H(K)/K$ and assume that L is faithful w.r.t. $(\alpha_1, ..., \alpha_r)$. Then L/k is Galois if and only if $\forall\ 1 \leq i \leq r$:*

$$L_i = S_{l_i}(H(K)_{\alpha_i}),\ \textit{for some}\ 1 \leq p^{l_i} \leq exp(A(K)_{\alpha_i}).$$

Proof. First observe that for all $1 \leq i \leq r$, we have that $exp(A(K)_{\alpha_i}) = subexp(A(K)_{\alpha_i})$ by Corollary 5.6.2. (For the definition of the subexponent of an abelian group, see Section 4.1). Moreover, we have shown that the $\mathbb{Z}_p[G]$-cyclicity of $A(K)_{\alpha_i}$ is inherited to all socles of $A(K)_{\alpha_i}$. Thus, $\mathbb{Z}_p[G]$ acts transitively on all socles of $A(K)_{\alpha_i}$ as $A(K)_{\alpha_i}$ is irreducible. Hence, if M is an intermediate field of $H(K)_{\alpha_i}/K$ and M is not a socle of $H(K)_{\alpha_i}/K$, then M is not Galois over k. As L is faithful, the above arguments extend to L. Indeed, L is given as in (5.2). A moment of reflection then shows that

$$Gal(H(K)/\prod_{i=1}^{r} L_i) \ = \ \prod_{i=1}^{r} Gal(H(K)_{\alpha_1}/L_i), \tag{5.3}$$

where $\prod$ denotes the Cartesian product. Now assume that there exists an $1 \leq i \leq r$ such that L_i is not a socle in $H(K)_{\alpha_i}/K$. Without restriction of generality, we may say that L_1 is not a socle in $H(K)_{\alpha_1}/K$. By the above arguments, there exists some $\sigma \in Gal(K/k)$ such that $L_1^\sigma = \sigma(L_1) \neq L_1$. It follows that $G(H(K)_\alpha/L_1) \neq G(H(K)_\alpha/L_1^\sigma)$. By (5.3), we then obtain that L is not Galois over k. The converse direction is also obviously true. $\square$

We have seen how powerful the decomposition of $A(K)$ into irreducible α-components is in the context of the capitulation problem. The capitulation problem becomes particularly well-accessible when the irreducible submodules $\alpha\mathbb{Z}_p[G]$ of $\mathbb{Z}_p[G]$ are $\mathbb{Z}_p$-cyclic. Indeed, in the case where $A(K)$ is $\mathbb{Z}_p[G]$-cyclic it has the consequence that all α-components are either trivial or a cyclic subgroup of $A(K)$. In light of that, we pose the following question: Under which circumstances are the irreducible submodules of $\mathbb{Z}_p[G]$ definitely $\mathbb{Z}_p$-cyclic? In this context, we need the following

Theorem 5.6.5. *Let μ_{p-1} denote the group of $(p-1)$-th roots of unity. Then the group of roots of unity in $\mathbb{Q}_p$ is precisely*

$$\mu(\mathbb{Q}_p) = \mu_{p-1} \quad \textit{when } p \textit{ is an odd prime, and}$$

$$\mu(\mathbb{Q}_2) = \{\pm 1\}.$$

In fact, Hensel's Lemma yields that all $(p-1)$-th roots of unity lie in $\mathbb{Z}_p$.

Proof. See Corollary 2, page 110, of [20]. □

Proposition 5.6.6. *Let G be a finite abelian group of order n. Then the following is equivalent:*
(i) $exp(G)$ divides $p-1$.
(ii) There exist primitive orthogonal idempotents $\alpha_1, ..., \alpha_n \in \mathbb{Z}_p[G]$ such that

$$\mathbb{Q}_p[G] = \alpha_1\mathbb{Q}_p[G] \oplus ... \oplus \alpha_n\mathbb{Q}_p[G].$$

In particular, in this case $\alpha_i\mathbb{Q}_p[G]$ is a 1-dimensional $\mathbb{Q}_p$-vector space, $\forall\ 1 \leq i \leq n$.

Proof. The proof follows immediately from the previous theorem and Proposition 5.5.5. Indeed, as G is abelian, all characters of G over $\overline{\mathbb{Q}_p}$ are 1-dimensional, i.e. their images are l-th roots of unity, where $l = exp(G)$. The images of all characters lie in $\mathbb{Q}_p$ if and only if $\mathbb{Q}_p$ contains all l-th roots of unity. This is the case if and only if $l|(p-1)$. □

Lemma 5.6.7. *Let G be a finite abelian group and $\alpha \in \mathbb{Z}_p[G]$ an idempotent. Then $\alpha\mathbb{Q}_p[G]$ is a 1-dimensional $\mathbb{Q}_p$-vector space if and only if $\mathbb{Z}_p - rk(\alpha\mathbb{Z}_p[G]) = 1$.*

Proof. First note that $\alpha\mathbb{Q}_p[G] \cap \mathbb{Z}_p[G] = \alpha\mathbb{Z}_p[G]$. Indeed, let $x \in \mathbb{Q}_p[G]$ with $\alpha x \in \mathbb{Z}_p[G]$. Let us say $\alpha x = y$. Then $y = \alpha y \in \alpha\mathbb{Z}_p[G]$. The other inclusion is obvious. Now assume that $\alpha\mathbb{Q}_p[G]$ is a 1-dimensional $\mathbb{Q}_p$-vector space. Let us say, $\alpha\mathbb{Q}_p[G] = \mathbb{Q}_p\alpha x$, for some $x \in \mathbb{Q}_p[G]$. By the previous arguments, this implies that $\alpha\mathbb{Z}_p[G] = \mathbb{Q}_p\alpha x \cap \mathbb{Z}_p[G]$. Furthermore, we may write

$$\alpha x = p^k y = p^k \alpha y \text{ with } y \in \mathbb{Z}_p[G],\ v_p(y) = 0,\ k \in \mathbb{Z}.$$

Let $z \in \mathbb{Q}_p[G]$. Then $z\alpha x \in \mathbb{Z}_p[G] \Leftrightarrow z \in p^{-k}\mathbb{Z}_p$, i.e.

$$\alpha\mathbb{Z}_p[G] = \mathbb{Z}_p p^{-k}\alpha x = \mathbb{Z}_p \alpha y.$$

As y lies in $\mathbb{Z}_p[G]$, we have shown that $\mathbb{Z}_p - rk(\alpha\mathbb{Z}_p[G]) = 1$. The other implication is analogous. □

Observe that the assumption that $exp(G)|(p-1)$, implies that $|G|$ and p are coprime. Combining the above lemma and Proposition 5.6.6, we thus obtain

Corollary 5.6.8. *Let K/k be an abelian extension with Galois group $G = Gal(K/k)$, and assume that $exp(G)|(p-1)$. Also suppose that $A(K)$ is $\mathbb{Z}_p[G]$-cyclic. For $r = rk(A(K))$, there exist idempotents $\alpha_1, ..., \alpha_r \in \mathbb{Z}_p[G]$ such that*

$$A(K) = A(K)_{\alpha_1} \times ... \times A(K)_{\alpha_r},\ \textit{and}$$
$$rk(A(K)_{\alpha_i}) = 1,\ \forall\ 1 \leq i \leq r.$$

The situation as in Corollary 5.6.8 can be realized in the context of cyclotomic $\mathbb{Z}_p$-extensions for example: Let K be a number field, ζ_{p^n} be a primitive p^n-th root of unity ($n \in \mathbb{N}$), and assume that $\zeta_p \notin K$. Then we define $K_n = K(\zeta_{p^n})$. By Galois theory and the previous theorem, it follows that there exists a subfield $K'_n \subset K_n$ such that $Gal(K_n/K'_n)$ is abelian with $|Gal(K_n/K'_n)| = p-1$. Hence, one only has to check if $A(K_n)$ is $\mathbb{Z}_p[Gal(K_n/K'_n)]$-cyclic. If this is the case, we are in the situation of Corollary 5.6.8. Applying Theorem 5.6.1 now, the capitulation problem becomes particularly well-accessible.

We conclude this section with two interesting examples:

Example: Consider the imaginary quadratic number field

$$K = \mathbb{Q}(\alpha) \text{ with } \alpha^2 = -3299.$$

MAGMA yields that $A(K) \cong C_3 \times C_9$.
Obviously, $A(K)$ is not $\mathbb{Z}_3[G]$-cyclic, where $G = Gal(K/\mathbb{Q})$. Moreover, all

intermediate fields of $H(K)/K$ are Galois over $\mathbb{Q}$. Using MAGMA, one can verify that there is an intermediate field L of $H(K)/K$ with $Gal(L/K) \cong C_9$, but $P_K(L) \cong C_3 \times C_3$. For more details see [21]. Although $exp(G) = p-1 = 2$, we cannot decompose $A(K)$ as in Corollary 5.6.8. This example demonstrates that the assumption that $A(K)$ is $\mathbb{Z}_p[G]$-cyclic is essential.

We proceed with an example which shows that the l-socle of $A(K)$ does not capitulate completely in the l-socle of $H(K)$ in general. We have

Example: Consider the imaginary quartic number field

$$K = \mathbb{Q}(\alpha) \text{ with } \alpha^4 + 313 = 0.$$

Then MAGMA yields: 1. $A(K) \cong C_2 \times C_{16}$;
2. $P_K(S_1(H(K))) \cong C_4$, i.e. the 1-socle of $A(K)$ does not capitulate completely in the 1-socle of $H(K)$.

5.7 Decomposition of $A(K)$ into a Direct Product of $\mathbb{Z}_p[G]$-Cycles

Throughout this section, we assume $G = Gal(K/k)$ to be abelian and $p \nmid |G|$. In Section 5.2, we have decomposed $A(K)$ into a direct product of irreducible α-components. In the following, we pursue an even finer decomposition of $A(K)$ into a direct product of $\mathbb{Z}_p[G]$-cycles. By $\mathbb{Z}_p[G]$-cycles, we mean subgroups of $A(K)$ of the form $a^{\mathbb{Z}_p[G]} = \{a^x | \ x \in \mathbb{Z}_p[G]\}$, for some ideal class a in K. In view of that, we can thus relax the assumption of the previous section that $A(K)$ is $\mathbb{Z}_p[G]$-cyclic, i.e. all the results of the previous section can then be applied to $\mathbb{Z}_p[G]$-cycles within irreducible α-components of $A(K)$. Furthermore, we show that such a decomposition is unique in a certain sense and present various consequences of the above result.

By the previous sections, the irreducible components $A(K)_\alpha$ of $A(K)$ are $\mathbb{Z}_p[G]$-closed since $\mathbb{Z}_p[G]$ is abelian. Hence, we may restrict ourselves to considering a fixed irreducible α-component $A(K)_\alpha$ when we intend to decompose $A(K)$ into a direct product of $\mathbb{Z}_p[G]$-cycles. Before we start with the actual proof, we need three easy lemmata first.

Lemma 5.7.1. *Let a be an ideal class in the irreducible component $A(K)_\alpha$. Then all p-maximal elements in $a^{\mathbb{Z}_p[G]}$ are of the same order, i.e.*

$$a^{\mathbb{Z}_p[G]} \cong \underbrace{C_{p^k} \times ... \times C_{p^k}}_{r-times},$$

where $r, k \in \mathbb{Z}_{>0}$.

Proof. Follows immediately from the proof of Corollary 5.6.2. □

Lemma 5.7.2. *Let* $A_1 \subset A(K)_\alpha$ *be a direct product of* $\mathbb{Z}_p[G]$*-cycles, i.e.*

$$A_1 = a_1^{\mathbb{Z}_p[G]} \times ... \times a_n^{\mathbb{Z}_p[G]}, \text{ for some } a_1, ..., a_n \in A_1.$$

Then A_1 *is closed by the action of* $\mathbb{Z}_p[G]$.

Proof. Elementary. □

Lemma 5.7.3. *Let* $A_1 = a^{\mathbb{Z}_p[G]} \subset A(K)_\alpha$*, for some* $a \in A(K)_\alpha$*, and* $A_2 \subset A(K)_\alpha$ *be a direct product of* $\mathbb{Z}_p[G]$*-cycles. Then either* $A_1 \cap A_2 = \{1\}$ *or the 1-socle* $S_1(A_1)$ *is contained in* $S_1(A_2)$.

Proof. Assume that $A_1 \cap A_2 \neq \{1\}$. Then there exists an ideal class $b \in A(K)$ of order p such that $b \in A_1 \cap A_2$. By the previous section, we obtain that $\mathbb{Z}_p[G]$ acts transitively on the 1-socle of A_1. Since A_2 is $\mathbb{Z}_p[G]$-closed, it follows that $S_1(A_1)$ is contained in $S_1(A_2)$. □

Theorem 5.7.4. *Let* K/k *be abelian with Galois group* $G = Gal(K/k)$ *and* $p \nmid ord(G)$*. Then* $A(K)$ *can be decomposed into a direct product of* $\mathbb{Z}_p[G]$*-cycles.*

Proof. Let us assume that the fixed irreducible component $A(K)_\alpha$ is decomposed into cyclic subgroups as follows:

$$A(K)_\alpha = \underbrace{C_{p^{n_1}} \times ... \times C_{p^{n_1}}}_{r_1-\text{times}} \times ... \times \underbrace{C_{p^{n_s}} \times ... \times C_{p^{n_s}}}_{r_s-\text{times}},$$

where $r_1, ..., r_s \in \mathbb{Z}_{>0}$ and $0 < n_1 < n_2 < ... < n_s$. Now we start to construct a decomposition into $\mathbb{Z}_p[G]$-cycles by induction on t, where t runs backwards from s to 1.
$t = s$: Choose some element $a_{s,1}$ in $A(K)_\alpha$ of order p^{n_s}. If $rk(a_{s,1}^{\mathbb{Z}_p[G]}) = r_s$, we can continue with $t = s - 1$. If $rk(a_{s,1}^{\mathbb{Z}_p[G]}) < r_s$, then there exists an $a_{s,2} \in A(K)_\alpha$ of order p^{n_s} such that $< a_{s,2} >$ and $a_{s,1}^{\mathbb{Z}_p[G]}$ are disjoint. In particular, $S_1(< a_{s,2} >)$ is not contained in $S_1(a_{s,1}^{\mathbb{Z}_p[G]})$. By the previous lemma, it follows that the $\mathbb{Z}_p[G]$-cycles $a_{s,1}^{\mathbb{Z}_p[G]}$ and $a_{s,2}^{\mathbb{Z}_p[G]}$ are disjoint. In this

fashion, we can continue until $rk(a_{s,1}^{\mathbb{Z}_p[G]}, ..., a_{s,k_s}^{\mathbb{Z}_p[G]}) = r_s$, for suitable $k_s \in \mathbb{N}$. The initial lemma then yields that

$$A_s := a_{s,1}^{\mathbb{Z}_p[G]} \times ... \times a_{s,k_s}^{\mathbb{Z}_p[G]} \cong \underbrace{C_{p^{n_s}} \times ... \times C_{p^{n_s}}}_{r_s-\text{times}}.$$

$t < s$: Choose an element $a_{t,1} \in A(K)_\alpha$ of order p^{n_t} such that $< a_{t,1} >$ and $A_{t+1} \times ... \times A_s$ are disjoint. (See definition for A_s and assume that A_{s-1},..., A_{t+1} have been constructed accordingly by induction hypothesis). By the previous lemma, it then follows that $a_{t,1}^{\mathbb{Z}_p[G]}$ and $A_{t+1} \times ... \times A_s$ are disjoint. If $rk(a_{t,1}^{\mathbb{Z}_p[G]}) = r_t$, we can continue with $t-1$. If $rk(a_{t,1}^{\mathbb{Z}_p[G]}) < r_t$, then there exists an $a_{t,2} \in A(K)_\alpha$ of order p^{n_t} such that $< a_{t,2} >$ and $A_{t+1} \times ... \times A_s$ are disjoint. With the same arguments as before, we thus obtain, for suitable $k_t \in \mathbb{N}$, that

$$A_t = a_{t,1}^{\mathbb{Z}_p[G]} \times ... \times a_{t,k_t}^{\mathbb{Z}_p[G]} \cong \underbrace{C_{p^{n_t}} \times ... \times C_{p^{n_t}}}_{r_t-\text{times}},$$

where A_t and $A_{t+1} \times ... \times A_s$ are disjoint. One easily verifies that this eventually leads to a $\mathbb{Z}_p[G]$-basis for the irreducible component $A(K)_\alpha$ and hence for $A(K)$. □

Remark: 1. In Section 2.8, we have seen that the above statement is not true in general when p divides the order of G. So the assumption that $p \nmid |G|$ is essential here.

2. Certainly, the statement of the above theorem is true in general for finite abelian p-groups on which $\mathbb{Z}_p[G]$ acts. For instance, we may apply the above theorem also in the following context: Let $H(K) \supset L \supset K \supset k$ with $[L : K] = p^l$, for some $l \in \mathbb{N}$, and L/k Galois. Clearly, $\mathcal{H}^0(G(L/K), \mathcal{O}_L^*)$ is a finite abelian p-group and it is closed by the action of $\mathbb{Z}_p[G]$. Thus, it can be decomposed into a direct product of $\mathbb{Z}_p[G]$-cycles.

3. The above theorem is very useful in the context of capitulation: Let L be an intermediate field of $H(K)/K$ with L/k Galois and $[L : K] = p^l$. Let $A_1 = a^{\mathbb{Z}_p[G]} \subset A(K)_\alpha$ be a $\mathbb{Z}_p[G]$-cycle in a given irreducible α-component. Then either all elements in A_1 of order p^l capitulate in L or none of them.

Furthermore, one may pose the question to which extent the above decomposition of $A(K)$ into a direct product of $\mathbb{Z}_p[G]$-cycles is unique. One easily verifies that the $\mathbb{Z}_p[G]$-cycles themselves are not unique but we have the following

Proposition 5.7.5. *Notations being like above, let*

$$A(K) = \prod_{\alpha} \prod_{i=1}^{k_\alpha} a_{i,\alpha}^{\mathbb{Z}_p[G]}$$

be a direct product of $\mathbb{Z}_p[G]$-cycles, where α runs through the set of primitive orthogonal idempotents in $\mathbb{Z}_p[G]$ and $a_{i,\alpha} \in A(K)_\alpha$, $k_\alpha \in \mathbb{N}$. We then define $r_{i,\alpha} = rk(a_{i,\alpha}^{\mathbb{Z}_p[G]})$ and $n_{i,\alpha} = exp(a_{i,\alpha}^{\mathbb{Z}_p[G]})$. Let

$$A(K) = \prod_{\alpha} \prod_{i=1}^{l_\alpha} b_{i,\alpha}^{\mathbb{Z}_p[G]}$$

be another direct product of $\mathbb{Z}_p[G]$-cycles with $b_{i,\alpha} \in A(K)_\alpha$ and $l_\alpha \in \mathbb{N}$. For $r'_{i,\alpha} = rk(b_{i,\alpha}^{\mathbb{Z}_p[G]})$ and $n'_{i,\alpha} = exp(b_{i,\alpha}^{\mathbb{Z}_p[G]})$, we obtain that $k_\alpha = l_\alpha$, for all primitive idempotents α, and

$$\{(r_{i,\alpha}, n_{i,\alpha})_{1 \le i \le k_\alpha}\} = \{(r'_{i,\alpha}, n'_{i,\alpha})_{1 \le i \le k_\alpha}\},\ \forall\ \alpha,\ \textit{i.e.}$$

up to order, the ranks and the exponents of the $\mathbb{Z}_p[G]$-cycles in a decomposition of an irreducible component $A(K)_\alpha$ into a direct product are unique.

Proof. The proof is straightforward. Essentially, one observes that in an irreducible component of $A(K)$, the $\mathbb{Z}_p[G]$-cycles of different rank must be disjoint by Lemma 5.7.3. The rest follows from the unique decomposition of $A(K)$ into cyclic subgroups. □

Now let L/K be a p-extension with L/k Galois and set $A(K)' = N_{L/K}(A(L))$. As L/k is Galois, G acts on $A(L)$ and $A(K)'$. Hence, we can also decompose $A(K)'$ into a direct product of $\mathbb{Z}_p[G]$-cycles. The following result describes to which extent the structure of $A(K)'$ is transferred to $A(L)$. We have

Proposition 5.7.6. *In the situation as above, there exist $a_i \in A(K)'$, $b_i \in A(L)$ with $N_{L/K}(b_i) = a_i$ ($\forall\ 1 \le i \le k$) such that*
(i) $A(K)' = \prod_{i=1}^{k} a_i^{\mathbb{Z}_p[G]}$ is a direct product of $\mathbb{Z}_p[G]$-cycles and
(ii) $rk(a_i^{\mathbb{Z}_p[G]}) = rk(b_i^{\mathbb{Z}_p[G]})$.

Proof. Let $1 \le i \le k$ be fixed. By the previous arguments, we may choose $a_i \in A(K)'$ such that a_i lies in an irreducible α-component of $A(K)'$ and $b_i \in A(L)$ lies in an irreducible component of $A(L)$. Since $N_{L/K}(b_i^{\mathbb{Z}_p[G]}) = a_i^{\mathbb{Z}_p[G]}$, it obviously follows that $rk(b_i^{\mathbb{Z}_p[G]}) \ge rk(a_i^{\mathbb{Z}_p[G]})$. Suppose that $rk(b_i^{\mathbb{Z}_p[G]}) > rk(a_i^{\mathbb{Z}_p[G]})$. As all basis elements of $b_i^{\mathbb{Z}_p[G]}$ have the same order, we can conclude that $exp(b_i^{\mathbb{Z}_p[G]}) = exp(b_i^{\mathbb{Z}_p[G]} \cap ker N_{L/K})$, which yields that $b_i^{\mathbb{Z}_p[G]} \subset ker N_{L/K}$, a contradiction to a_i being non-zero. This completes the proof. □

5.8 Some Results on the Genus Field

Let K/k be an abelian extension with Galois group $G = Gal(K/k)$. The genus field of K/k is the maximal unramified extension of K, which is abelian over k. Henceforth, let M denote the maximal unramified p-extension of K, which is abelian over k, i.e. M is the so-called p-genus field of K/k. In what follows, we want to make use of the decomposition of $A(K)$ into a direct product of $\mathbb{Z}_p[G]$-cycles. On account of that, we assume that $p \nmid |G|$ as in the previous sections. The main result of this section is

Theorem 5.8.1. *Let K/k be an abelian extension with Galois group $G = Gal(K/k)$ and $p \nmid |G|$. Let $H(k)$ be the p-Hilbert class field of k and M be the p-genus field of K/k. Then: $M = KH(k)$.*

Proof. Obviously, $KH(k)$ is abelian over k as K/k and $H(k)/k$ are abelian. By Theorem 1.3.8, $KH(k)$ is also unramified and hence $KH(k) \subset M$. We will now show that also $KH(k) \supset M$. Indeed, let $A(k)$ be the p-part of $Cl(k)$. As $p \nmid |G|$ by assumption, it follows that $\imath_{K/k}$ embeds $A(k)$ into $A(K)$ and we obtain that

$$A(K) = A(k) \times ker N_{K/k}.$$

Now assume that $KH(k)$ is contained in $L \subset M$. It then follows that $G(H(K)/L)$ is $\mathbb{Z}_p[G]$-invariant. As in the previous section, we may decompose $G(H(K)/K)$ and $G(H(K)/L)$ into a direct product of $\mathbb{Z}_p[G]$-cycles. Let us assume that there is a primitive idempotent $\alpha \in \mathbb{Z}_p[G]$ such that $G(H(K)/K)_\alpha$ contains a $\mathbb{Z}_p[G]$-cycle $B = \tau^{\mathbb{Z}_p[G]}$, $\tau \in G(H(K)/K)_\alpha$, of rank larger than 1. Then B is contained in $G(H(K)/L)_\alpha$. Indeed, suppose this is not the case. Then $\tau \notin G(H(K)/L)_\alpha$ since $G(H(K)/L)_\alpha$ is $\mathbb{Z}_p[G]$-invariant. As L/k is abelian, it also follows that $G(L/K)$ commutes with $\tilde{G}$, where $\tilde{G}$ is a lift of G to $G(L/k)$. Thus, $\tilde{\tau}^{\mathbb{Z}_p[G]}$ has rank 1, where $\tilde{\tau} = res_{H(K)/L}(\tau)$. It follows that

$$\tau^{\mathbb{Z}_p[G]} \equiv < \tau > \ mod\ G(H(K)/L). \tag{5.4}$$

As $\tau^{\mathbb{Z}_p[G]}$ is of rank larger than 1 by assumption, there exists an $x \in \mathbb{Z}_p[G]$ such that $< \tau > \cap < \tau^x > = \{1\}$ and $ord(\tau) = ord(\tau^x)$. Corollary 5.6.2 then yields that $< \tau, \tau^x > \cong C_{p^n} \times C_{p^n}$, where $ord(\tau) = p^n$. Since $\tau \notin G(H(K)/L)_\alpha$, we also obtain that $exp(\tau^{\mathbb{Z}_p[G]} \cap G(H(K)/L)) < p^n$. As $\tau^x = \tau y$ for some $y \in \tau^{\mathbb{Z}_p[G]} \cap G(H(K)/L)_\alpha$ by (5.4), it follows that

$$< \tau, \tau^x > \cong C_{p^n} \times C_{p^l}$$

with $l < n$, which yields the desired contradiction. Let

$$G(H(K)/K) = \prod_{\alpha} \prod_{i=1}^{k_\alpha} \tau_{i,\alpha}^{\mathbb{Z}_p[G]}$$

be a direct product of $\mathbb{Z}_p[G]$-cycles, where α runs through a set of primitive idempotents in $\mathbb{Z}_p[G]$ and $\tau_{i,\alpha} \in A(K)_\alpha$, $k_\alpha \in \mathbb{N}$. By the previous arguments, all $\mathbb{Z}_p[G]$-cycles $\tau_{i,\alpha}^{\mathbb{Z}_p[G]}$ of rank larger than 1 must lie in $G(H(K)/L)$. Now recall that $A(K) = A(k) \times ker N_{K/k}$ and let $C = \varphi(ker N_{K/k})$, where φ denotes the Artin symbol of K. Let

$$C = C_1 \times C_2,$$

where C_1, C_2 are subgroups of C and where C_1 contains all $\mathbb{Z}_p[G]$-cycles in C of rank 1 and C_2 contains all $\mathbb{Z}_p[G]$-cycles in C of rank larger than 1. Let $L' = H(K)^{C_2}$ and thus $G(L'/K) \cong \varphi(A(k)) \times C_1$. By the previous arguments, then $L \subset L'$. Also observe that $ker N_{K/k} \cap A(K)^{G(K/k)} = \{1\}$ due to $p \nmid |G|$. Let $\{\tau_1, ..., \tau_k\} \subset C_1$ form a $\mathbb{Z}$-basis of C_1 ($k \in \mathbb{N}$). Let us fix some τ_i and let us denote it by τ_1. By the previous remark, there exists some $\sigma \in G(K/k)$ such that $(\tau')^{\sigma-1} \neq 1$, for all non-trivial $\tau' \in < \tau_1 >$. Since $< \tau_1 >$ is $\mathbb{Z}_p[G]$-invariant, we then obtain that $< \tau > = < \tau >^{\sigma-1}$. This shows that C_1 lies in the commutator subgroup of $G(L'/k)$ and hence $G(L/K) \cong A(k)$. This finally reveals that $M \subset L$. □

Corollary 5.8.2. *Notations being like above, assume that there is a prime $q < p$ with $q | ord(G)$ and $q \nmid (p-1)$. Then $ker N_{K/k}$ contains no $\mathbb{Z}_p[G]$-cycles of rank 1. In particular, if $rk(ker N_{K/k}) \leq 3$, then $ker N_{K/k}$ is $\mathbb{Z}_p[G]$-cyclic.*

Proof. Assume that $ker N_{K/k}$ contains a $\mathbb{Z}_p[G]$-cycle of rank 1. By previous arguments, then there is also a $\mathbb{Z}_p[G]$-cycle of rank 1 in a decomposition of $ker N_{K/k}$ into $\mathbb{Z}_p[G]$-cycles. Hence, this gives rise to an extension $L \supset K \supset k$ with L/k Galois and $[L : K] = p$. By assumption there is also a field $K \supset k' \supset k$ with $[K : k'] = q$. As L/k is Galois, a fortiori L/k' is Galois and $|G(L/k')| = pq$. It is well-known that groups of order pq with p, q prime, $q < p$, $q \nmid (p-1)$, are cyclic and hence abelian. (See Theorem 12, page 250, of [10]). It follows that L lies in the genus field of K/k, but not in $KH(k)$. This, however, is a contradiction to the fact that $KH(k)$ is the genus field of K/k. The second statement of the above corollary follows immediately from the first part. □

5.9 The Automorphisms of $G(H^{(2)}(K)/K)$ Acting on $A(K)$

In the previous sections, we had the Galois group $G(K/k)$ acting on the ideal class group of K. By the Theorem of Schur-Zassenhaus, we have that $G(H^{(2)}(K)/k)$ is a semi-direct product of $G(H^{(2)}(K)/K)$ and $G(K/k)$. Hence, each $\sigma \in G(K/k)$ gives rise to an automorphism

$$\varphi_\sigma : \ G(H^{(2)}(K)/K) \to G(H^{(2)}(K)/K), \ \tau \mapsto \tilde{\sigma}\tau\tilde{\sigma}^{-1},$$

where $\tilde{\sigma}$ is a lift of σ to $G(H^{(2)}(K)/k)$. (Note that $G(H^{(2)}(K)/K)$ is not abelian. Hence, φ_σ is dependent on the choice of $\tilde{\sigma}$). On the other hand, in general not every automorphism of $G(H^{(2)}(K)/K)$ is of the above form. Usually, the automorphism group of $G(H^{(2)}(K)/K)$ is rather large even if there is no subfield $k \subset K$ with K/k Galois. Thus, in this section, we are striving for a generalization of the previous approach by investigating the action of the automorphism group of $G(H^{(2)}(K)/K)$ on $A(K)$. Before we start this analysis, we want to mention some basic properties of the automorphism groups of finite p-groups:
As the easy example of the automorphism group of C_p shows, the automorphism group of a p-group is not necessarily a p-group. Moreover, one verifies that $Aut(G(H^{(2)}(K)/K))$ tends to have a lot more outer automorphisms than inner ones. (Of course, there always exist non-trivial outer automorphisms of a p-group as a p-group has a non-trivial center). In [41], Helleloid and Martin show that the automorphism group of a finite p-group is almost always a p-group. For further details, see Theorem 1.1, page 2, of [41]. Nonetheless, if p is a small prime and G is a p-group with few generators, the automorphism group of G is often not a p-group. For instance, in the following table Helleloid and Martin state the proportion of p-groups of a given order whose automorphism group is a p-group:

Order	$p = 2$	$p = 3$	$p = 5$
p^3	3 of 5	0 of 5	0 of 5
p^4	9 of 14	0 of 15	0 of 15
p^5	36 of 51	0 of 67	1 of 77
p^6	211 of 267	30 of 504	65 of 685
p^7	2067 of 2328	2119 of 9310	11895 of 34297

Another interesting result in this context is due to Burnside. We have the following

Theorem 5.9.1. *Let G be a finite p-group, $\Phi(G) = G'G^p$ be the Frattini subgroup of G. Then the kernel of the canonic group homomorphism*

$$\varphi : Aut(G) \to Aut(G/\Phi(G))$$

is a p-group.

Proof. See Theorem 5.1.4, page 174, of [40]. □

Let us now combine the above arguments. Henceforth, let K be a number field such that the automorphism group of $G(H^{(2)}(K)/K)$ is not a p-group. As $G(H^{(2)}(K)/K)/\Phi(G(H^{(2)}(K)/K)) \cong S_1(A(K))$, the previous theorem then implies that the reduction of $Aut(G(H^{(2)}(K)/K))$ acts non-trivially on $S_1(A(K))$. We now intend to use this machinery to obtain more information on the structure of the various capitulation kernels. In this context, we need some basic properties of the group transfer. For a finite group G and a subgroup H of G, let $Ver_{G\to H} : G \to H/[H,H]$ be the transfer of G to H and $\overline{Ver}_{G\to H} : G/[G,G] \to H/[H,H]$ the induced map. In the following, we will replace Ver by V in the notation. We then have

Proposition 5.9.2. *Let Ψ be a homomorphism of a group G to another group G_1, and suppose that the kernel of Ψ lies in a subgroup H of G. Then we have*

$$V_{\Psi(G)\to\Psi(H)} \circ \Psi = \bar{\Psi} \circ V_{G\to H}$$

where $\bar{\Psi} : H/[H,H] \to \Psi(H)/[\Psi(H),\Psi(H)]$ is the homomorphism induced by Ψ.

Proof. See Proposition 4, page 298, of [4]. □

We are now prepared to state and prove the following

Proposition 5.9.3. *In the situation as before, let $K \subset L \subset H(K) \subset H(L) \subset F \subset H^{(2)}(K)$ be a tower of number fields with the common notation. Then: $\bar{V}_{G(F/K)\to G(F/L)} = \bar{V}_{G(H(L)/K)\to G(H(L)/L)}$.*

Proof. First observe that $\bar{V}_{G(F/K)\to G(F/L)}$ maps $G(H(K)/K)$ to $G(H(L)/L)$. The same is true for $\bar{V}_{G(H(L)/K)\to G(H(L)/L)}$. We now apply the above proposition for $\Psi = res_{|H(L)}$ and $H = G(F/L)$, verifying that $ker\Psi = G(F/H(L))$ lies in H. We then obtain:

$$V_{G(H(L)/K)\to G(H(L)/L)} \circ res_{|H(L)} = \overline{res}_{|H(L)} \circ V_{G(F/K)\to G(F/L)}.$$

Since $res_{|H(K)} = res_{|H(K)} \circ res_{|H(L)}$, the claim easily follows. □

Assuming the situation as above, let $\varphi \in Aut(G(H^{(2)}(K)/K))$ and L be a subfield of $H(K)/K$. Recall that φ restricts canonically to $Aut(G(H(K)/K))$ and hence acts on $A(K)$. Thus, we may set $\varphi(L) = H(K)^{\varphi(G(H(K)/L))}$, which is well-defined. This leads us to the next

Proposition 5.9.4. *Let K be a number field, $\varphi \in Aut(G(H^{(2)}(K)/K))$ and L be a subfield of $H(K)/K$. Then:*

$$\varphi(P_K(L)) = P_K(\varphi(L)).$$

Proof. The proof follows immediately from the previous propositions and Artin's Theorem. □

By the assumption that the automorphism group of $G(H^{(2)}(K)/K)$ is not a p-group, we may find a non-trivial subgroup $V \subset Aut(G(H^{(2)}(K)/K))$ of order coprime to p and thus acting non-trivially on $A(K)$. Then the decomposition of $\mathbb{Z}_p[V]$ via idempotents goes analogously to the decomposition of $\mathbb{Z}_p[G(K/k)]$ and the results of the previous sections can be extended to this case one to one.
In Section 5.3, we could not dispense of the assumption that the lift of a central idempotent $\alpha \in \mathbb{Z}_p[G(K/k)]$ to $\mathbb{Z}_p[G(H(K)_\alpha/k)]$ is central. When we now consider the action of $Aut(G(H^{(2)}(K)/K))$ on $A(K)$ instead of the action of $G(K/k)$, the problem persists in a certain way. To be more precise, we give the following

Definition: Let G be a finite group and H be a subgroup of G. Then H is called *characteristic* in G, denoted by H char G, if $\varphi(H) = H$ for every automorphism φ of G.

Obviously, the higher commutator subgroups of a group are characteristic in G. Hence, $G(H^{(2)}(K)/H(K))$ char $G(H^{(2)}(K)/K)$ and thus V restricts to a subgroup of the automorphism group of $G(H(K)/K)$. Let V' denote the restriction of V to $H(K)$, i.e. $V' \subset Aut(G(H(K)/K))$. Now let $\alpha \in \mathbb{Z}_p[V]$ be an idempotent which restricts to an idempotent in $\mathbb{Z}_p[V']$, which we will also denote by α. As in Section 5.3, we may define $H(K)_\alpha = H(K)^{G(H(K)/K)^{1-\alpha}}$. Of course, α also restricts to an idempotent in $\mathbb{Z}_p[V'']$, where V'' denotes the restriction of V to $G(H(H(K)_\alpha)/K)$ and where $H(H(K)_\alpha)$ is the Hilbert class field of $H(K)_\alpha$. Then we define $A(H(K)_\alpha)_\alpha = A(H(K)_\alpha)^{\alpha\mathbb{Z}_p[V'']}$. It follows that $A(H(K)_\alpha)_\alpha$ is a uniquely determined well-defined subgroup of $A(H(K)_\alpha)$. Indeed, let $G_\alpha = G(H^{(2)}(K)/H(K)_\alpha)$, having the commutator subgroup $G'_\alpha = G(H^{(2)}(K)/H(H(K)_\alpha))$. Since by the definition of $H(K)_\alpha$, $\Psi(G_\alpha) = G_\alpha$ and $\Psi(G'_\alpha) = G'_\alpha$, for all $\Psi \in \alpha\mathbb{Z}_p[V]$, each such Ψ also acts

on $G_\alpha/G'_\alpha \cong G(H(H(K)_\alpha)/H(K)_\alpha)$ via reduction. The problem now is that $A(H(K)_\alpha)_\alpha$ is not necessarily invariant by the action of $G(H(K)_\alpha)$, in other words, G_α does not need to be characteristic in $G(H^{(2)}(K)/K)$. This has the consequence that $H(K)_{\alpha,\alpha} = H(H(K)_\alpha)^{G(H(H(K)_\alpha)/H(K)_\alpha)^{1-\alpha}}$ is not Galois over K in general, which leads to the same complications as in Section 5.3. If, however, G_α is characteristic in $G(H^{(2)}(K)/K)$, then $H(K)_{\alpha,\alpha}/K$ is Galois and the component wise Suzuki holds on the given α-component.

We conclude this section with a remarkable theorem due to Bryant and Kovacs. Let G be a finite p-group as before. Then $V := G/\Phi(G)$ is an n-dimensional $\mathbb{F}_p$-vector-space for some $n \in \mathbb{N}$. Hence, the group of automorphisms of G induces a subgroup $\mathcal{H}$ of $GL(n,p)$ on V. The following theorem asserts that any subgroup $\mathcal{H}$ of $GL(n,p)$ can arise in this way:

Theorem 5.9.5. *(Bryant and Kovacs). Let V be an n-dimensional $\mathbb{F}_p$-vector-space, and $\mathcal{H}$ be a subgroup of the group of non-singular linear transformations of V. Then there exists a finite p-group G such that $G/\Phi(G) \cong V$ and the group of automorphisms of $G/\Phi(G)$ induced by all the automorphisms of G corresponds to $\mathcal{H}$.*

Proof. See Theorem 13.5, page 403, of [38]. □

This is a strong result and it underlines the importance of analyzing the automorphism group of $G(H^{(2)}(K)/K)$ with respect to the capitulation problem. Combining the above result with Ozaki's theorem, Theorem 5.9.5 can be translated as follows: Let V be an n-dimensional $\mathbb{F}_p$-vector-space, and $\mathcal{H}$ be a subgroup of the group of non-singular linear transformations of V. Then there exists a number field K with $G = G(H^{(2)}(K)/K)$ such that $G/\Phi(G) \cong V$ and the group of automorphisms of $G/\Phi(G)$ induced by all the automorphisms of G corresponds to $\mathcal{H}$. For instance, this can be used to construct all possible different types of capitulation.

Chapter 6

Capitulation in Extensions of Imaginary Quadratic Fields

In the following chapter, we investigate capitulation in the case that the base field K is imaginary quadratic and L/K is an unramified cyclic extension of degree p. In Section 6.1, we analyze the structure of $ker N_{L/K}$, where $N_{L/K} : A(L) \to A(K)$ is the norm of ideal classes. In particular, we show that the rank of $ker N_{L/K}$ is non-trivial and even.
In Section 6.2, we yield a heuristic on the structure of $ker N_{L/K}$. To this end, we generalize a paper due to Wittmann, who has given a heuristic for the case of a cyclic p-extension of the rationals. Bearing in mind that the rank of $ker N_{L/K}$ is even, we essentially modify some ideas of the celebrated Cohen-Lenstra heuristics for the case of an imaginary quadratic base field. Subsequently, we compare our developed heuristics with the given numerical data, seeing that the heuristics are in good accordance with them.
Supported by MAGMA, Section 6.3 yields a database for capitulation in extensions of imaginary quadratic fields of degree 5 and 7. So far, numerical data only existed for the case of extensions of degree 2 and 3. Evaluating the numerical data, we are particularly interested in questions of the following type: For instance, let K be an imaginary quadratic field with ideal class group $A(K) \cong C_p \times C_p$. Then there exist $p+1$ intermediate fields of $H(K)/K$ of degree p over K. How are the various capitulation kernels $P_K(L_i)$, $1 \leq i \leq p+1$, correlated? Do the capitulation kernels tend to be pairwise distinct or are there any other patterns? Whereas there seem to be no regular patterns in the case of extensions of degree 3, the database of Section 6.3 reveals a surprising phenomenon in the case of extensions of degree 5 and 7. In the numerical data, only the following two extreme scenarios occurred: Either all capitulation kernels $P_K(L_i)$, $1 \leq i \leq p+1$, are pairwise distinct, or there exists a non-trivial ideal class a in K that capitulates in at least p fields

of the given intermediate fields L_1,...,L_{p+1}. In the first case, we say K has 1-1-capitulation and in the latter case we speak of p-capitulation.
In Section 6.4, we prove the main theorem of this chapter which shows that under certain assumptions we always have 1-1-capitulation or p-capitulation provided that $p > 3$. In particular, we show what goes wrong when $p \leq 3$. Appealing to the results of Section 6.1 and the heuristics of Section 6.2, we observe that the assumptions we made are satisfied with high likelihood. The proof of the theorem is divided into several propositions and lemmata. It makes frequent use of the transfer of groups and group theory. Altogether, the proof extends to around 10 pages.

6.1 Structure of Class Groups of Extensions of Imaginary Quadratic Fields

Henceforth, let K be an imaginary quadratic field and L/K be an unramified cyclic extension of odd prime degree p. Let $G = Gal(H(L)/K)$ and $g_1 \in G$ such that the restriction of g_1 to L, denoted by $\bar{g}_1$, generates $G(L/K)$. For the ease of notation, we will subsequently simply write g_1 instead of $\bar{g}_1$, as it is usually clear from the context if we mean g_1 or its restriction to L. Moreover, we set $s = g_1 - 1$. Recall the following definition which we introduced in Section 2.7. We have

Definition: Let a be an ideal class in L. Then we define

$$r(a) = max\{n \in \mathbb{N} : \ a^{s^n} \neq 1\}.$$

We call $r(a)$ the *length of the flag of* a.

This leads us to the following remarkable

Theorem 6.1.1. *Notations being like above, let* $< a_1, ..., a_l >$ *be a* $\mathbb{Z}[s]$*-basis of* $A(L)$ *in standard form, i.e.* $(a_i^{s\mathbb{Z}[s]})_{1 \leq i \leq l}$ *is a* $\mathbb{Z}[s]$*-basis of* $A(L)^s$*. (See Section 2.8). Then* $r(a_i)$ *is even,* $\forall\ 1 \leq i \leq l$*.*

Proof. Let $\varphi = \varphi_L$ be the Artin symbol of L, $a = a_1$, and $\varphi(a) = g_2 \in G(H(L)/L)$. Also, let $G(K/\mathbb{Q}) =< \tau >$. As τ acts on $G(H(K)/K)$ by taking the inverse, it follows that $L/\mathbb{Q}$ is Galois and hence $H(L)/\mathbb{Q}$ Galois. Let $\tilde{\tau} \in Gal(H(L)/\mathbb{Q})$ be a lift of τ. (That exists due to the theorem of Schur-Zassenhaus). Then $\tilde{\tau}$ gives rise to an automorphism on $G = Gal(H(L)/K)$, which we denote by Ψ. Observe that $\forall\ g \in G$: $\Psi(g\ mod\ G') = g^{-1}\ mod\ G'$, where $G' = [G, G]$. By assumption we know that $g_1, g_2 \notin G'$ and thus

$\Psi(g_i) = g_i^{-1}h_i$, for some $h_i \in G'$, $i = 1, 2$. We will first show, for all $k \in \mathbb{N}$, that

$$(g_2^{-1})^{(g_1^{-1}-1)^k} = (g_2^{(g_1-1)^k})^{(p-1)^{k+1}+(g_1-1)x_k},$$

where $x_k \in \mathbb{Z}[s]$. We prove this statement by induction on k:
$k = 1$: Using Taylor-expansion, we have that

$$\begin{aligned}
(g_2^{-1})^{g_1^{-1}-1} &= (g_2^{-1})^{g_1^{p-1}-1} \\
&= ((g_2^{-1})^{g_1-1})^{1+g_1+g_1^2+\ldots+g_1^{p-2}} \\
&= ((g_2^{-1})^{g_1-1})^{p-1+x_1's} \quad (x_1' \in \mathbb{Z}[s]) \\
&= (g_1^{g_2^{-1}-1})^{-(p-1+x_1's)} \\
&= ((g_1^{g_2-1})^{p-1})^{-(p-1+x_1''s)} \quad (x_1'' \in \mathbb{Z}[s]) \\
&= (g_2^{g_1-1})^{(p-1)^2+x_1s} \quad (x_1 \in \mathbb{Z}[s]).
\end{aligned}$$

Let us now assume the induction hypothesis for $k-1$. It then follows

$$\begin{aligned}
(g_2^{-1})^{(g_1^{-1}-1)^k} &= ((g_2^{-1})^{(g_1^{-1}-1)^{k-1}})^{g_1^{-1}-1} \\
&= ((g_2^{s^{k-1}})^{(p-1)^k+sx_{k-1}})^{g_1^{-1}-1} \\
&= ((g_2^{s^{k-1}})^{(p-1)^k+sx_{k-1}})^{s(p-1+x_k's)} \\
&= (g_2^{s^k})^{(p-1)^{k+1}+sx_k} \quad (x_k \in \mathbb{Z}[s]).
\end{aligned}$$

This proves the above statement. As $\{a_1, ..., a_l\}$ is a $\mathbb{Z}[s]$-basis of $A(L)$ in standard form, we may write

$$h_2 = g_2^{sy}g^{sz} \tag{6.1}$$

such that $y, z \in \mathbb{Z}[s]$, $g \in G(H(L)/L)$, and $< g_2^{sy} >_{\mathbb{Z}[s]} \cap < g^{sz} >_{\mathbb{Z}[s]} = \{1\}$. It thus follows that

$$\begin{aligned}
\Psi(g_2^{(g_1-1)^k}) &= \Psi(g_2)^{(\Psi(g_1)-1)^k} \\
&= (g_2^{-1}h_2)^{(g_1^{-1}h_1-1)^k} \\
&= (g_2^{-1})^{(g_1^{-1}h_1-1)^k}h_2^{(g_1^{-1}h_1-1)^k} \\
&= (g_2^{-1})^{(g_1^{-1}-1)^k}h_2^{(g_1^{-1}-1)^k} \\
&= (g_2^{s^k})^{(p-1)^{k+1}+sx_k}h_2^{(g_1^{-1}-1)^k}. \\
&= (g_2^{s^k})^{(p-1)^{k+1}+sx_k}((g_2^{sy}g^{sz})^{s^k})^{p-1+sw}, \ w \in \mathbb{Z}[s] \\
&= (g_2^{s^k})^{(p-1)^{k+1}+sx_k''}(g^{s^{k+1}z})^{p-1+sw}, \ x_k'' \in \mathbb{Z}[s].
\end{aligned}$$

Let $r = r(a)$, which implies that $a^{s^r} \in \imath_{L/K}(A(K))$ due to $\mathcal{H}^0(Gal(L/K), \mathcal{O}_L^*)$ being trivial. Hence, we obviously obtain that $\Psi(g_2^{s^r}) = g_2^{-s^r}$. It follows that

$$(g_2^{s^r})^{(p-1)^{r+1}}(g^{s^{k+1}z})^{p-1+sw} = g_2^{-s^r}.$$

Due to (6.1), we can then derive that

$$(g_2^{s^r})^{(p-1)^{r+1}} = g_2^{-s^r}.$$

Finally, observe that $(g_2^{s^r})^p = 1$, which yields that

$$(g_2^{s^r})^{(-1)^{r+1}} = g_2^{-s^r}.$$

This equation obviously holds if and only if r is even. This proves the theorem. □

Corollary 6.1.2. *Let $< a_1, ..., a_l >$ be a $\mathbb{Z}[s]$-basis of $A(L)$ in standard form as above and assume that $r(a_i) \leq r(a_j)$, $\forall\ i < j$. If $rk(N_{L/K}(A(L))) = rk(A(K)) - 1$, then $r(a_i) \geq 2$, $\forall\ 1 \leq i \leq l$. If $rk(N_{L/K}(A(L))) = rk(A(K))$, then $rk(a_1) = 0$ and $rk(a_i) \geq 2$, $\forall\ 1 < i \leq l$. In particular, $rk(A(L)^s)$ is even.*

Proof. As K is imaginary quadratic, it follows that $\mathcal{H}^0(Gal(L/K), \mathcal{O}_L^*) = \{1\}$ and $|P_K(L)| = p$. This implies that $rk(\imath_{L/K}(S_1(A(K)))) = rk(S_1(A(K))) - 1$ and thus $rk(A(L)^s \cap A(L)^{G(L/K)}) = rk(A(K)) - 1$. The further arguments are straightforward. □

Remark: More generally, one can show that the Galois group of $H(L)/K$ is a so-called Schur σ-group. For further details, we refer to [44]. The results developed above also hold for such Schur σ-groups.

6.2 Heuristics on Class Groups of Unramified Cyclic Extensions of Imaginary Quadratic Fields

There is quite a lot of literature on cyclic extensions of prime degree. In [43], Gras studies arbitrary cyclic extensions of prime degree in greatest generality. This, however, has the disadvantage that one can hardly extract any explicit information on unramified cyclic extensions of imaginary quadratic fields. Specifically, cyclic extensions of $\mathbb{Q}$ of prime degree are first discussed by Gerth in the 1970s, see [45]. In 2005, his results are then taken up by Wittmann, who gives a heuristic on the class groups of cyclic extensions of $\mathbb{Q}$ of prime degree. The heuristic can be found in [42] and leans on the famous Cohen-Lenstra heuristics, see [47]. As extensions of $\mathbb{Q}$ are ramified, we

cannot simply generalize Wittmann's heuristics to unramified cyclic extensions of imaginary quadratic fields. In the following, we will show how to generalize his ideas for the above case, though. Related questions have also been discussed by Bush, Boston, and Hajir in greater generality, see [46]. In the specific situation as above, however, our following approach seems to be more straight forward and more applicable.

Henceforth, let K be an imaginary quadratic field and L/K be an unramified cyclic extension of odd prime degree p with Galois group $G = Gal(L/K)$. Let $\sigma \in G$ be a generator of G and set $s = \sigma - 1$. In what follows, we intend to deduce heuristics on the structure of $ker N_{L/K}$, i.e. we do not consider the whole ideal class group of L but only the kernel of the norm $N_{L/K}$. As we have learned in the previous section, $rk(ker N_{L/K})$ is even. It is also worth mentioning that the structure of $ker N_{L/K}$ is uniquely determined by the length of the various flags of a given $\mathbb{Z}[s]$-basis of $A(L)^s$. This follows immediately from Furtwängler's Theorem and the fact that for all ideal classes $b \in A(L)$: $b^{s^p} = b^{psu}$ for some unit $u \in \mathbb{Z}[s]$. As we have already announced, we plan to generalize a paper due to C. Wittmann. He has given a substantiated heuristic for the case that $M/\mathbb{Q}$ is a cyclic extension of odd prime degree. Let us say $Gal(M/\mathbb{Q}) =< \sigma_M >$ and $s_M = \sigma_M - 1$. In order to answer the question of a heuristic adequately, we must fix $t = rk(A(K))$. One then easily verifies that $rk(A(L)^s/A(L)^{s^2}) = t - 1$. Observe that this is very analogous to Wittmann's paper: He defines t to be the number of ramified primes in $M/\mathbb{Q}$. And Chevalley's Theorem then yields that $rk(A(M)/A(M)^{s_M}) = t - 1$. Also observe that $ker N_{M/\mathbb{Q}} = A(M)$, which yields another analogy to our case as we also only investigate the structure of the kernel of $N_{L/K}$. Having fixed $t = rk(A(K))$, it remains open which ratio we exactly want to predict. We want to make this precise now. We define the following sets:

$$\mathcal{K}_D = \{\text{imaginary quadratic fields of abs. discriminant not exceeding } D\},$$

$$\mathcal{K}_{D,t} = \{K \in \mathcal{K}_{\mathcal{D}} : \ rk(A(K)) = t\},$$

$$\mathcal{L}_{D,t} = \{L \text{ field} \mid \exists\ K \in \mathcal{K}_{D,t} : \ L/K \text{ unramified cyclic of degree } p\}.$$

Note: If $L \in \mathcal{L}_{D,t}$, then $L/\mathbb{Q}$ is Galois and there exists exactly one field $K \in \mathcal{K}_{D,t}$ with L/K unramified cyclic of degree p.

Let M be a finite $\mathbb{Z}[s]$-module and $M_0 := sM$ be a submodule of M such that

$$M_0 = \oplus_{i=1}^{t-1} s\mathbb{Z}[s] \cdot m_i$$

with $m_i \in M$ and $r_i := r(m_i) = max\{n \in \mathbb{N} : s^n m_i \neq 0\} < \infty$. As we have already argued, M_0 is uniquely determined by $r_1, ..., r_{t-1}$ and we write $M_0 = M_0(r_1, ..., r_{t-1})$. We may now apply this notation in the case that $A(L)^s = \prod_{i=1}^{t-1} b_i^{s\mathbb{Z}[s]}$, where $\prod$ is a direct product, $b_i \in A(L)$, and $r_i = r(b_i)$. (Observe that we write $A(L)$ multiplicatively and not additively). We also mention that such a decomposition of $A(L)^s$ is always possible by Section 2.8. We can now write $A(L)^s \cong_{\mathbb{Z}[s]} M_0(r_1, ..., r_{t-1})$. By the previous section, we obtain that $r_i = 2k_i$, for some $k_i \in \mathbb{Z}_{>0}$ $(1 \leq i \leq t-1)$. We may thus define

$$\sqrt{M_0(2k_1, ..., 2k_{t-1})} := M_0(k_1, ..., k_{t-1}).$$

With the notations from above, we set

$$\begin{aligned} \mathcal{L}_{D,t,(2k_1,...,2k_{t-1})} &= \{L \in \mathcal{L}_{D,t} |\ \exists\ K \in \mathcal{K}_{D,t} :\ L/K \text{ cyclic unram.}, \\ &\quad [L:K] = p,\ ker N_{L/K} \cong_{\mathbb{Z}[s]} M_0(2k_1, ..., 2k_{t-1})\}. \end{aligned}$$

We set: $Freq_t(2k_1, ..., 2k_{t-1}) := lim_{D\to\infty} \frac{|\mathcal{L}_{D,t,(2k_1,...,2k_{t-1})}|}{|\mathcal{L}_{D,t}|}$, conjecturing that this limes does exist.

We now set $q = 1/p$, $(q_m) = \prod_{i=1}^{m}(1 - q^i)$, and

$$C_t = \frac{(q)_{t-1} \cdot (q)_t}{q^{t(t-1)} \cdot (q)_1}.$$

Conjecture: Notations being like above, we have that

$$Freq_t(2k_1, ..., 2k_{t-1}) = C_t \cdot \frac{1}{|Aut_{\mathbb{Z}[s]}(M_0(k_1, ..., k_{t-1}))|} \cdot \frac{1}{|M_0(k_1, ..., k_{t-1})|}.$$

Remark: 1) By Theorem 2.2, page 988, of [42], the map $Freq_t$ yields indeed a probability measure. The factor C_t is used to norm the measure.

2) $|Aut_{\mathbb{Z}[s]}(M_0(k_1, ..., k_{t-1}))|$ can be computed by Lemma 2.1 of [42] and Theorem 2.11 of [49].

3) In the above heuristic only $t = rk(A(K))$ matters but not the exponent of $A(K)$. This makes sense as we are only interested in the kernel of $N_{L/K}$ and not in the whole class group of L. As we will see, this point of view is supported by the numerical data.

In the remainder of this section, we want to see how good the accordance of the heuristic with the given numerical data is. To this end, we consider the numerical data for $t = 2, 3$ and $p = 3$. Any other situations, for instance for $p > 3$, are computationally beyond the scope. The computations were done by MAGMA, using the various Gauss servers in the University of Goettingen. Particular thanks goes to Michael Jacobson, who sent us a table of imaginary quadratic number fields with non-cyclic p-class groups for $p = 3, 5, 7$. In this context, we also refer to his joined paper on class groups of imaginary quadratic fields, see [48].

First let $t = 2$: Then $C_2 = p^2(1 - 1/p)(1 - 1/p^2)$, $|Aut_{\mathbb{Z}[s]}(M_0(k))| = p^{k-1}(p-1)$, and $|M_0(k)| = p^k$, where $k \in \mathbb{Z}_{>0}$. Altogether, we obtain that

$$Freq_2(2k) = \frac{p^2 - 1}{p^{2k}}.$$

In order to support Remark 3, we will consider the case $A(K) \cong C_3 \times C_3$ and $A(K) \cong C_3 \times C_9$ separately. We begin with $t = 2$, $p = 3$, $A(K) \cong C_3 \times C_3$. We set:

$$\mathcal{L}_{D,C_3\times C_3} = \{L \in \mathcal{L}_{D,2} \quad | \quad \exists\ K \in \mathcal{K}_D :\ A(K) \cong C_3 \times C_3, \\ L/K \text{ unramified cyclic of degree } p\}.$$

($\mathcal{L}_{D,C_3\times C_9}$ is defined accordingly). We then have:

Number of fields considered: $|\mathcal{L}_{D,C_3\times C_3}| = 8080$, where $|D| < 10^6$.

$\mathcal{L}_{D,C_3\times C_3,2k}$	$ratio = \frac{\lvert\mathcal{L}_{D,C_3\times C_3,2k}\rvert}{\lvert\mathcal{L}_{D,C_3\times C_3}\rvert}$	$pred.\ ratio = Freq_2(2k)$
$k = 1$	0.8979	0.8889
$k = 2$	0.0950	0.0988
$k = 3$	0.0071	0.0110

The numerical data were taken from the following website:

$$http://www.algebra.at/SciRes2010TrfType.htm$$

We need to add the following

Remark: The data given at that website yield exactly the information we need. It is just stated there in a different context. In what follows, we shortly explain how we can extract the desired information from that website. There

it says: For each of the 2020 complex quadratic fields K with discriminant D, we have four simply real cubic fields L_1,...,L_4 with fundamental discriminant D. Question: Let K be a complex quadratic field with discriminant D, L/K be unramified cyclic of degree 3, $G(L/K) =< \sigma >$, $s = \sigma - 1$, and L_1 be the simply real cubic subfield of L. How are $A(L_1)$ and $A(L)$ related? By Gerth, see [45], we know that $A(L_1)$ is cyclic. Moreover, we have:
Claim: $exp(kerN_{L/K}) = ord(A(L_1))$.
Proof: Let $b \in A(L)$ with $N_{L/K}(b) \cong C_3$ and $Gal(L/L_1) =< \tau >$. As K is imaginary quadratic, we obtain that $A(L)^{G(L/K)} =< \imath_{L/K}(a) >$, for some $a \in A(K)$. As the restriction of τ to K acts as inversion on $A(K)$, it follows that $\imath_{L/K}(a)^{\tau} = \imath_{L/K}(a)^{-1}$. Also observe that $N_{L/L_1}(A(L)) = A(L_1)$ as $2 = [L : L_1]$ is coprime to 3. We now differentiate:
Case 1. $ord(b) = 3$. By Theorem 6.1.1, it follows that $A(L) \cong C_3 \times C_3 \times C_3$. By Gerth, we have that $ord(A(L_1)) = 3$.
Case 2. $ord(b) = 3^k$ for some $k > 1$. By Theorem 6.1.1 , we can deduce that $A(L) =< b, b^s > \cong C_{3^k} \times C_{3^{k-1}}$.
Let $\alpha = \frac{1+\tau}{2}$. Then clearly, $A(L) = A(L)_{\alpha} \times A(L)_{1-\alpha}$. By the above arguments, $A(L)_{\alpha}$ contains $< \imath_{L/K}(a) >$. As $A(L)_{\alpha}$ can be extended to a basis of $A(L)$, one easily verifies that $ord(A(L)_{\alpha}) = 3^k$. As $A(L)_{\alpha} = kerN_{L/L_1}$, the claim follows. On account of that result, we can easily determine the structure of $kerN_{L/K}$ by considering $ord(A(L_1))$.

Let us now consider the case, where $t = 2$, $p = 3$, $A(K) \cong C_3 \times C_9$:

Number of fields considered: $|\mathcal{L}_{D,C_3 \times C_9}| = 2404$, where $|D| < 10^6$.

$\mathcal{L}_{D,C_3 \times C_9,2k}$	$ratio = \frac{\lvert\mathcal{L}_{D,C_3 \times C_9,2k}\rvert}{\lvert\mathcal{L}_{D,C_3 \times C_9}\rvert}$	$pred.\ ratio = Freq_2(2k)$
$k = 1$	0.9053	0.8889
$k = 2$	0.0902	0.0988

We learn that the numerical data are in good accordance with the developed heuristic. Moreover, there is little difference between the ratios in the cases where $A(K) \cong C_3 \times C_3$ and $A(K) \cong C_3 \times C_9$, which supports Remark 3. Last but not least, let us consider the case where $t = 3$. Due to the scarcity of numerical data, we will not differentiate between the various structures of $A(K)$, but we will consider all imaginary quadratic fields of rank 3.

Number of fields considered: $|\mathcal{L}_{D,3}| = 1062$, where $|D| < 10^7$.

$\mathcal{L}_{D,3,(2k_1,2k_2)}$	$ratio = \frac{\lvert\mathcal{L}_{D,3,(2k_1,2k_2)}\rvert}{\lvert\mathcal{L}_{D,3}\rvert}$	$pred.\ ratio = Freq_2(2k_1, 2k_2)$

$(2k_1, 2k_2) = (2, 2)$	0.8633	0.8559
$(2k_1, 2k_2) = (2, 4)$	0.1158	0.1268
$(2k_1, 2k_2) = (2, 6)$	0.0209	0.0141

We see that the heuristic and the numerical data are in good accordance.

6.3 Database for Capitulation in Degree 5-and-7-Extensions

In the existing literature, the capitulation kernel has essentially only been computed for unramified cyclic extensions of degree 2 and 3, where the base field is quadratic. This is due to the enormous complexity of computing the capitulation kernel. One basic problem is that one has to compute ideal class groups, which becomes increasingly difficult when the considered number field is of higher degree over the rationals. In [25], Heider and Schmithals have started to analyze the capitulation types for the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-12451})$ with ideal class group $A(K) \cong C_5 \times C_5$. It follows that K has 6 unramified cyclic extensions of degree 5. For 2 of these 6 intermediate fields, let us say L_1 and L_2, Heider and Schmithals have been able to compute the capitulation kernels $P_K(L_i)$, $i = 1, 2$. For the other 4 fields, they could not determine the capitulation kernel. By extensive use of MAGMA and the Gauss-servers at the University of Goettingen, we have been able to find the capitulation kernels for these 4 fields. Moreover, we computed the capitulation kernels for all 6 unramified cyclic 5-extensions for more than 50 other imaginary quadratic fields. We used the lists of [33], [34], and [48] to find imaginary quadratic fields having a 5-primary part isomorphic to $C_5 \times C_5$ or $C_5 \times C_{25}$. All following computations have been performed by MAGMA, see [35]. The results can be verified on MAGMA. Observe that MAGMA always uses the same basis of ideal classes for a given class group $A(K)$, i.e. one can repeat the computations and one obtains exactly the same results. (MAGMA denotes the ideal classes by g_1, g_2, and so on. We have denoted them by a_1, a_2, and so on).

In the following table, we list imaginary quadratic number fields with absolute discriminant not exceeding 10^6, whose 5-class group is isomorphic to $C_5 \times C_5$. For the ease of notation, we make the following arrangements: Let K be an imaginary quadratic field with $A(K) =< a_1, a_2 > \cong C_5 \times C_5$, for some ideal classes $a_1, a_2 \in A(K)$. Then there exist 6 subgroups of $A(K)$ of order 5 and accordingly 6 unramified cyclic extensions of K of degree 5. Let $C_1 =< a_2 >$,

$C_2 =< a_1a_2 >$, $C_3 =< a_1^2a_2 >$, $C_4 =< a_1^3a_2 >$, $C_5 =< a_1^4a_2 >$, $C_6 =< a_1 >$. And accordingly, $L_i = H(K)^{\varphi(C_i)}$, $\forall\ 1 \leq i \leq 6$. We aggregate the various capitulation kernels in the form of 6-tuples, i.e. $(P_K(L_1), ..., P_K(L_6))$. Instead of writing $P_K(L_j) = C_i$, for some $1 \leq i, j \leq p+1$, we will suppress the C and simply write i instead of C_i. For example: $(1, 2, 3, 4, 5, 6)$ means that $P_K(L_j) = C_j$, $\forall\ 1 \leq j \leq p+1$. Accordingly, $(3, 6, 4, 1, 5, 2)$ means that C_3 capitulates in L_1, C_6 capitulates in L_2, an so on.

Remark: 1) We are only interested in the relation of the various capitulation kernels, i.e. in the question whether they are pairwise distinct or all equal for example. Hence, it does not matter if one chooses a different notation for the intermediate fields.

2) Olga Taussky coined the following expression: She says L_j/K is of capitulation type (A) if $P_K(L_j) = C_j$ and of type (B) otherwise. The question whether L_j/K is of type (A) or (B) can also be properly addressed despite the arbitrary notation of the intermediate fields.

Nr.	Discriminant	$(P_K(L_1), ..., P_K(L_6))$
1	-12451	(3,6,4,1,5,2)
2	-17944	(2,1,5,4,6,3)
3	-30263	(6,5,3,4,2,1)
4	-33531	(3,2,4,6,1,5)
5	-37363	(1,2,3,4,6,5)
6	-38047	(3,1,6,4,2,5)
7	-39947	(5,1,4,6,2,3)
8	-42871	(2,1,6,5,4,3)
9	-53079	(2,6,4,1,5,3)
10	-54211	(2,6,3,4,1,5)
11	-58424	(3,2,1,5,4,6)
12	-61556	(6,5,4,1,3,2)
13	-62632	(2,6,6,6,6,6)
14	-63411	(5,2,6,4,1,3)
15	-64103	(1,3,6,5,2,4)
16	-65784	(3,6,4,5,2,1)
17	-66328	(6,2,4,3,5,1)
18	-67031	(4,4,4,1,4,4)
19	-67063	(1,1,1,6,1,1)
20	-67128	(3,2,4,6,1,5)
21	-69811	(3,1,4,2,5,6)

22	-72084	(3,1,5,6,4,2)
23	-74051	(2,1,3,6,5,4)
24	-75688	(5,6,5,5,5,5)
25	-81287	(4,1,3,5,2,6)
26	-83767	(5,4,3,2,1,6)
27	-84271	(5,4,2,1,6,3)
28	-85099	(6,2,1,4,3,5)
29	-85279	(3,1,4,2,5,6)
30	-87971	(2,3,6,4,5,6)
31	-89751	(1,3,5,2,4,6)
32	-90795	(5,5,5,5,5,5)
33	-90868	(1,3,1,1,1,1)
34	-92263	(3,1,4,2,5,6)
35	-98591	(5,1,3,4,6,2)
36	-99031	(4,1,1,1,1,1)
37	-99743	(2,6,4,1,5,3)
38	-104503	(3,5,1,6,2,4)
39	-105151	(5,3,1,4,2,6)
40	-112643	(1,4,6,2,5,3)
41	-113140	(2,3,4,5,1,6)
42	-114395	(2,3,1,6,4,5)
43	-115912	(5,2,6,4,1,3)
44	-116187	(2,1,3,6,5,4)
45	-119191	(3,6,4,5,2,1)
46	-119915	(1,4,4,4,4,4)
47	-120463	(6,3,5,4,1,2)
48	-127103	(6,4,2,3,1,5)
49	-128680	(6,6,6,4,6,6)
50	-132520	(4,2,6,5,3,1)
51	-134312	(6,5,3,4,2,1)
52	-135167	(5,3,2,6,1,4)
53	-135176	(6,4,2,3,1,5)
54	-140696	(6,2,5,1,4,3)
55	-143508	(3,6,2,5,1,4)
56	-146184	(1,5,6,4,3,2)

The above table shows that in the given numerical data there is a rigorous relationship between the various capitulation kernels. We say an imaginary quadratic field K with $rk(A(K)) = 2$ has *1-1-capitulation* if

$P_K(L_j) \neq P_K(L_i)$, $\forall\ 1 \leq i \neq j \leq p+1$. In this case, we have a 1-1-correspondence between the subgroups of $C_1, ..., C_6$ and the intermediate fields $L_1, ..., L_6$. We say such a field K as above has *p-capitulation* if there exists a subgroup C_i $(1 \leq i \leq p+1)$ such that $P_K(L_j) = C_i$, for all but at most one $j \in \{1, ..., p+1\}$. In the above table, all imaginary fields either have 1-1-capitulation or p-capitulation. More precisely, 47 out of 56 fields have 1-1-capitulation and 9 fields have p capitulation. In the subsequent section, we give substantiated reasons for the phenomena observed above. Before doing so, we add some examples of imaginary quadratic fields K with $rk(A(K)) = 2$ and $exp(A(K)) > 5$. The observed phenomenon stays the same. Indeed, in all following computed examples, the given imaginary quadratic field either has 1-1-capitulation or p-capitulation. With a slight abuse of notation, we subsequently identify $A(K)$ with $Gal(H(K)/K)$.

Example 1: $K = \mathbb{Q}(\sqrt{-50783})$ is an imaginary quadratic number field with $A(K)_5 =< a_1, a_2 > \cong C_5 \times C_{25}$. Then:
For $L_1 = H(K)^{<a_2>}$: $P_K(L_1) =< a_1^2 a_2^5 >$;
For $L_2 = H(K)^{<a_1 a_2>}$: $P_K(L_2) =< a_1 a_2^5 >$;
For $L_3 = H(K)^{<a_1^2 a_2>}$: $P_K(L_3) =< a_1 >$;
For $L_4 = H(K)^{<a_1^3 a_2>}$: $P_K(L_4) =< a_2^5 >$;
For $L_5 = H(K)^{<a_1^4 a_2>}$: $P_K(L_5) =< a_1^4 a_2^5 >$;
For $L_6 = H(K)^{<a_1, a_2^5>}$: $P_K(L_6) =< a_1^3 a_2^5 >$;

In this example, L_4/K and L_6/K are of type (A). The other extensions are of type (B). Moreover, K has 1-1-capitulation.

Example 2: $K = \mathbb{Q}(\sqrt{-178004})$ is an imaginary quadratic number field with $A(K)_5 =< a_1, a_2 > \cong C_5 \times C_{25}$. Then:
For $L_1 = H(K)^{<a_2>}$: $P_K(L_1) =< a_1 a_2^{20} >$;
For $L_2 = H(K)^{<a_1 a_2>}$: $P_K(L_2) =< a_1 >$;
For $L_3 = H(K)^{<a_1^2 a_2>}$: $P_K(L_3) =< a_2^5 >$;
For $L_4 = H(K)^{<a_1^3 a_2>}$: $P_K(L_4) =< a_1 a_2^5 >$;
For $L_5 = H(K)^{<a_1^4 a_2>}$: $P_K(L_5) =< a_1 a_2^{10} >$;
For $L_6 = H(K)^{<a_1, a_2^5>}$: $P_K(L_6) =< a_1 a_2^{15} >$;

In this example, L_3/K and L_6/K are of type (A). The other extensions are of type (B). Moreover, K has 1-1-capitulation.

Example 3: $K = \mathbb{Q}(\sqrt{-258563})$ is an imaginary quadratic number field with $A(K)_5 =< a_1, a_2 > \cong C_5 \times C_{25}$. Then:
For $L_1 = H(K)^{<a_2>}$: $P_K(L_1) =< a_2^5 >$;
For $L_2 = H(K)^{<a_1 a_2>}$: $P_K(L_2) =< a_1 a_2^5 >$;

For $L_3 = H(K)^{<a_1^2 a_2>}$: $P_K(L_3) =< a_1^4 a_2^5 >$;
For $L_4 = H(K)^{<a_1^3 a_2>}$: $P_K(L_4) =< a_1 >$;
For $L_5 = H(K)^{<a_1^4 a_2>}$: $P_K(L_5) =< a_1^2 a_2^5 >$;
For $L_6 = H(K)^{<a_1, a_2^5>}$: $P_K(L_6) =< a_1^3 a_2^5 >$;

In this example, L_1/K and L_6/K are of type (A). The other extensions are of type (B). Moreover, K has 1-1-capitulation.

Example 4: $K = \mathbb{Q}(\sqrt{-309263})$ is an imaginary quadratic number field with $A(K)_5 =< a_1, a_2 > \cong C_5 \times C_{25}$. Then:
For $L_1 = H(K)^{<a_2>}$: $P_K(L_1) =< a_1 a_2^{10} >$;
For $L_2 = H(K)^{<a_1 a_2>}$: $P_K(L_2) =< a_1 a_2^{15} >$;
For $L_3 = H(K)^{<a_1^2 a_2>}$: $P_K(L_3) =< a_1 a_2^5 >$;
For $L_4 = H(K)^{<a_1^3 a_2>}$: $P_K(L_4) =< a_2^5 >$;
For $L_5 = H(K)^{<a_1^4 a_2>}$: $P_K(L_5) =< a_1 a_2^{20} >$;
For $L_6 = H(K)^{<a_1, a_2^5>}$: $P_K(L_6) =< a_1 >$;

In this example, L_4/K and L_6/K are of type (A). The other extensions are of type (B). Moreover, K has 1-1-capitulation.

Example 5: $K = \mathbb{Q}(\sqrt{-1287491})$ is an imaginary quadratic number field with $A(K)_5 =< a_1, a_2 > \cong C_5 \times C_{125}$. Then:
For $L_1 = H(K)^{<a_2>}$: $P_K(L_1) =< a_1 a_2^{25} >$;
For $L_2 = H(K)^{<a_1 a_2>}$: $P_K(L_2) =< a_1^4 a_2^{25} >$;
For $L_3 = H(K)^{<a_1^2 a_2>}$: $P_K(L_3) =< a_1^3 a_2^{25} >$;
For $L_4 = H(K)^{<a_1^3 a_2>}$: $P_K(L_4) =< a_1 >$;
For $L_5 = H(K)^{<a_1^4 a_2>}$: $P_K(L_5) =< a_1^2 a_2^{25} >$;
For $L_6 = H(K)^{<a_1, a_2^5>}$: $P_K(L_6) =< a_2^{25} >$;

In this example, L_6/K is of type (A). The other extensions are of type (B). Besides, K has 1-1-capitulation.

Example 6: $K = \mathbb{Q}(\sqrt{-1390367})$ is an imaginary quadratic number field with $A(K)_5 =< a_1, a_2 > \cong C_{25} \times C_{25}$. Then:
For $L_1 = H(K)^{<a_1^5, a_2>}$: $P_K(L_1) =< a_1^5 a_2^5 >$;
For $L_2 = H(K)^{<a_1^5, a_1 a_2>}$: $P_K(L_2) =< a_1^5 a_2^5 >$;
For $L_3 = H(K)^{<a_1^5, a_1^2 a_2>}$: $P_K(L_3) =< a_1^5 a_2^5 >$;
For $L_4 = H(K)^{<a_1^5, a_1^3 a_2>}$: $P_K(L_4) =< a_1^5 a_2^5 >$;
For $L_5 = H(K)^{<a_1^5, a_1^4 a_2>}$: $P_K(L_5) =< a_1^5 a_2^5 >$;
For $L_6 = H(K)^{<a_1, a_2^5>}$: $P_K(L_6) =< a_1^{15} a_2^5 >$;

In this example, all extensions are of type (A). Moreover, K has p-capitulation.

These examples demonstrate that we still only have 1-1-capitulation or p-capitulation as long as the rank of $A(K)$ is 2, no matter what the exponent is.

So far, we observed that the various capitulation kernels of extensions of degree 5 seem to be much more correlated as this is the case for extensions of degree 3. Due to the massive computational expenses, for $p = 7$ we have only been able to compute the capitulation kernels for two imaginary quadratic fields. We have:

Example 1: Let $K = \mathbb{Q}(\sqrt{-63499})$. Then $A(K)_7 =< a_1, a_2 > \cong C_7 \times C_7$. Furthermore, we have:
For $L_1 = H(K)^{<a_2>}$: $P_K(L_1) =< a_1 a_2 >$;
For $L_2 = H(K)^{<a_1 a_2>}$: $P_K(L_2) =< a_1^4 a_2 >$;
For $L_3 = H(K)^{<a_1^2 a_2>}$: $P_K(L_3) =< a_1^5 a_2 >$;
For $L_4 = H(K)^{<a_1^3 a_2>}$: $P_K(L_4) =< a_1^2 a_2 >$;
For $L_5 = H(K)^{<a_1^4 a_2>}$: $P_K(L_5) =< a_1^3 a_2 >$;
For $L_6 = H(K)^{<a_1^5 a_2>}$: $P_K(L_6) =< a_1^6 a_2 >$;
For $L_7 = H(K)^{<a_1^6 a_2>}$: $P_K(L_7) =< a_1 >$;
For $L_8 = H(K)^{<a_1>}$: $P_K(L_8) =< a_2 >$;

All extensions are of type (B) and K has 1-1- capitulation.

Example 2: Let $K = \mathbb{Q}(\sqrt{-159592})$. Then $A(K)_7 =< a_1, a_2 > \cong C_7 \times C_7$. Furthermore, we have:
For $L_1 = H(K)^{<a_2>}$: $P_K(L_1) =< a_2 >$;
For $L_2 = H(K)^{<a_1 a_2>}$: $P_K(L_2) =< a_1^2 a_2 >$;
For $L_3 = H(K)^{<a_1^2 a_2>}$: $P_K(L_3) =< a_1^2 a_2 >$;
For $L_4 = H(K)^{<a_1^3 a_2>}$: $P_K(L_4) =< a_1^2 a_2 >$;
For $L_5 = H(K)^{<a_1^4 a_2>}$: $P_K(L_5) =< a_1^2 a_2 >$;
For $L_6 = H(K)^{<a_1^5 a_2>}$: $P_K(L_6) =< a_1^2 a_2 >$;
For $L_7 = H(K)^{<a_1^6 a_2>}$: $P_K(L_7) =< a_1^2 a_2 >$;
For $L_8 = H(K)^{<a_1>}$: $P_K(L_8) =< a_1^2 a_2 >$;

The extensions L_1 and L_3 are of type (A), all other extensions are of type (B). Besides, K has p-capitulation.

6.4 Main Theorem on Capitulation in Extensions of Prime Degree

In Section 6.3, we have observed that the capitulation kernels in extensions of degree 5 and 7 of a given imaginary quadratic field are a lot more correlated

than that is the case in extensions of degree 3. (For numerical data in the case of extensions of degree 3, see [36]). In Section 5.9, we have investigated the action of the automorphism group of the Galois group $Gal(H^{(2)}(K)/K)$ on $A(K)$ with regard to the capitulation problem. That analysis gave us a deeper insight into the capitulation problem. On the other hand, we could not explain the numerical data of the previous section just by the developed theory of Section 5.9. Hence, we look for further explanations. In this context, the heuristics of the previous section will play a major role. Another key ingredient will be the theory of the group transfer. Henceforth, let K be an imaginary quadratic field, with $r = rk(A(K)) > 1$, and let L be an unramified cyclic extension of K of prime degree $p > 3$. Then the heuristics of Section 6.2 predict that $rk(kerN_{L/K}) = 2(r-1)$ with high probability. In the following treatise, we will show how this property leads to a remarkable phenomenon concerning capitulation. In the case for $r = 2$, we will prove

Theorem 6.4.1. *Let K be an imaginary quadratic field with $rk(A(K)) = 2$, and $p > 3$ be a prime. Let $L_1, ..., L_{p+1}$ be the intermediate fields of $H(K)/K$ of degree p over K such that $rk(kerN_{L_i/K}) \leq rk(kerN_{L_j/K})$, $\forall\ 1 \leq i < j \leq p+1$. Assume the following two assumptions:*

(A1) $exp(kerN_{L_j/K}) = p$, $\forall\ 1 \leq j \leq p+1$;
(A2) There exists some $1 \leq k \leq p+1$ such that $rk(kerN_{L_k/K}) = 2$.

Then: (i) $P_K(L_i) \neq P_K(L_j)$, $\forall\ 1 \leq i \neq j \leq p+1 \Leftrightarrow\ rk(kerN_{L_u/K}) = 2$, $\forall\ 1 \leq u \leq p+1$.

(ii) $P_K(L_i) = P_K(L_j)$, $\forall\ 1 \leq i \neq j \leq p$, otherwise.

In the first case, we say K has 1-1-capitulation *and in the second case we say K has p-*capitulation*. In a nutshell, assuming (A1) and (A2), K either has 1-1-capitulation or p-capitulation.*

Remark: (a) In light of the developed heuristics and Corollary 6.1.2, the assumptions (A1) and (A2) are satisfied with high likelihood. In fact, in the computed numerical data, we could not find a single example where these assumptions were violated. Moreover, it seems plausible that the probability that both (A1) and (A2) hold should go to 1 as p tends to infinity. One reason for this is that the rank of $kerN_{L_j/K}$ must be at least $p-1$ for (A1) to be violated. (See Theorem 2.6.3). Likewise, $A(L) = Cl(L)_p$ tends to be smaller, when p is increasing, which is in favor of (A2).

(b) In the end of this section, we also give a generalization of the above theorem for the case that $r > 2$. As the result becomes more complicated in

this case, though, we decided to state the theorem for $r = 2$ separately and in the beginning.

(c) The proof of the above theorem will show that it is essential that assumption (A2) implies that L_k/K has semi-stable growth. This is the case if and only if $p > 3$. That is why we have to exclude the case that $p = 3$.

The proof of the above theorem is divided into several lemmas and propositions. When possible, we prove the results in the general case that $r = rk(A(K)) > 1$. Throughout the following proof, we will make extensive use of assumption (A1). In the general case, this means that we assume, for all intermediate fields of $H(K)/K$ of degree p, that $exp(kerN_{L_j/K}) = p$, $\forall\ 1 \leq j \leq s$, where $s = (p^r - 1)/(p - 1)$.
In what follows, let $K \subset L \subset H(K) \subset H(L) \subset F \subset H^{(2)}(K)$ be an extension of number fields with the usual notation, F/K Galois, and $[L : K] = p$. Also, we set $G = Gal(F/K)$. We then have

Lemma 6.4.2. *Notations being like above, let $a \in A(K) \setminus N_{L/K}(A(L))$ and $g \in G$ with $\varphi_K(a) = g\ mod\ G'$, where φ_K denotes the Artin symbol of K. Then*

$$a \in P_K(L) \Leftrightarrow\ g^p \in Gal(F/H(L)).$$

Proof. Let $\bar{g} = g\ mod\ G'$. By Proposition 5.9.3, we know that $\bar{V}_{G\to G(F/L)}(\bar{g}) = 1$ if and only if $\bar{V}_{G(H(L)/K)\to G(H(L)/L)}(\bar{g}) = 1$. By Artin's Theorem, it thus follows that a capitulates in L if and only if $\bar{V}_{G\to G(F/L)}(\bar{g}) = 1$. Since $a \notin N_{L/K}(A(L))$ by assumption, it also follows that $g \notin G(F/L)$. Let $H = G(F/L)$. Then, $G/H = \{1\ mod\ H, g\ mod\ H, ..., g^{p-1}\ mod\ H\}$. By the definition of the transfer, we then obtain that

$$\bar{V}_{G\to H}(\bar{g}) = g^p\ mod\ H'.$$

Thus, $\bar{V}_{G\to H}(\bar{g}) = 1$ if and only if $g^p \in H' = G(F/H(L))$. □

Lemma 6.4.3. *Let $K \subset L \subset H(K) \subset H(L) \subset F \subset H^{(2)}(K)$ be as above and assume that L/K has semi-stable growth. Let $a \in N_{L/K}(A(L))$ and $g \in G = Gal(F/K)$ with $\varphi_K(a) = g\ mod\ G'$. Then*

$$a \in P_K(L) \Leftrightarrow\ g^p \in Gal(F/H(L)).$$

Proof. As $a \in N_{L/K}(A(L))$, it follows that $g \in Gal(F/L)$ and hence $\bar{g} := g\ mod\ G(F/H(L)) \in G(H(L)/L)$. Let $b \in A(L)$ with $\varphi_L(b) = \bar{g}$, where φ_L denotes the Artin symbol of L. It follows that $N_{L/K}(b) = a$. Let

$Gal(L/K) =< \sigma >$, and set $s = \sigma - 1$. Since L/K has semi-stable growth by assumption, it follows that $A(L)^{s^{p-1}} = \{1\}$. We then obtain that

$$\imath_{L/K}(a) = b^{pu+s^{p-1}} = b^{pu},$$

for some unit $u \in \mathbb{Z}[s]^*$. Thus, $a \in P_K(L)$ if and only if $\bar{g}^p = 1$, i.e. $g^p \in G(F/H(L))$. This proves the claim. □

Remark: The proof of the above lemma shows that the assumption that L/K is semi-stable is essential. It simply secures that the equivalence

$$a \in P_K(L) \Leftrightarrow \ g^p \in Gal(F/H(L))$$

holds for all ideal classes $a \in A(K)$ and not only for those classes in $A(K)$ that do not lie in $N_{L/K}(A(L))$.

As before let K be an imaginary quadratic field with ideal class group $A(K) =< a_1, ..., a_r >$, where $r > 1$. Let $L_1, ..., L_s$ denote the subfields of $H(K)/K$ of degree p over K, where $s = (p^r - 1)/(p - 1)$. Let $F = \prod_{i=1}^{s} H(L_i)$ with $G = Gal(F/K)$ and thus $G' = Gal(F/H(K))$. Also we set $G_j = Gal(F/H(L_j))$, $\forall\ 1 \leq j \leq s$. By assumption (A1), we know that $exp(kerN_{L_j/K}) = p$, $\forall\ 1 \leq j \leq s$. This implies that $exp(G') = p$ due to $Gal(H(L_i)/H(K)) \cong kerN_{L_i/K}$ having exponent p and as $G' = \prod_{i=1}^{s} Gal(H(L_i)/H(K))$. (Observe that $G' \neq 1$. Otherwise, we would obtain a contradiction to K being imaginary quadratic). In what follows, let $\{\bar{g}_1, ..., \bar{g}_r\}$ be a minimal generating system of $G(H(K)/K)$ and $\{g_1, ..., g_r\}$ be a minimal system of generators of $G = G(F/K)$ with $res_{|H(K)}(g_i) = \bar{g}_i$, $\forall\ 1 \leq i \leq r$. (By Burnside's Basis Theorem, such a choice is certainly possible). We then have

Proposition 6.4.4. *Notations being like above, assumption (A1) yields that*

$$(G')^{(g-1)^{p-1}} = \{1\},\ \forall\ g \in G.$$

Proof. Let us assume that there exists an $x \in G'$ and some $g \in G \setminus G'$ such that

$$y := x^{(g-1)^{p-1}} \neq 1.$$

Let $\bar{g} = res_{|H(K)}(g)$. We claim that $y \in G_i$, $\forall\ 1 \leq i \leq s$. Indeed, if $G(H(K)/L_i)$ contains $\bar{g}$, then certainly $y \in G_i$. Now suppose that $\bar{g} \notin G(H(K)/L_i)$ and $y \notin G_i$. Then

$$res_{|H(L_i)}(y) = res_{|H(L_i)}(x)^{(\bar{g}-1)^{p-1}} \neq 1,$$

i.e. $ord(res_{|H(L_i)}(x)) > p$ by Proposition 2.6.2 (i). It follows that the exponent of $kerN_{L_i/K}$ is larger than p, which contradicts (A1). Hence, $y \in G_j$, $\forall\ 1 \leq j \leq s$, which is again a contradiction to $\cap_{j=1}^{s} G_j = \{1\}$. This proves the proposition. □

Proposition 6.4.5. *Notations being like,* $\forall\ 1 \leq i \neq j \leq r$*:*

$$(g_i^p)^{g_j-1} = (g_j^{g_i^p-1})^{-1} = (g_j^{g_i-1})^{-p} = 1.$$

Proof. Obviously, $(g_i^p)^{g_j-1} = (g_j^{g_i^p-1})^{-1}$. Moreover,

$$(g_j^{g_i^p-1}) = (g_j^{g_i-1})^{1+g_i+\ldots+g_i^{p-1}}.$$

Actually, the proof for this statement is rather obvious, but we have to be cautious since G is not abelian and hence is not a $\mathbb{Z}[G]$-module. But observe that $g_j^{g_i-1} \in G'$. Since G' is abelian, it is a well-defined $\mathbb{Z}[G]$-module and hence the following terms make sense. Clearly,

$$\begin{aligned}(g_j^{g_i-1})^{g_i+1} &= g_i(g_ig_jg_i^{-1}g_j^{-1})g_i^{-1}(g_ig_jg_i^{-1}g_j^{-1})^{-1}\\ &= g_i^2g_jg_i^{-2}g_j^{-1}\\ &= g_j^{g_i^2-1}.\end{aligned}$$

Induction hypothesis: $(g_j^{g_i-1})^{1+g_i+\ldots+g_i^{n-2}} = g_j^{g_i^{n-1}-1}$, for some $n \in \mathbb{N}$. Then:

$$\begin{aligned}(g_j^{g_i-1})^{1+g_i+\ldots+g_i^{n-1}} &= (g_j^{g_i-1})^{1+g_i+\ldots+g_i^{n-2}}(g_j^{g_i-1})^{g_i^{n-1}}\\ &= (g_j^{g_i-1})^{g_i^{n-1}} \cdot g_j^{g_i^{n-1}-1}\\ &= g_i^{n-1}g_j^{g_i-1}g_j(g_i^{n-1})^{-1}g_j^{-1}\\ &= g_i^ng_jg_i^{-1}(g_i)^{n-1})^{-1}g_j^{-1}\\ &= g_j^{g_i^n-1}.\end{aligned}$$

For $n = p$, we obtain the desired result. By the previous proposition, we have that $(G')^{(g-1)^{p-1}} = \{1\}$, $\forall\ g \in G$. As $exp(G') = p$, Proposition 2.6.2 (iii) then yields that $g_j^{g_i^p-1} = (g_j^{g_i-1})^p$. All in all, we obtain that

$$(g_i^p)^{g_j-1} = (g_j^{g_i-1})^{-p} = (g_i^{g_j-1})^p.$$

□

Subsequently, we want to analyze the structure of G' more precisely. To this end, we define $K = F_0$, $F_1 = H(K)^{\varphi_K(<\bar{g}_2,...,\bar{g}_r>)}$, $F_2 = H(K)^{\varphi_K(<\bar{g}_3,...,\bar{g}_r>)}$,..., $F_{r-1} = H(K)^{\varphi_K(<\bar{g}_r>)}$, and $F_r = H(K)$. It follows that $K \subset F_1 \subset F_2 \subset ... \subset H(K)$. Henceforth, we make use of the group theoretic version of Furtwängler's Theorem to successively build up G' and to prove the following

Proposition 6.4.6. *Notations being like above, we have*

$$G' =< \{g_i^{g_j-1}\}_{1\leq j<i\leq r} > \cdot \prod_{k=1}^{r} (G')^{g_k-1}.$$

Proof. For the ease of notation, we set $res_{|(H(F_i)\cap F)}(g_j) = g_{j,i}$, $\forall\ 1 \leq i, j \leq r$. Obviously, then

$$G(H(K)/F_1) =< g_{2,0}, g_{3,0}, ..., g_{r,0} >, \text{ and hence}$$

$$G((H(F_1) \cap F)/F_1) =< g_{2,1}, g_{3,1}, ..., g_{r,1} >_{\mathbb{Z}[g_{1,1}-1]} .$$

A moment of reflection, now shows that

$$G((H(F_1) \cap F)/F_2) =< g_{2,1}^{g_{1,1}-1}, g_{3,1}, g_{4,1}, ..., g_{r,1} >_{\mathbb{Z}[g_{1,1}-1]}, \text{ and thus}$$

$$G((H(F_2) \cap F)/F_2) =<< g_{2,2}^{g_{1,2}-1}, g_{3,2}, g_{4,2}, ..., g_{r,2} >_{\mathbb{Z}[g_{1,2}-1]}>_{\mathbb{Z}[g_{2,2}-1]} .$$

Accordingly, we can conclude that

$$\begin{aligned} G((H(F_3) \cap F)/F_3) \ &= \ <<< g_{2,3}^{g_{1,3}-1}, g_{3,3}^{g_{1,3}-1}, g_{3,3}^{g_{2,3}-1}, \\ &\qquad g_{4,3}, ..., g_{r,3} >_{\mathbb{Z}[g_{1,3}-1]}>_{\mathbb{Z}[g_{2,3}-1]}>_{\mathbb{Z}[g_{3,3}-1]} . \end{aligned}$$

Iterating this procedure, we finally obtain the claimed structure for

$$G((H(F_r) \cap F)/F_r) = G(F/H(K)).$$

□

Now let L be an intermediate field of $H(K)/K$ of degree p over K. For the ease of notation, let us assume that $G(H(K)/L) =< \bar{g}_1, ..., \bar{g}_{r-1}, \bar{g}_r^p >$. (This assumption is possible due to a basis transformation for $G(H(K)/K)$). We then obtain

Proposition 6.4.7. *Notations being like above, we have*

$$G(F/H(L)) =< \{g_i^{g_j-1}\}_{1\leq j<i<r} > \cdot \prod_{k=1}^{r-1} G(F/H(K))^{g_k-1}.$$

Proof. "$\supset$": Obvious.
"$\subset$": For the ease of notation, let us say $\tilde{g}_i := res_{|H(L)}(g_i)$, $\forall\ 1 \leq i \leq r$. It follows that $G(H(L)/L) =< \tilde{g}_1, \tilde{g}_2, ..., \tilde{g}_{r-1}, \tilde{g}_r^p >_{\mathbb{Z}[\tilde{g}_r - 1]}$. We can now apply the previous proposition to determine the structure of $G(F/H(L))$ by replacing K by L. Note that $G((H^{(2)}(L) \cap F)/H(L)) = G(F/H(L))$ and that $G'^{g_r^p - 1} = \{1\}$ due to Proposition 6.4.5. The further arguments are straightforward. $\square$

Notations being like above, let $1 \leq u < v \leq s$. Then there exists a system $\{\hat{g}_1, ..., \hat{g}_{r-2}, \hat{g}_u, \hat{g}_v\}$ in $G(H(K)/K)$ such that these elements form a minimal system of generators of $G(H(K)/K)$, $\{\hat{g}_1, ..., \hat{g}_{r-2}, \hat{g}_u, \hat{g}_v^p\}$ forms a minimal system of generators of $G(H(K)/L_u)$, and $\{\hat{g}_1, ..., \hat{g}_{r-2}, \hat{g}_u^p, \hat{g}_v\}$ forms a minimal system of generators of $G(H(K)/L_v)$. For the ease of notation, we henceforth identify the $\hat{g}_i$'s with their extensions to G and suppress the hat. For $G_j = G(F/H(L_j))$, $1 \leq j \leq s$, we then have

Proposition 6.4.8. $G' =< g_u^{g_v - 1} > \times\ (G_u \cdot G_v)$.

Proof. By the previous proposition, we obtain that:

$$G_u =< g_i^{g_j - 1} >_{1 \leq j < i \leq r,\ i \neq v \neq j} \cdot \prod_{k=1, k \neq v}^{r} (G')^{g_k - 1};$$

$$G_v =< g_i^{g_j - 1} >_{1 \leq j < i \leq r,\ i \neq u \neq j} \cdot \prod_{k=1, k \neq u}^{r} (G')^{g_k - 1}.$$

Observe that $(G')^{g_k^p - 1} = 1$, $\forall\ 1 \leq k \leq r$, due to Proposition 6.4.5. By Proposition 6.4.6, it thus follows that

$$G' =< g_u^{g_v - 1} > \cdot (G_u \cdot G_v).$$

As $exp(G') = p$, it is now sufficient to show that $g_u^{g_v - 1} \notin G_u \cdot G_v$. Suppose that this is not the case. Then $G' = G_u \cdot G_v$. Let $\tilde{g}_v = res_{|L_u}$ and thus $G(L_u/K) =< \tilde{g}_v >$. As $|P_K(L_u)| = p$, it follows that $rk(\imath_{L_u/K}(S_1(A(K)))) = r - 1$, which implies that

$$rk(A(L_u)^{\tilde{g}_v - 1} \cap A(L_u)^{<\tilde{g}_v>}) = r - 1.$$

One verifies that this reveals that $rk(A(L_u)^{\tilde{g}_v - 1}/A(L_u)^{(\tilde{g}_v - 1)^2}) = r - 1$. If $G' = G_u \cdot G_v$, however, then restricting the groups to $H(L_u)$, one obtains that

$$\begin{aligned} G(H(L_u/H(K)) &= res_{|H(L_u)}(G_v) \\ &= < res_{|H(L_u)}(g_i^{g_v - 1}) >_{1 \leq i \leq r, i \neq u, v} \cdot G(H(L_u/H(K))^{\tilde{\tilde{g}}_v - 1}, \end{aligned}$$

where $\tilde{\tilde{g}}_v = res_{|H(L_u)}(g_v)$. This implies that

$$rk(G(H(L_u)/H(K))/G(H(L_u)/H(K))^{\tilde{\tilde{g}}_v - 1}) = r - 2,$$

which yields the desired contradiction. This proves the claim. □

Proposition 6.4.9. *Notations being like above, let $m = rk(G')$ and $m_i = rk(G_i)$, $\forall\ 1 \leq i \leq s$. Then there is at most one intermediate field L_i of $H(K)/K$, $1 \leq i \leq s$, such that*

$$m_i < \lfloor m/2 \rfloor.$$

Proof. Suppose L_i is an intermediate field of $H(K)/K$, for some $1 \leq i \leq s$, such that $m_i < \lfloor m/2 \rfloor$. Then

$$\begin{aligned} rk(G(H(L_i)/H(K))) &= rk(G'/G_i) \\ &= m - m_i \\ &\geq \lceil m/2 \rceil + 1. \end{aligned}$$

By the previous propositions, it then follows, $\forall\ 1 \leq j \neq i \leq s$:

$$rk(G_j) \geq (\lceil m/2 \rceil + 1) - 1, \text{ i.e.}$$

$$rk(G_j) \geq \lceil m/2 \rceil.$$

□

Whereas the previous results are valid for all $r \geq 2$, we will now restrict ourselves to the case that $r = rk(A(K)) = 2$. Later we will come back to the general case. We have

Proposition 6.4.10. *Notations being like above, let $r = 2$. Assume the assumptions (A1) and (A2) as in Theorem 6.4.1. By assumption, we have that $rk(kerN_{L_i/K}) \leq rk(kerN_{L_j/K})$, $\forall\ i < j$. Hence, $rk(kerN_{L_1/K}) = 2$ by (A2). It follows that*

$$Z(G) \cap G_1 \cong C_p.$$

Proof. As $p > 3$ by assumption, we can derive that L_1/K has semi-stable growth. (This is a crucial point, where the following proof becomes wrong for $p \leq 3$). By Proposition 6.4.5, we obtain that $< g_1^{p^{k_1}}, g_2^{p^{k_2}} > \subset Z(G) \cap G'$, where $ord(g_i\ mod\ G') = p^{k_i}$ in $G(H(K)/K)$, $i = 1, 2$. Since L_1/K is semi-stable, it follows for $i = 1, 2$:

$$Ver_{G \to G(F/L_1)}(g_i^{p^{k_i - 1}}) \in G_1 \ \Leftrightarrow\ g_i^{p^{k_i}} \in G_1.$$

Let us say that $L_1 = H(K)^{<\bar{g}_1, \bar{g}_2^p>}$, where $\bar{g}_i$ is the restriction of g_i to $H(K)$, for $i = 1, 2$. By Proposition 6.4.6, we obtain that $G' =< g_1^{g_2-1} > \cdot (G')^{g_1-1}(G')^{g_2-1}$ and $G_1 = (G')^{g_1-1}$. By (A2), it follows that $G'/G_1 \cong C_p \times C_p$, which implies that $|G'/(G')^{g_1-1}| = p^2$ and hence $|(G')^{<g_1>}| = p^2$. In particular, we can conclude that $rk(Z(G) \cap G') \leq 2$. By Theorem 6.1.1, we also obtain that $rk(ker N_{L_i/K}) \geq 2$, $\forall\ 1 \leq i \leq p+1$. By group theory, we can then conclude that $Z(G) \cap G_1$ is non-trivial. If $rk(Z(G) \cap G_1) = 2$, it would follow that $|P_K(L_1)| = p^2$, a contradiction to K being imaginary quadratic. This proves the claim. □

Proposition 6.4.11. *Assuming the above situation, it follows that*

$$rk(ker N_{L_j/K}) = 2,\ \forall\ 1 \leq j \leq p.$$

Proof. By (A2), we know that $rk(ker N_{L_1/K}) = 2$ and hence $m_1 = m-2$. By the previous proposition, we have that $|Z(G) \cap G_1| = p$. Assume now that $m_{p+1} \geq 2$, then $m_1 + m_{p+1} \geq m$. As m_{p+1} is minimal among the m_i and due to $Z(G) \cap G_1 \cong C_p$, we thus obtain that $\cap_{j=1}^{p+1} G_j \neq \{1\}$, which yields a contradiction. Hence, $m_{p+1} = 1$. (Note that $m_{p+1} \neq 0$ by Theorem 6.1.1). By the proof of Proposition 6.4.9, it follows that $m_i \geq m - m_{p+1} - 1 = m-2$, $\forall\ 1 \leq i \leq p$, and hence $rk(ker N_{L_i/K}) = 2$. □

We are now in the position to finally prove Theorem 6.4.1. We proceed with the following

Proof. First assume that $rk(ker N_{L_j/K}) = 2$, $\forall\ 1 \leq j \leq p+1$, and thus $m_j = m-2$. We know that $Z(G) \cap G_1 =< z >$, for some $1 \neq z \in G'$. Also recall that $rk(G_1 \cdot G_2) = m-1$. This implies that $m-2+m-2 < m$ since otherwise $z \in \cap_{j=1}^{p+1} G_j$, a contradiction to $\cap_{j=1}^{p+1} G_j = \{1\}$. It follows that $rk(G') = m = 3$ and thus $rk(G_j) = 1$, $\forall\ 1 \leq j \leq p+1$. Due to $rk(G_1 \cdot G_2) = m-1 = 2$, we obtain that $G_j \cap G_i = \{1\}$, $\forall\ 1 \leq j \neq i \leq p+1$, i.e. the G_j's have pairwise distinct centers, which almost yields the claim. It is only left to show that $g_i^{p^{k_i}} \neq 1$, for $i = 1, 2$. Suppose this were not the case, let us say $g_1^{p^{k_1}} = 1$. Then $g_2^{p^{k_2}} \notin G_j$, $\forall\ 1 \leq j \leq p+1$, as $|P_K(L_i)| = p$, $\forall\ i$. On the other hand, we have $p+1$ G_j's with pairwise distinct center. By the pigeon hole principle then, however, $< g_2^{p^{k_2}} > \in G_j$, for some j, which yields the desired contradiction. Hence, K has 1-1-capitulation in that case. Let us now assume (ii). By Proposition 6.4.11, it follows that $rk(ker N_{L_j/K}) = 2$, $\forall\ 1 \leq j \leq p$, and $rk(ker N_{L_{p+1}/K}) > 2$. By the previous arguments, we know that $m_j = m-2$, $\forall\ 1 \leq j \leq p$, and $m_{p+1} = 1$, i.e. $m =$

$rk(kerN_{L_{p+1}/K}) + 1 \geq 4$. This implies that $m - 2 + m - 2 \geq m$ and hence $m_i + m_j \geq m$, $\forall\ 1 \leq i, j \leq p$. For $Z(G) \cap G_1 =< z >$ as above, we thus obtain that $1 \neq z \in \cap_{j=1}^{p} G_j$. If $rk(< g_1^{p^{k_1}}, g_2^{p^{k_2}} >) = 1$, we are done as clearly $1 \in G_j, \forall\ G_j$. Otherwise, we have that $Z(G) \cap G' =< g_1^{p^{k_1}}, g_2^{p^{k_2}} >$. Let us say that $z = g_1^{l_1 p^{k_1}} g_2^{l_2 p^{k_2}}$, for some $0 \leq l_i < p$. As $L_1, ..., L_p$ all have semi-stable growth over K, it follows $\forall\ 1 \leq i \leq p$:

$$Ver_{G \to G(F/L_i)}(g_1^{l_1 p^{k_1 - 1}} g_2^{l_2 p^{k_2 - 1}}) \equiv z\ mod\ G_i.$$

As $z \in G_i$, $\forall\ 1 \leq i \leq p$, the claim in statement (ii) follows. □

If the assumption (A1), is violated we can still recover the above theorem for those intermediate fields where (A1) holds. More precisely, we have

Theorem 6.4.12. *Notations being like above, assume assumption (A2) and that $exp(kerN_{L_j/K}) = p$, $\forall\ 1 \leq j \leq t$, where $t \leq p + 1$. Then either:*

(i) $P_K(L_j) \neq P_K(L_i)$, $\forall\ 1 \leq i \neq j \leq t$, or

(ii) $P_K(L_j) = P_K(L_i)$, $\forall\ 1 \leq i \neq j \leq t$.

Proof. The proof is rather analogous. Simply replace F by $\prod_{j=1}^{t} H(L_j)$. □

Subsequently, we want to deal with the case that $r = rk(A(K)) > 2$. One can show that it is not possible to 1-1-generalize Theorem 6.4.1 to the case where $r > 2$, but again we can recover it to some extent:

Let K be an imaginary quadratic field and $K \subset M \subset H(K)$ be an intermediate field with $G(M/K) \cong C_p \times C_p$, $p > 3$. Let $L_1, ..., L_{p+1}$ be the intermediate fields of $K \subset M$ of degree p over K and let us say that $rk(kerN_{L_i/K}) \leq rk(kerN_{L_j/K})$, $\forall\ 1 \leq i < j \leq p+1$. Let $L_1, ..., L_t$ $(t \leq p+1)$ be such that $rk(kerN_{L_j/K}) = 2(r-1)$, $\forall\ 1 \leq j \leq t$. Then we have

Theorem 6.4.13. *Notations being like above, we either have*

$$(i)\ P_K(L_i) \neq P_K(L_j),\ \forall\ 1 \leq i \neq j \leq t,\ or$$

$$(ii)\ P_K(L_i) = P_K(L_j),\ \forall\ 1 \leq i \neq j \leq t.$$

Proof. We set $F = \prod_{j=1}^{t} H(L_j)$. Since $rk(kerN_{L_j/K}) = 2(r-1)$, $\forall\ 1 \leq j \leq t$, it readily follows that $exp(kerN_{L_j/K}) = p$ and hence $exp(G(F/H(K))) = p$. Henceforth, we write $G = Gal(F/K)$, $G' = Gal(F/H(K))$, and $G_j = Gal(F/H(L_j))$, $\forall\ 1 \leq j \leq t$. Let $\{g_1, ..., g_r\} \subset G$ be a minimal system of

generators of G, $\bar{g}_i = g_i \; mod \; G'$ $(1 \leq i \leq r)$, and $ord(\bar{g}_i) = p^{k_i}$, with $k_i \in \mathbb{N}$. By previous arguments, we obtain that

$$Z_{(p)} := \{g_1^{p^{k_1}}, ..., g_r^{p^{k_r}}\} \subset Z(G) \cap G'.$$

Claim: Assume that $G_{l_1} \cap G_{l_2} \neq \{1\}$, for some $1 \leq l_1, l_2 \leq t$. Then $G_{l_1} \cap G_{l_2} \cap Z_{(p)} \neq \{1\}$.
Proof: For the ease of notation, let us say $l_1 = 1$ and $l_2 = 2$. First observe that L_j/K is semi-stable, for all $1 \leq j \leq t$, and hence for all $1 \leq i \leq r$:

$$g_i^{p^{k_i}} \in G_j \Leftrightarrow \varphi_K^{-1}(g_i) \in P_K(L_j),$$

where φ_K is the Artin symbol of K. If $rk(Z_{(p)}) < r$, it easily follows that $P_K(L_i) = P_K(L_j)$, $\forall \; 1 \leq i \neq j \leq t$. We may thus assume that $rk(Z_{(p)}) = r$. By assumption, we have that $Gal(M/K) \cong C_p \times C_p$. Without loss of generality, we may assume that $Gal(H(K)/M) = G(H(K)/K)^p \cdot < \bar{g}_3, ..., \bar{g}_r >$. Let $h_1, ..., h_t \in G$ be such that $L_j = M^{<\bar{h}_j>}$ $(1 \leq j \leq t)$, where $\bar{h}_j = h_j \; mod \; G(F/M)$. (In a nutshell: $h_1, ..., h_t$ are products of g_1 and g_2). Also: $Gal(M/K) =< \bar{h}_i, \bar{h}_j >$, $\forall \; 1 \leq i \neq j \leq t$. Suppose now that there is some $1 \leq k \leq t$ and some $1 \leq i \leq r$ such that $g_i^{(h_k-1)^3} \neq 1$. Then, however, $g_i^{(h_k-1)^3} \in G_j$, $\forall \; 1 \leq j \leq t$, which yields a contradiction to $\cap_{j=1}^t G_j = \{1\}$. A moment of reflection then reveals that

$$Z(G) \cap G' =< g_i^{(g_1-1)^2} >_{1<i\leq r} \times < g_j^{(g_2-1)^2} >_{1\leq j\neq 2\leq r} .$$

In particular, $rk(Z(G) \cap G') = 2(r-1)$ and $rk(Z(G) \cap G_1) = rk(Z(G) \cap G_2) = r-1$. Assume that $G_1 \cap G_2 \neq \{1\}$ and $G_1 \cap G_2 \cap Z_{(p)} = \{1\}$. We know that $G_i \cap Z_{(p)} =< z_i > \cong C_p$, for $i = 1, 2$, and some $z_1, z_2 \in Z(G) \cap G'$. We write $Z_{(p)} =< z_1, z_2, z_3, ..., z_r >$, for suitable z_i, and extend this system to a basis of

$$Z(G) \cap G' =< z_1, ..., z_{2(r-1)} >,$$

where $z_j \in Z(G) \cap G'$, for all $1 \leq j \leq 2(r-1)$. Without loss of generality, we may also assume that $G_1 \cap G_2 =< z_{r+1} >$. Observe that $rk(< z_1, z_2, z_{r+1} >) = 3$ by assumption. Let $(Z(G) \cap G_1) \setminus < z_1, z_{r+1} > =< x_1, ..., x_{r-3} >$ and $(Z(G) \cap G_2) \setminus < z_2, z_{r+1} > =< y_1, ..., y_{r-3} >$. For all $j = 3, ..., r$, we may then write

$$z_j = \prod_{i=1}^{r-3} x_i^{k_{i,j}} \cdot y_i^{l_{i,j}},$$

where $k_{i,j}$ and $l_{i,j} \in \mathbb{Z}$. Now consider the matrix $M_y := (k_{i,j})_{1\leq i\leq r-3, \; 3\leq j\leq r}$. Obviously, M_y is a $(r-2) \times (r-3)$-matrix with integer entries. By elementary

linear algebra, it follows that the column rank is strictly smaller than $r-2$. This, however, implies that $< z_3, ..., z_r > \cap G_2 \neq \{1\}$, which yields the desired contradiction. This proves the claim. The rest is analogous to the usual arguments. $\square$

Eventually, we want to use the developed heuristic of Section 6.2 in order to evaluate how likely it is that the assumptions (A1) and (A2) are satisfied. Having done that, we will also ask how likely it is that a given imaginary quadratic field has 1-1-capitulation or p-capitulation, respectively. For the upcoming discussion, we restrict ourselves to the case $t = 2$ and $p > 3$. By the heuristics, we have that

$$\sum_{k \geq 2}^{\infty} Freq_2(2k) = \frac{1}{p^2}.$$

Question: How likely is it that (A1) is satisfied, i.e. that $exp(kerN_{L_j/K}) = p$, $\forall\ 1 \leq j \leq p+1$? We know that $exp(kerN_{L_j/K}) > p \Leftrightarrow rk(kerN_{L_j/K}) > p-1$. Also,

$$\sum_{k \geq (p+1)/2}^{\infty} Freq_2(2k) = \frac{1}{p^{p+1}}.$$

Let Γ(Ai) denote the event that (Ai) is violated ($i = 1, 2$). By the pigeon hole principle, we deduce that

$$lim_{D \to \infty} \frac{|\{K \in \mathcal{K}_{D,2} :\ \Gamma(A1)\}|}{|\{K \in \mathcal{K}_{D,2}\}|} \leq \frac{p+1}{p^{p+1}} \approx 1/p^p.$$

How likely is it that assumption (A2) is violated, i.e. that $rk(kerN_{L_j/K}) \geq 4$, $\forall\ 1 \leq j \leq p+1$? By the pigeon hole principle, we obtain the following defensive upper bound:

$$lim_{D \to \infty} \frac{|\{K \in \mathcal{K}_{D,2} :\ \Gamma(A2)\}|}{|\{K \in \mathcal{K}_{D,2}\}|} \leq \frac{1/p^2}{p+1} < \frac{1}{p^3}.$$

In a nutshell, it is very likely that the assumptions (A1) and (A2) are satisfied. When p grows larger, the respective likelihoods go to 1.

Question: What is the likelihood that an imaginary quadratic field K, with $rk(A(K)) = 2$, has 1-1-capitulation, provided that it satisfies (A1) and (A2)? By the previous arguments, this is the case when $rk(kerN_{L_j/K}) = 2$, $\forall\ 1 \leq j \leq p+1$. By the pigeon hole principle, we have that

$$lim_{D \to \infty} \frac{|\{K \in \mathcal{K}_{D,2} :\ K \text{ has 1-1-capitulation}\}|}{|\{K \in \mathcal{K}_{D,2}\}|} \geq 1 - (p+1)\frac{1}{p^2} \approx 1 - \frac{1}{p}.$$

Hence, it becomes more and more likely that K has 1-1-capitulation as p goes to infinity.

Chapter 7

The Capitulation Problem in $\mathbb{Z}_p$-Extensions

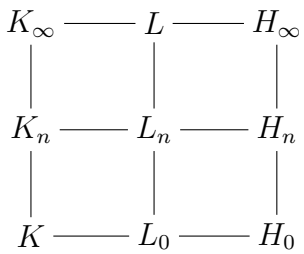
In this chapter, we want to investigate horizontal capitulation in a given $\mathbb{Z}_p$-extension. (We will specify this below). For a comprehensive study of Iwasawa Theory, we refer to [8], [11]. Throughout this chapter, let K be a number field and K_∞ be a given $\mathbb{Z}_p$-extension of K for a fixed prime $p > 2$. Let $\Gamma = Gal(K_\infty/K)$ with topological generator σ and $\Gamma_n = \Gamma/\Gamma^{p^n}$. Then, we obtain a tower of fields K_n/K with $\Gamma_n = Gal(K_n/K)$ cyclic of order p^n. It is well known that

$$\lim_{\leftarrow} \mathbb{Z}_p[\Gamma_n] \cong \mathbb{Z}_p[[T]], \text{ via}$$

$$\sigma \mapsto T + 1.$$

We call $\Lambda := \mathbb{Z}_p[[T]]$ the *Iwasawa algebra*. (For further details, see Theorem 7.1, page 114, of [8]).

Let A_n be the p-part of the ideal class group of K_n and H_n be the p-part of the Hilbert class field of K_n. Then we define $H_\infty = \cup_{n\geq 0} H_n$. By Section 5.1, H_n/K is Galois for all $n \in \mathbb{N}$. Thus, H_∞/K is Galois. Now let L be an intermediate field of H_∞/K_∞ with L/K Galois. For $L_n = L \cap H_n$, it follows that L_n/K is Galois. The situation is given as in the following diagram:



For simplicity, we will assume that all primes in K that ramify in K_∞ are totally ramified. It follows that $K_{n+1} \cap L_n = K_n$ and that $N_{K_{n+1}/K_n} : A(K_{n+1}) \to A(K_n)$ is surjective by Proposition 1.3.4. We now want to analyze the capitulation kernels $X_n = ker(\imath_{L_n/K_n} : A(K_n) \to A(L_n))$. We start with a useful

Lemma 7.0.14. *Notations being like above, we have $\forall\ n \in \mathbb{N}$:*

$$N_{K_{n+1}/K_n}(X_{n+1}) \subset X_n.$$

Proof. Let $a \in X_{n+1}$ with $a = [\mathfrak{P}]$, for some prime $\mathfrak{P}$ in K_{n+1} lying above the prime $\mathfrak{p}$ in K_n. By assumption, $\mathfrak{P}\mathcal{O}_{L_{n+1}} = \alpha\mathcal{O}_{L_{n+1}}$, for some $\alpha \in L_{n+1}^*$. Moreover, we have that

$$\prod_{\tau \in Gal(K_{n+1}/K_n)} \mathfrak{P}^\tau = N_{K_{n+1}/K_n}(\mathfrak{P})\mathcal{O}_{K_{n+1}}.$$

Due to $res_{L_{n+1}/K_{n+1}}(Gal(L_{n+1}/L_n)) = Gal(K_{n+1}/K_n)$, it follows that

$$\begin{aligned} N_{K_{n+1}/K_n}(\mathfrak{P})\mathcal{O}_{L_{n+1}} &= \prod_{\tau \in Gal(K_{n+1}/K_n)} \mathfrak{P}^\tau \mathcal{O}_{L_{n+1}} \\ &= \prod_{\tau' \in Gal(L_{n+1}/L_n)} (\mathfrak{P}\mathcal{O}_{L_{n+1}})^{\tau'} \\ &= (\prod_{\tau' \in Gal(L_{n+1}/L_n)} (\alpha^{\tau'})). \end{aligned}$$

As L_{n+1}/L_n is Galois, we obtain that $\alpha' := \prod_{\tau' \in Gal(L_{n+1}/L_n)}(\alpha^{\tau'}) \in L_n$. It follows that $(\alpha')^{-1} \cdot N_{K_{n+1}/K_n}(\mathfrak{P})\mathcal{O}_{L_{n+1}} = \mathcal{O}_{L_{n+1}}$. Since α' and $N_{K_{n+1}/K_n}(\mathfrak{P})$ lie in L_n and as the lift of ideals from L_n to L_{n+1} is injective, we obtain that

$$N_{K_{n+1}/K_n}(\mathfrak{P})\mathcal{O}_{L_n} = \alpha\mathcal{O}_{L_n} \text{ i.e.}$$

$N_{K_{n+1}/K_n}([\mathfrak{P}])$ capitulates in L_n. This completes the proof. □

By the previous lemma, we may define the projective limit of the X_n with respect to the norms N_{K_m/K_n}, $\forall\ m \geq n \geq 0$. Let us say

$$X := \lim_{\leftarrow} X_n,$$

i.e. $X = \{(x_0, x_1, ...) \in \prod_{n\geq 0} X_n |\ N_{K_{n+1}/K_n}(x_{n+1}) = x_n\}$. Since L_n is Galois over K, $\forall\ n \in \mathbb{N}$, it follows that X_n is a $\mathbb{Z}_p[Gal(K_n/K)]$-module. Hence, X is a Λ-module, where the action of Λ on X is defined component wise. This poses the natural question if X may be trivial? We have the following

Theorem 7.0.15. *Notations being like above, assume that L/K_∞ is an infinite extension. Then X is a non-trivial Λ-module. Moreover, there exist constants $\lambda(X)$, $\mu(X)$, $\nu(X) \geq 0$ such that*

$$|X_n| = p^{\lambda(X)n+\mu(X)p^n+\nu(X)}.$$

Proof. Since L/K is Galois by assumption, there exist Iwasawa invariants $\lambda, \mu, \nu \geq 0$ such that

$$|Gal(L_n/K_n)| = p^{\lambda n+\mu p^n+\nu}.$$

Since L/K_∞ is supposed to be infinite, it follows that $Gal(L/K)$ is an infinite Λ-module implying that $\lambda > 0$ or $\mu > 0$. By Suzuki's Theorem, we also have that

$$|X_n| \geq p^{\lambda n+\mu p^n+\nu}.$$

In particular, $|X_n|$ is not constant as n runs through $\mathbb{N}$.
For all $n \in \mathbb{N}$, let $\varphi_n : A(K_n) \to Gal(H_n/K_n)$ denote the Artin symbol of H_n/K_n and set $M_n = H_n^{\varphi_n(X_n)}$. By Proposition 1.3.4, it follows that

$$res_{H_{n+1}/H_n}(\varphi_{n+1}(X_{n+1})) \subset \varphi_n(X_n).$$

Hence, we can conclude that

$$\begin{aligned} M_{n+1} \cap H_n &= H_n^{res_{H_{n+1}/H_n}(\varphi_{n+1}(X_{n+1}))} \\ &\supset H_n^{\varphi_n(X_n)} \\ &= M_n \end{aligned}$$

Now we may define $M = \cup_{n\geq 0} M_n$, which is an intermediate field of $K_\infty \subset H_\infty$ and which is Galois over K as all X_n are closed by the action of Λ. Thus, there are Iwasawa-invariants $\lambda', \mu', \nu' \geq 0$ such that

$$|Gal(M_n/K_n)| = p^{\lambda' n+\mu' p^n+\nu'}.$$

Assume that $M = H_\infty$. Then $\lambda(Gal(M/K_\infty)) = \lambda(Gal(H_\infty/K_\infty))$ and $\mu(Gal(M/K_\infty)) = \mu(Gal(H_\infty/K_\infty))$. (" $\leq$ " certainly holds in both cases). This implies that $|X_n| = |Gal(H_n/K_n)|/|Gal(M_n/K_n)|$ is constant, for all n, which yields a contradiction to the above assertions. Thus, $M \neq H_\infty$. It follows that

$$\begin{aligned} \{1\} &\neq Gal(H_\infty/M) \\ &= \varprojlim Gal(H_\infty/M)/Gal(H_\infty/H_nM) \\ &= \varprojlim Gal(H_n/H_n \cap M) \\ &\subset \varprojlim Gal(H_n/M_n) \\ &= \varprojlim X_n \\ &= X. \end{aligned}$$

Let $\lambda'' := \lambda(G(H_\infty/K_\infty))$, $\mu'' := \mu(G(H_\infty/K_\infty))$, and $\nu'' = \nu(G(H_\infty/K_\infty))$. Then:

$$|X_n| = p^{(\lambda''-\lambda')n+(\mu''-\mu')p^n+\nu''-\nu'}.$$

□

Appendix A

List of Notations

The following table lists notations which we frequently used throughout the thesis and indicates on which page the given notation occurs for the first time. However, this list does not claim to be exhaustive. Special notations will be explained in the various contexts. Moreover, we use two different notations both for the Artin symbol and for a Galois group (see below). The reason for this is that depending on the context it is convenient to have a more precise or shorter notation.

Notation	Explanation	Page
p	Some fixed prime	8
K	Number field	3
$\mathfrak{J}_K$	Group of fractional ideals of K	3
$Cl(K)$	Ideal class group of K	3
$A(K)$	p-Sylow subgroup of $Cl(K)$	13
A	Finite abelian p-group	13
$rk(A)$	p-Rank of A	13
$S_l(A)$	l-Socle of A	13
A^G	G-invariant elements in A	13
$\mathcal{O}_K$	Ring of integers of K	11
$\mathcal{O}_K^*$	Unit group of $\mathcal{O}_K$	17
$H(K)$	Hilbert class field of K	4
$H(K)^{(i)}$	Hilbert class field of $H(K)^{(i-1)}$	33
$H(K)_p$	p-Hilbert class field of K	13
L/K	Extension of number fields	3
$[L:K]$	Degree of L/K	12
$Gal(L/K)$	Galois group of L/K	11
$G(L/K)$	Galois group of L/K	11
$P_K(L)$	Capitulation kernel of L/K	3
$\left(\frac{L/K}{\cdot}\right)$	Artin symbol of L/K	12
$\varphi_{L/K}$	Artin symbol of L/K	12
φ_K	Artin symbol of $H(K)/K$	12
$\imath_{L/K}$	Lift of ideal classes	3
$N_{L/K}$	Norm of ideal classes	12
$Ver_{G\to H}$	Transfer from G to H	14
$\mathcal{H}^i(G,A)$	i-th cohomology group of G in A	16
$res_{\mid K}$	Restriction to K	13
$\mathcal{D}_{\mathcal{P}_i\mid P_i}$	Decomposition group of $\mathcal{P}_i\mid P_i$	11
C_{p^k}	Cyclic group of order p^k	4
$\mathbb{Z}_p$	Ring of p-adic integers	6
$\Phi(G)$	Frattini group of G	33
$Z(G)$	Center of a group G	34
α	Idempotent in $\mathbb{Z}_p[G]$	8
$b^{\mathbb{Z}[s]}$	$\mathbb{Z}[s]$-cycle of b	36
$r(b)$, $l(b)$	Length of the flag of b	36
$< .., .., .. >$	$\mathbb{Z}$-span	23
$< .., .., .. >_{\mathbb{Z}[s]}$	$\mathbb{Z}[s]$-span	54

Appendix B

Source Codes Used in MAGMA

Here we want to add the various source codes that we used in MAGMA. For further details, we refer to [35] and the handbook of MAGMA. Using the following code, one can compute if a given ideal class capitulates in a given unramified abelian extension L/K or not. In the following illustration, we consider capitulation in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-63499})$. Its class group is isomorphic to $C_7 \times C_7$, implying that K has 8 unramified cyclic extensions of degree 7. The following example shows how to construct such an extension, which is denoted by $aK2$ below. Then we check whether a given ideal class of K capitulates in that extension:

$k := NumberField(Polynomial([63499, 0, 1]));$
$g, m := ClassGroup(k);$
$aK := AbelianExtension(m);$
$q, mq := quo < g| \ (5 * g.1) * g.2 >;$
$m2 := Inverse(mq) * m; m2;$
$aK2 := AbelianExtension(m2);$
$O := MaximalOrder(aK2); O;$
$I := O!!m(g.1);$
$IsPrincipal(I);$

In order to compute the class group of $aK2$ from above, we use the following source code:

$L := NumberField(aK2);$
$M := SimpleExtension(L);$
$ClassGroup(M);$

Remark: In some cases, we also used the computer program pari/gp, which seems to be better when it comes to the computation of class numbers.

When we are concerned with capitulation, however, MAGMA shows obvious advantages.

Last but not least, we also used MAGMA for group theoretic computations. For instance, we constructed certain finitely presented p-groups. We then computed the order of the respective group G, the commutator subgroup G' of G, and the order of G'. We give the following example:

$G := Group < a, b |\ a^{25}, b^{25}, ab = a^5ba, ba^5 = a^5b, ab^5 = b^5a >; G;$
$n := Order(G); Factorization(n);$
$H := CommutatorSubgroup(G); H;$
$Order(H); CommutatorSubgroup(H);$

Bibliography

[1] Ph. Furtwängler. Existenzbeweis für den Klassenkörper. Math. Ann. 63 (1907).

[2] Jürgen Neukirch. Algebraische Zahlentheorie. Springer-Verlag, 1992.

[3] Falko Lorenz. Algebraische Zahlentheorie. Wissenschaftsverlag, 1993.

[4] Katsuya Miyake. Algebraic investigations of Hilbert's Theorem '94. Expo. Math.7, (1989), 289-346.

[5] Gruenberg, Weiss. Capitulation and Transfer Kernels. Journal de Theorie des Nombres de Bordeaux **12** (2000), 219-226.

[6] Christopher Ambrose, Diploma thesis, 2010.

[7] M.J. Collins. Representations and characters of finite groups. Cambridge studies in advanced mathematics 22.

[8] Lawrence Washington. Introduction to Cyclotomic Fields. Springer-Verlag, Second Edition.

[9] Joseph J. Rotman. An Introduction to the Theory of Groups. Springer-Verlag, Fourth Edition.

[10] Bosch. Algebra. Springer-Verlag, Fifth Edition.

[11] Serge Lang. Cyclotomic Fields. Springer-Verlag. 1978.

[12] Manabu Ozaki. Construction of maximal unramified p-extensions with prescribed Galois group. Inventiones Mathematicae, Volume 183, Number 3, 649-680.

[13] O. Yahagi. Construction of number fields with prescribed l-class group. Tokyo J. of Math. 1978.

[14] Kenkichi Iwasawa. A note on the group of units of an algebraic number field. Journal de Mathematiques pures et appliques. 1956.

[15] Robert J. Bond. Some results on the capitulation problem. Journal of number theory 13, 246-254. 1981.

[16] Steven H. Weintraub. Representation Theory of Finite Groups: Algebra and Arithmetic. Springer, New York, 1995.

[17] Joachim Schwermer, Jens Carsten Jantzen. Algebra. Springer, Berlin, 2009.

[18] Fernando Q. Gouvea. P-adic Numbers. Springer, 1997. Second Edition.

[19] Jung-Je Son, Soun-Hi Kwon. On The Principal Ideal Theorem. J.Korean Math. Soc. **44** (2007), No.4, pp.747-756.

[20] Alain M.Robert. A Course in p-adic Analysis. Springer-Verlag. 1999.

[21] Scholz und Taussky. Die Hauptideale der kubischen Klassenkörper imaginär quadratischer Zahlkörper. Journal für die reine und angewandte Mathematik. Volume 171. 1934.

[22] D. Hilbert. Die Theorie der algebraischen Zahlkörper. Jahresbericht der Deutschen Mathematiker- Vereinigung 4 (1897), pp. 175-546, re-edited in D. Hilbert, Gesammelte Abhandlungen, vol. 1, Berlin, Heidelberg, etc.: Springer, 1932 (second edition 1970).

[23] Serge Lang. Algebraic Number Theory. Springer-Verlag, 1994. Second Edition.

[24] Kenkichi Iwasawa. A Note on the Capitulation Problem for Number Fields. Proc. Japan Acad., **65**, Ser. A (1989).

[25] Heider-Schmithals. Zur Kapitulation der Idealklassen in unverzweigten primzyklischen Erweiterungen. Journal für die reine und angewandte Mathematik. Volume 336. 1982.

[26] Franz Lemmermeyer. Class Field Towers. www.rzuser.uni-heidelberg.de/hb3/publ/pcft.pdf

[27] Cristian D. Gonzalez-Aviles. Capitulation, ambiguous classes and the cohomology of the units. J. reine und angew. Math. 613 (2007).

[28] J. E. Cremona and R. W. K. Odoni. A generalization of a result of Iwasawa on the capitulation problem. Mathematical Proceedings of the Cambridge Philosophical Society (1990), 107: 1-3.

[29] Golod, E.S; Shafarevich, I.R. (1964). "On the class field tower", Izv. Akad. Nauk SSSSR 28: (in Russian) MR0161852.

[30] T. Tannaka. A generalized principal ideal theorem and a proof of a conjecture of Deuring. Ann. Math. 67 (1958).

[31] Hisako Furuya. Principal ideal theorems in the genus field for absolutely abelian extensions. Journal of Number Theory, Volume 9, Issue 1, February 1977, Pages 4-15.

[32] Olga Taussky. A remark concerning Hilbert's Theorem 94. Journal für die reine und angewandte Mathematik (1969). Volume 239-240, p.435-438.

[33] Duncan A. Buell. Class Groups of Quadratic Fields. Mathematics of Computation (1987). Volume 48, Number 177, p. 85-93.

[34] R. Schoof. Class Groups of Complex Quadratic Fields. Mathematics of Computation (1983). Volume 41, Number 163, p. 295-302.

[35] Wieb Bosma, John Cannon, and Catherine Playoust. The MAGMA algebra system. I. The user language, J. Symbolic Computation, 24 (1997).

[36] http://www.algebra.at/Memorial2009Principalization.htm.

[37] B. Huppert. Endliche Gruppen. Volume 1, Berlin-Heidelberg-New York (1967).

[38] B. Huppert, N. Blackburn. Endliche Gruppen. Volume 2, Berlin-Heidelberg-New York (1967).

[39] Olga Taussky. Über eine Verschärfung des Hauptidealsatzes für algebraische Zahlkörper. Journal reine und angewandte Mathematik (1932). Band 168, p. 193-210.

[40] D. Gorenstein. Finite groups. Chelsea Publishing Co., New York, second edition, 1980.

[41] Geir T. Helleloid and Ursula Martin. The Automorphism Group of a Finite p-Group is Almost Always a p-Group. Formal Power Series and Algebraic Combinatorics, Nankai University, Tianjin, China, 2007.

[42] Christian Wittmann (2005). p-Class Groups of Certain Extensions of Degree p. Mathematics of Computation, Vol. 74, No 250, pp. 937-947.

[43] Georges Gras (1973). Sur les l-classes d'ideaux dans les extensions cycliques relative de degre premier l. Annales de l'institut Fourier, tome 23, No 3, p. 1-48.

[44] M. Arrigoni. On Schur σ-Groups. Tokyo Metropolitan University Mathematics Preprint Series, 1995.

[45] Frank Gerth. On p-class groups of cyclic extensions of prime degree p of quadratic fields. Mathematika, 36 (1989), 89-102.

[46] N. Boston, M. R. Bush, F, Hajir. Heuristics for p-class towers of imaginary quadratic fields. Submitted in November 2011.

[47] Cohen, Lenstra: Heuristics on class groups of number fields. Number theory, Noordwijkerhout 1983, volume 1068 of Lecture Notes in Math.. Springer, Berlin (1984).

[48] Michael J. Jacobson, Shantha Ramachandran und Hugh C. Williams. Numerical Results on Class Groups of Imaginary Quadratic Fields. Lecture Notes in Computer Science, 2006, Volume 4076/2006, 87-101.

[49] H. Cohen and J. Martinet. Class Groups of Number Fields: Numerical Heuristics. Mathematics of Computation, Vol. 48, No. 177 (Jan., 1987), pp. 123-137.

Lebenslauf

Persönliche Angaben

Name:	**Tobias Bembom**
Geburtsdatum:	3. Februar 1983
Geburtsort:	Neustadt (Rbge)
Familienstand:	ledig/keine Kinder
Emailadresse:	TBembom@gmx.de

Hochschulstudium

05/2009-04/2012 Promotion in Mathematik an der Georg-August-Universität Göttingen

- Schwerpunkt: Algebraische Zahlentheorie
- Vertrag als wissenschaftlicher Mitarbeiter mit Lehrtätigkeit

09/2007-08/2008 Master of Pure Mathematics in Cambridge, UK

- Einjähriges Master-Programm

02/2004-03/2009 Stipendiat der Studienstiftung des deutschen Volkes

10/2003-03/2009 Studium in Mathematik auf Diplom an der Carl-von-Ossietzky-Universität in Oldenburg

- Schwerpunkt: Algebraische Zahlentheorie
- Nebenfach: Volkswirtschaftslehre
- Abschlussnote: 1,0 / Vordiplomsnote: 1,0

Schulbildung

08/1996-05/2003 Abitur an der Albert-Schweitzer-Schule in Nienburg

- Gesamtnote: 1,2