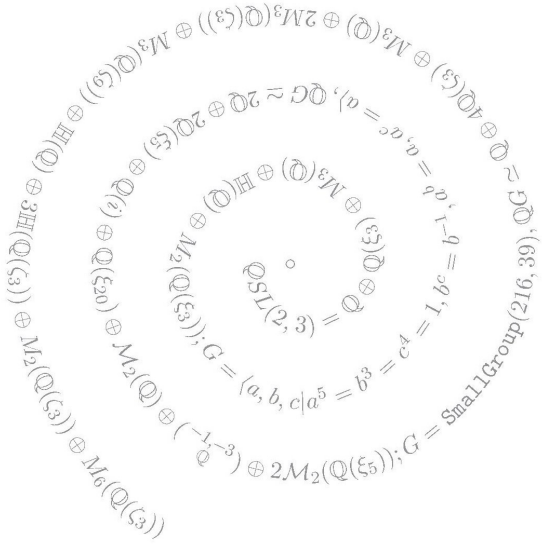
Gabriela Olteanu

WEDDERBURN DECOMPOSITION OF GROUP ALGEBRAS AND APPLICATIONS



EFES

Gabriela Olteanu

Wedderburn Decomposition of Group Algebras and Applications

EDITURA FUNDAŢIEI PENTRU STUDII EUROPENE

Cluj-Napoca 2008

Editura Fundaţiei pentru Studii Europene
Str. Emanuel de Martonne, Nr. 1
Cluj–Napoca, Romania
Director: Ion Cuceu

Descrierea CIP a Bibliotecii Naţionale a României
OLTEANU, GABRIELA

Wedderburn decomposition of group algebras and applications / Gabriela Olteanu. - Cluj-Napoca : Editura Fundaţiei pentru Studii Europene, 2008

Bibliogr.

Index

ISBN 978-973-7677-98-3

519.6

To my family

Contents

Preface

Group rings are algebraic structures that have attracted the attention of many mathematicians since they combine properties of both groups and rings and have applications in many areas of Mathematics. Their study often requires techniques from Representation Theory, Group Theory, Ring Theory and Number Theory and, in some cases, the use of properties of central simple algebras or local methods. By the Maschke Theorem, if G is a finite group and F is a field of characteristic not dividing the order of the group G, then the group algebra FG is semisimple artinian. In this case, the structure of FG is quite easy, but the explicit computation of the Wedderburn decomposition of the group algebra knowing the group G and the field F is not always an easy problem. On the other hand, the explicit knowledge of the Wedderburn decomposition has applications to different problems.

The Wedderburn decomposition of a semisimple group algebra FG is the decomposition of FG as a direct sum of simple algebras, that is, minimal two-sided ideals. Our main motivation for the study of the Wedderburn decomposition of group algebras is given by its applications. The main applications that we are interested in are the study of the groups of units of group rings with coefficients of arithmetic type and of the Schur groups of abelian number fields. Other applications of the Wedderburn decomposition that, even if not extensively studied in this book we have had in mind during its preparation, are the study of the automorphism group of group algebras, of the Isomorphism Problem for group algebras and of the error correcting codes with ideal structure in a finite group algebra, known as group codes.

We start by presenting with more details the first application, which is the computation of units of group rings relying on the Wedderburn decomposition of group algebras. It is well known that the integral group ring $\mathbb{Z}G$ is a $\mathbb{Z}$-order in the rational group algebra $\mathbb{Q}G$ and it has been shown that a good knowledge and understanding of $\mathbb{Q}G$ is an essential tool for the study of $\mathcal{U}(\mathbb{Z}G)$. For example, some results of E. Jespers and G. Leal and of J. Ritter and S.K. Sehgal [JL, RitS2] show that, under some

hypotheses, the Bass cyclic units and the bicyclic units (see Section 1.3. for definitions) generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$. These hypotheses are usually expressed in terms of the Wedderburn decomposition of the rational group algebra $\mathbb{Q}G$. Their theorems were later used by E. Jespers, G. Leal and C. Polcino Milies [JLPo] to characterize the groups G that are a semidirect product of a cyclic normal subgroup and a subgroup of order 2 such that the Bass cyclic units and the bicyclic units generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$. This latter characterization also had as starting point the computation of the Wedderburn decomposition of $\mathbb{Q}G$ for these groups.

As a consequence of a result of B. Hartley and P.F. Pickel [HP], if the finite group G is neither abelian nor isomorphic to $Q_8 \times A$, for Q_8 the quaternion group with 8 elements and A an elementary abelian 2-group, then $\mathcal{U}(\mathbb{Z}G)$ contains a non-abelian free group. The finite groups for which $\mathcal{U}(\mathbb{Z}G)$ has a non-abelian free subgroup of finite index were characterized by E. Jespers [Jes]. Furthermore, the finite groups such that $\mathcal{U}(\mathbb{Z}G)$ has a subgroup of finite index which is a direct product of free groups were classified by E. Jespers, G. Leal and Á. del Río in a series of articles [JLdR, JL, LdR]. In order to obtain the classification, they used the characterization of these groups in terms of the Wedderburn components of the corresponding rational group algebra. Furthermore, for every such group G, M. Ruiz and Á. del Río explicitly constructed a subgroup of $\mathcal{U}(\mathbb{Z}G)$ that had the desired structure and minimal index among the ones that are products of free groups [dRR]. Again, a fundamental step in the used arguments is based on the knowledge of the Wedderburn decomposition of the rational group algebra.

The use of the methods of Kleinian groups in the study of the groups of units was started by M. Ruiz [Rui], A. Pita, Á. del Río and M. Ruiz [PdRR] and led to the notion of algebra of Kleinian type and of finite group of Kleinian type. The classification of the finite groups of Kleinian type has been done by E. Jespers, A. Pita, Á. del Río and P. Zalesski, by using again useful information on the Wedderburn components of the corresponding rational group algebras [JPdRRZ]. One of the first applications of the present book is a generalization of these results, obtaining a classification of the group algebras of Kleinian type of finite groups over number fields [OdR3]. This is explained in detail in Chapter 4 of the present book, dedicated to the applications of the Wedderburn decomposition to the study of the group algebras of Kleinian type.

Another important application is to the study of the automorphism group of a semisimple group algebra. The automorphism group of a semisimple algebra can be computed by using the automorphism groups of the simple components of its Wedderburn decomposition. By the Skolem–Noether Theorem, the automorphism group of

every simple component S can be determined by using the automorphism group of the center of S and the group of inner automorphisms of S. These ideas were developed by S. Coelho, E. Jespers, C. Polcino Milies, A. Herman, A. Olivieri, Á. del Río and J.J. Simón in a series of articles [CJP, Her3, OdRS2], where the automorphism group of group algebras of finite groups with rational coefficients is studied. The same type of considerations shows that the Isomorphism Problem for semisimple group algebras can be reduced to the computation of the Wedderburn decomposition of such algebras and to the study of the existence of isomorphisms between the simple components.

On the other hand, the knowledge of the Wedderburn decomposition of a group algebra FG allows one to compute explicitly all two-sided ideals of FG. This has direct applications to the study of error correcting codes, in the case when F is a finite field, since the majority of the most used codes in practice are ideals of group rings. For example, this is the case of cyclic codes, which are exactly the ideals of the group algebras of cyclic groups [PH]. In the last years, some authors have investigated families of group codes having in mind the applications to Coding Theory (see for the example the survey [KS]).

The problem of computing the Wedderburn decomposition of a group algebra FG naturally leads to the problem of computing the primitive central idempotents of FG. The classical method used to do this starts by calculating the primitive central idempotents $e(\chi)$ of $\mathbb{C}G$ associated to the irreducible characters of G, for which there is a well known formula, and continues by summing up all the primitive central idempotents of the form $e(\sigma \circ \chi)$ with $\sigma \in \mathrm{Gal}(F(\chi)/F)$ (see for example Proposition 1.24, Section 1.2). An alternative method to compute the primitive central idempotents of $\mathbb{Q}G$, for G a finite nilpotent group, that does not use the character table of G has been introduced by E. Jespers, G. Leal and A. Paques [JLPa]. A. Olivieri, Á. del Río and J.J. Simón [OdRS1] pointed out that this method relies on the fact that nilpotent groups are monomial and, using a theorem of Shoda [Sho], they gave an alternative presentation. In this way, the method that shows how to produce the primitive central idempotents of $\mathbb{Q}G$, for G a finite monomial group, depends on certain pairs of subgroups (H, K) of G and it was simplified in [OdRS1]. These pairs (H, K) were named *Shoda pairs* of G. Furthermore, A. Olivieri, Á. del Río and J.J. Simón noticed that if a Shoda pair satisfies some additional conditions, then one can describe the simple component associated to such a Shoda pair as a matrix algebra of a specific cyclotomic algebra, that can be easily computed using the arithmetics of H and K as subgroups of G. This new method was the starting point to produce a GAP package, called `wedderga`, able

to compute the Wedderburn decomposition of $\mathbb{Q}G$ for a family of finite groups G that includes all abelian-by-supersolvable groups (see [OdR1], where the main algorithm of the first version of `wedderga` is explained). A similar approach to that presented in [OdRS1] is still valid for F a finite field, provided FG is semisimple (i.e. the characteristic of F is coprime with the order of G), and this was presented by O. Broche Cristo and Á. del Río in the strongly monomial case [BdR]. A survey on central idempotents in group algebras is given by O. Broche Cristo and C. Polcino Milies [BP].

The purpose of present book is to offer an explicit and effective computation of the Wedderburn decomposition of group algebras of finite groups over fields of characteristic zero. The core of the book is the author's Ph.D. thesis [Olt3] on this topic. The method presented here relies mainly on an algorithmic proof of the Brauer–Witt Theorem. The Brauer–Witt Theorem is closely related to the study of the Schur subgroup of the Brauer group, study that was started by I. Schur (1875–1941) in the beginning of the last century. Afterwards, in 1945 R. Brauer (1901–1977) proved that every irreducible representation of a finite group G of exponent n can be realized in every field which contains an n-th primitive root of unity, result that allowed further developments [Bra1]. In the early 1950's, R. Brauer [Bra2] and E. Witt (1911–1991) [Wit] shown independently that questions on the Schur subgroup are reduced to a treatment of cyclotomic algebras. The result has been called the Brauer–Witt Theorem and it can be said that almost all detailed results about Schur subgroups depend on it. During the 1960's, the Schur subgroup had been extensively studied by many mathematicians, who obtained results such as: a complete description of the Schur subgroup for arbitrary local fields and for several cyclotomic extensions of the rational field $\mathbb{Q}$ [Jan2], a simple formula for the index of a p-adic cyclotomic algebra and other remarkable properties of Schur algebras (see [Yam] for an exhaustive and technical account of various results related to this topic).

The book starts with a preliminary chapter, where we gather notation, methods and results used throughout the book. The remaining chapters may by divided into two parts that contain the original results: the first part is dedicated to the explicit computation of the Wedderburn decomposition of groups algebras, and the second one deals with the applications of the presented decomposition to the study of the groups of units of group rings and of the Schur subgroup of an abelian number field, with a special emphasis on the role of the cyclic cyclotomic algebras. Now we present a more detailed contents of each chapter.

Chapter 1 is dedicated to the preliminaries. There we establish the basic notation and we recall concepts and well known results, which will be frequently used throughout the subsequent chapters. The reader who is familiar with the concepts of this chapter can only concentrate on the introduced notation. Our notation and terminology follow closely that of [Mar], [Rei] and [Pie]. The intention was to make it self-contained from the point of view of the theory of central simple algebras, so we tried to gather the necessary ingredients in order to be able to do this. The chapter starts by collecting some basic properties of number fields and orders, since these fields are the base fields in most of our results. Next we recall the basic properties of group algebras FG and representations of finite groups, as well as some results on units of group rings, with special emphasis on their relationship with the Wedderburn decomposition of group algebras. The crossed product algebras are presented as an essential construction for the description of central simple algebras. This description is associated to the so-called Brauer group of a field. In order to understand the structure of the Brauer group of a number field, sometimes it is convenient to start by understanding the Brauer group of local fields. This also presumes a better understanding of the local Schur indices and the Hasse invariants of a central simple algebra seen as an element of the Brauer group of its center. Gathering this local information, we can now have a description of the Brauer group over a number field. The central simple algebras that arise as simple components of group algebras form a subgroup called the Schur subgroup. This is the part of the Brauer group that is directly related to this work. We finish the preliminary chapter by collecting some results on the Schur subgroup.

The first part of the book, dedicated to the Wedderburn decomposition of group algebras contains two chapters that present two aspects of the proposed method for the computation of the Wedderburn components: one more theoretical and the other one more technical from the implementation point of view.

Chapter 2 is dedicated to the presentation of our approach on the Wedderburn decomposition of group algebras. In the first section we recall the useful results obtained by A. Olivieri, Á. del Río and J.J. Simón [OdRS1] on the computation of the primitive central idempotents and the simple components of semisimple group algebras of some special finite groups, namely the monomial and the strongly monomial groups. We will intensively use these results and we will base the constructive approach of the Brauer–Witt Theorem on these types of groups. The second section is mainly focused on the presentation of the classical result due to R. Brauer and E. Witt, together with a proof of the theorem with a computational emphasis. The main goal is to look

for a constructive approach of the theorem, using the strongly monomial characters introduced in [OdRS1], in order to obtain a precise and constructive description of the cyclotomic algebras that appear in the theorem. An algorithmic proof of the Brauer–Witt Theorem obtained by using these strong Shoda pairs is given. These results are published in [Olt2].

Let G be a finite group, χ a complex irreducible character of G and F a field of characteristic zero. The group algebra FG has a unique simple component A such that $\chi(A) \neq 0$. Following T. Yamada's book [Yam], we denote this simple component by $A(\chi, F)$. Moreover, every simple component of FG is of this form for an irreducible character χ of G. The center of $A(\chi, F)$ is $E = F(\chi)$, the field of character values of χ over F and $A(\chi, F)$ represents an element of the Schur subgroup of the Brauer group of E. The Brauer–Witt Theorem states that $A(\chi, F)$ is Brauer equivalent to a cyclotomic algebra over E, that is, a crossed product $(E(\zeta)/E, \tau)$, where ζ is a root of 1, and all the values of the 2-cocycle τ are roots of 1 in $E(\zeta)$. We present a constructive proof of the Brauer–Witt Theorem in four steps. The first step deals with the strongly monomial case, that is, the constructible description of the simple component associated to a strongly monomial character. Then we present the part that gives the reduction of the problem to strongly monomial characters and, furthermore, we show the existence of such strongly monomial characters. The last step gives the desired description of the simple component $A(\chi, F)$ as an algebra Brauer equivalent to a specific cyclotomic algebra by using the corestriction map.

The existent proofs of the Brauer–Witt Theorem (see e.g. [Yam]) rely on the existence, for each prime integer p, of a p-elementary subgroup of G that determines the p-part of a given simple component up to Brauer equivalence, but do not offer an algorithmic method to determine it. This subgroup arises from the use of the Witt–Berman Theorem. Schmid extended the theorem by identifying precise types of p-quasi-elementary groups, which are the minimal groups one can reduce to by using this theorem [Sch]. The fact that the Brauer–Witt Theorem does not provide an algorithmic method to determine sections of G suitable for computing the Schur index for arbitrary finite groups suggested the idea of considering some particular cases of groups for which a constructible method can be done. Some of these approaches are the following. A. Herman considered the case of finite solvable groups that are Clifford reduced over an algebraic number field with respect to a faithful irreducible character [Her2]. For groups with these properties, a character theoretic condition is given that makes the p-part of the division algebra of this simple component to be generated by a predetermined p-quasi-elementary subgroup of the group, for any prime p. This gives a

constructive Brauer–Witt Theorem for groups satisfying this condition. Furthermore, A. Herman [Her5] used the theory of G-algebras with Schur indices, as developed by A. Turull in a series of articles starting with [Tur], to obtain constructive methods for the proof of the Brauer–Witt Theorem.

We are interested in establishing the results for fields F as small as possible, for instance $\mathbb{Q}(\chi)$, for (every) irreducible character χ of the finite group G. The reason is that if L is a field containing F, then $A(\chi, L) = L(\chi) \otimes_{F(\chi)} A(\chi, F)$ and, therefore, the cyclotomic structure of $A(\chi, F)$ up to Brauer equivalence determines the cyclotomic structure of $A(\chi, L)$ as an algebra Brauer equivalent to the crossed product $(L(\chi)(\zeta)/L(\chi), \tau)$. The last section of the chapter gives a theoretical algorithm for the computation of the Wedderburn decomposition of group algebras that uses the previously presented algorithmic approach of the Brauer–Witt Theorem.

The theoretical algorithm for the computation of the Wedderburn decomposition of a cyclic algebra, introduced in Chapter 2, is not exactly the implemented one. The main reason is that there are more efficient alternatives for the search of the sections that give rise to the simple components. In Chapter 3 we explain some aspects of the implementation of our algorithm in the `wedderga` package for the computer system GAP [BKOOdR]. The presented working algorithm is more appropriate for our computational purposes than the previously presented theoretical algorithm. In our presentation we try to avoid some technical aspects of the development of the software and we focus more on the mathematical aspects of the implementation of the chosen strategy. Hence, the algorithm is still not the real one, but it is closer to it and gives an idea about the steps to be followed in order to be able to implement it. This version of `wedderga` upgrades a previous form of the package. In order to give an idea of its usefulness, we include various examples, the computations of which have been made by using the `wedderga` package. In some examples it is given a complete description of the Wedderburn decomposition of the considered group algebra FG. In some other examples it is given a description of the simple component corresponding only to an irreducible character χ of the group G. The new implementation is able to compute the Wedderburn decomposition of a semisimple algebra FG for those fields F which allow GAP to realize effective computations, that is, essentially abelian number fields and finite fields. For a better understanding of other aspects of the package we have included the complete manual of `wedderga` in the Appendix at the end of the book. We would like to thank all the authors of `wedderga` for their contribution to the construction of the package, and especially to A. Konovalov who helped us to solve many technical problems during the programming and optimization process. The implementation of

this new part of the `wedderga` package is joint work with Á. del Río, and the theoretical background is presented in [OdR2].

The second part of the book is dedicated to the applications of the explicit computation of the Wedderburn decomposition of group algebras that we have proposed, mainly to group algebras of Kleinian type, groups of units and Schur groups.

In Chapter 4 we establish some applications of the explicit computation of the Wedderburn decomposition of group algebras to the study of group algebras of Kleinian type KG and to the units of RG for R an order in K. These algebras are finite dimensional semisimple rational algebras A such that the group of units of an order in A is commensurable with a direct product of Kleinian groups. The finite groups of Kleinian type were introduced by M. Ruiz, A. Pita and Á. del Río in [Rui] and [PdRR] as a class of finite groups that make possible the use of geometrical methods in hyperbolic spaces in order to provide presentations of groups commensurable with the group of units of $\mathbb{Z}G$. The finite groups of Kleinian type were classified by E. Jespers, A. Pita, Á. del Río, M. Ruiz and P. Zalesski in [JPdRRZ] and characterized in terms of the Wedderburn decomposition of the group algebra with rational coefficients. It can be said that all known results that provide a very explicit description on the structure of $\mathcal{U}(\mathbb{Z}G)$ are included in the result that characterizes the finite groups G of Kleinian type as the ones with $\mathcal{U}(\mathbb{Z}G)$ virtually a direct product of free-by-free groups. The concept of finite group of Kleinian type comes from a property of the group algebra with rational coefficients that makes sense when changing the field of rationals with an arbitrary number field. The algebras with this property are called group algebras of Kleinian type. The origin of the study included in this chapter comes from a question of A. Reid, asking about groups of units of group rings RG, with R the ring of integers of a number field K, in case KG is of Kleinian type. In this chapter we classify the Schur algebras of Kleinian type, as a first step needed later on in order to characterize the group algebras of Kleinian type. As an application of this classification, we were able to extend various results about the units of $\mathbb{Z}G$ to the case of the group rings RG, with R an order in a number field. In this way, we characterize when the group of units of RG is finite, virtually abelian, virtually a direct product of free groups and virtually a direct product of free-by-free groups. This part is published in [OdR3].

In Chapter 5 we study the Schur group of an abelian number field K, that is, a subfield of a finite cyclotomic extension of the rationals. The results of this chapter were produced as instruments to be applied in Chapter 6, where we need to know the maximum of the local indices of a Schur algebra over such fields K. The approach is

to consider separately the Schur algebras of index a power of p, for every prime p. The cases of p odd or $\zeta_4 \in K$ were studied by G.J. Janusz in [Jan3], and the remaining case by J.W. Pendergrass [Pen1]. In our analysis of these results and their applications to the problem studied in Section 6.2, we discovered that Pendergrass results are not correct, as a consequence of errors in the calculations of 2-cocycles. This led us to checking the proofs of Janusz and Pendergrass, obtaining a new approach. In our approach we correct the errors in [Pen1] and we provide a more conceptual presentation of the results that the one in [Jan3] and [Pen1]. In order to be able to do this, we embed the field K in a special cyclotomic field, bigger than the one considered by Janusz and Pendergrass, avoiding in this way the artificial-looking results presented by them. In fact, the results of this chapter were developed in view of the applications in the next chapter. As a consequence of the Benard–Schacher Theorem, $S(K) = \bigoplus_p S(K)_p$, where p runs over the primes p such that K contains a primitive p-th root of unity ζ_p, and $S(K)_p$ is the p-primary component of $S(K)$. Moreover, if A is a Schur algebra and R_1 and R_2 are two primes of K such that $R_1 \cap \mathbb{Q} = \mathbb{R}_2 \cap \mathbb{Q} = r\mathbb{Z}$, for r a rational prime number, then the local indices of A in R_1 and R_2 are equal, and it makes sense to denote this common local index by $m_r(A)$. Hence, in order to compute the maximum local index of Schur algebras with center K, it is enough to calculate $\beta_p(r)$, where $p^{\beta_p(r)} = \max\{m_r(A) : [A] \in S(K)_p\}$, for every prime p with $\zeta_p \in K$ and r a rational prime number. The case of $r = \infty$ is easy and it depends on K being included in $\mathbb{R}$ or not. Theorem 5.13 provides an explicit value for $\beta_p(r)$, in the case of r odd. The case $r = 2$ can be obtained by using results of Janusz [Jan1].

In Chapter 6 we introduce the notion of cyclic cyclotomic algebra and we study some of its properties. A cyclic cyclotomic algebra is a cyclic algebra $(K(\zeta)/K, \sigma, \xi)$, with ζ and ξ roots of unity. Notice that a cyclic cyclotomic algebra is an algebra that has at the same time a representation as cyclic algebra and as cyclotomic algebra. Moreover, every element of the Schur subgroup is represented, on one hand by a cyclotomic algebra (by the Brauer–Witt Theorem) and, on the other hand by a cyclic algebra (by a classical result from Class Field Theory). However, it is not true in general that every element of the Schur group is represented by a cyclic cyclotomic algebra.

In the first section we study when two cyclic cyclotomic algebras over abelian number fields are isomorphic. The main motivation for this study is based on its applications to the study of the automorphisms of a group algebra and the Isomorphism Problem for group algebras. The reason is that the problem of describing the automorphism group of a semisimple group algebra FG reduces to two problems: first compute the Wedderburn decomposition of FG and second, decide which pairs of this decomposition

are isomorphic. Also the Isomorphism Problem between two group algebras can be obviously reduced to that of deciding if the simple components of the given algebras can be put in isomorphic pairs. Note that the isomorphism concept here is the ring isomorphism and not the algebra isomorphism. An algorithmic method for the computation of the Wedderburn decomposition of $\mathbb{Q}G$ for G a metacyclic group has been obtained in [OdRS2]. That method provides a precise description of each simple component in terms of the numerical parameters that determine the group, that is, m, n, r and s which appear in a presentation of the form $G = \langle a, b | a^m = 1, b^n = a^s, bab^{-1} = a^r \rangle$. However, to decide if two simple components are isomorphic is more difficult, and in [OdRS2] this problem has been solved only in the case when n is a product of two primes. The case of n being prime has been studied before by A. Herman [Her3]. Two simple algebras are isomorphic as algebras if and only if they have the same center, the same degree and the same local invariants. In this case, the algebras are isomorphic as rings, but the converse is not true. In the first section of Chapter 6 we show that two cyclic cyclotomic algebras over an abelian number field are isomorphic if and only if they have the same center, the same degree and the same list of local Schur indices at all rational primes. We provide an example that shows that this result cannot be extended to arbitrary cyclotomic algebras.

The classes of the Brauer group of a field K that contain cyclic cyclotomic algebras generate a subgroup $CC(K)$ of the Schur group $S(K)$. In many cases this subgroup is exactly the Schur group. For example, this is the case if K is a cyclotomic extension of the rationals. Nevertheless, as we show in the second section of Chapter 6, in general $CC(K) \neq S(K)$. In this section we study the gap between $CC(K)$ and $S(K)$. More precisely, we characterize when $CC(K)$ has finite index in the Schur group $S(K)$ in terms of the relative position of K in the lattice of cyclotomic extensions of the rationals. We consider a tower of fields $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\zeta)$, where ζ is a root of unity that we precisely define depending on K. That $[S(K) : CC(K)]$ is finite or not, depends on the fact that every element of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ satisfies a property which is easy to check by computations on the Galois groups $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ and $\mathrm{Gal}(\mathbb{Q}(\zeta)/K)$ (see Theorem 6.8). We also provide relevant examples covering the reasonable cases. The results of the last two chapters are joint work with Á. del Río and A. Herman and are contained in the papers [HOdR1], [HOdR2] and [HOdR3].

We end the book with a few brief conclusions on the advances of this work and we also give some perspectives for further investigations. We want to point out that the study of different aspects of classical problems like the Wedderburn decomposition of semisimple algebras can still provide useful new information with applications in active

topics of research.

I would like to thank all the collaborators of this work and especially Professor Ángel del Río for all the work, time, dedication and hospitality during my stay at the University of Murcia, Spain.

This work was partially supported by the Romanian PN-II-ID-PCE-2007-1 project ID_532, contract no. 29/28.09.2007.

Gabriela Olteanu

Cluj–Napoca, May 2008

Notation

Throughout G is a group, R an associative ring with identity, K a field, $K \leq L$ a field extension, A a central simple K-algebra, p a prime number and χ a character of G. We set the following notation.

$\mathrm{Aut}(G)$	=	automorphism group of G
$\mathrm{Cen_G(H)}$	=	centralizer of a subgroup H of G
$N_G(H)$	=	normalizer of a subgroup H of G
x^g	=	$g(x)$, where $g \in \mathrm{Aut}(G)$ and $x \in G$
x^g	=	conjugate $g^{-1}xg$ of $x \in G$ by $g \in G$
H^g	=	$\{g^{-1}xg \mid x \in H\}$, where $H \leq G$ and $g \in G$
$\lvert g \rvert$	=	order of the element $g \in G$
$[x, y]$	=	commutator $x^{-1}y^{-1}xy$ of the elements $x, y \in G$
ζ_n	=	complex n-th root of unity
$N \rtimes H$	=	semidirect product of the group N by H
$\mathrm{Char}(G)$	=	set of complex characters of G
$\mathrm{Irr}(G)$	=	set of irreducible complex characters of G
χ_H	=	restriction of the character χ of G to some subgroup H of G
χ^G	=	character induced to G by the character χ of some subgroup of G
$\mathcal{U}(R)$ or R^*	=	group of units of R
$\mathcal{O}_K$	=	ring of algebraic integers of a number field K
$[L : K]$	=	degree of the extension $L \leq K$
$\mathrm{Gal}(L/K)$	=	Galois group of the field extension $L \leq K$
RG	=	group ring of G with coefficients in R
$R *_\tau^\alpha G$	=	crossed product of G with coefficients in R, action α and twisting τ
KG	=	group algebra of G with coefficients in K

$(L/K,\tau)$	=	crossed product algebra $L *_\tau^\alpha \mathrm{Gal}(L/K)$, where L/K is finite Galois, α is the natural action and τ is a 2-cocycle
$(K(\zeta_n)/K,\tau)$	=	cyclotomic algebra over K
$(L/K,\sigma,a)$	=	cyclic algebra over K, with $\mathrm{Gal}(L/K)=\langle\sigma\rangle$, $a\in K^*$
$\left(\frac{a,b}{K}\right)$	=	quaternion algebras $K[i,j\|i^2=a,j^2=b,ji=-ij]$, with $a,b\in K^*$
$\mathbb{H}(K)$	=	quaternion algebra $\left(\frac{-1,-1}{K}\right)$
$K(\chi)$	=	field of character values over K of χ (i.e. $K(\chi(g):g\in G)$)
$e(\chi)$	=	primitive central idempotent of $\mathbb{C}G$ determined by χ
$e_{\mathbb{Q}}(\chi)$	=	primitive central idempotent of $\mathbb{Q}G$ determined by χ
$\mathrm{Br}(K)$	=	Brauer group of K
$\mathrm{Br}(L/K)$	=	relative Brauer group of K with respect to L
$[A]$	=	equivalence class in the Brauer group containing the algebra A
$A(\chi,K)$	=	simple component of KG corresponding to χ
$S(K)$	=	Schur subgroup of the Brauer group $\mathrm{Br}(K)$
$CC(K)$	=	subgroup of $S(K)$ generated by cyclic cyclotomic algebras over K
$H^n(G,M)$	=	n-th cohomology group of G with coefficients in M
Res	=	restriction map
Cor	=	corestriction or transfer map
Inf	=	inflation map
$\deg(A)$	=	degree of A
$\exp(A)$	=	exponent of A
$\mathrm{ind}(A)$	=	Schur index of A
$m_K(\chi)$	=	Schur index of χ over K
$m_p(\chi)$	=	p-local index corresponding to χ
$\mathrm{inv}(A)$	=	Hasse invariant of A
$\mathbb{Z}_p$	=	p-adic integers
$e(L/K,P)$	=	ramification index of L/K at the prime P
$f(L/K,P)$	=	residue degree of L/K at the prime P
$N_{L/K}$	=	norm of the extension L/K
$\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$	=	sets of natural numbers, integers, rational numbers, real numbers and complex numbers respectively

Chapter 1

Preliminaries

In this chapter we gather the needed background. We establish the notation and we introduce the basic concepts to be used throughout this work. We also recall some well known results that will be needed in the subsequent chapters. In most cases we will not provide a proof, but we will give classical references where it can be found. The reader who is familiar with the concepts of this chapter can only concentrate on the introduced notation.

1.1 Number fields and orders

In this section we present classical information on number field and orders. These fields are the base fields in most of our results. The results in this section are mainly from [Mar].

Definition 1.1. A *(algebraic) number field* K is a finite extension of the field $\mathbb{Q}$ of rational numbers.

Every such field has the form $\mathbb{Q}(\alpha)$ for some algebraic number $\alpha \in \mathbb{C}$. A complex number is called an *algebraic integer* if it is a root of some monic polynomial with coefficients in $\mathbb{Z}$. The set of algebraic integers in $\mathbb{C}$ is a ring, which we will denote by the symbol $\mathbb{A}$. In particular $\mathbb{A} \cap K$ is a subring of K for any number field K, that we refer as the *number ring* corresponding to K or the *ring of integers* of K.

Let K be a number field of degree n over $\mathbb{Q}$. There are exactly n embeddings (i.e. field homomorphisms) of K in $\mathbb{C}$. These are easily described by writing $K = \mathbb{Q}(\alpha)$ for some α and observing that α can be sent to any one of its n conjugates over $\mathbb{Q}$, i.e. the roots of the minimal polynomial over $\mathbb{Q}$. Each conjugate β determines a unique embedding of K in $\mathbb{C}$ by $f(\alpha) \mapsto f(\beta)$ for every $f \in \mathbb{Q}[X]$, and every embedding must arise in this way since α must be sent to one of its conjugates.

We refer to the field homomorphisms $K \to \mathbb{R}$ as *real embeddings* of K. A pair of *complex embeddings* of K is, by definition, a pair of conjugate field homomorphisms $K \to \mathbb{C}$ whose images are not embedded in $\mathbb{R}$.

Let n be a positive integer. Throughout the book, ζ_n will denote a complex primitive root of unity of order n. The field $\mathbb{Q}(\zeta_n)$ is called the n-th *cyclotomic field*. L. Kronecker (1821–1891) observed that certain abelian extensions (i.e. normal with abelian Galois group) of imaginary quadratic number fields are generated by the adjunction of special values of automorphic functions arising from elliptic curves. Kronecker wondered whether all abelian extensions of K could be obtained in this manner (Kronecker's Jugendtraum). This leads to the question of "finding" all abelian extensions of number fields that is nowadays the study object of Class Field Theory. Kronecker conjectured and Weber proved:

Theorem 1.2 (Kronecker–Weber). *Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension of $\mathbb{Q}$.*

Number rings are not always unique factorization domains, that is, elements may not factor uniquely into irreducibles. However, we will see that the nonzero ideals in a number ring always factor uniquely into prime ideals. This can be regarded as a generalization of unique factorization in $\mathbb{Z}$, where the ideals are just the principal ideals (n) and the prime ideals are the ideals (p), where p is a prime integer. Number rings have three special properties and that any integral domain with these properties also has the unique factorization property for ideals. Accordingly, we have the following definition.

Definition 1.3. A *Dedekind domain* is an integral domain R such that the following conditions hold:

(1) Every ideal is finitely generated;

(2) Every nonzero prime ideal is a maximal ideal;

(3) R is integrally closed in its field of fractions K, that is, if $\alpha/\beta \in K$ is a root of a monic polynomial over R, then $\alpha/\beta \in R$, i.e. β divides α in R.

Every ideal in a Dedekind domain is uniquely representable as a product of prime ideals and every number ring is a Dedekind domain, hence the ideals in a number ring factor uniquely into prime ideals.

There are example of primes in $\mathbb{Z}$ which are not irreducible in a larger number ring. For example $5 = (2+i)(2-i)$ in $\mathbb{Z}[i]$. And although 2 and 3 are irreducible in $\mathbb{Z}[\sqrt{-5}]$, the corresponding principal ideals (2) and (3) are not prime ideals: $(2) = (2, 1+\sqrt{-5})^2$

and $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$. This phenomenon is called *splitting*. Slightly abusing notation, we say that 3 *splits* into the product of two primes in $\mathbb{Z}[\sqrt{-5}]$ (or in $\mathbb{Q}[\sqrt{-5}]$, the ring being understood to be $\mathbb{A} \cap \mathbb{Q}[\sqrt{-5}] = \mathbb{Z}[\sqrt{-5}]$).

We consider the problem of determining how a given prime splits in a given number field. More generally, if P is any prime ideal in any ring of integers $R = \mathbb{A} \cap K$, for K a number field, and if L is a number field containing K, we consider the prime decomposition of the ideal generated by P in the ring of integers $S = \mathbb{A} \cap L$, which is PS. The term "prime" will be used to mean "non-zero prime ideal".

Theorem 1.4. *Let P be a prime of R and Q a prime of S. Then $Q|PS$ if and only if $Q \supset PS$ if and only if $Q \cap R = P$ if and only if $Q \cap K = P$.*

When one of the previous equivalent conditions holds, we say that Q *lies above* (or *over*) P or that P *lies under* (or *divides*) Q. It can be proved that every prime Q of S lies above a unique prime P of R and every prime P of R lies under at least one prime Q of S.

The primes lying above a given prime P are the ones which occur in the prime decomposition of PS. The exponents with which they occur are called the *ramification indices*. Thus, if Q^e is the exact power of Q dividing PS, then e is the *ramification index* of Q over P, denoted by $e(Q|P)$ or by $e(L/K, P)$.

Example 1.5. Let $R = \mathbb{Z}$ and $S = \mathbb{Z}[i]$. The principal ideal $(1-i)$ in S lies over 2 (we really mean $2\mathbb{Z}$ when we are writing 2) and is a prime ideal. Then $2S = (1-i)^2$, hence $e((1-i)|2) = 2$. On the other hand $e(Q|p) = 1$ whenever p is an odd prime and the prime Q lies over p.

More generally, if $R = \mathbb{Z}$ and $S = \mathbb{Z}[\zeta_m]$, where $m = p^r$ for some prime $p \in \mathbb{Z}$, then the principal ideal $(1-\zeta_m)$ in S is a prime ideal lying over p and $e((1-\zeta_m)|p) = \varphi(m) = p^{r-1}(p-1)$, where φ denotes the Euler function. On the other hand, $e(Q|q) = 1$ whenever q is a prime different from p and Q lies over q.

There is another important number associated with a pair of primes P and Q, Q lying above P in an extension $K \leq L$ of number fields. The factor rings R/P and S/Q are fields since P and Q are maximal ideals. There is an obvious way in which R/P can be viewed as a subfield of S/Q: the inclusion of R in S induces a ring homomorphism $R \to S/Q$ with kernel $R \cap Q = P$, so we obtain an embedding $R/P \to S/Q$. These are called the *residue class fields* associated with P and Q and are denoted by $\widehat{R} = R/P$ and $\widehat{S} = S/Q$. We know that they are finite fields, hence $\widehat{S}$ is an extension of finite degree f over $\widehat{R}$. Then f is called the *inertia degree* of Q over P and is denoted by $f(Q|P)$ or $f(L/K, P)$.

Example 1.6. Let again $R = \mathbb{Z}$ and $S = \mathbb{Z}[i]$ and consider the prime 2 in $\mathbb{Z}$ lying under the prime $(1-i)$ in $\mathbb{Z}[i]$. $S/2S$ has order 4, and $(1-i)$ properly contains $2S$, therefore $|S/(1-i)|$ must be a proper divisor of 4, and the only possibility is 2. So R/P and S/Q are both fields of order 2 in this case, hence $f = 1$. On the other hand, $3S$ is a prime in S and $|S/3S| = 9$, so $f(3S|3) = 2$.

Theorem 1.7. *Let n be the degree $[L : K]$, for K, L, R, S as before and let $Q_1, \ldots, Q_r$ be the primes of S lying over a prime P of R. Denote by $e_1, \ldots, e_r$ and $f_1, \ldots, f_r$ the corresponding ramification indices and inertial degrees. Then $\sum_{i=1}^{r} e_i f_i = n$.*

Corollary 1.8. *With the above notation, if $[L : K] = 2$, that is, L is a quadratic extension of K, there are only three possibilities for the numbers e_i and f_i:*

(1) *$e_1 = e_2 = 1$, $f_1 = f_2 = 1$, $P = Q_1 Q_2$, with $Q_1 \neq Q_2$ and we say that P splits;*

(2) *$e = 1$, $f = 2$, $P = Q$ and we say that P is inert;*

(3) *$e = 2$, $f = 1$, $P = Q^2$ and we say that P ramifies.*

The discriminant D of a quadratic extension $\mathbb{Q}(\sqrt{d})$, with d a square-free positive integer is $D = d$, if $d \equiv 1(\mod 4)$, and $D = 4d$ otherwise. The three options of Corollary 1.8 that give the type of decomposition of a prime number p are determined by the discriminant.

Theorem 1.9. *Let p be a prime number and let L be a quadratic extension of the rationales with discriminant D. Then*

(1) *p ramifies in L if and only if p divides D;*

(2) *If p is odd and coprime with D, then p splits in L if and only if D is a square modulo p;*

(3) *If $p = 2$ and D is odd, then 2 splits in L if and only if D is a square modulo 8.*

If L is a normal extension of K and P is a prime of $R = \mathbb{A} \cap K$, the Galois group $\mathrm{Gal}(L/K)$ permutes transitively the primes lying over P, that is, if Q is such a prime and $\sigma \in \mathrm{Gal}(L/K)$, then $\sigma(Q)$ is a prime ideal in $\sigma(S) = S$, lying over $\sigma(P) = P$, and if Q and Q' are two primes of S lying over the same prime P of R, then $\sigma(Q) = Q'$ for some $\sigma \in \mathrm{Gal}(L/K)$. Moreover, $e(Q|P) = e(Q'|P)$ and $f(Q|P) = f(Q'|P)$. Hence, in the normal case, a prime P of R splits into $(Q_1 Q_2 \cdots Q_r)^e$ in S, where the Q_i are the distinct primes, all having the same inertial degree f over P. Moreover, $ref = [L : K]$ by Theorem 1.7.

Definition 1.10. Let K, L, R and S be as before. We say that the prime P is *unramified* in L/K if $e(L/K, P) = 1$ and S/Q is a separable extension of R/P for all the distinct primes Q of S lying above P. A prime P of R is *ramified* in S (or in L) if and only if $e(Q|P) > 1$ for some prime Q of S lying above P. (In other words, PS is not square-free.) The prime P is *totally ramified* in S or in L if and only if $PS = Q^n$, where $n = [L : K]$.

Lemma 1.11. *If R is a Dedekind domain with quotient field K, P is a prime of R and P does not divide Rm, then P is unramified in the extension $K(\zeta_m)$ of K.*

Definition 1.12. Let K, L, R and S be as before and fix a prime P of R. A finite extension L/K of number fields is called: *unramified at P* if $\widehat{S}/\widehat{R}$ is a separable extension and $e(L/K, P) = 1$; *completely* (or *totally*) *ramified at P* if $f(L/K, P) = 1$ or equivalently $\widehat{S} = \widehat{R}$; *tamely ramified at P* if $\widehat{S}/\widehat{R}$ is a separable extension and $p \nmid e(L/K, P)$ where $p > 0$ is the characteristic of the finite field $\widehat{R}$; *wildly ramified at P* if $\widehat{S} = \widehat{R}$ and the degree of the extension L/K is a power of p, which is the characteristic of $\widehat{R}$.

We now introduce the notion of R-order in a finite dimensional K-algebra, for R a Dedekind domain with quotient field K.

Definition 1.13. An *R-order* in the finite dimensional K-algebra A is a subring Δ of A which is a finitely generated R-module and contains a K-basis of A, i.e. $K\Delta = A$. A *maximal* R-order in A is an R-order which is not properly contained in any other R-order in A.

Example 1.14. Let us give some examples of orders. Let K be a number field and R its ring of integers.

(1) R is the unique maximal R-order of K.

(2) $M_n(R)$ is a maximal R-order in the algebra $M_n(K)$.

(3) If G is a finite group, let RG be its group ring over R and KG its group algebra over K (for the definitions see the next section). Then RG is an R-order in KG.

We say that two subgroups of a given group are *commensurable* if their intersection has finite index in both of them. The following lemma from [Seh] offers a useful property in the study of units in group rings, as we will see in a forthcoming section dedicated to them.

Lemma 1.15. *If Δ and Δ' are two orders in a finite dimensional K-algebra, then the groups of units of Δ and Δ' are commensurable. Therefore, if S is any order in a group algebra KG, then the unit groups of S and RG are commensurable.*

1.2 Group algebras and representations

Now we introduce group algebras, or more general group rings, as main algebraic structures in this work.

Definition 1.16. Let R be a ring and G a group. The *group ring* RG of G with coefficients in R is defined as the free R-module having G as basis, with the product defined by

$$r_1g_1 \cdot r_2g_2 = (r_1r_2)(g_1g_2),$$

for $r_1, r_2 \in R$ and $g_1, g_2 \in G$ and extended by linearity. Therefore, RG is the ring whose elements are all formal sums $\sum_{g\in G} r_g g$, with each coefficient $r_g \in R$ and all but finitely many of the coefficients equal zero. Addition is defined component-wise and the multiplication is given by

$$\left(\sum_{g\in G} r_g g\right)\left(\sum_{g\in G} q_g g\right) = \sum_{g\in G}\left(\sum_{uv=g} r_u q_v\right) g.$$

If $R = F$ is a field, then FG is called a *group algebra*.

One can think of R and G as being contained in RG through the applications $r \mapsto r1_G$ and $g \mapsto 1g$, for $r \in R$, $g \in G$ and 1_G the identity of G. The element 11_G is the identity of RG and it is denoted by 1.

The function $\omega : RG \to R$ given by $\sum_{g\in G} r_g g \mapsto \sum_{g\in G} r_g$ is a ring homomorphism called the *augmentation* of RG. Its kernel

$$\Delta_R(G) = \{\sum_{g\in G} r_g g \in RG : \sum_{g\in G} r_g = 0\}$$

is called the *augmentation ideal* of RG. More generally, for N a normal subgroup of G, there exists a natural homomorphism $\omega_N : RG \to R(G/N)$ given by $\sum_{g\in G} r_g g \mapsto \sum_{g\in G} r_g gN$. The kernel of ω_N is given by

$$\Delta_R(G,N) = \{\sum_{g\in G} r_g g \in RG : \sum_{x\in N} r_{gx} = 0 \text{ for all } g \in G\} = \sum_{n\in N} RG(n-1) = \sum_{n\in N} (n-1)RG.$$

In particular, $\Delta_R(G) = \Delta_R(G,G)$.

If H is a finite subgroup of G, we denote $\widehat{H} = \frac{\sum_{h\in H} h}{|H|} \in \mathbb{Q}G$. Notice that $\widehat{H}$ is an idempotent of $\mathbb{Q}G$. Moreover, $\widehat{H}$ is contained in the center of $\mathbb{Q}G$ precisely when H is normal in G. In this case, it can be showed that $\Delta_{\mathbb{Q}}(G,H) = \{a \in \mathbb{Q}G | a\widehat{H} = 0\}$, hence $\mathbb{Q}(G/H) \cong (\mathbb{Q}G)\widehat{H}$.

We are mainly interested in a special type of group algebras, namely semisimple group algebras FG. The semisimple group algebras are characterized by the following classical theorem, which can be given even more generally, for group rings.

Theorem 1.17 (Maschke). *The group ring RG is semisimple if and only if R is semisimple, G is finite and the order of G is a unit in R.*

The theoretical description of the structure of semisimple group algebras is given by the following classical theorem.

Theorem 1.18 (Wedderburn–Artin). *Every semisimple artinian ring is a direct sum of matrix rings over division rings.*

The decomposition of the algebra in this way is usually called *Wedderburn decomposition* and the simple components are called *Wedderburn components*. A more structural description of the Wedderburn components of a semisimple group algebra in terms of cyclotomic algebras up to Brauer equivalence in the corresponding Brauer group is the object of the second chapter of the book.

The simple components in the Wedderburn decomposition of a group algebra FG are parameterized by the irreducible characters of the group G. We present some basic information about representations and characters of a finite group G and of a corresponding group algebra FG.

Definition 1.19. If G is a finite group and F is a field, then an *F-representation* of G is a group homomorphism $\rho : G \to \mathrm{GL}(V)$, where V is a finite dimensional F-vector space called the representation space of ρ. The *degree* $\deg(\rho)$ of the representation ρ is the dimension $\dim_F(V)$ of V. A *matrix F-representation* of G is a group homomorphism $\rho : G \to \mathrm{GL}_n(F)$ for some positive integer n. The integer n is the *degree* of the representation and is denoted by $\deg(\rho)$. Using linear algebra, one can establish an obvious parallelism between F-representations and matrix F-representations. We use vectorial or matricial representations as suitable for each situation.

If G is a finite group and F is a field, denote by $\mathrm{rep}_F(G)$ the category of F-representations of G. Similarly, one can define the category of matrix F-representations of G, which is equivalent to the category $\mathrm{rep}_F(G)$. Note that every F-representation $\rho : G \to \mathrm{GL}(V)$ of a finite group extends uniquely by F-linearity to an algebra representation $\widehat{\rho} : FG \to \mathrm{End}_F(V)$, and so the category $\mathrm{rep}_F(G)$ of group representations of G is equivalent to the category $\mathrm{rep}(FG)$ of representations of the group algebra FG (i.e. of left FG-modules which are finite dimensional over F).

Definition 1.20. The *F-character* of the group G afforded by the matrix F-representation $\rho : G \to \mathrm{GL}_n(F)$ is the map $\chi : G \to F$ given by $\chi(g) = \mathrm{tr}(\rho(g))$, where tr denotes the trace map from $GL_n(F)$ to F.

An F-representation of G is *irreducible* if the associated module is simple, that is, it is non-zero and the only submodules of it are the trivial ones. An *F-irreducible character* is a character afforded by an irreducible representation.

If $F = \mathbb{C}$, the field of complex numbers, we name the $\mathbb{C}$-characters simply characters. Hence, in what follows, the word "character" means $\mathbb{C}$-character unless otherwise stated. Denote by $\mathrm{Irr}(G)$ the set of all irreducible characters of G. If χ is any character of G afforded by a representation corresponding to a $\mathbb{C}G$-module M, we can decompose M into a direct sum of irreducible modules. It follows that every character χ of G can be uniquely expressed in the form $\chi = \sum_{\chi_i \in \mathrm{Irr}(G)} n_i \chi_i$, where n_i are non-negative integers. Those χ_i's with $n_i > 0$ are called the irreducible *constituents* of χ and the n_i's are the *multiplicities* of χ_i as constituents of χ.

If χ is a character of G, then $\chi(1) = \deg(\rho)$, where ρ is a representation of G which affords χ. We call $\chi(1)$ the *degree* of χ. A character of degree 1 is called *linear character*. Let F be a subfield of the complex field $\mathbb{C}$ and χ be a character. We write $F(\chi)$ to denote the minimal extension of F that contains the character values $\chi(g)$ for $g \in G$ and we call it the *field of character values* of χ over F. A field $\mathbb{Q} \subset F \subset \mathbb{C}$ is a *splitting field* for G if every irreducible character of G is afforded by some F-representation of G.

Theorem 1.21 (Brauer). *Let G have exponent n and let $F = \mathbb{Q}(\zeta_n)$. Then F is a splitting field for G.*

If H is a subgroup of G, F is a field and ρ is an F-representation of H with associated module ${}_{FH}M$, then the *induced representation* of ρ to G, denoted by ρ^G, is defined as the associated F-representation to the FG-module $FG \otimes_{FH} M$, denoted M^G. If ψ is the character afforded by ρ, we define the *induced character* of ψ to G, denoted by ψ^G, as the afforded character by ρ^G. A straightforward calculation shows that

$$\psi^G(g) = \sum_{x \in T} \overline{\psi}(g^x), \tag{1.1}$$

where T is a left transversal of H in G and $\overline{\psi}(h) = \begin{cases} \psi(h)\,, & \text{if } h \in H \\ 0\,, & \text{if } h \notin H. \end{cases}$

Let χ be a complex irreducible character of the group G and F a field of characteristic zero. The Wedderburn component of the group algebra FG corresponding to χ is the unique simple ideal I of FG such that $\chi(I) \neq 0$. Following [Yam], we denote this simple algebra by $A(\chi, F)$. The center of the simple algebra $A(\chi, F)$ is $\mathbb{F} = F(\chi)$, the field of character values of χ over F and $A(\chi, F)$ represents an element of the Schur subgroup of the Brauer group of $\mathbb{F}$ as we will see in a subsequent section of this chapter. If L is a field extension of F then $A(\chi, L) = L(\chi) \otimes_{\mathbb{F}} A(\chi, F)$ and, therefore, the structure of $A(\chi, F)$ up to Brauer equivalence determines the structure of $A(\chi, L)$. Thus, we try to consider F as small as possible, for instance the field of rational numbers $\mathbb{Q}$.

The number of factors in the Wedderburn decomposition coincides with the number of irreducible $\mathbb{F}$-characters of G and, equivalently, with the number of isomorphism classes of simple $\mathbb{F}G$-modules. In particular, the number of factors in the Wedderburn decomposition of $\mathbb{C}G$ is equal to the cardinality of $\mathrm{Irr}(G)$ and to the number of conjugacy classes of G. The number of irreducible rational characters is given by the following theorem (e.g. see [CR]).

Theorem 1.22 (Artin). *The number of irreducible rational characters of a finite group G (or equivalently the number of simple components in the Wedderburn decomposition of $\mathbb{Q}G$) coincides with the number of conjugacy classes of cyclic subgroups of the group G.*

Recall that an element e of a ring is a *primitive central idempotent* if $e^2 = e \neq 0$, e is central and it cannot be expressed as a sum of central orthogonal idempotents. If χ is an irreducible complex character of the group G, then by the primitive central idempotent of $\mathbb{C}G$ associated to χ we mean the unique primitive central idempotent e of $\mathbb{C}G$ such that $\chi(e) \neq 0$, and we denote it by $e(\chi)$. Similarly, for F a field of characteristic zero, the primitive central idempotent of FG associated to χ, denoted $e_F(\chi)$, is the unique primitive central idempotent of FG such that $\chi(e_F(\chi)) \neq 0$.

The following proposition is a classical result of character theory for the computation of the primitive central idempotent $e(\chi)$.

Proposition 1.23. *Let G be a finite group and $\chi \in \mathrm{Irr}(G)$. Then $e(\chi)$, the primitive central idempotent of $\mathbb{C}G$ associated to χ, is given by the formula*

$$e(\chi) = \frac{\chi(1)}{|\ G\ |} \sum_{g \in G} \chi(g^{-1})g. \tag{1.2}$$

By the orthogonality relations for characters one has that $\chi(e(\chi)) = \chi(1)$ and $\psi(e(\chi)) = 0$ for any irreducible complex character ψ of G different from χ.

For the computation of the primitive central idempotents of FG, with F a field of characteristic zero, the classical method is to calculate the primitive central idempotents $e(\chi)$ of $\mathbb{C}G$ associated to the irreducible characters of G and then sum up all the primitive central idempotents of the form $e(\sigma \circ \chi)$ with $\sigma \in \mathrm{Gal}(F(\chi)/F)$ and $\chi \in \mathrm{Irr}(G)$ (see e.g. [Yam]).

Proposition 1.24. *For G a finite group and χ an irreducible complex character of G, $e_F(\chi)$ is given by the formula*

$$e_F(\chi) = \sum_{\sigma \in \mathrm{Gal}(F(\chi)/F)} e(\chi^\sigma) \tag{1.3}$$

where χ^σ is the character of G given by $\chi^\sigma(g) = \sigma(\chi(g))$, for $g \in G$.

The description of the simple components in the Wedderburn decomposition of a group algebra FG takes a nice form in the case of strongly monomial groups. These types of groups are also main ingredients in the proof of the Brauer–Witt Theorem that we present in the second chapter. The strongly monomial groups are particular cases of monomial groups and are more general than the abelian-by-supersolvable groups. Some of the following definitions can be given for arbitrary groups but we are only interested in the finite case so, unless otherwise stated, throughout G is a (finite) group. We start by presenting some classical information about monomial characters.

Definition 1.25. A character χ of G is called *monomial* if there exist a subgroup $H \leq G$ and a linear character ψ of H such that $\chi = \psi^G$. The group G is called *monomial* or *M-group* if all its irreducible characters are monomial.

In some sense the monomial characters are the obvious characters of a group. Notice that if $\chi : G \to \mathbb{C}^*$ is a linear character and $K = \mathrm{Ker}\chi$, then G/K is isomorphic to a finite subgroup of $\mathbb{C}^*$ and hence G/K is cyclic. Moreover, if $[G : K] = n$ and $g \in G$ is such that the image of g in G/K is a generator of G/K, then every element of G has a unique form as $g^i k$ for $i = 0, \ldots, n-1$ and $k \in K$, and $\chi(g^i k) = \zeta^i$, where $\chi(g) = \zeta$ is an n-th primitive root of 1. Conversely, if K is a normal subgroup of G such that G/K is cyclic, say of order n, and if $G = \langle g, K \rangle$, then for every n-th primitive root of 1, say ζ, there is a unique linear character χ of G such that $\chi(g) = \zeta$ and $K = \mathrm{Ker}\chi$.

A criterion for the irreducibility of monomial characters is given in the following theorem of Shoda [Sho].

Theorem 1.26 (Shoda). *Let ψ be a linear character of a subgroup H of G. Then the induced character ψ^G is irreducible if and only if for every $g \in G \setminus H$ there exists $h \in H \cap H^g$ such that $\psi(ghg^{-1}) \neq \psi(h)$.*

A natural method to construct irreducible characters of a given finite group G is to take the cyclic sections of G, that is, the pairs of subgroups (H, K) of G such that K is normal in H and H/K is cyclic, then for each cyclic section (H, K) construct all the linear characters χ of H with kernel K, and finally take the induced (monomial) character. Some of these monomial characters are irreducible (later on we call these sections *Shoda pairs* by connection with Theorem 1.26 due to Shoda). Taking all these irreducible monomial characters we have a bunch of irreducible characters of G. For many groups these irreducible monomial characters amount to all the irreducible characters, for example this is the case for any abelian-by-supersolvable group. In other words, any abelian-by-supersolvable group is monomial. Unfortunately, not every group is monomial. The smallest example of a non monomial group is a group of order 24 given in the next example from [Hup].

Example 1.27. The special linear group over the finite field $\mathbb{F}_3$

$$\mathrm{SL}_2(\mathbb{F}_3) = \{A \in GL_2(\mathbb{F}_3) : \det(A) = 1\} \cong Q_8 \rtimes C_3,$$

where $Q_8 = \langle x, y\rangle$ is the quaternion group, $C_3 = \langle a\rangle$ and $x^a = y$ and $y^a = xy$, is the only non monomial group of order 24. More generally, if G is a finite group containing a normal subgroup or an isomorphic image isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$, then G is not monomial.

The following two results of Taketa and Dade (e.g. see [CR]) show that the class of monomial groups is closely related to the class of solvable groups.

Theorem 1.28 (Taketa). *Every monomial group is solvable.*

Theorem 1.29 (Dade). *Every solvable group is isomorphic to a subgroup of a monomial group.*

As a consequence of Dade's Theorem and Example 1.27, the class of monomial groups is not closed under subgroups. On the other hand, it is easy to see that the class of monomial groups is closed under epimorphic images and finite direct products. Dade's Theorem is seen by Huppert as an evidence that there is no "hope to obtain structural restrictions for monomial groups, beyond the solvability". It is also mentioned in [Hup] that a group–theoretical characterization is unknown. However, A. Parks has recently given such a group–theoretical characterization, maybe not very satisfactory, in terms of some pairs of subgroups which are exactly the Shoda pairs [Park]. An important class of examples of monomial groups is that of abelian-by-supersolvable groups.

Definition 1.30. A group G is said to be *supersolvable* if it has a series of normal subgroups with cyclic factors. An *abelian-by-supersolvable* group is a group G having an abelian normal subgroup N such that G/N is supersolvable.

A group G is called *metabelian* if it has an abelian normal subgroup N such that G/N is abelian, or equivalently, if G' is abelian. G is said to be a *metacyclic* group if it contains a cyclic normal subgroup $N = \langle a\rangle$ such that $G/N = \langle bN\rangle$ is cyclic. In this case, G has a presentation with generators and relations as follows:

$$G = \langle a, b | a^m = 1, b^{-1}ab = a^r, b^n = a^s\rangle,$$

where m, n, r, s are integers that satisfy the conditions

$$\gcd(r, m) = 1, m | r^n - 1, m | s(r - 1).$$

Definition 1.31. Let F be a field of characteristic 0. The group G is *F-elementary with respect to a prime p* if $G = C \rtimes P$, where C is a cyclic, normal subgroup of G whose order is relatively prime to p and P is a p-group; and if $C = \langle c \rangle$, ζ is a primitive $|C|$-th root of unity and c^i is conjugated to c^j in G, then there exists $\sigma \in \mathrm{Gal}(F(\zeta)/F)$ such that $\sigma(\zeta^i) = \zeta^j$. The group G is *F-elementary* if it is F-elementary with respect to some prime p.

The Witt-Berman theorem is a generalization of Brauer's theorem on induced characters to the case where the underlying field F is an arbitrary subfield of the complex field $\mathbb{C}$.

Theorem 1.32 (Witt, Bermann). *For F a subfield of $\mathbb{C}$, every F-character of G is a $\mathbb{Z}$-linear combination $\sum_i a_i \theta_i^G$, with $a_i \in \mathbb{Z}$ and the θ_i's are F-characters of F-elementary subgroups of G.*

1.3 Units

For a ring R with unity 1, we denote by $\mathcal{U}(R)$ or R^* the *unit group* of R, i.e. the group of invertible elements in R. The knowledge of the unit group of an integral group ring $\mathbb{Z}G$ of a group G is a useful tool in the investigation of the group ring $\mathbb{Z}G$ and has been intensively studied. However, it seams that a complete description of the unit group in terms of generators and relations still seems to be a difficult task, even for special classes of groups.

The study of units of group rings relies in many situations on the Wedderburn decomposition of the corresponding group algebra. We follow this approach in our research of the applications of the explicit Wedderburn decomposition that we provide.

A natural approach to study $\mathcal{U}(\mathbb{Z}G)$ is to consider $\mathbb{Z}G$ as an order in the rational group algebra $\mathbb{Q}G$. This idea comes from the commutative case where the ring of algebraic integers $\mathcal{O}_K$ in a number field K is an order for which the unit group is completely described in the following famous theorem.

Theorem 1.33 (Dirichlet Unit Theorem). *Let K be a number field of degree $[K : \mathbb{Q}] = r_1 + 2r_2$, where K has r_1 real and r_2 pairs of complex embeddings. Then*

$$\mathcal{U}(\mathcal{O}_K) \cong F \times C,$$

where F is a free abelian group of rank $r_1 + r_2 - 1$, and C is a finite cyclic group (namely the group of roots of unity in K).

A basis of a free abelian group F satisfying the conditions of Theorem 1.33 is called a set of *fundamental units* of K. In general, there is an algorithm for the construction of a fundamental set of units presented in [BoS]. Moreover, in the special case of the n-th *cyclotomic field* $K = \mathbb{Q}(\zeta_n)$, where ζ_n denotes a primitive nth root of unity, the *cyclotomic units* $(1-\zeta_n^i)/(1-\zeta_n)$, where i is a natural number greater than one and relatively prime to n, generate a subgroup of finite index in $\mathcal{U}(\mathcal{O}_K)$. Note that in this case we have that $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$. The Dirichlet Unit Theorem was generalized to integral group rings of finite abelian groups by Higman (see for example [Seh, Theorem 2.9]).

Theorem 1.34 (Higman). *Let G be a finite abelian group. Then*

$$\mathcal{U}(\mathbb{Z}G) = \pm G \times F,$$

where F is a finitely generated free abelian group of rank $\frac{1}{2}(|G| + n_2 - 2c + 1)$, where n_2 denotes the number of elements of order 2 and c the number of cyclic subgroups of G.

In particular, it follows that this unit group $\mathcal{U}(\mathbb{Z}G)$ is finitely generated [BH]. In fact, the unit group of any $\mathbb{Z}$-order Γ in a finite dimensional $\mathbb{Q}$-algebra is finitely presented. This follows from the fact that $\mathcal{U}(\Gamma)$ is a so-called *arithmetic group*. For a rigorous definition of this notion we refer the reader to [Hum]. However, specific generators of a subgroup of finite index are not known and only for few examples one has managed to describe them, see for example [JL]. Unfortunately, there does not exist a general structure theorem covering the group ring case of arbitrary finite groups.

Theorem 1.35 (Hartley-Pickel). *If the group G is neither abelian nor isomorphic to $Q_8 \times C_2^n$ for some non-negative integer n, then $\mathcal{U}(\mathbb{Z}G)$ contains a free subgroup of rank 2.*

We present now some examples of units of $\mathbb{Z}G$. The elements of $\mathbb{Z}G$ of the form $\pm g$ with $g \in G$ are clearly units, having the inverses $\pm g^{-1}$. These units are called *trivial*. There are not too many general methods to construct non-trivial units. We mention two important types of units. First, we introduce some notation. Given an element $g \in G$, denote by $\overline{g}$ the sum in $\mathbb{Z}G$ of the elements of the cyclic group $\langle g \rangle$, that is, if n is the order of g, then

$$\overline{g} = \sum_{i=0}^{n-1} g^i.$$

The bicyclic units were introduced by Ritter and Sehgal. They can be constructed as follows.

Definition 1.36. Let $g, h \in G$ and let n be the order of g. Notice that $(1-g)\overline{g} = \overline{g}(1-g) = 0$. Then

$$u_{g,h} = 1 + (1-g)h(1 + g + g^2 + \cdots + g^{n-1}) = 1 + (1-g)h\overline{g},$$
$$v_{g,h} = 1 + (1 + g + g^2 + \cdots + g^{n-1})h(1-g) = 1 + \overline{g}h(1-g),$$

have inverses, which are respectively

$$u_{g,h}^{-1} = 1 - (1-g)h\overline{g},$$
$$v_{g,h}^{-1} = 1 - \overline{g}h(1-g).$$

The units $u_{g,h}$ and $v_{g,h}$ are called *bicyclic units*.

Notice that $u_{g,h} = 1$ if and only if $v_{g,h} = 1$ if and only if h normalizes $\langle g \rangle$. Hence, all the bicyclic units are 1 if and only if all the subgroups of G are normal, that is, G is Hamiltonian. In particular, the bicyclic units of $\mathcal{U}(ZG)$ are trivial for G an abelian group.

Definition 1.37. The *Bass cyclic units* are defined as

$$b = b(g, i, m, n) = (1 + g + \cdots + g^{i-1})^m + \frac{1 - i^m}{n}\overline{g},$$

where $g \in G$ has order m, $1 < i < m$ is coprime with m and $i^m \equiv 1 \mod n$.

In order to see that b is a unit, it is enough to check for G a cyclic group, since $b \in \mathbb{Z}\langle g \rangle$. Projecting b on the simple components of the Wedderburn decomposition of $\mathbb{Q}G$, one can notice that each such projection is a cyclotomic unit, hence b is a unit. Bass proved that if G is an abelian group, then the Bass cyclic units generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$ [Bas]. In many cases, it was proved that the group B_G generated by the Bass cyclic units and the bicyclic units (of one type) has finite index in $\mathcal{U}(\mathbb{Z}G)$ (see for example [RitS2, RitS3]). In [RitS1] it was proved that if G is a nilpotent group such that $\mathbb{Q}G$ does not have in his Wedderburn decomposition certain types of algebras, then B_G has finite index in $\mathcal{U}(\mathbb{Z}G)$. Furthermore, Jespers and Leal in [JL] have extended these results to bigger classes of groups. However, it is not true in general that B_G has finite index in $\mathcal{U}(\mathbb{Z}G)$.

The following results are examples of a family of similar theorems which prove that the Wedderburn decomposition of the group algebra $\mathbb{Q}G$ encodes useful information on the group of units of $\mathbb{Z}G$. This was the main motivation in the first place for our interest in explicit computation of the Wedderburn components of rational group algebras.

Theorem 1.38. [Jes] *$\mathcal{U}(\mathbb{Z}G)$ is virtually free non-abelian if and only if the Wedderburn components of $\mathbb{Q}G$ are either $\mathbb{Q}$, $\mathbb{Q}(\sqrt{-d})$ or $M_2(\mathbb{Q})$, for d a square-free non-negative integer. Moreover, there are only four groups G with this property.*

Theorem 1.39. [JLdR, JdR, LdR] *$\mathcal{U}(\mathbb{Z}G)$ is virtually a direct product of free groups if and only if every Wedderburn component of $\mathbb{Q}G$ is either a field or isomorphic to $M_2(\mathbb{Q})$, $(\frac{-1,-3}{\mathbb{Q}})$ or $\mathbb{H}(K)$ with K either $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{3})$.*

Theorem 1.40. [JPdRRZ] *$\mathcal{U}(\mathbb{Z}G)$ is virtually a direct product of free-by-free groups if and only if every Wedderburn component of $\mathbb{Q}G$ is either a field, a totally definite quaternion algebra or $M_2(\mathbb{K})$, where K is either $\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-3})$.*

1.4 Crossed products

In this section we present crossed products as an essential construction for the description of central simple algebras.

Definition 1.41. Let R be a unitary ring and G a group. A *crossed product* of G with coefficients in R is an associative ring $R * G$ with a decomposition

$$R * G = \bigoplus_{g \in G} R_g$$

such that every R_g is a subgroup of the additive group of $R * G$ with $R = R_1$, $R_g R_h = R_{gh}$ for all $g, h \in G$ and every R_g contains an invertible element $\overline{g}$.

Note that, for every $g \in G$, we have $R_g = R\overline{g} = \overline{g}R$, so every element in $R * G$ has a unique expression as $\sum_{g \in G} \overline{g} r_g$ with $r_g \in R$, for every $g \in G$. The crossed product $R * G$ is a right (and a left) free R-module, $\mathcal{G} = \{\overline{g} : g \in G\}$ (a set theoretical copy of G) is an R-basis of $R * G_R$ and we say that $\mathcal{G}$ is a homogeneous basis of $R * G$. Associated to a homogeneous basis $\mathcal{G}$ one has two maps

$$\alpha : G \to \mathrm{Aut}(R) \quad \text{and} \quad \tau : G \times G \to \mathcal{U}(R)$$

called *action* and *twisting* (or *factor set*, *factor system* or 2-*cocycle*) of $R * G$, given by

$$r^{\alpha(g)} = \overline{g}^{-1} r \overline{g} \quad \text{and} \quad \tau(g, h) = \overline{gh}^{-1} \overline{g}\overline{h}, \quad g, h \in G, r \in R.$$

The action and the twisting are interrelated by conditions precisely equivalent to $R * G$ being associative, that is, for every $x, y, z \in G$:

$$\tau(xy, z)\tau(x, y)^{\alpha(z)} = \tau(x, yz)\tau(y, z) \tag{1.4}$$

$$\alpha(y)\alpha(z) = \alpha(yz)\eta(y, z), \tag{1.5}$$

where $\eta(y, z)$ is the inner automorphism of R induced by the unit $\tau(y, z)$. Equation (1.4) above asserts that τ is a 2-cocycle for the action of G on $\mathcal{U}(R)$ (as we shall see

in the next section) and we call it the *cocycle condition*. Note that, by definition, a crossed product is merely an associative ring which happens to have a particular structure relative to R and G and which we denote by $R *_\tau^\alpha G$.

Conversely, if $\alpha : G \to \mathrm{Aut}(R)$ and $\tau : G \times G \to \mathcal{U}(R)$ are two maps satisfying the previous relations (1.4) and (1.5), then one can construct a crossed product having α and τ as the action and the twisting of a homogeneous basis. More precisely, one chooses a set of symbols $\mathcal{G} = \{\overline{g} : g \in G\}$ and defines $R*G$ as a right free R-module with basis $\mathcal{G}$ and the multiplication given by $r\overline{g} = \overline{g}r^{\alpha(g)}$ and $\overline{g}\overline{h} = \overline{gh}\tau(g,h), g, h \in G, r \in R$ and extended by linearity.

The R-basis $\{\overline{g} : g \in G\}$ of a crossed product $R * G$ is not unique. For example, if a_g is a unit of R for each $g \in G$ then $\{\widehat{g} = a_g\overline{g} : g \in G\}$ is another R-basis. Changing $\{\overline{g} : g \in G\}$ by $\{\widehat{g} = a_g\overline{g} : g \in G\}$ is called a *diagonal change of basis* [Pas2]. A diagonal change of basis induces a change on the action and on the twisting, but not of the algebra. The new action differs from the old action by an inner automorphism.

Certain special cases of crossed products have their own names. For example, a group ring is a crossed product with trivial action ($\alpha(x) = 1_R$ for all $x \in G$) and trivial twisting ($\tau(x, y) = 1$ for all $x, y \in G$). If the action is trivial, then $R * G = R^tG$ is a *twisted group ring*. Finally, if the twisting is trivial, then $R * G$ is a *skew group ring*.

Let $\mathrm{Inn}(R)$ be the group of inner automorphisms of R. The property (1.5) shows that $\alpha : G \to \mathrm{Aut}(R)$ is not a group homomorphism unless the twisting takes values in the center of R, but the composition $\widehat{\alpha}$ of α with the projection $\pi : \mathrm{Aut}(R) \to \mathrm{Out}(R)$ is a group homomorphism, where $\mathrm{Out}(R) = \mathrm{Aut}(R)/\mathrm{Inn}(R)$ denotes the group of outer automorphisms of R. We say that the action α is *outer* if $\widehat{\alpha}$ is injective, i.e. if the identity of G is the unique element $g \in G$ such that $\alpha(g)$ is inner in R. Notice that if R is commutative, then the action is outer if and only if it is *faithful*. The following theorem can be found in [Mon] for skew group rings and in [Rei] for crossed products over fields. In both cases, the proof applies for arbitrary crossed products.

Theorem 1.42. *Let G be a finite group, S a simple ring and α an outer action. Then $S * G$ is a simple ring.*

For some special cases of crossed products we use the following classical notation [Rei]. If L/F is a finite Galois extension with Galois group $G = \mathrm{Gal}(L/F)$, α is the natural action of G on L and τ is a 2-cocycle on $G \times G$, then the crossed product $L *_\tau^\alpha G$ is denoted by $(L/F, \tau)$ and we call it *classical crossed product* or *crossed product algebra*. If in the previous notation the extension is $F(\zeta)/F$, where ζ is a root of 1 and all the values of the 2-cocycle τ are roots of 1 in $F(\zeta)$, then we use the notation $(F(\zeta)/F, \tau)$ and we call it *cyclotomic algebra* (see Section 1.9 for more information). A diagonal change of basis in $(L/F, \tau)$ does not affect the action because L is commutative, hence it

induces a new representation of $(L/F, \tau)$ as $(L/F, \tau')$, where τ' is a new factor set which differs from τ in a 2-coboundary (see Section 1.5 for the definition of a 2-coboundary).

Historically, crossed products arose in the study of division rings. Let F be a field and let D be a division algebra finite dimensional over its center F. If L is a maximal subfield of D, then $\dim_F(D) = (\dim_F L)^2$. Suppose that L/F is normal, although this is not always true. If $g \in \mathrm{Gal}(L/F) = G$, then the Skolem–Noether Theorem implies that there exists $\overline{g} \in D^*$ with $\overline{g}^{-1} l \overline{g} = g^l$ for all $l \in L$. Furthermore, $\overline{g}\,\overline{h}$ and $\overline{gh}$ agree in their action on L, so $\tau(g,h)^{-1} = \overline{h}^{-1}\overline{g}^{-1}\overline{gh} \in C_D(L) = L$. Once we show that the elements $\overline{g}$ for $g \in G$ are linearly independent over L, then we conclude by computing dimensions that $D = (L/K, \tau)$.

More generally, let A be a finite dimensional central simple F-algebra. Thus $A = \mathcal{M}_n(D)$ for some n and division ring D with $Z(D) = F$. Roughly speaking, two such algebras are equivalent if they have the same D and the division algebra can be given as $(L/K, \tau)$. This is the base of the cohomological description of the Brauer group and will be explained more precisely in the next section.

Remark 1.43. The theory of factor systems (the original name for crossed products) was developed by E. Noether in her Göttingen lecture 1929/30. Noether herself never published her theory. Deuring took notes of that lecture, and these were distributed among interested people. Brauer as well as Hasse had obtained a copy of those notes. The Deuring notes are now included in Noether's Collected Papers. The first publication of Noether's theory of crossed products was given, with Noether's permission, in a Hasse's paper where a whole chapter is devoted to it. The theory was also included in the book "Algebren" by Deuring.

The German terminology for crossed product is "verschränktes Produkt". The English term "crossed product" had been used by Hasse in his American paper [Has1]. When Noether read this she wrote to Hasse: "Are the 'crossed products' your English invention? This word is good." We do not know whether Hasse himself invented this terminology, or perhaps it was H.T. Engstrom, the American mathematician who helped Hasse to translate his manuscript from German into English. In any case, in English the terminology "crossed product" has been in use since then [Roq].

The first examples of division algebras that were found after the quaternions belong to the class of cyclic division algebras. This class still plays a major role in the theory of central simple algebras. The construction of cyclic algebras has been given by L.E. Dickson in 1906, therefore they were also called "algebras of Dickson type".

Definition 1.44. A *cyclic algebra* over K is a classical crossed product algebra $(L/K, \tau)$, where L/K is a cyclic extension (i.e. a finite Galois extension with $\mathrm{Gal}(L/K)$ cyclic).

If $A = (L/K, \tau)$ is a cyclic algebra, σ is a generator of $G = \mathrm{Gal}(L/K)$, $n = [L : K] = |G|$ and $\{\overline{\sigma^i} : 0 \leq i \leq n-1\}$ is an L-basis of A then $\overline{\sigma^i} = a_i \overline{\sigma}^{\,i}$ with $a_i \in L^*$. Thus $\{\overline{\sigma}^{\,i} : 0 \leq i \leq n-1\}$ is another L-basis obtained via a diagonal change of basis from the original one. Furthermore $a = \overline{\sigma}^{\,n} = \prod_{j=0}^{n-1} \tau(\sigma^j, \sigma)$ is a unit of L and the 2-cocycle τ_a associated to the basis $\{\overline{\sigma}^{\,i} : 0 \leq i \leq n-1\}$ only depends on a. Namely

$$\tau_a(\sigma^i, \sigma^j) = \begin{cases} 1, & i + j < n \\ a, & i + j \geq n, \ 0 \leq i, j \leq n-1. \end{cases}$$

Conversely, for a given generator σ of G and an element $a \in L^*$, the map $\tau_a : G^2 \to L^*$ given as above is a 2-cocycle and the cyclic algebra $(L/K, \tau_a)$ is usually denoted by $(L/K, \sigma, a)$.

Example 1.45. Quaternion algebras are cyclic algebras of degree 2 and take the form $\left(\frac{a,b}{K}\right) = K[i, j | i^2 = a, j^2 = b, ji = -ij]$, for $a, b \in K^*$. We abbreviate $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$ and $\mathbb{H}(K) = \left(\frac{-1,-1}{K}\right)$.

If $A = \left(\frac{a,b}{K}\right)$ and σ is a real embedding of K then A is said to *ramify* at σ if $\mathbb{R} \otimes_{\sigma(K)} A \simeq \mathbb{H}(\mathbb{R})$, or equivalently, if $\sigma(a), \sigma(b) < 0$. A *totally definite quaternion algebra* is a quaternion algebra A over a totally real field which is ramified at every real embedding of its center.

1.5 Brauer groups

In this section we recall the definition of the Brauer group as principal tool for the study of central simple algebras and the relation with the cohomology groups.

The explicit calculation of the Brauer group of a field is usually a formidable task. The theorems in this section are fundamental tools for research in the theory of central simple algebras. The only available way to construct the Brauer groups of arbitrary fields is by using these techniques of cohomology of groups and Galois cohomology. Moreover, Galois cohomology provides the bridge between central simple algebras and class field theory that leads to the fundamental theorems on the Brauer groups of local fields and number fields. The results of this section are classical and can be found in many books, such as [Pie], [Rei] or [FD].

Throughout we assume that K is a field and, unless otherwise specified, all algebras are finite dimensional K-algebras. The *center* of a K-algebra A is the subalgebra $Z(A) = \{a \in A | \ xa = ax, \forall x \in A\}$ of A. Note that $K \subseteq Z(A)$. If $K = Z(A)$, we say that A is a *central* algebra. We call A *central simple* if A is central, simple and finite dimensional.

If A is a central simple K-algebra, then $\dim_K(A)$ is a square and we define the *degree* of A, denoted $\deg(A)$, to be the square root of the dimension of A as a vector space over K, that is, $\deg(A) = (\dim_K A)^{1/2}$.

Definition 1.46. Let A and B be central simple K-algebras. We introduce an equivalence relation on the class of central simple K-algebras. We say that A and B are *Brauer equivalent*, or simply *equivalent* and write $A \sim B$, if there is a division algebra D and positive integers n and m such that $A \simeq \mathcal{M}_n(D)$ and $B \simeq \mathcal{M}_m(D)$ as K-algebras.

This is also equivalent to any of the following conditions:

(1) There exist m, n such that $\mathcal{M}_m(A) \simeq \mathcal{M}_n(B)$.

(2) If M is the unique simple A-module and N is the unique simple B-module, then $\mathrm{End}_A(M) \simeq \mathrm{End}_B(N)$.

All the isomorphisms here are K-algebra homomorphisms. The equivalence class of a central simple K-algebra A is denoted by $[A]$.

An important reason for introducing this equivalence relation is the following. We wish to define an algebraic structure on the set of division algebras, which are central over K. The tensor product over K of two finite dimensional division algebras with center K is K-central simple, but NOT necessarily a division algebra. In other words, the set of division algebras is not closed under $\otimes_K$. For example, $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \simeq \mathcal{M}_4(\mathbb{R})$. Now, the tensor product of two central simple algebras is again a central simple algebra, that is, the set of central simple algebras is closed under tensor product. This allows one to put a group structure on the Brauer equivalence classes of central simple algebras. The group structure imposes constraints which can be exploited to give information about the central simple K-algebras.

Definition 1.47. The *Brauer group* of a field K, denoted $\mathrm{Br}(K)$, is the set of equivalence classes of central simple K-algebras under the Brauer equivalence, with the tensor product acting as the group operation and the equivalence class of K acting as the identity element. The inverse of $[A]$ is $[A^{\mathrm{op}}]$, where A^{op} is the opposite algebra of A.

Remark 1.48. The term "Brauer group" honors Richard Brauer (1901–1977), who made the first systematic study of this fundamental invariant and first defined this group in 1929. The importance of the Brauer groups in the theory of rings and fields is now firmly established.

Brauer had developed the theory of division algebras and matrix algebras in a series of several papers in the foregoing years, starting from his 1927 *Habilitationsschrift*

at the University of Königsberg. His main interest was in the theory of group representations, following the ideas of his academic teacher I. Schur. It was E. Noether who gradually had convinced him that the representation theory of groups could and should be profitably discussed within the framework of the abstract theory of algebras (or *hypercomplex systems* in her terminology) instead of matrix groups and semigroups as Schur had started it [Roq].

Now we present some basic examples of Brauer groups of different fields.

Example 1.49. If $K = \overline{K}$ is algebraically closed, then $\mathrm{Br}(K) = 0$. This follows from the fact that there are no non-trivial K-central simple division algebras over K. The proof of this affirmation is the following. Assume D is a K central division algebra and let $d \in D \setminus K$. Since $\dim_K(D) < \infty$, d is algebraic over K. Let $P \in K[X]$ be a non-zero polynomial of minimal degree with $P(d) = 0$. If the independent coefficient of P is 0 then d is a zero divisor, contradicting that D is a division algebra. Thus $d \in K$, because K is algebraically closed. □

Example 1.50. If K is a finite field, then $\mathrm{Br}(K) = 0$. This is because if D is K-central simple over K, then D is finite dimensional over a finite field and hence a finite algebra. Now, a theorem of Wedderburn states that there are no noncommutative finite division algebras, so $\mathrm{Br}(K) = 0$. □

Example 1.51. It is known that the only $\mathbb{R}$-central division algebras are $\mathbb{R}$ and $\mathbb{H}$. So, $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}_2$. The generator of $\mathrm{Br}(\mathbb{R})$ is $[\mathbb{H}]$ and $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \simeq \mathcal{M}_4(\mathbb{R})$, i.e. $[\mathbb{H}][\mathbb{H}] = 1 = [\mathbb{R}]$. □

The Brauer group is the object map of a functor.

Proposition 1.52. *If $\phi : K \to L$ is a field homomorphism, then ϕ induces a group homomorphism $\phi_* : \mathrm{Br}(K) \to \mathrm{Br}(L)$ defined by $\phi_*([A]) = [A \otimes {}_\phi L]$. The correspondences $K \mapsto \mathrm{Br}(K)$ and $\phi \mapsto \phi_*$ define a functor from the category of fields to the category of abelian groups.*

The notation ${}_\phi L$ in the previous proposition has the meaning that ${}_\phi L$ is the K-algebra with scalar multiplication defined by $sa = \phi(s)a$ for $s \in K$ and $a \in L$.

Let A be a central simple K-algebra and L be a field extension of K. Then we denote by A^L the L-algebra $A \otimes L$ obtained from A by extension of scalars from K to L. One says that L is a *splitting field* of A (or that L *splits* A) if $A^L \sim L$ (that is, if $A^L \simeq \mathcal{M}_n(L)$ as L-algebras for some n) or equivalently if $[A]$ belongs to the kernel of ϕ_*, where $\phi : K \to L$ is the inclusion homomorphism. If K is already a splitting field of A (i.e. $A \sim K$) then one says that A is a *split algebra*.

The *relative Brauer group* of K with respect to L, denoted by $\mathrm{Br}(L/K)$, is the kernel of the homomorphism $\phi_* : \mathrm{Br}(K) \to \mathrm{Br}(L)$ given by $\phi_*([A]) = [A \otimes_\phi L]$. The subgroup $\mathrm{Br}(L/K)$ is the set of Brauer equivalence classes of central simple algebras over K which are split by L. Every element of $\mathrm{Br}(L/K)$ has the form $[A]$, where A is a central simple algebra that contains L as a maximal subfield. The algebra A with this property is unique up to isomorphism. The relative Brauer group is useful for studying the Brauer group, for one can reduce questions about $\mathrm{Br}(K)$ to questions about $\mathrm{Br}(L/K)$ for certain L, and $\mathrm{Br}(L/K)$ is often easier to work with.

Now we introduce cohomology as another point of view from which to study the Brauer group. We present the notion in a slightly more general setting than will be actually used here. The cohomology groups of a group were first defined by Hopf in the early 1940's by means of algebraic topology, and were used to study the relationship between the homology and homotopy groups of spaces. The definition of $H^n(G, M)$ was algebraicized by Eilenberg–MacLane and independently by Eckmann in the course of the development of homological algebra. It was they who realized that many classical constructions, such as equivalence classes of factor sets, could be described as cohomology groups in dimensions 0, 1, 2 and 3.

If G is a group, then a $\mathbb{Z}G$-module is simply an abelian group together with an action of G on M by group automorphisms. We consider the action of G on the right. Classically, a $\mathbb{Z}G$-module is called a G-module, so that the category of right G-modules is simply the category of right $\mathbb{Z}G$-modules.

Definition 1.53. For any group G and any abelian group M on which G acts, define $C^0(G, M) = M$ and for $n \geq 1$ define $C^n(G, M) = \{f | f : G^n \to M\}$. Notice that $C^n(G, M)$ is an abelian group under pointwise addition of functions and it is called the *n-th cochain group*. Let $\delta^0 : C^0(G, M) \to C^1(G, M)$ be defined by $\delta^0(f)(g_0) = f \cdot g_0 - f$ for $f \in C^0(G, M)$. For $n \geq 1$, define $\delta^n : C^n(G, M) \to C^{n+1}(G, M)$ by $\delta^n(f)(g_0, \ldots, g_n) = f(g_1, \ldots, g_n) + \sum_{i=1}^{n} (-1)^i f(g_0, \ldots, g_{i-2}, g_{i-1}g_i, \ldots, g_n) + (-1)^{n+1} f(g_0, \ldots, g_{n-1}) \cdot g_{n+1}$, for $f \in C^n(G, M)$. The map δ^n is called the *n-th coboundary map.*

In particular, for $n = 1$ this map is defined by $\delta^1(f)(g_0, g_1) = f(g_1) - f(g_0 g_1) + f(g_0) \cdot g_1$ and for $n = 2$ one has $\delta^2(f)(g_0, g_1, g_2) = f(g_1, g_2) - f(g_0 g_1, g_2) + f(g_0, g_1 g_2) - f(g_0, g_1) \cdot g_3$.

Each δ^n is a group homomorphism and $\delta^{n+1} \circ \delta^n = 0$. Therefore, $\{C^n, \delta^n\}$ forms a *cochain complex* of the form

$$0 \longrightarrow C^0 \xrightarrow{\delta^0} C^1 \longrightarrow \cdots \longrightarrow C^n \xrightarrow{\delta^n} C^{n+1} \longrightarrow \cdots$$

Let $Z^n = \mathrm{Ker}(\delta^n)$ and $B^n = Im(\delta^{n-1})$, so that $B^n \subseteq Z^n$ because of the property

$\delta^{n+1} \circ \delta^n = 0$. The elements of Z^n are called *n-cocycles* and the elements of B^n are the *n-coboundaries*. The *n-th cohomology group* of G with coefficients in M is defined as $H^n(G, M) = Z^n/B^n$.

An alternative construction of the cohomology groups $H^n(G, M)$ using complexes and projective resolutions from homological algebra, is the following. Take a projective resolution

$$P_\bullet = (\cdots \to P_2 \xrightarrow{p_2} P_1 \xrightarrow{p_1} P_0 \to \mathbb{Z} \to 0)$$

of the trivial G-module $\mathbb{Z}$, i.e. an infinite exact sequence with every P_i projective. Consider the sequence $\mathrm{Hom}_G(P_\bullet, M)$ defined by

$$\mathrm{Hom}_G(P_0, M) \to \mathrm{Hom}_G(P_1, M) \to \mathrm{Hom}_G(P_2, M) \to \cdots$$

where the maps $\mathrm{Hom}_G(P_i, M) \to \mathrm{Hom}_G(P_{i+1}, M)$ are given by $f \mapsto f \circ p_{i+1}$. The fact that $P_\bullet$ is a complex of G-modules implies that $\mathrm{Hom}_G(P_\bullet, M)$ is a complex of abelian groups. We index it by defining $\mathrm{Hom}_G(P_i, M)$ to be the term in degree i. We may now put

$$H^i(G, M) = H^i(\mathrm{Hom}_G(P_i, M))$$

for $i \geq 0$. The defined groups do not depend on the choice of the projective resolution $P_\bullet$.

The above construction is a special case of that of Ext-groups in homological algebra: for two R-modules M and N, these are defined by $\mathrm{Ext}^n(M, N) = H^n(\mathrm{Hom}_R(P_\bullet, N))$ with a projective resolution $P_\bullet$ of M. In our case we get

$$H^n(G, M) = \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, M)$$

where $\mathbb{Z}$ is to be regarded as trivial G-module.

The *cohomological dimension* of a group G is n if n is the maximal non-negative integer for which $H^n(G, M) \neq 0$, for some $\mathbb{Z}G$-module M and $H^n(G, M)$ is the cohomology of G with coefficients in M. Equivalently, G has the cohomological dimension n if the trivial $\mathbb{Z}G$-module $\mathbb{Z}$ has a projective resolution of length n. See for example [Bro]. The *virtual cohomological dimension* of a group is n if it has a torsion-free subgroup of finite index that has the cohomological dimension n.

We are interested in the special case when $G = \mathrm{Gal}(L/K)$ and $M = L^*$ for a Galois extension L/K. The groups $H^n(G, L^*)$ are called the *Galois cohomology groups of the extension L/K with coefficients in L^**. In particular, we need $H^2(\mathrm{Gal}(L/K), L^*)$, the second Galois cohomology group of the extension L/K with coefficients in L^*.

The cocycle condition (1.4) can be interpreted as cohomology relation for a suitable abelian group, which is L^*. The second coboundary homomorphism takes the following

form $\delta^2(\tau)(x,y,z) = \tau(y,z)\tau(xy,z)^{-1}\tau(x,yz)(\tau(x,y)^z)^{-1}$ for a mapping $\tau : G \times G \to L^*$. Therefore, the cocycle condition on a mapping $\tau : G \times G \to L^*$ is identical with the assumption that $\tau \in Z^2(G, L^*)$. Thus, every 2-cocycle $\tau \in Z^2(G, L^*)$ gives rise to a crossed product algebra $(L/K, \tau)$. A diagonal change of basis in $(L/K, \tau)$ produces a new representation of $(L/K, \tau)$ as $(L/K, \tau')$ with $\tau' \equiv \tau \mod B^2(G, L^*)$. Conversely, if $\tau, \tau' \in Z^2(G, L^*)$ are congruent modulo $B^2(G, L^*)$ then $(L/K, \tau)$ and $(L/K, \tau')$ are isomorphic as K-algebras. This induces a map $H^2(G, L^*) \to \mathrm{Br}(L/K)$. The next theorem provides a cohomological interpretation of the relative Brauer group.

Theorem 1.54. *For a Galois extension L/K with $G = \mathrm{Gal}(L/K)$, $H^2(G, L^*)$ is isomorphic to the relative Brauer group $\mathrm{Br}(L/K)$ and the isomorphism is given by $[\tau] \mapsto [(L/K, \tau)]$, where τ is a 2-cocycle from $Z^2(G, L^*)$ and $[\tau]$ denotes the class of τ in $H^2(G, L^*)$.*

To prove that the above correspondence is a group homomorphism, one uses the following proposition.

Proposition 1.55 (The Product Theorem). *Let L/K be a Galois extension with $G = \mathrm{Gal}(L/K)$. If $\tau_1, \tau_2 \in Z^2(G, L^*)$, then $(L/K, \tau_1) \otimes_K (L/K, \tau_2) \sim (L/K, \tau_1\tau_2)$.*

As a consequence of Theorem 1.55, we can now state the following properties of cyclic algebras. First, let us set $N_{L/K}(L^*) = \{N_{L/K}x : x \in L^*\}$, where $N_{L/K} : L \to K$ denotes the norm of the extension L/K.

Proposition 1.56. *Let $G = \mathrm{Gal}(L/K) = \langle\sigma\rangle$ be cyclic of order n, and let $a, b \in K^*$. Then*

(i) $(L/K, \sigma, a) \cong (L/K, \sigma^s, a^s)$ *for each $s \in \mathbb{Z}$ such that $(s, n) = 1$.*

(ii) $(L/K, \sigma, 1) \cong \mathcal{M}_n(K)$.

(iii) $(L/K, \sigma, a) \cong (L/K, \sigma, b)$ *if and only if $b = (N_{L/K}c)a$ for some $c \in L^*$. In particular, $(L/K, \sigma, a) \sim K$ if and only if $a \in N_{L/K}(L^*)$.*

(iv) $(L/K, \sigma, a) \otimes_K (L/K, \sigma, b) \sim (L/K, \sigma, ab)$.

The following corollary gives an important result, helping to compute the Schur index of cyclic algebras.

Corollary 1.57. *Let $A = (L/K, \sigma, a)$. Then $\exp[A]$ is the least positive integer t such that $a^t \in N_{L/K}(L^*)$.*

Proof. We have $[A]^t = [(L/K, \sigma, a^t)]$ in $\mathrm{Br}(K)$. Thus, by Proposition 1.56, $[A]^t = 1$ if and only if a^t belongs to $N_{L/K}(L^*)$. □

Theorem 1.54 provides a cohomological description of the relative Brauer groups. The cohomological description of $\mathrm{Br}(K)$ is now a consequence of the following proposition.

Proposition 1.58. *For a field K, $\mathrm{Br}(K) = \bigcup \mathrm{Br}(L/K)$, where L ranges over all finite Galois extensions of K. In other words, for every central simple K-algebra there is a finite Galois extension of K which splits A.*

Summarizing, the Brauer group $\mathrm{Br}(K)$ is the union over all Galois extensions L/K of the relative Brauer groups $\mathrm{Br}(L/K)$ and the relative Brauer groups can be identified with cohomology groups. In order to relate the full Brauer group to cohomological data, an interpretation is needed for the inclusion mappings $\mathrm{Br}(L/K) \to \mathrm{Br}(E/K)$ that arise when $K \subseteq L \subseteq E$ with L/K and E/K Galois extensions. Those inclusions correspond to the inflation homomorphisms.

Let L/K and E/K be finite Galois extensions with $L \subseteq E$. Denote $G = \mathrm{Gal}(E/K)$ and $H = \mathrm{Gal}(L/K)$. The restriction mapping $\sigma \mapsto \sigma|_L$ is a surjective homomorphism of G to H that induces an adjoint homomorphism $C^n(H, L^*) \to C^n(G, E^*)$ by $f \mapsto f^*$, where $f^*(\sigma_1, \ldots, \sigma_n) = f(\sigma_1|_L, \ldots, \sigma_n|_L)$. A simple calculation shows that this map commutes with the coboundary, i.e. $(\delta^n f)^* = \delta^n(f^*)$. Thus, the adjoint map carries $Z^n(H, L^*)$ to $Z^n(G, E^*)$ and $B^n(H, L^*)$ to $B^n(G, E^*)$. Consequently, it induces a group homomorphism of $H^n(H, L^*)$ to $H^n(G, E^*)$ that it is called the *inflation mapping* and is denoted by Inf or, if necessary, $\mathrm{Inf}^n_{L/K \to E/K}$. Explicitly, $\mathrm{Inf}[f] = [f^*]$ for $f \in Z^n(H, L^*)$.

In particular, given the 2-cocycle $\tau : H \times H \to L^*$, we define the 2-cocycle $\mathrm{Inf}(\tau) : G \times G \to L^* \subset E^*$ by $\mathrm{Inf}(\tau)(g_1, g_2) = \tau(g_1|_H, g_2|_H)$, for $g_1, g_2 \in G$, that is, the initial 2-cocycle from H to L^* inflates to a 2-cocycle from G to E^*. Furthermore, if we consider the crossed product algebras $(L/K, \tau)$ and $(E/K, \mathrm{Inf}(\tau))$, then

$$(L/K, \tau) \sim (E/K, \mathrm{Inf}(\tau))$$

as K-algebras. This is equivalent to the following proposition.

Proposition 1.59. *Let $K \subseteq L \subseteq E$ be field extensions. If $i : \mathrm{Br}(L/K) \to \mathrm{Br}(E/K)$ is the inclusion homomorphism, then the following diagram commutes*

$$\begin{array}{ccc} H^2(H, L^*) & \xrightarrow{\mathrm{Inf}} & H^2(G, E^*) \\ \downarrow & & \downarrow \\ \mathrm{Br}(L/K) & \xrightarrow[i]{} & \mathrm{Br}(E/K), \end{array}$$

where the vertical arrows are the isomorphisms of Theorem 1.54.

The action of the inflation on cyclic algebras is given by the following result.

Theorem 1.60. *Let $K \leq L \leq E$, where $G = \mathrm{Gal}(E/K) = \langle \sigma \rangle$ is cyclic of finite order t. Let $H = \mathrm{Gal}(E/L)$, $\widehat{G} = G/H = \mathrm{Gal}(L/K) = \langle \widehat{\sigma} \rangle$, where $\widehat{\sigma}$ is the image of σ in $\widehat{G}$. Then for any $a \in K^*$,*

$$(L/K, \widehat{\sigma}, a) \sim (E/K, \sigma, a^{[E:L]}).$$

The next result establishes an isomorphism between the Brauer group of a field K and the second Galois cohomology group of K which is obtained as a direct limit of the groups $H^2(\mathrm{Gal}(L/K), L^*)$. Theorem 1.61 can be stated as follows: Every element of the group $\mathrm{Br}(K)$ is determined by a 2-cocycle in a finite Galois extension L/K.

Theorem 1.61. *The isomorphism $\mathrm{Br}(L/K) \cong H^2(\mathrm{Gal}(L/K), L^*)$ lifts to an isomorphism between $\mathrm{Br}(K)$ and the direct limit $\varinjlim H^2(\mathrm{Gal}(L/K), L^*) = H^2(\mathrm{Gal}(K_s/K), K_s^*)$, where K_s is the maximal separable extension of K.*

If K is a subfield of L, then the inclusion mapping $\iota : K \to L$ induces a homomorphism $\iota_* : \mathrm{Br}(K) \to \mathrm{Br}(L)$. When these Brauer groups are represented as unions of relative Brauer groups corresponding to cohomology groups, the description of ι_* can be given in terms of certain homomorphisms that are standard tools in cohomology theory. We now define these homomorphisms and we relate them to the mappings of the Brauer groups.

Definition 1.62. Let H be a subgroup of the finite group G. If M is a right $\mathbb{Z}G$-module, then M can also be viewed as a $\mathbb{Z}H$-module and the trivial left action of G and H on M yields a $\mathbb{Z}G$-bimodule and a $\mathbb{Z}H$-bimodule. Let $f \in C^n(G, M)$ be an n-cochain, considered as a mapping from G^n to M. The restriction $f|_{H^n}$ is then an element of $C^n(H, M)$. The coboundary homomorphism clearly satisfies $\delta^n(f|_{H^n}) = (\delta^n f)|_{H^n}$, so that $f \mapsto f|_{H^n}$ maps $Z^n(G, M)$ to $Z^n(H, M)$ and $B^n(G, M)$ to $B^n(H, M)$. Therefore, $f \mapsto f|_{H^n}$ induces a group homomorphism

$$\mathrm{Res}_{G \to H} : H^n(G, M) \to H^n(H, M)$$

which is called the *restriction* map . Explicitly, $\mathrm{Res}_{G \to H}[f] = [f|_{H^n}]$ for all $f \in Z^n(G, M)$.

The applications of the restriction mapping that we are interested in occur when $n = 2$, $G = \mathrm{Gal}(E/K)$ and $H = \mathrm{Gal}(E/L)$, where $K \subseteq L \subseteq E$ are field extensions and E/K is Galois. Moreover, M will generally be E^* with the usual $\mathbb{Z}G$-bimodule structure. By Hilbert's so-called 'Theorem 90', $H^0(G, E^*) = (E^*)^G = K^*$ and $H^1(G, E^*) = 1$. Similarly, $H^0(H, E^*) = (E^*)^H = L^*$ and the restriction $\mathrm{Res}_{G \to H} : H^0(G, E^*) \to H^0(H, E^*)$ is the inclusion map of K^* into L^*.

Proposition 1.63. Let $K \subseteq L \subseteq E$ be fields with E/K a Galois extension. If $\iota : K \to L$ is the inclusion mapping, then $\iota_*(\mathrm{Br}(E/K)) \subseteq \mathrm{Br}(E/L)$ and the diagram

$$\begin{array}{ccc} H^2(G, E^*) & \xrightarrow{\mathrm{Res}_{G\to H}} & H^2(H, E^*) \\ \cong\downarrow & & \downarrow\cong \\ \mathrm{Br}(E/K) & \xrightarrow[\iota_*|_{\mathrm{Br}(E/K)}]{} & \mathrm{Br}(E/L) \end{array}$$

is commutative, where the vertical isomorphisms are those of Theorem 1.54.

The family of restriction homomorphisms induces a restriction homomorphism of the Galois cohomology groups $\mathrm{Res} : H^n(\mathrm{Gal}(K_s/K), K_s^*) \to H^n(\mathrm{Gal}(K_s/L), K_s^*)$. If $\iota : K \to L$ is the inclusion mapping, then $\iota_* : \mathrm{Br}(K) \to \mathrm{Br}(L)$ is the limit of $\iota_*|_{\mathrm{Br}(E/K)}$ for E running through the finite Galois extensions of K containing L. Then, when L/K is a finite separable extension, the diagram

$$\begin{array}{ccc} H^2(\mathrm{Gal}(K_s/K), K_s^*) & \xrightarrow{\mathrm{Res}} & H^2(\mathrm{Gal}(K_s/L), K_s^*) \\ \varinjlim\downarrow & & \downarrow\varinjlim \\ \mathrm{Br}(K) & \xrightarrow[\iota_*]{} & \mathrm{Br}(L) \end{array}$$

is commutative.

We denote by $\mathrm{Res}_{K\to L}$ or simply by Res the *restriction* homomorphism induced by extension of scalars $\mathrm{Res}_{K\to L} : \mathrm{Br}(K) \to \mathrm{Br}(L)$ and defined by $\mathrm{Res}_{K\to L}([A]) = [A \otimes_K L]$, for $[A] \in \mathrm{Br}(K)$. In particular, if χ is an irreducible character of the finite group G with $K(\chi) = K$, then $\mathrm{Res}([A(\chi, K)]) = [A(\chi, L)]$, where $A(\chi, K)$ denotes the simple component of the group algebra KG associated to the character χ. The action of the restriction on cyclic algebras is summarized in the following result.

Theorem 1.64. *Let $G = \mathrm{Gal}(L/K) = \langle\sigma\rangle$ be cyclic of order n, and let $a \in K^*$. Let E be any field containing K, and let EL be the composite of E and L in some large field containing both E and L. We may write $H = \langle\sigma^k\rangle = \mathrm{Gal}(L/L \cap E) \cong \mathrm{Gal}(EL/E)$, where k is the least positive integer such that σ^k fixes $L \cap E$. Then*

$$E \otimes_K (L/K, \sigma, a) \sim (EL/E, \sigma^k, a).$$

Now we define the corestriction map which is a weak inverse to restriction. The definition starts in dimension 0 and is extended to n by *dimension shifting*, which is the technique to extend a result or construction from dimension 0 to dimension n.

Definition 1.65. Let H be a subgroup of index m in the finite group G, $T = \{x_1, \ldots, x_m\}$ a right transversal of H in G and M a right $\mathbb{Z}G$-module. For $u \in M^H$,

define

$$\mathrm{Cor}_{H\to G}\, u = u \cdot \sum_{k=1}^{m} x_k.$$

The definition does not depend on the choice of coset representatives and $\mathrm{Cor}_{H\to G}$ is a group homomorphism from $M^H = H^0(H, M)$ to $M^G = H^0(G, M) = \mathrm{Hom}_G(\mathbb{Z}, M)$, the group of invariants, that is, the largest submodule of M on which G acts trivially.

Fix an exact sequence $0 \to M \to N \to P \to 0$ of right $\mathbb{Z}G$-modules such that $H^n(G, N) = 0$ for all $n \geq 1$. By induction on n we get a sequence of homomorphisms $\mathrm{Cor}_{H\to G} : H^n(H, M) \to H^n(G, M)$ such that the following diagram commutes:

$$\begin{array}{ccccccc} H^{n-1}(H,N) & \longrightarrow & H^{n-1}(H,P) & \longrightarrow & H^n(H,M) & \longrightarrow & 0 \\ \downarrow{\scriptstyle \mathrm{Cor}_{H\to G}} & & \downarrow{\scriptstyle \mathrm{Cor}_{H\to G}} & & \downarrow{\scriptstyle \mathrm{Cor}_{H\to G}} & & \\ H^{n-1}(G,N) & \longrightarrow & H^{n-1}(G,P) & \longrightarrow & H^n(G,M) & \longrightarrow & 0 \end{array}$$

The defined homomorphisms are called *corestriction mappings*. Usually we denote the corestriction simply by Cor.

The following result from [HS] establishes the relation between the restriction and the corestriction.

Theorem 1.66. *If H is a subgroup of index m in the finite group G and M is a right $\mathbb{Z}G$-module, then $\mathrm{Cor}_{H\to G} \circ \mathrm{Res}_{G\to H} : H^n(G, M) \to H^n(G, M)$ $(n \geq 0)$ is just the multiplication by m.*

For a field extension L of K, denote by $\mathrm{Cor}_{L\to K}$ or simply by Cor the *corestriction* homomorphism from the Brauer group $\mathrm{Br}(L)$ to $\mathrm{Br}(K)$. Then the previous theorem can be restated as follows.

Theorem 1.67. *If L is a finite Galois extension of K with $[L : K] = n$, then*

$$\mathrm{Cor}_{L\to K} \circ \mathrm{Res}_{K\to L}([A]) = ([A])^n.$$

The degree mapping is clearly not invariant under the Brauer equivalence. Because of this fact, and for other reasons, it is useful to define a different numerical function on central simple algebras. This is given by the Schur index of a central simple algebra.

Definition 1.68. Let A be a central simple K-algebra, so that $A \cong \mathcal{M}_m(D)$ for some unique division K-algebra D. We define the *Schur index* of A, denoted $\mathrm{ind}(A)$, to be the degree of D, that is, the square root of the dimension of D as a vector space over K.

If χ is an irreducible complex character of a finite group G and K is a field of characteristic zero, then the *Schur index of χ with respect to K*, denoted $m_K(\chi)$, is the Schur index of the simple component of the group algebra KG corresponding to the character χ, denoted $A(\chi, K)$.

The Schur index was introduced by Issai Schur (1875–1941) in 1906. As a student of Frobenius, he worked on group representations (the subject with which he is most closely associated), but also in combinatorics and even theoretical physics. He is perhaps best known today for his result on the existence of the Schur decomposition. He had a number of students, among them R. Brauer.

Brauer proved that the Brauer group is torsion, that is, every element of $\mathrm{Br}(K)$ has finite order. The *exponent* of a central simple K-algebra A, denoted $\exp(A)$, is the order of $[A]$ in the Brauer group $\mathrm{Br}(K)$. That is, $\exp(A)$ is the smallest number m such that $A^{\otimes m} \cong \mathcal{M}_r(K)$ for some r, where $A^{\otimes m}$ denotes the tensor product of m copies of A. In other words, the exponent of A is the least $m \in \mathbb{N}$ such that the tensor product of m copies of A is a matrix algebra over K. This terminology had been chosen by Brauer because, he said, in the context of the theory of algebras the word "order" is used for another concept [Roq].

The exponent is similar to the index in many ways and for important classes of algebras these invariants are equal. In the following proposition we collect some of Brauer's results about the connection between the exponent and the index of a central simple algebra.

Proposition 1.69 (Brauer). *Let A be a central simple K-algebra. Then:*

(1) $\mathrm{ind}(A)$ *divides* $\deg(A)$ *and* $\mathrm{ind}(A) = \deg(A)$ *if and only if A is a division algebra.*

(2) $\exp(A)$ *divides* $\mathrm{ind}(A)$ *and every prime divisor of* $\mathrm{ind}(A)$ *also divides* $\exp(A)$.

(3) *If K is a number field, then* $\exp(A) = \mathrm{ind}(A)$.

There is an alternative way of defining the Schur index of an irreducible complex character with respect to a field K which is related to the following question:

> For which fields $K \leq \mathbb{C}$ is the character $\chi \in \mathrm{Irr}(G)$ afforded by a K-representation?

If $K \leq \mathbb{C}$ is not one of these fields, we wish to measure the extent to which χ fails to be afforded over K. This suggests the following definition from [Isa].

Definition 1.70. Let $K \leq L$, where L is any splitting field for the finite group G. Choose an irreducible L-representation ρ which affords χ and an irreducible K-representation φ such that ρ is a constituent of φ^L. Then the multiplicity of ρ as a constituent of φ^L is the *Schur index* of χ over K and is denoted by $m_K(\chi)$.

Apparently, $m_K(\chi)$ as given in Definition 1.70 could depend on the splitting field L. However, an easy exercise shows that the definition of $m_K(\chi)$ in Definition 1.68 and Definition 1.70 are equivalent, and so $m_K(\chi)$ is independent of L.

If K is a field with positive characteristic then $m_K(\chi) = 1$ for every irreducible character χ of a finite group. This is because if L is the prime field of K then $A(\chi, L)$ is finite and therefore split as central simple algebra over its center. Hence the characteristic zero case is the one that presents interest for the computation of the Schur indices of irreducible characters of finite groups. Many important results about Schur indices appear to depend on deep facts about division algebras and number theory. Nevertheless, much can be done by means of character theory, as presented in [Isa] or [CR], where it is also proved that every positive integer can occur as Schur index, despite of the fact that most of the elementary results are directed to showing that the Schur indices are small.

1.6 Local fields

In order to understand the Brauer group of a number field, it is convenient to start by studying the Brauer groups of some special fields called local fields. The results presented in this section are mainly from [Rei] and [Pie].

Throughout R is an integral domain with quotient field K, $R \neq K$. We describe some properties of the ring R and of R-modules with respect to localization at prime ideals of R.

We start with some basic facts about localization at prime ideals. Starting with a prime ideal P of R, we may form the multiplicative set $S = R - P$, and then define the ring of quotients $R_P := S^{-1}R$, called the *localization* of R at P. Since every element of $R - P$ is invertible in R_P, it is easily verified that R_P has a unique maximal ideal, namely $P \cdot R_P$. We should remark that the ring homomorphism $i : R \to R_P$, $i(x) = x/1$, $x \in R$, enables us to view R_P (and all R_P-modules) as R-modules ($\ker i$ is precisely the set of S-torsion elements of R). Thus, $P \cdot R_P$ is the same as $i(P) \cdot R_P$. Since R is an integral domain, the mapping $i : R \to R_P$ is an embedding. In particular, when $P = \{0\}$ then R_P is precisely the quotient field of the domain R. Let now M be any R-module. We define $M_P = R_P \otimes M$, an R_P-module called the *localization* of M at P.

We often refer to problems concerning R-modules and R-homomorphisms as *global* problems, whereas those involving R_P-modules are called *local* problems. A fundamental technique in commutative algebra, algebraic number theory and algebraic geometry is the method of solving global questions by first settling the local case, and then applying this information to the global case.

Let us now introduce some concepts from valuation theory. Let $\mathbb{R}_+$ denote the set of non-negative real numbers.

Definition 1.71. A *valuation* of K is a mapping $\varphi : K \to \mathbb{R}_+$ such that for $a, b \in K$

(i) $\varphi(a) = 0$ if and only if $a = 0$;

(ii) $\varphi(ab) = \varphi(a)\varphi(b)$;

(iii) $\varphi(a + b) \leq \varphi(a) + \varphi(b)$.

If the valuation also satisfies the stronger condition

(iv) $\varphi(a + b) \leq \max(\varphi(a), \varphi(b))$, we call φ *non-archimedean*. It is easily verified that every non-archimedean valuation satisfies

(v) $\varphi(a + b) = max(\varphi(a), \varphi(b))$ whenever $\varphi(a) \neq \varphi(b)$.

The *trivial* valuation is defined by $\varphi(0) = 0$ and $\varphi(a) = 1$ for $a \in K$, $a \neq 0$. By default all valuations are considered to be non-trivial.

The *value group* of a valuation φ is the multiplicative group $\{\varphi(a) : a \in K, a \neq 0\}$. If this value group is an infinite cyclic group, φ is a *discrete valuation*, and it is necessarily non-archimedean. Two valuations φ and ψ are *equivalent* if for $a \in K$, $\varphi(a) \leq 1$ if and only if $\psi(a) \leq 1$. Each valuation φ on K gives rise to *a topology* on K, by taking as basis for the neighborhoods of a point $a \in K$ the sets $\{x \in K : \varphi(x - a) < \epsilon\}$, where ϵ ranges over all positive real numbers. Equivalent valuations give the same topology on K.

Given any non-archimedean valuation φ on K, let $R = \{a \in K : \varphi(a) \leq 1\}$. Then R is a subring of K and is called the *valuation ring* of φ. The set $P = \{a \in K : \varphi(a) < 1\}$ is the unique maximal ideal of R. If φ is a discrete valuation, then P is a principal ideal, namely $P = R\pi$, where π is any element of P such that $\varphi(\pi) < 1$ and $\varphi(\pi)$ generates the value group of φ. In this case, R is a *discrete valuation ring*, by which we shall mean a principal ideal domain having a unique maximal ideal P such that $P \neq 0$.

Example 1.72 (Example of discrete valuation ring). Let p be a prime number, and let $\mathbb{Z}_{(p)}$ be the subset of the field $\mathbb{Q}$ of rationals consisting of the fractions r/s, where s is not divisible by p. This is a discrete valuation ring with residue field the field $\mathbb{F}_p$ with p elements. □

One way of obtaining *archimedean valuations* is the following. The ordinary absolute value $|\ |$ on the complex field $\mathbb{C}$ is an archimedean valuation, whose restriction to any subfield of $\mathbb{C}$ is an archimedean valuation on that subfield. Now let K be a field which can be embedded in $\mathbb{C}$, and let $\mu : K \to \mathbb{C}$ be an embedding. Define $\varphi : K \to \mathbb{R}_+$ by setting $\varphi(a) = |\mu(a)|$, $a \in K$. Then φ is an archimedean valuation on K. In particular, if K is a number field with r_1 embeddings in $\mathbb{R}$ and r_2 pairs of complex embeddings in $\mathbb{C}$ then one can obtain in this way $r_1 + r_2$ archimedean valuations. The Ostrowski

Theorem states that every archimedean valuation of K (a number field) is equivalent to exactly one of these $r_1 + r_2$ valuations.

Now we give the connection between prime ideals of Dedekind domains and the non-archimedean valuations. From the standpoint of ideal theory, Dedekind domains are the simplest type of domains beyond principal ideal domains, and share many of their arithmetical properties. They arise naturally, as follows. Let R be a principal ideal domain with quotient field K, let L be a finite extension of K, and let S be the integral closure of R in L. Then S is a Dedekind domain with quotient field L. For a rigorous definition see Definition 1.3.

Definition 1.73. Let R be a Dedekind domain, and let P be a nonzero prime ideal of R, or equivalently, a maximal ideal of R. For each nonzero $a \in K$, we may factor the principal ideal Ra into a product of powers of prime ideals. Let $v_P(a)$ denote the exponent to which P occurs in this factorization. If P does not occur, set $v_P(a) = 0$. Also, put $v_P(0) = +\infty$. We call v_P the *exponential valuation* associated with P.

Now fix some $\kappa \in \mathbb{R}_+$, $\kappa > 1$, and define $\varphi_P(a) = \kappa^{-v_P(a)}, a \in K, a \neq 0$, and $\varphi_P(0) = 0$. Then φ_P is a discrete non-archimedean valuation on K, whose value group is the cyclic group generated by κ. (If instead of κ we used another real number κ' with $\kappa' > 1$, the valuation φ'_P thus obtained would be equivalent to the above-defined valuation φ_P). The properties of φ_P are consequences of the following properties of v_p:

(i) $v_P(a) = \infty$ if and only if $a = 0$.

(ii) $v_P(ab) = v_P(a) + v_P(b)$.

(iii) $v_P(a + b) \geq \min(v_P(a), v_P(b))$, with equality whenever $v_P(a) \neq v_P(b)$.

Let R_P be the *localization* of R at P, defined as before by $R_P = \{x/s : x \in R, s \in R - P\}$. This ring is in fact the valuation ring of the P-adic valuation φ_P on R and its unique maximal ideal is precisely $P \cdot R_P$. Thus R_P is a discrete valuation ring and is automatically a principal ideal domain. We may choose a *prime element* π of the ring R_P, that is, an element $\pi \in R_P$ such that $\pi R_P = P \cdot R_P$. Indeed, π may be chosen to lie in R. The fractional R_P-ideals of K are $\{\pi^n R_P : n \in \mathbb{Z}\}$. It follows that localization does not affect residue class fields, that is, $R/P \cong R_P/(P \cdot R_P)$. This isomorphism is not only an R-isomorphism, but is in fact a field isomorphism. More generally, there are ring isomorphisms $R/P^n \cong R_P/(P^n \cdot R_P)$, for $n \geq 1$.

A *prime* of K is an equivalence class of valuations of K. We exclude the "trivial" valuation φ defined by $\varphi(0) = 0$, $\varphi(a) = 1$ for $a \in K$, $a \neq 0$. If K is a number field, there are the archimedean or *infinite primes*, arising from embeddings of K into the complex field $\mathbb{C}$ and the non-archimedean or *finite primes* of K, arising from discrete P-adic valuations of K, with P ranging over the distinct maximal ideals in the ring of

algebraic integers of K. Every other valuation is equivalent to one of these valuations, so the concept of prime in K is equivalent to the concept of equivalence class of valuations. In many references the primes in K are also called *places*.

The completion of a valuation field is a field which usually has better properties than the original one. Let K be a field with a valuation φ, topologized as before. Let $\widehat{K}$ denote the completion of K relative to this topology. Then $\widehat{K}$ is a field whose elements are equivalence classes of Cauchy sequences of elements of K, two sequences being *equivalent* if their difference is a sequence converging to zero. The field K is embedded in $\widehat{K}$ and the valuation φ extends to a valuation $\hat{\varphi}$ on $\widehat{K}$. The field $\widehat{K}$ is *complete* relative to the topology induced by $\widehat{\varphi}$, that is, every Cauchy sequence from $\widehat{K}$ has a limit in $\widehat{K}$.

If φ is an archimedean valuation, then so is $\widehat{\varphi}$, and $\widehat{K}$ is a complete field with respect to an archimedean valuation. The only possibilities for $\widehat{K}$ are $\mathbb{R}$, the real field or $\mathbb{C}$, the complex field, and in each case $\widehat{\varphi}$ is equivalent to the usual absolute value.

If φ is non-archimedean, so is $\widehat{\varphi}$. The two valuations have the same value group, and the same residue class field (up to isomorphism). In particular, let R be a Dedekind domain with quotient field K, where $K \neq R$, and let P be a maximal ideal of R. The completion of K with respect to the P-adic valuation φ_P on K will be denoted by $\widehat{K}_P$ (or just $\widehat{K}$ or even K_P, if there is no danger of confusion). Call $\widehat{K}_P$ a *P-adic* field, and its elements *P-adic* numbers.

The discrete valuation φ_P extends to a discrete valuation $\widehat{\varphi}_P$ on $\widehat{K}_P$. We have already remarked that the valuation ring of φ_P is the localization R_P. Let $\widehat{R}_P$ be the valuation ring of $\widehat{\varphi}_P$. Every element of $\widehat{R}_P$ can be represented by a Cauchy sequence from R_P (or from R, for that matter). If π is a prime element of R_P, then π is also a prime element of $\widehat{R}_P$. Let $\mathcal{S}$ denote a full set of residue class representatives in R of the residue class field $\widehat{R} = R/P$, with $0 \in \mathcal{S}$. Each $x \in \widehat{R}_P$ is uniquely expressible as $x = X_0 + X_1\pi + X_2\pi^2 + \ldots, \quad X_i \in \mathcal{S}$, and each $y \in \widehat{K}_P \setminus \{0\}$ is uniquely of the form $y = \pi^k \cdot x$, with $k = \widehat{\varphi}_P(y) \in \mathbb{Z}$ and x as above, with $X_0 \neq 0$. If $y = 0$, take $k = -\infty$.

Example 1.74 (Complete valuation fields). (1) The completion of $\mathbb{Q}$ with respect to v_p is denoted by $\mathbb{Q}_p$ and is called the *field of p-adic numbers*. Certainly, the completion of $\mathbb{Q}$ with respect to the absolute value is $\mathbb{R}$. Embeddings of $\mathbb{Q}$ in $\mathbb{Q}_p$ for all prime p and in $\mathbb{R}$ is a tool to solve various problems over $\mathbb{Q}$. An example is the Minkowski–Hasse Theorem: an equation $\sum a_{ij}X_iX_j = 0$ for $a_{ij} \in \mathbb{Q}$ has a nontrivial solution in $\mathbb{Q}$ if and only if it admits a nontrivial solution in $\mathbb{Q}_p$ for all prime p (including infinity). The ring of integers of $\mathbb{Q}_p$ is denoted by $\mathbb{Z}_p$ and is called the *ring of p-adic integers*. The residue field of $\mathbb{Z}_p$ is the finite field $\mathbb{F}_p$ consisting of p elements.

(2) The completion of $K(X)$ with respect to v_X is the formal power series field

$K((X))$ of all formal series $\sum_{-\infty}^{+\infty} \alpha_n X^n$ with $\alpha_n \in K$ and $\alpha_n = 0$ for almost all negative n. The ring of integers with respect to v_X is $K[[X]]$, that is, the set of all formal series $\sum_0^{+\infty} \alpha_n X^n$, $\alpha_n \in K$. Its residue field may be identified with K. □

Definition 1.75. A *complete discrete valuation ring* R is a principal ideal domain with unique maximal ideal $P = \pi R \neq 0$ such that R is complete relative to the P-adic valuation. If K is the quotient field of R and $\widehat{R} = R/P$ is its residue class field, we call K a *local field*.

The following theorem is a useful result that we will use later.

Theorem 1.76. *Let W be an unramified extension of K of degree f, and let v be the P-adic valuation on K. Given any element $\alpha \in K$, the equation $N_{W/K}(x) = \alpha$, with $x \in W$ is solvable for x if and only if f divides $v(\alpha)$.*

Let K be a field which is complete with respect to a valuation φ, and let $\widetilde{K}$ be an algebraic closure of K. Then we may extend φ to a valuation $\widetilde{\varphi}$ on $\widetilde{K}$ as follows. Every $a \in \widetilde{K}$ lies in some field L with $K \leq L \leq \widetilde{K}$, $[L : K]$ finite (for example, $L = K(a)$ will do). Set $\widetilde{\varphi}(a) = \{\varphi(N_{L/K}a)\}^{1/[L:K]}$. Then the value $\widetilde{\varphi}(a)$ is independent on the choice of L and every finite extension of K contained in $\widetilde{K}$ is complete with respect to the valuation $\widetilde{\varphi}$.

If φ is archimedean, there are only two possibilities: one with $K = \mathbb{C} = \widetilde{K}$ and $\varphi = \widetilde{\varphi}$ and the other one with $K = \mathbb{R}$, $\widetilde{K} = \mathbb{C}$ and $\widetilde{\varphi}$ extends φ, where $\widetilde{\varphi}$ and φ are the usual absolute values on $\mathbb{R}$ or $\mathbb{C}$.

If φ is non-archimedean, so is $\widetilde{\varphi}$. However, $\widetilde{\varphi}$ need not be a discrete valuation, even if φ is discrete. If φ is a discrete valuation on K, denote by o_K its valuation ring and by p_K the maximal ideal of o_K. Let $\widehat{o}_K = o_K/p_K$ be the residue class field and let $p_K = \pi_K \cdot o_K$, so π_K is a prime element of o_K. Let v_K be the *exponential valuation* on K, defined by setting $aR = p_K^{v_K(a)}$, for $a \in K$ and $a \neq 0$, and $v_K(0) = +\infty$. Any finite extension L of the complete field K can be embedded in $\widetilde{K}$ and the restriction of $\widetilde{\varphi}$ to L gives a discrete valuation ψ which extends φ. It can be shown that, for each $a \in L$, $v_L(a) = f(L/K)^{-1} \cdot v_K(N_{L/K}(a))$. In this case, the *ramification index* $e = e(L/K)$ and the *residue class degree* $f = f(L/K)$ are given by the formulas $v_L(\pi_K) = e$ and $[\widehat{o}_L : \widehat{o}_K] = f$. Moreover, the extension L of K is *unramified* if $e(L/K) = 1$ and $\widehat{o}_L$ is a separable extension of $\widehat{o}_K$, and it is *completely* (or *totally*) *ramified* if $\widehat{o}_L = \widehat{o}_K$, that is $f(L/K) = 1$.

Theorem 1.77. *Let L be a finite extension of K and assume the complete field K has finite residue class field $\widehat{o}_K$ with q elements. Then, for each positive integer f, there is a unique unramified extension W of K with $[W : K] = f$, namely $W = K(\zeta)$, for ζ*

a primitive (q^f-1)*th root of unity over* K*. Furthermore,* $o_W = o_K[\zeta]$*,* $\widehat{o}_W = \widehat{o}_K(\widehat{\zeta})$*, where* $\widehat{\zeta}$ *is a primitive* (q^f-1)*th root of unity.*

Corollary 1.78. *The extensions* W/K *and* $\widehat{o}_W/\widehat{o}_k$ *are Galois with cyclic Galois groups of order* f*, generated by the Frobenius automorphism* σ *defined by* $\zeta \mapsto \zeta^q$*, and respectively by the automorphism* $\widehat{\sigma}$ *which maps* $\widehat{\zeta}$ *to* $\widehat{\zeta}^q$*.*

Theorem 1.79. *With the above notation, let* $L = K(\alpha)$*, where* α *has the minimal polynomial over* K *given by the* n*th degree Eisenstein polynomial over* o_K*, for* n *a positive integer. Then* L *is completely ramified over* K*,* $[L:K] = n$*, and* α *is a prime element of* o_L*. Furthermore,* $o_L = o_K(\alpha)$*.*

Summarizing, if L/K is finite, we assume that the residue class field $\widehat{o}_K$ is finite, and W is the inertia field of the extension L/K, then we have $K \subseteq W \subseteq L$, $\widehat{o}_W = \widehat{o}_L$, $e(L/K) = 1$, $f(L/W) = 1$, $f(W/K) = f(L/K)$, $e(L/W) = e(L/K)$. Thus, the step from K to L is divided into an unramified step from K to W, followed by a completely ramified step from W to L.

Now let K be a field with a valuation φ (archimedean or not) and $\widehat{\varphi}$ the extension of φ to the algebraic closure Ω of the completion $\widehat{K}$. Given a separable extension L of K, we wish to determine all extensions of the valuation φ from K to L. Each such extension determines an embedding of L in Ω which preserves the embeddings of K in $\widehat{K}$. Two embeddings μ, μ' of L in Ω are called *equivalent* if there exists a K-isomorphism $\sigma : \mu(L) \cong \mu'(L)$ such that $\sigma\mu = \mu'$. Let $\mu_1, \ldots, \mu_r$ be a full set of inequivalent isomorphisms of L into Ω which preserve the embeddings of K in $\widehat{K}$. Let $\widehat{L}_i = \widehat{K} \cdot \mu_i(L)$ be the composite of $\widehat{K}$ and $\mu_i(L)$ in Ω and set $n_i = [\widehat{L}_i : \widehat{K}]$. Then, there are precisely r inequivalent valuations $\psi_1, \ldots, \psi_r$ of L which extend φ, and these are given by the formula $\psi_i(a) = \widehat{\mu}_i(a) = \{\widehat{\varphi}(N_{\widehat{L}_i/\widehat{K}}(\mu_i(a)))\}^{1/n_i}$, for $1 \leq i \leq r$.

If R is now a Dedekind domain with quotient field K and S the integral closure of R in L, then for every maximal ideal P of R let $P \cdot S = \prod_{i=1}^{r} P_i^{e_i}$ be the factorization of $P \cdot S$ into a product of distinct maximal ideals $\{P_i\}$ of S. Then there are precisely r inequivalent valuations $\psi_1, \ldots, \psi_r$ of L which extend the P-adic valuation φ_P on K, obtained by choosing ψ_i to be the P_i-adic valuation on L. The fields $\widehat{L}_i$ are precisely the P_i-adic completions of L. If K is a number field so that the residue class fields R/P and S/P_i are finite, we may *normalize* the P-adic valuation φ_P of K and the P_i-adic valuation φ_i of L, by setting $\varphi_P(a) = \mathrm{card}(R/P)^{-v_P(a)}$ and $\varphi_{P_i}(b) = \mathrm{card}(S/P_i)^{-v_{P_i}(b)}$, for $a \in K$ and $b \in L$. In this case, $\varphi_{P_i} = \varphi_P^{n_i}$ on K, so $\varphi_{P_i}^{1/n_i}$ is the *valuation* on $\widehat{L}_i$ which *extends* φ_P on $\widehat{K}_P$.

1.7 Simple algebras over local fields

In this section we define the local index of a central simple algebra. The description of the Brauer group appears in what is called *local class field theory.* This theory is about extensions, primarily abelian, of local fields (i.e. complete for a discrete valuation) with finite residue class field. Throughout let R be a complete discrete valuation ring with field of quotients K, that is, R is a principal ideal domain with a unique maximal ideal $P = \pi R \neq 0$ and R is complete relative to the P-adic valuation v on K. Let $\widehat{R} = R/P$, the residue class field. We assume that $\widehat{R}$ is a finite field with q elements.

Let D be a division algebra with center K and index m. The valuation v on K can be extended to a valuation v_D on D given by the formula $v_D(a) = m^{-1}v(N_{D/K}a)$ for $a \in D$. The next result shows that D contains a unique maximal R-order.

Theorem 1.80. $\Delta = \{a \in D : v_D(a) \geq 0\}$ *is the integral closure of* R *in* D*, hence* Δ *is the unique maximal* R*-order in* D *with* $\mathfrak{p} = \{a \in D : v_D(a) > 0\}$ *the unique maximal ideal.*

Furthermore, $\pi\Delta$ is a power of $\mathfrak{p}$ and it can be shown that $\pi\Delta = \mathfrak{p}^m$ and $\widehat{\Delta} = \Delta/\mathfrak{p}$, is a field of order q^m, where π is a prime element of R.

We shall see that the structures of D and Δ can be described explicitly in this case, and depend only on the index m and some integer r such that $1 \leq r \leq m$, $(r, m) = 1$. The unique unramified extension of K of degree m is $K(\zeta)$, where ζ is a primitive $(q^m - 1)$-th root of unity over K. By Corollary 1.78, the Galois group $\mathrm{Gal}(K(\zeta)/K)$ is cyclic of order m, and has as canonical generator the Frobenius automorphism of $K(\zeta)/K$ denoted by $\sigma_{K(\zeta)/K}$. Recall that it is defined only for unramified extensions.

We wish to show that, in analogy with the results for the case of fields, the division ring D comes from an unramified extension, followed by a complete ramified extension. To begin with, D contains a subfield W isomorphic to $K(\zeta)$, so that W is an unramified extension of K such that $[W : K] = [\widehat{\Delta} : \widehat{R}] = m$. So, W is a maximal subfield of D, W is the inertia field of D and it is unique up to conjugacy.

Let π_D be a prime element of Δ, that is, a generator of $\mathfrak{p}$. Since $\pi\Delta = \pi_D^m\Delta$, the field $K(\pi_D)$ is a completely ramified extension of K of degree m, and is a maximal subfield of D. Furthermore, $\Delta = R[\zeta, \pi_D]$ and $D = K[\zeta, \pi_D]$. Thus D is obtained by adjoining the element π_D to any of its inertia fields $K(\zeta)$, or equivalently, by adjoining ζ to the field $K(\pi_D)$. Note that ζ and π_D do not commute, unless $m = 1$. The inertia field $K(\zeta)$ is uniquely determined up to K-isomorphism by the index m. The next theorem shows that one can select the prime element π_D with better properties.

Theorem 1.81. *Let* $\zeta \in D$ *be a primitive* $(q^m - 1)$*-th root of* 1*, and let* π *be any prime element of* R*. Then there exists a prime element* $\pi_D \in \Delta$ *such that* $\pi_D^m = \pi$*,*

$\pi_D \zeta \pi_D^{-1} = \zeta^{q^r}$, where r is a positive integer such that $1 \leq r \leq m$, $(r,m) = 1$. Then $D = K(\zeta, \pi_D) = (K(\zeta)/K, \sigma_{K(\zeta)/K}, \pi_D)$, where $\sigma_{K(\zeta)/K}(\zeta) = \zeta^{q^r}$ and the integer r is uniquely determined by D, and does not depend upon the choice of ζ or π.

The above shows that once the complete field K is given, the division ring D is completely determined by its index m, and by the integer r. Indeed, we first form the field $K(\zeta)$, with ζ any primitive $(q^m - 1)$-th root of 1. Then we pick any prime $\pi \in R$, and adjoin to the field W an element π_D satisfying the conditions listed in Theorem 1.81. This determines the division ring $D = K(\zeta, \pi_D)$ up to K-isomorphism. The fraction r/m is called the *Hasse invariant* of D.

Theorem 1.82. *Let $1 \leq r \leq m$, $(r,m) = 1$. Given the complete field K, there exists a division ring D with center K, index m, and Hasse invariant r/m, that is each fraction r/m arises from some division ring.*

We showed that W can be embedded in D, and that there exists a prime element $z \in D$ such that

$$D = \bigoplus_{j=0}^{m-1} W z^j, \quad z\alpha z^{-1} = \sigma^r(\alpha), \quad \alpha \in W, \quad z^m = \pi.$$

The integer r is relatively prime to the index m, and D determines $r \mod m$ uniquely. Further, it can be shown that each pair r, m with $(r,m) = 1$ arises from some D. In terms of the notation for cyclic algebras, we have $D \simeq (W/K, \sigma^r, \pi)$. Choose $s \in \mathbb{Z}$ so that $rs \equiv 1 (\mathrm{mod}\ m)$. Then also $(s,m) = 1$ and $D \cong (W/K, \sigma^r, \pi) \cong (W/K, \sigma^{rs}, \pi^s) = (W/K, \sigma, \pi^s)$. Furthermore, we could have restricted s to lie in the range $1 \leq s \leq m$. An important consequence of this is the following result.

Theorem 1.83. *Let D be a division algebra with center K and index m. Then $m = \exp[D]$. Hence, for each $[A] \in \mathrm{Br}(K)$, $\exp[A] = \mathrm{ind}[A]$.*

Whether or not $(s,m) = 1$, we may still form the cyclic algebra $A = (W/K, \sigma, \pi^s)$. The isomorphism class of A depends only on $s (\mathrm{mod}\ m)$, that is, on the fraction s/m viewed as an element of the additive group $\mathbb{Q}/\mathbb{Z}$. Let us find the division algebra part of A. Of course, we already know that A is a division algebra whenever $(s,m) = 1$.

Theorem 1.84. *Let W/K be an unramified extension of degree m, with Frobenius automorphism σ, and let $s \in \mathbb{Z}$. Write $s/m = s'/m'$, where $(s', m') = 1$. Then $(W/K, \sigma, a\pi^s) \sim (W'/K, \sigma', \pi^{s'})$, where the latter is a division algebra of index m' and W'/K is an unramified extension of degree m', with Frobenius automorphism σ'. Furthermore, if $a \in K^*$, then the cyclic algebra $(W/K, \sigma, a)$ is a division algebra if and only if $(m, v_K(a)) = 1$.*

Let W/K be an unramified extension of degree m, with Frobenius automorphism $\sigma_{W/K}$. Given an integer s, not necessarily prime to m, let us consider the cyclic algebra $A = (W/K, \sigma_{W/K}, \pi^s)$.

Definition 1.85. We define the *Hasse invariant* of A, denoted by $\mathrm{inv}A$, by the formula

$$\mathrm{inv}(W/K, \sigma_{W/K}, \pi^s) = s/m \in \mathbb{Q}/\mathbb{Z}.$$

The division algebra part of A can be calculated by use of Theorem 1.84, and it has the same Hasse invariants as A. Therefore, $\mathrm{inv}A$ depends only upon the class $[A] \in \mathrm{Br}(K)$, and we shall write $\mathrm{inv}[A]$ rather than $\mathrm{inv}A$ hereafter. Furthermore, by Theorem 1.81, every class in $\mathrm{Br}(K)$ is represented by some cyclic algebra $(W/K, \sigma_{W/K}, \pi^s)$ with W/K unramified, and hence there is a well defined map

$$\mathrm{inv} : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}.$$

Let L/K be a cyclic extension with Galois group $\langle\sigma\rangle$ cyclic of order n, and let $a \in K^*$. Then the cyclic algebra $B = (L/K, \sigma, a)$ determines a class $[B]$ in $\mathrm{Br}(K)$. However, it is not necessarily true that $\mathrm{inv}[B] = v_K(a)/m$. Indeed, even when L/K is unramified, the formula is valid only when σ equals the Frobenius automorphism $\sigma_{L/K}$. In the ramified case, the Frobenius automorphism $\sigma_{L/K}$ is not even defined and in order to compute $\mathrm{inv}[B]$ when L/K is ramified, we must first write $B \sim (W/K, \sigma_{W/K}, \pi^s) = A$ for some unramified extension W/K, and then we have $\mathrm{inv}[B] = \mathrm{inv}[A] = s/m$.

Theorem 1.86. $\mathrm{inv} : \mathrm{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$.

We shall denote inv by inv_K when we need to specify the underlying field K. The next result describes the effect on inv of a change in ground fields.

Theorem 1.87. *Let L be any finite extension of K. The following diagram commutes:*

$$\begin{array}{ccc} \mathrm{Br}(K) & \xrightarrow{\mathrm{inv}_K} & \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle L\otimes_K -}\downarrow & & \downarrow{\scriptstyle [L:K]} \\ \mathrm{Br}(L) & \xrightarrow[\mathrm{inv}_L]{} & \mathbb{Q}/\mathbb{Z}, \end{array}$$

where the horizontal maps are isomorphisms, and the second vertical map is defined to be the multiplication by $[L : K]$.

Corollary 1.88. *Let D be a division algebra with center K and index m, and let L be any finite extension of K. Then L splits D if and only if $m|[L : K]$.*

A further consequence of Theorem 1.86 and Theorem 1.87 is the following result.

Theorem 1.89. *Let L/K be any finite extension of degree m. Then* $\mathrm{Br}(L/K)$ *is cyclic of order m. Hence,* $\mathrm{Br}(L/K) = \{[A] \in \mathrm{Br}(K) : [A]^m = 1\}$.

1.8 Simple algebras over number fields

This section contains some deep and beautiful results in modern algebra such as the theorems that classify and describe the central simple algebras over number fields. This work is associated with the names of several of the greatest heroes of mathematics: Hasse, Brauer, Noether, and Albert. It is based on developments in number theory that are due to Kronecker, Weber, Hilbert, Minkovski, Furtwangler, Artin, Takagi, Hasse, Witt and many others.

Throughout K denotes a number field. We have seen that a *prime* of K is an equivalence class of valuations of K. If K is a number field, there are the archimedean or *infinite primes*, arising from embeddings of K into the complex field $\mathbb{C}$ and the non-archimedean or *finite primes* of K, arising from discrete P-adic valuations of K, with P ranging over the distinct maximal ideals in the ring of all algebraic integers of K.

Let A be a central simple K-algebra and let P range over the primes of K. We shall use K_P (rather than $\widehat{K}_P$) to denote the P-adic completion of K. Put

$$A_P = K_P \otimes_K A = P\text{-adic completion of } A.$$

Then, A_P is a central simple K_P-algebra and the map $[A] \to [A_P]$ yields a homomorphism of Brauer groups $\mathrm{Br}(K) \to \mathrm{Br}(K_P)$.

Definition 1.90. The *local Schur index* of A at P is defined as $m_P(A) = \mathrm{ind}[A_P]$.

Clearly $A_P \sim K_P$ if and only if $m_P(A) = 1$. We say that A *ramifies* at P, or that P is *ramified* in A, if $m_P(A) > 1$. In the present discussion, the infinite primes of K will play an important role. Such infinite primes occur only when K is a number field. In this case, an infinite prime P of K corresponds to an archimedean valuation on K which extends the ordinary absolute value on the rational field $\mathbb{Q}$. The P-adic completion K_P is either the real field $\mathbb{R}$ (in which case P is called a *real prime*), or else the complex field $\mathbb{C}$ (and P is a *complex prime*).

Theorem 1.91. *Let A be a central simple K-algebra, and let m_P be the local index of A at an infinite prime P of K.*

(i) *If P is a complex prime, then $A_P \sim K_P$ and $m_P = 1$.*

(ii) *If P is a real prime, then either $A_P \sim K_P$ and $m_P = 1$, or else $A_P \sim \mathbb{H}$ and $m_P = 2$, where $\mathbb{H}$ is the division algebra of real quaternions.*

If P is any finite prime of K, then K_P is a complete field relative to a discrete valuation, and has a finite residue class field. We defined the Hasse invariant $\mathrm{inv}[A_P]$ of

a central simple K_P-algebra, thereby obtaining an isomorphism $\text{inv} : \text{Br}(K_P) \simeq \mathbb{Q}/\mathbb{Z}$. We showed that

$$\begin{cases} \text{inv}[A_P] = s_P/m_P, \\ \exp[A_P] = m_P, \end{cases} \tag{1.6}$$

where $m_P = \text{ind}[A_P]$, $(s_P, m_P) = 1$.

We would like to have the same formulas true for the case of infinite primes. First we define Hasse invariants when P is an infinite prime, and it is sufficient to define these invariants for the three cases $\mathbb{C}$, $\mathbb{R}$ and $\mathbb{H}$. Set

$$\text{inv}[\mathbb{C}] = 0, \quad \text{inv}[\mathbb{R}] = 0, \quad \text{inv}[\mathbb{H}] = 1/2.$$

Formulas (1.6) then hold equally well when P is infinite provided we know that $\exp[\mathbb{H}] = 2$ when $[\mathbb{H}]$ is considered as an element of $\text{Br}(\mathbb{R})$.

Now let A be any central simple K-algebra, and let P be any prime of K (finite or infinite). Clearly, $A \sim K \Rightarrow A_P \sim K_P$ for all P. It can be proved the extremely important converse of this implication, by using the Hasse Norm Theorem. Let L be a finite Galois extension of K, with Galois group $G = \text{Gal}(L/K)$. Let P be a prime of K, finite or infinite.

Even when P is a finite prime, it is convenient to think of P as representing a class of valuations on K, rather than an ideal in some valuation ring. From this point of view, the valuation P extends to a finite set of inequivalent valuations on L, denoted by $\mathfrak{p}(= \mathfrak{p}_1), \mathfrak{p}_2, \ldots, \mathfrak{p}_g$. For each $\sigma \in G$, there is a valuation $\mathfrak{p}^\sigma$ on L, defined by the formula $\mathfrak{p}^\sigma(x) = \mathfrak{p}(\sigma^{-1}x), x \in L$. We call $\mathfrak{p}^\sigma$ a *conjugate* of $\mathfrak{p}$. If $\mathfrak{p}$ is a finite prime, then σ carries the valuation ring of $\mathfrak{p}$ onto the valuation ring of $\mathfrak{p}^\sigma$. Whether or not $\mathfrak{p}$ is finite, each $\mathfrak{p}_i$ is of the form $\mathfrak{p}^\sigma$ for some $\sigma \in G$.

We set $G_\mathfrak{p} = \{\sigma \in G : \mathfrak{p}^\sigma = \mathfrak{p}\}$, and call $G_\mathfrak{p}$ the *decomposition group* of $\mathfrak{p}$ relative to the extension L/K. The groups $\{G_{\mathfrak{p}_i}\}$ are mutually conjugate in G. Each $\sigma \in G_\mathfrak{p}$ induces a K_P-automorphism $\widehat{\sigma}$ of the $\mathfrak{p}$-adic completion $L_\mathfrak{p}$, since σ maps each Cauchy sequence from L (relative to the $\mathfrak{p}$-adic valuation) onto another such sequence. The map $\sigma \to \widehat{\sigma}$ yields an isomorphism $G_\mathfrak{p} \cong \text{Gal}(L_\mathfrak{p}/K_P)$. We define $n_P = [L_\mathfrak{p} : K_P]$ the *local degree* of L/K at P. Then $n_P = |G_\mathfrak{p}|$ and $n_P | [L : K]$ for each P. Notice that the fields $\{L_{\mathfrak{p}_i} : 1 \leq i \leq g\}$ are mutually K_P-isomorphic, so n_P does not depend on the choice of the prime $\mathfrak{p}$ of L which extends P.

The next theorem is of fundamental importance for the entire theory of simple algebras over number fields.

Theorem 1.92 (Hasse Norm Theorem). *Let L be a finite cyclic extension of the number field K and let $a \in K$. For each prime P of K, we choose a prime $\mathfrak{p}$ of L which*

extends P. Then

$$a \in N_{L/K}(L) \iff a \in N_{L_\mathfrak{p}/K_P}(L_\mathfrak{p}) \text{ for each } P.$$

The theorem asserts that a is a *global* norm (from L to K) if and only if at each P, a is a *local* norm (from $L_\mathfrak{p}$ to K_P). Notice that the theorem does not refer to algebras, it concerns number fields only. In the case when the degree n of L/K is a prime number, the Norm Theorem was known for a long time already, in the context of the reciprocity law of class field theory. It has been included in Hasse's class field report from 1930 where Hasse mentioned that it had first been proved by Furtwängler in 1902. For quadratic fields ($n = 2$) the Norm Theorem had been given by Hilbert in 1897. In 1931 Hasse succeeded to generalize this statement to arbitrary cyclic extensions L/K of number fields, not necessarily of prime degree.

If $\mathfrak{p}$ and $\mathfrak{p}'$ are primes of L, both of which extend P, then there is a K_P-isomorphism $L_\mathfrak{p} \cong L_{\mathfrak{p}'}$, and therefore

$$N_{L_\mathfrak{p}/K_P}(L_\mathfrak{p}) = N_{L_{\mathfrak{p}'}/K_P}(L_{\mathfrak{p}'}).$$

This shows that in determining local norms at P, it does not matter which prime $\mathfrak{p}$ of L we use, provided only that $\mathfrak{p}$ is an extension of the valuation P from K to L.

It can be easily proved that every global norm is also a local norm at each P. The difficult part of the proof of Hasse's Norm Theorem is the converse: if $a \in K$ is a local norm at each P, then a is a global norm. In proving this, it is necessary to know that A is a local norm at EVERY prime P of K, including the infinite primes. The theorem breaks down if we drop the hypothesis that L/K be cyclic. There are counterexamples even when L/K is abelian.

Corollary 1.93. *Let $A = (L/K, \sigma, a)$ be a cyclic algebra, where $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ and $a \in K^*$. Then $A \sim K$ if and only if $A_P \sim K_P$ for each prime P of K.*

The following result is also known as the "Local–Global Principle for algebras".

Theorem 1.94 (Hasse–Brauer–Noether–Albert). *Let A be a central simple K-algebra. Then*

$$A \sim K \iff A_P \sim K_P \text{ for each prime } P \text{ of } K.$$

Remarks 1.95. (i) For each prime P of K, there is a homomorphism $\mathrm{Br}(K) \to \mathrm{Br}(K_P)$ defined by $K_P \otimes_K -$. Let $[A] \in \mathrm{Br}(K)$ and m_P be the local index of A at P. Then $m_P = 1$ almost everywhere, which means that $[A_P] = 1$ almost everywhere. Hence there is a well defined homomorphism

$$\mathrm{Br}(K) \to \bigoplus_P \mathrm{Br}(K_P).$$

The Hasse–Brauer–Noether–Albert Theorem is precisely the assertion that this map is monic.

(ii) A stronger result, due to Hasse, describes the image of $\mathrm{Br}(K)$ in $\bigoplus_P \mathrm{Br}(K_P)$ by means of Hasse invariants. It can be shown that the following sequence is exact:

$$1 \to \mathrm{Br}(K) \to \bigoplus_P \mathrm{Br}(K_P) \stackrel{\mathrm{inv}}{\to} \mathbb{Q}/\mathbb{Z} \to 0, \tag{1.7}$$

where inv denotes the Hasse invariant map, computed locally on each component: $\mathrm{inv} = \bigoplus \mathrm{inv}_{K_p}$. From the exactness of the previous sequence (1.7) it follows the next relation which is considered many times a formulation of the Hasse–Brauer–Noether–Albert Theorem in terms of Hasse invariants:

$$\sum_P \mathrm{inv}[A_P] = 0,\ [A] \in \mathrm{Br}(K). \tag{1.8}$$

Of course, $\mathrm{inv}[A_P] = 0$ if P is a complex prime, while $\mathrm{inv}[A_P] = 0$ or $1/2$ if P is a real prime. The exactness of (1.7) also tells us that, other than (1.8), these are the *only* conditions which the set of local invariants $\{\mathrm{inv}[A_P]\}$ must satisfy. In other words, suppose that we are given in advance any set of fractions $\{x_P\}$ from $\mathbb{Q}/\mathbb{Z}$, such that $x_P = 0$ almost everywhere, $\sum x_P = 0$, $x_P = 0$ if P is complex, $x_P = 0$ or $1/2$ if P is real. Then there is a unique $[A] \in \mathrm{Br}(K)$ such that

$$\mathrm{inv}[A_P] = x_P \text{ for all } P.$$

As a first application of Theorem 1.94, we give a simple criterion for deciding whether a finite extension of the global field K splits a given central simple K-algebra.

Theorem 1.96. *Let A be a central simple K-algebra. For each prime P of K, let $m_P = \mathrm{ind}[A_P]$. Let L be any finite extension of K, not necessarily a Galois extension. Then L is a splitting field extension for A if and only if for each prime $\mathfrak{p}$ of L,*

$$m_P | [L_\mathfrak{p} : K_P], \tag{1.9}$$

where P is the restriction of $\mathfrak{p}$ to K.

Proof. If P is the restriction to K of a prime $\mathfrak{p}$ of L, then $L_\mathfrak{p} \otimes_{K_P} A_P \cong L_\mathfrak{p} \otimes_L (L \otimes_K A)$. If L splits A, then $L \otimes_K A \sim L$, whence $L_\mathfrak{p} \otimes_{K_P} A_P \sim L_\mathfrak{p}$, and so $L_\mathfrak{p}$ splits A_P and relation (1.9) follows.

Conversely, suppose that (1.9) holds for each $\mathfrak{p}$. Then (for each $\mathfrak{p}$) $L_\mathfrak{p}$ splits A_P, by Corollary 1.88. It follows that the central simple L-algebra $L \otimes_K A$ is split locally at every prime $\mathfrak{p}$ of L. Hence by Theorem 1.94, $L \otimes_K A \sim L$. Therefore, L splits A, as claimed. □

Theorem 1.97. *Let A be a central simple K-algebra with local indices $\{m_P\}$, where P ranges over the primes of K. Then* $\exp[A] = \operatorname{lcm}\{m_P\}$*, the least common multiple of the m_P's.*

Proof. By Theorem 1.94, $[A]^t = 1$ in $\mathrm{Br}(K)$ if and only if $[A_P]^t = 1$ in $\mathrm{Br}(K_P)$ for each P. But $\exp[A_P] = m_P$, so $[A_P]^t = 1$ if and only if $m_P | t$, by each m_P, hence $\exp[A] = \operatorname{lcm}\{m_P\}$. □

Two of the major consequences of the Brauer–Hasse–Noether–Albert Theorem are the following two theorems.

Theorem 1.98. *Let $[A] \in \mathrm{Br}(K)$ have local indices $\{m_P\}$. Then*

$$\operatorname{ind}[A] = \exp[A] = \operatorname{lcm}\{m_P\}.$$

Theorem 1.99. *Every central simple K-algebra is isomorphic to a cyclic algebra.*

Remark 1.100. Theorem 1.99 has become known as the Brauer–Hasse–Noether Theorem and was also called the "Main Theorem" in the theory of algebras. It appeared for the first time in a special volume of Crelle's Journal who was dedicated to Kurt Hensel (the mathematician who had discovered p-adic numbers) on his 70th birthday, since he was the chief editor of the journal at that time. The paper [BHN] had the title: *Proof of a Main Theorem in the theory of algebras* and was originally stated as follows:

> **Main Theorem.** *Every central division algebra over a number field is cyclic (or as it is also said, of Dickson type).*

The theorem asserts that every central division algebra over a number field K is isomorphic to $(L/K, \sigma, a)$ for a suitable cyclic extension L/K with generating automorphism σ and suitable $a \in K^*$. Equivalently, A contains a maximal commutative subfield L which is a cyclic field extension of K. The authors themselves, in the first sentence of their joint paper from 1932, tell us that they see the importance of the Main Theorem in the following two directions:

1. *Structure of division algebras*, since the theorem allows a complete classification of division algebras over a number field by means of what today are called Hasse invariants. Thereby the structure of the Brauer group of a number field is determined. This was elaborated in Hasse's subsequent paper from 1933 [Has2] which was dedicated to E. Noether on the occasion of her 50th birthday on March 23, 1932. The splitting fields of a division algebra can be explicitly described by their local behavior. This is important for the representation theory of groups and had been the main motivation for R. Brauer in this project.

2. *Beyond the theory of algebras*, the theorem opened new directions into one of the most exciting ares of algebraic number theory at the time, namely the understanding of Class Field Theory (its foundation, its structure and its generalization) by means of the structure of algebras. This had been suggested for some time by E. Noether.

Example 1.101. Let us determine some of the local Hasse invariants of the cyclic algebra $A = (L/K, \sigma, a)$, where $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ and $a \in K^*$. Let P denote a prime of K, and $\mathfrak{p}$ an extension of P to L. Then by [Rei, Proposition 30.8] we have $A_P \sim (L_\mathfrak{p}/K_P, \sigma^k, a)$, where k is the least positive integer such that σ^k lies in the decomposition group $G_\mathfrak{p}$ of $\mathfrak{p}$ relative to L/K. Of course, $\mathrm{inv}[A_P] = 0$ whenever $A_P \sim K_P$.

(i) If P is complex, or if both P and $\mathfrak{p}$ are real, then $A_P \sim K_P$.

(ii) Suppose that P is real, $\mathfrak{p}$ complex. Then $A_P \sim K_P$, if $a_P > 0$, and $A_P \sim \mathbb{H}$, if $a_P < 0$, where a_P represents the image of a under the embedding $K \to K_P$. In the latter case, $\mathrm{inv}[A_P] = \frac{1}{2}$.

(iii) Let P be a finite prime, and assume that P is unramified in the extension L/K. This is equivalent to assuming that $L_\mathfrak{p}/K_P$ is unramified. Since $G_\mathfrak{p} = \langle\sigma^k\rangle$, we may choose $r \in \mathbb{Z}$ relatively prime to the local degree $n_P = |G_\mathfrak{p}|$, such that σ^{kr} is the Frobenius automorphism of the extension $L_\mathfrak{p}/K_P$. We obtain

$$\mathrm{inv}[A_P] = r \cdot v_P(a)/n_P,$$

where v_P is the exponential P-adic valuation. If we reduce the fraction $r \cdot v_P(a)/n_P$ to lowest terms, then m_P is the denominator of the fraction thus obtained. In particular, $m_P = 1$ whenever $v_P(a) = 0$. Thus, $m_P = 1$ for every finite prime P, except possibly for those primes P which ramify in L/K, or which contain a. □

1.9 Schur groups

The simple components of a semisimple group algebra are called *Schur algebras* and represent the elements of a subgroup in the Brauer group, called the *Schur subgroup*. In this section we provide information about Schur algebras and cyclotomic algebras, main ingredients in the Brauer–Witt Theorem. The study of the Schur subgroup of the Brauer group was begun by Issai Schur (1875–1941) in the beginning of the last century. The Schur group of a field K, denoted by $S(K)$, is the answer to the following question:

> What are the classes in $\mathrm{Br}(K)$ occurring in the Wedderburn decomposition of the group algebra KG?

Considering an irreducible character of the group G that takes values in the field K, the Wedderburn component of KG corresponding to the character is a central simple K-algebra. The Schur group of K hence delimits the possibilities for the division ring part of this component, independently on the group G under consideration. There are interesting problems related to this topic such as to compute the associated Schur subgroup $S(K)$ of a given field K or to find properties of a given Schur algebra over K. The Brauer–Witt Theorem has been the corner stone result for solving these questions. It asserts that in order to calculate $S(K)$, one may restrict to the classes in $\mathrm{Br}(K)$ containing cyclotomic algebras.

In this section we consider a field K of characteristic 0. In fact, the Schur group over fields of positive characteristic is trivial, as we already explained at the end of section 1.5.

Definition 1.102. Let A be a central simple algebra over K. If A is spanned as a K-vector space by a finite subgroup of its group of units A^*, then A is called a *Schur algebra* over K. Equivalently, A is a Schur algebra over K if and only if A is a simple component central over K of the group algebra KG for some finite group G. The *Schur subgroup*, denoted by $S(K)$, of the Brauer group $\mathrm{Br}(K)$, consists of those classes that contain a Schur algebra over K. The fact that $S(K)$ is a subgroup of $\mathrm{Br}(K)$ is a direct consequence of the isomorphism $KG \otimes_K KH \cong K(G \times H)$.

Definition 1.103. A *cyclotomic algebra* over K is a crossed product algebra $(K(\zeta)/K, \tau)$, where ζ is a root of 1, the action is the natural action of $\mathrm{Gal}(K(\zeta)/K)$ on $K(\zeta)$ and all the values of the 2-cocycle τ are roots of 1 in $K(\zeta)$.

Lemma 1.104. *Let $C_1 = (K(\zeta_{n_1})/K, \tau_1)$ and $C_2 = (K(\zeta_{n_2})/K, \tau_2)$ be two cyclotomic algebras over K, where ζ_{n_i} are roots of 1, for $i = 1, 2$.*

Then the tensor product $C_1 \otimes_K C_2$ is Brauer equivalent to a cyclotomic algebra $C = (K(\zeta_m)/K, \tau)$, where m is the least common multiple of n_1 and n_2 and τ is the 2-cocycle $\mathrm{Inf}(\tau_i)\mathrm{Inf}(\tau_2)$ for $\mathrm{Inf} = \mathrm{Inf}_{K(\zeta_{n_i})/K \to K(\zeta_m)/K}$.

Proof. Using Proposition 1.59 and $\mathrm{Inf}_{K(\zeta_{n_i})/K \to K(\zeta_m)/K}$, we inflate the cyclotomic algebras C_i, for $i = 1, 2$ to the crossed product algebras $C_i' = (K(\zeta_m)/K, \mathrm{Inf}(\tau_i))$ that are similar to C_i. Moreover, the algebras C_i' are cyclotomic algebras because the values of its 2-cocycles $\mathrm{Inf}(\tau_i)$ are roots of 1 in $K(\zeta_m)$ by the definition of the inflation.

Furthermore, using Proposition 1.55 we can now have the tensor product over K of the cyclotomic algebras C_1' and C_2' and obtain an algebra which is Brauer equivalent to the cyclotomic algebra $C = (K(\zeta_m)/K, \mathrm{Inf}(\tau_i)\mathrm{Inf}(\tau_2))$. Denote now by τ the 2-cocycle $\mathrm{Inf}(\tau_i)\mathrm{Inf}(\tau_2)$ and obtain the desired result. □

Let us consider the set of all those elements of the Brauer group $\mathrm{Br}(K)$ which are represented by a cyclotomic algebra over K. Then this is a subgroup of $\mathrm{Br}(K)$. One can consider this subgroup and the Schur subgroup $S(K)$ of $\mathrm{Br}(K)$. The following proposition gives one inclusion between these two subgroups.

Proposition 1.105. *A cyclotomic algebra over K is a Schur algebra over K.*

Proof. Let $A = (K(\zeta)/K, \tau)$ be a cyclotomic algebra over K, that is, a crossed product

$$K(\zeta) *_\tau^\alpha \mathrm{Gal}(K(\zeta)/K) = \bigoplus_{\sigma \in \mathrm{Gal}(K(\zeta)/K)} K(\zeta)\overline{\sigma},$$

where ζ is a root of 1, the action α is the natural action of $\mathrm{Gal}(K(\zeta)/K)$ on $K(\zeta)$ and all the values of the 2-cocycle τ are roots of 1 in $K(\zeta)$. The values of the 2-cocycle τ and ζ generate a finite cyclic group $\langle \zeta' \rangle$ in the group of units $K(\zeta)^*$ and $K(\zeta') = K(\zeta)$, where ζ' is some root of unity, so we may assume that $\zeta = \zeta'$. The Galois group $\mathrm{Gal}(K(\zeta)/K)$ can be regarded as a subgroup of the group of automorphisms of the cyclic group $\langle \zeta \rangle$ and the values of the 2-cocycle belong to $\langle \zeta \rangle$.

The elements $\overline{\sigma}$, for $\sigma \in \mathrm{Gal}(K(\zeta)/K)$ and ζ generate a finite subgroup G in the multiplicative group of units of the algebra A. This happens because from the formulas $\overline{\sigma}\zeta^i = \zeta^\sigma \overline{\sigma}$ and $\overline{\sigma}\overline{\beta} = \tau(\sigma, \beta)\overline{\sigma\beta}$ one deduces that $\langle \zeta \rangle$ is a normal subgroup of G and the factor group $G/\langle \zeta \rangle$ is isomorphic to $\mathrm{Gal}(K(\zeta)/K)$, hence one has the short exact sequence

$$1 \to \langle \zeta \rangle \to G \to \mathrm{Gal}(K(\zeta)/K) \to 1.$$

Since G spans A with coefficients in K, the center of A, it follows that A is a Schur algebra over K. □

The other inclusion, namely of $S(K)$ in the subgroup formed by classes in $\mathrm{Br}(K)$ that are represented by a cyclotomic algebra over K, is given by the Brauer–Witt Theorem. In the 1950's, R. Brauer and E. Witt independently found that questions on the Schur subgroup are reduced to a treatment for a cyclotomic algebra. It follows that $S(K) = C(K)$ and so, one only has to study cyclotomic algebras over K on all matters about the Schur subgroup $S(K)$. A precise formulation of the theorem is the following and a proof of Theorem 1.106 is given in the next chapter.

Theorem 1.106 (Brauer–Witt). *A Schur algebra over K, that is, a simple component of a group algebra KG with center K, is Brauer equivalent to a cyclotomic algebra over K.*

The elements of the Brauer group are characterized by invariants, hence it is reasonable to ask whether the elements of $S(K)$ are distinguished in $\mathrm{Br}(K)$ by behavior of invariants. M. Benard had shown the following [Ben].

Theorem 1.107. *If $[A] \in S(K)$, for K an abelian number field, p is a rational prime and P_1, P_2 are primes of K over the prime p, then $A \otimes_K K_{P_1}$ and $A \otimes_K K_{P_2}$ have the same index.*

Furthermore, M. Benard and M. Schacher in [BeS] have shown the following.

Theorem 1.108. *If $[A] \in S(K)$ then:*

(1) *If the index of A is m then ζ_m is in K, where ζ_m is a primitive m-th root of unity.*

(2) *If P is a prime of K lying over the rational prime p and $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ with $\zeta_m^\sigma = \zeta_m^b$ then the p-invariant of A satisfies:* $\mathrm{inv}_P(A) \equiv b\,\mathrm{inv}_{P^\sigma}(A) \mod 1$.

If a central simple algebra A over K satisfies (1) and (2) above then A is said to have *uniformly distributed invariants*. Based on this result, R.A. Mollin defined the group $U(K)$ as the subgroup of $\mathrm{Br}(K)$ consisting of those algebra classes which contain an algebra with uniformly distributed invariants [Mol]. It follows from the Benard-Schacher result that $S(K)$ is a subgroup of $U(K)$. General properties of $U(K)$ and the relationship between $S(K)$ and $U(K)$ are investigated in [Mol].

There are additional restrictions on the collection of local indices of central simple algebras that lie in the Schur subgroup of an abelian number field. The following is a consequence of results of Witt ([Wit], Satz 10 and 11). It also holds in the more general setting of central simple algebras over K that have uniformly distributed invariants [Mol].

Theorem 1.109. *If K is an abelian number field, $A \in S(K)$ and p is an odd prime, then $p \equiv 1 \mod m_p(A)$. If $p = 2$ then $m_2(A) \leq 2$.*

The previous result is also a consequence of a result from [Jan1] and [Yam] describing the Schur group of a subextension of a cyclotomic extension of the local field $\mathbb{Q}_p$, for p an odd prime number.

Theorem 1.110. *Let k be a subfield of the cyclotomic extension $\mathbb{Q}_p(\zeta_m)$, $e = e(k/\mathbb{Q}_p)$ and e_0 the largest factor of e coprime to p. Then $S(k)$ is a cyclic group of order $(p-1)/e_0$ and it is generated by the class of the cyclic algebra $(k(\zeta_p)/k, \sigma, \zeta)$, where ζ is a generator of the group of roots of unity in k with order coprime to p.*

For a field K and a positive integer n, let $W(K, n)$ denote the group of roots of unity in K whose multiplicative order divides some power of n. In particular, if p is a prime, $W(K, p)$ denotes the roots of unity of p-power order in K. The next result from [Jan1] is a very useful reduction theorem.

Theorem 1.111. *Let K be a field of characteristic zero, L/K an extension and $G = \mathrm{Gal}(L/K)$. Let n be a fixed integer and suppose that $W(L,n)$ is finite. Let $K \leq F \leq L$ be such that*

(i) $\mathrm{Gal}(L/F) = \langle\theta\rangle$ *is cyclic,*

(ii) *the norm map $N_{L/F}$ carries $W(L,n)$ onto $W(F,n)$.*

Let $(L/K,\alpha)$ be a crossed product such that $\alpha \in W(L,n)$. Then there is a crossed product $(F/K,\beta)$, with $\beta \in W(F,n)$ such that $(L/K,\alpha)$ and $(F/K,\beta)$ lie in the same class of the Brauer group of K.

To fix the notation, let q be a prime integer, $\mathbb{Q}_q$ the complete q-adic rationals, and k a subfield of $\mathbb{Q}_q(\zeta_m)$ for some positive integer m. The following lemma from [Jan1] is helpful to compute the index of cyclic algebras over the local field k.

Proposition 1.112. *Let E/k be a Galois extension with ramification index $e = e(E/k)$ and ζ be a root of unity in k having order relatively prime to q. Then*

$$\zeta = N_{E/k}(x) \text{ for some } x \in E \quad \Longleftrightarrow \quad \zeta = \xi^e \text{ for } \xi \text{ a root of unity in } k.$$

Notice that by Corollary 1.57, having $A = (E/k,\sigma,a)$ a cyclic algebra, $\exp[A]$ is the least positive integer t such that $a^t \in N_{E/k}(E^*)$. Moreover, if $\exp[A] = [E:k]$, then A is a division algebra. This is a corollary of Theorem 1.56 which says that $(E/k,\sigma,a) \sim k$ if and only if $a \in N_{E/k}(E^*)$.) Proposition 1.112 gives a criterion to decide when $a^t \in N_{E/k}(E^*)$, for a a root of 1, that is, exactly when $a^t = \xi^{e(E/k)}$, for ξ a root of 1 in k.

By the Brauer–Witt Theorem, every Schur algebra is equivalent to a cyclotomic algebra and, if the center is a number field, then it is isomorphic to a cyclic algebra. We call *cyclic cyclotomic algebra* the algebra with these two features. Let K be a number field.

Definition 1.113. A *cyclic cyclotomic algebra* over K is a cyclic algebra that can be presented in the form $(K(\zeta)/K,\sigma,\xi)$, where ζ and ξ are roots of unity.

A Schur algebra over K is cyclic cyclotomic algebra if and only if it is generated over K by a metacyclic group if and only if it is a simple component of a group algebra KG for G a metacyclic group (see e.g. [OdRS1]).

In Chapter 6 we will study some properties of these algebras. The next proposition gives information about the local indices of cyclic cyclotomic algebras.

Proposition 1.114. *Let $A = (K(\zeta_n)/K, \sigma, \zeta_m)$, where K is a number field and ζ_n and ζ_m are roots of unity of orders n and m respectively. If p is a prime of K, then $m_p(A)$ divides m and if $m_P(A) \neq 1$ and p is a finite prime then p divides n.*

Proof. $[A]^m = [(K(\zeta_n)/K, \sigma, 1)] = 1$, hence $m_p(A)$ divides $m(A)$ which divides m. Furthermore, if $p \nmid n$, then $K(\zeta_n)/K$ is unramified at p and $v_p(\zeta_m) = 0$ since ζ_m is a unit in the ring of integers of K. By Theorem 1.76, the equation $N_{K_p(\zeta_n)/K_p}(x) = \zeta_m$ has a solution in $K(\zeta_n)$ and so $m_p(A) = 1$. □

Notes on Chapter 1

This chapter mainly contains standard material on the topics listed as sections of the chapter. The references used to collect the definitions and results presented in this chapter are mainly [Bro, CR, FD, Hup, Isa, Pie, Rei, Seh, Ser].

Now we give a few biographical notes about the main contributors to the development of the theory of central simple algebras, principal structures in this book. We reserve some space at the end of the next chapter for R. Brauer.

Emmy Noether (1882–1935) had a great influence on the development of many of the results presented in this chapter. She strongly proposed that the non-commutative theory of algebras should be used for a better understanding of commutative algebraic number theory, in particular class field theory. She also had an important contribution to the theory of algebras and an important role, together with R. Brauer and H. Hasse, in the proof of the "Main Theorem in the theory of algebras".

Helmut Hasse (1898–1979) was the one who actually wrote the article [BHN] with the proof of the Main Theorem. He also established a collaboration with A. Albert who had, mainly independently, an important contribution to the development of the theory of algebras.

A. Adrian Albert (1905–1972) was a disciple of L.E. Dickson. Albert remained interested for the rest of his career with the crossed product algebras he had studied in his earliest work.

Chapter 2

Wedderburn decomposition of group algebras

Let F be a field of characteristic zero and G a finite group. By the Maschke Theorem, the group algebra FG is semisimple and then FG is a direct sum of simple algebras. This decomposition is usually known as the Wedderburn decomposition of FG because the Wedderburn–Artin Theorem describes the simple factors, known as the Wedderburn components of FG, as matrix algebras over division rings.

The Wedderburn decomposition of a semisimple group algebra FG is a helpful tool for studying several problems. For example, a good description of the Wedderburn components has applications to the study of units [JL, JLdR, JdR, LdR, dRR, RitS2, Seh], automorphisms of group rings [CJP, Her3, OdRS2] or in coding theory if F is a finite field [KS, PH]. The computation of the Wedderburn decomposition of group algebras and, in particular, of the primitive central idempotents, has attracted the attention of several authors [BP, BdR, JLPo, OdR1, OdRS1].

In this chapter we present an algorithmic method to compute the Wedderburn decomposition of FG, for G an arbitrary finite group and F an arbitrary field of characteristic 0, which is based on a constructive approach of the Brauer–Witt Theorem. The Brauer–Witt Theorem states that the Wedderburn components of FG (i.e. the factors of its Wedderburn decomposition) are Brauer equivalent to cyclotomic algebras (see [Yam] or the original papers of R. Brauer [Bra2] and E. Witt [Wit]). By the computation of the Wedderburn decomposition of FG we mean the description of its Wedderburn components as Brauer equivalent to cyclotomic algebras. The Brauer–Witt Theorem is also a standard theoretical method for computing the Schur index of a character in the above situation. See [Shi], [Her2], [Her4] or [Her5] for an approach that studies this aspect of the theorem, i.e. the computation of the Schur index of the

simple components.

The computation of the Wedderburn decomposition of FG (i.e. the precise description of a list of cyclotomic algebras Brauer equivalent to the simple factors of FG) for a given semisimple group algebra FG is not obvious from the proofs of the Brauer–Witt Theorem available in the literature (e.g. see [Yam]). The proof of the Brauer–Witt Theorem presented in [Yam] relies on the existence, for each prime integer p, of a p-elementary subgroup of G that determines the p-part of a given simple component up to Brauer equivalence in the corresponding Brauer group. Our approach of the proof of the theorem uses strongly monomial characters or strongly monomial subgroups, that allow a good description of the simple algebras, instead of p-elementary subgroups. Moreover, with this approach the number of subgroups to look for is larger and eventually one could obtain easier a description of a simple component or even a description in which it is not necessary to consider each prime separately as it has to be done in general.

The identities of the Wedderburn components of FG are the primitive central idempotents of FG and can be computed from the character table of the group G. A character-free method to compute the primitive central idempotents of $\mathbb{Q}G$ for G nilpotent has been introduced in [JLPo]. In [OdRS1], it was shown how to extend the methods of [JLPo] to compute not only the primitive central idempotents of $\mathbb{Q}G$, if G is a strongly monomial group, but also the Wedderburn decomposition of $\mathbb{Q}G$. See section 2.1 for the definition of strongly monomial groups, where we also present several results on strongly monomial characters, mainly from [OdRS1]. This approach was generalized to arbitrary groups by using the Brauer–Witt Theorem in [Olt2]. We present this method in Section 2.2 of this chapter and we give the algorithmic proof of the Brauer–Witt Theorem in four steps. In section 2.3 we give a theoretical algorithm for the computation of the Wedderburn decomposition of a semisimple group algebra based on the algorithmic proof presented in the previous section.

2.1 Strongly monomial characters

The problem of computing the Wedderburn decomposition of a group algebra leads naturally to the problem of computing the primitive central idempotents of $\mathbb{Q}G$. The classical method used to do this is to calculate the primitive central idempotents $e(\chi)$ of $\mathbb{C}G$ associated to the irreducible characters of G and then sum up all the primitive central idempotents of the form $e(\sigma \circ \chi)$ with $\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$ and $\chi \in \mathrm{Irr}(G)$ (see Proposition 1.24).

Recently, Jespers, Leal and Paques introduced a method to compute the primitive central idempotents of $\mathbb{Q}G$ for G a finite nilpotent group that does not use the character

table of G [JLPo]. Olivieri, del Río and Simón pointed out that the method from [JLPo] relies on the fact that nilpotent groups are monomial and used an old theorem of Shoda (see Theorem 1.26) to give an alternative presentation [OdRS1]. In this way, the method introduced by Jespers, Leal and Paques, that shows how to produce the primitive central idempotents of $\mathbb{Q}G$ from certain pairs of subgroups (H, K) of G, was simplified in [OdRS1] and the mentioned pairs (H, K) were named *Shoda pairs* of G. Furthermore, Olivieri, del Río and Simón noticed that if a Shoda pair satisfies some additional conditions, then one can describe the simple component associated to the given primitive central idempotent, denoted $e(G, H, K)$, as a specific cyclotomic algebra. This gives a constructive means of the Brauer–Witt Theorem for computing the Wedderburn decomposition of every semisimple group algebra, as we are going to see in this section.

The following results are mostly from [OdRS1] and play an important role in our proof of the Brauer–Witt Theorem. We present a method to calculate the primitive central idempotents of $\mathbb{Q}G$ in the case of finite monomial groups given in [OdRS1]. The primitive central idempotent of $\mathbb{Q}G$ associated to a monomial complex character of G is of the form $\alpha e(G, H, K)$, for $\alpha \in \mathbb{Q}$ and (H, K) a pair of subgroups of G that satisfy some easy to check conditions. We call these pairs of subgroups *Shoda pairs* due to their relation with a theorem of Shoda (Theorem 1.26).

Now we introduce some useful notation, mainly from [JLPo] and [OdRS1]. If $K \trianglelefteq H \leq G$ then let $\varepsilon(K, K) = \widehat{K} = \frac{1}{|K|}\sum_{k\in K} k \in \mathbb{Q}K$, and if $H \neq K$ then let

$$\varepsilon(H, K) = \prod_{M/K \in \mathcal{M}(H/K)} (\widehat{K} - \widehat{M}),$$

where $\mathcal{M}(H/K)$ denotes the set of all minimal normal subgroups of H/K.

Furthermore, let $e(G, H, K)$ denote the sum of the different G-conjugates of $\varepsilon(H, K)$ in $\mathbb{Q}G$, that is, if T is a right transversal of $\mathrm{Cen_G}(\varepsilon(\mathrm{H}, \mathrm{K}))$ in G, then $e(G, H, K) = \sum_{t\in T} \varepsilon(H, K)^t$, where $\mathrm{Cen_G}(\varepsilon(\mathrm{H}, \mathrm{K}))$ is the centralizer of $\varepsilon(H, K)$ in G. Clearly, $e(G, H, K)$ is a central element of $\mathbb{Q}G$. If the G-conjugates of $\varepsilon(H, K)$ are orthogonal, then $e(G, H, K)$ is a central idempotent of $\mathbb{Q}G$.

A *Shoda pair* of G is a pair (H, K) of subgroups of G with the properties that $K \trianglelefteq H$ and there is $\psi \in \mathrm{Lin}(H, K)$ such that the induced character ψ^G is irreducible, where $\mathrm{Lin}(H, K)$ denotes the set of linear characters of H with kernel K. Using Theorem 1.26, it is easy to show that a pair (H, K) of subgroups of G is a Shoda pair if and only if $K \trianglelefteq H$, H/K is cyclic, and if $g \in G$ and $[H, g] \cap H \subseteq K$ then $g \in H$. Moreover, if (H, K) is a Shoda pair of G, there is a unique rational number α such that $\alpha e(G, H, K)$ is a primitive central idempotent of $\mathbb{Q}G$ [OdRS1].

A *strong Shoda pair* of G is a Shoda pair (H, K) of G such that $H \trianglelefteq N_G(K)$ and the different conjugates of $\varepsilon(H, K)$ are orthogonal. If (H, K) is a strong Shoda pair then $e(G, H, K)$ is a primitive central idempotent of $\mathbb{Q}G$.

If (H, K) is a strong Shoda pair of G and $\psi_1, \psi_2 \in \mathrm{Lin}(H, K)$, then $A(\psi_1^G, \mathbb{Q}) = A(\psi_2^G, \mathbb{Q})$, so we denote $A(G, H, K) = A(\psi^G, \mathbb{Q})$ for any $\psi \in \mathrm{Lin}(H, K)$. In other words, the sum of the different characters induced by the elements of $\mathrm{Lin}(H, K)$ is an irreducible rational character of G and $A(G, H, K)$ is the simple component of $\mathbb{Q}G$ associated to this character. Consider now $\psi \in \mathrm{Lin}(H, K)$ and let $\psi(h) = \zeta_m$, an m-th primitive root of unity, where $H/K = \langle h \rangle$ and $m = [H : K]$. Denote by θ the induced character ψ^G. Notice that the character θ depends not only on the strong Shoda pair (H, K), but also on the choice of ζ_m. We refer to any of the possible characters $\theta = \psi^G$ with $\psi \in \mathrm{Lin}(H, K)$ as a *character induced by* the strong Shoda pair (H, K). If θ and θ' are two characters of G induced by (H, K) (with different choice of m-th roots of unity) then $e_{\mathbb{Q}}(\theta) = e(G, H, K) = e_{\mathbb{Q}}(\theta')$, i.e. θ and θ' are $\mathbb{Q}$-equivalent. Two strong Shoda pairs of G are said to be *equivalent* if they induce $\mathbb{Q}$-equivalent characters.

Definition 2.1. An irreducible *monomial* (respectively *strongly monomial*) *character* χ of G is a character of the form $\chi = \psi^G$ for $\psi \in \mathrm{Lin}(H, K)$ and some Shoda (respectively strong Shoda) pair (H, K) of G, or equivalently $A(\chi, \mathbb{Q}) = A(G, H, K)$ for some Shoda (respectively strong Shoda) pair (H, K) of G. Then we say that $A(G, H, K)$ is a monomial (respectively strongly monomial) component of $\mathbb{Q}G$.

Recall that a finite group G is *monomial* if every irreducible character of G is monomial. Similarly, we say that G is *strongly monomial* if every irreducible character of G is strongly monomial. It is well known that every abelian-by-supersolvable group is monomial, and recently it was proved that it is even strongly monomial [OdRS1]. In the same article it is shown that every monomial group of order less than 500 is strongly monomial. We recently found using the package `wedderga` that all monomial groups of order smaller than 1000 are strongly monomial and the smallest monomial non-strongly monomial group is a group of order 1000, the 86-th one in the library of the GAP system. However, there are irreducible monomial characters that are not strongly monomial in groups of smaller order. The group of the smallest order with such irreducible monomial non-strongly monomial characters has order 48.

If (H, K) is a strong Shoda pair of a group G, then one can give a description of the structure of the simple component $A(G, H, K)$ as a matrix algebra over a crossed product of an abelian group by a cyclotomic field with action and twisting that can be described with easy arithmetic using information from the group G. Namely, in [OdRS1, Proposition 3.4] it is shown the following.

Theorem 2.2. *Let (H, K) be a strong Shoda pair of G and $m = [H : K]$, $N = N_G(K)$, $n = [G : N]$, hK a generator of H/K and $n, n' \in N$. Then*

$$A(G, H, K) \simeq \mathcal{M}_n(\mathbb{Q}(\zeta_m) *_\tau^\alpha N/H),$$

where the action α and the twisting τ are given as follows: $\alpha(nH) = \zeta_m^i$, if $n^{-1}hnK = h^iK$ and $\tau(nH, n'H) = \zeta_m^j$, if $[n, n']K = h^jK$ and $i, j \in \mathbb{Z}$.

Proof. Let $\varepsilon = \varepsilon(H, K)$, $e = e(G, H, K)$ and T a right transversal of N in G, so that $e = \sum_{g\in T} \varepsilon^g$. First we prove that $\mathrm{Cen_G}(\varepsilon) = \mathrm{N_G(K)}$ and e is a primitive central idempotent of $\mathbb{Q}G$. Since $H \trianglelefteq N_G(K)$, it follows that $N_G(K) \leq \mathrm{Cen_G}(\varepsilon)$ because $\varepsilon^g = \varepsilon(H^g, K^g)$, for all $g \in G$. Now let $g \in \mathrm{Cen_G}(\varepsilon)$ and $k \in K$. Then $g^{-1}kg\varepsilon = g^{-1}k\varepsilon g = g^{-1}\varepsilon g = \varepsilon$, so $g^{-1}kg \in K$, hence $\mathrm{Cen_G}(\varepsilon) \subseteq \mathrm{N_G(K)}$. Furthermore, the action of N/H is faithful since (H, K) is a strong Shoda pairs, hence if $g \in N \setminus H$, then $[H, g] \cap H \not\subseteq K$. By Theorem 1.42, the algebra $\mathbb{Q}Ge$ is simple and e is a primitive central idempotent.

The elements of $\{\varepsilon^g | g \in G\}$ are orthogonal, hence $\mathbb{Q}Ge = \bigoplus_{g\in T} \mathbb{Q}G\varepsilon^g$. If $g \in G$, then the map given by $h \mapsto hg$ is an isomorphism between $\mathbb{Q}G\varepsilon$ and $\mathbb{Q}G\varepsilon^g$. Then ${}_{\mathbb{Q}G}\mathbb{Q}Ge = \bigoplus_{g\in T} \mathbb{Q}G\varepsilon^g \cong (\mathbb{Q}G\varepsilon)^n$. We have

$$\mathbb{Q}Ge \cong \mathrm{End}_{\mathbb{Q}G}(\mathbb{Q}Ge) \cong \mathrm{End}_{\mathbb{Q}G}(\mathbb{Q}G\varepsilon)^n \cong \mathcal{M}_n(\mathrm{End}_{\mathbb{Q}G}(\mathbb{Q}G\varepsilon)) \cong \mathcal{M}_n(\varepsilon\mathbb{Q}G\varepsilon).$$

But $\varepsilon\mathbb{Q}G\varepsilon = \mathbb{Q}N\varepsilon$ because, if $g \in G \setminus N$ then $\varepsilon g\varepsilon = gg^{-1}\varepsilon g\varepsilon = g\varepsilon^g\varepsilon = 0$. Furthermore, ε is a central idempotent in $\mathbb{Q}N$, so that $\varepsilon\mathbb{Q}N\varepsilon = \mathbb{Q}N\varepsilon$.

So far we obtained $\mathbb{Q}Ge \cong \mathcal{M}_n(\mathbb{Q}N\varepsilon)$. To finish the proof we show that $\mathbb{Q}N\varepsilon \cong \mathbb{Q}(\zeta_m) *_\tau^\sigma N/H$. Using the crossed product structure $\mathbb{Q}N \cong \mathbb{Q}H * N/H$, one has that $\mathbb{Q}N\varepsilon = \mathbb{Q}H\varepsilon *_{\tau'}^{\sigma'} N/H$ is a crossed product of N/H over the field $\mathbb{Q}H\varepsilon$. Since H/K is cyclic, $\varepsilon = e_{\mathbb{Q}}(\psi)$, where ψ is a linear character of H with kernel K, hence $\mathbb{Q}H\varepsilon = \mathbb{Q}He_{\mathbb{Q}}(\psi) \cong \mathbb{Q}(\zeta_m)$ and the isomorphism of $\mathbb{Q}H\varepsilon$ to $\mathbb{Q}(\zeta_m)$ is given by $K \mapsto 1$ and $h \mapsto \zeta_m$, where $H = \langle K, h\rangle$. The isomorphism $\mathbb{Q}H\varepsilon \cong \mathbb{Q}(\zeta_m)$ extends naturally to an N/H-graded isomorphism

$$\mathbb{Q}H\varepsilon *_{\tau'}^{\sigma'} N/H \cong \mathbb{Q}(\zeta_m) *_\tau^\sigma N/H,$$

where σ, τ are the action and the twisting $\sigma : N/H \to \mathrm{Aut}(\mathbb{Q}(\zeta_m))$, $\tau : N/H \times N/H \to \mathcal{U}(\mathbb{Q}(\zeta_m))$ given by $\sigma_n(\zeta_m) = \zeta_m^i$, if $h^nK = h^iK$ and $\tau(n, n') = \zeta_m^j$, if $[n, n']K = h^jK$, for $i, j \in \mathbb{Z}$. So we have that $\mathbb{Q}N\varepsilon \cong \mathbb{Q}(\zeta_m) *_\tau^\sigma N/H$. □

The action σ and the twisting τ of the crossed product are the action and the twisting associated to the short exact sequence of the group extension

$$1 \to H/K \cong \langle\zeta_m\rangle \to N/K \to N/H \to 1.$$

The action is provided by the action of N/K on H/K by conjugation, that gives the action σ of N/K in $\mathrm{Aut}(\mathbb{Q}(\zeta_m))$.

2.2 An algorithmic approach of the Brauer–Witt Theorem

The Brauer–Witt Theorem states that the simple component $A(\chi, F)$ corresponding to the irreducible character χ of the group G over the field F is a simple algebra which is Brauer equivalent to a cyclotomic algebra over its center $\mathbb{F} = F(\chi)$, that is, a crossed product algebra $(\mathbb{F}(\zeta)/\mathbb{F}, \tau)$, with ζ a root of unity and all the values of the 2-cocycle τ roots of unity in $\mathbb{F}(\zeta)$.

In this section we present a new proof of the Brauer–Witt Theorem that gives a method to explicitly construct the above cyclotomic algebra. Our proof of the Brauer–Witt Theorem is divided into four steps that one could name as: *constructible description* for the strongly monomial case, *reduction* to the strongly monomial case, *existence* of strongly monomial characters and *change of field*.

First we present the strongly monomial case, that is, the *constructible description* of the simple component associated to a strongly monomial character. The *reduction* of the problem to strongly monomial subgroups is presented next. The reduction step consists of describing the p-part of $A(\chi, F)$ as the p-part of the algebra $A(\theta, F)$ associated to a strongly monomial character θ of a subgroup of G. Then we are faced with the problem of showing that the desired strongly monomial character θ does exist, for every prime p. One of the conditions on θ in the reduction step is that $\mathbb{F}(\theta) = \mathbb{F}$, and it is not always true that such a character with this condition exists. However, it does exist a character θ such that $\mathbb{F}(\theta) \subseteq L_p$, where L_p is the p'-splitting field of $A(\chi, F)$ (see 3.2. for the definition). The proof of the *existence* of the desired strongly monomial character uses the Witt–Berman Theorem. This step is the third step. So we have gone up to each L_p to describe the p-part and now we have to return to the initial field F. The way back is the *change of field* part which is obtained through the corestriction map.

The strongly monomial case

The following proposition provides the constructible Brauer–Witt Theorem for strongly monomial characters. It gives a precise description of the simple algebra associated to a strongly monomial character as a matrix algebra of a cyclotomic algebra. In this particular case, one obtains the description of the strongly monomial simple component at once, without the need to follow the next steps as it has to be done in the general case.

Proposition 2.3. *Let (H, K) be a strong Shoda pair of the group G, $\psi \in \mathrm{Lin}(H, K)$, $N = N_G(K)$, $m = [H : K]$ and $n = [G : N]$. Then $N/H \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\psi^G))$.*

Furthermore, if F is a field of characteristic 0, $\mathbb{F} = F(\psi^G)$, $d = \frac{[\mathbb{Q}(\zeta_m):\mathbb{Q}(\psi^G)]}{[\mathbb{F}(\zeta_m):\mathbb{F}]}$ and τ' is the restriction to $\mathrm{Gal}(\mathbb{F}(\zeta_m)/\mathbb{F})$ of the cocycle τ associated to the natural extension

$$1 \to H/K \simeq \langle \zeta_m \rangle \to N/K \to N/H \to 1 \tag{2.1}$$

then

$$A(\psi^G, F) \simeq \mathcal{M}_{nd}(\mathbb{F}(\zeta_m)/\mathbb{F}, \tau'). \tag{2.2}$$

Proof. It is proved in Theorem 2.2 that

$$A(\psi^G, \mathbb{Q}) \simeq \mathcal{M}_n(\mathbb{Q}(\zeta_m) *_\tau^\alpha N/H),$$

where the action α is induced by the natural conjugation map $f : N \to \mathrm{Aut}(H/K) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ and the twisting is the cocycle τ given by the exact sequence (2.1). Since H/K is maximal abelian in N/K, the kernel of f is H. The center of $A(\psi^G, \mathbb{Q})$ is $\mathbb{Q}(\psi^G)$, hence $f(N/H) \subseteq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\psi^G))$ and the isomorphism holds because $[N : H] = \frac{\deg(A(\psi^G,\mathbb{Q}))}{n} = [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\psi^G)]$.

Furthermore, $[A(\psi^G, F)] = \mathrm{Res}_{\mathbb{Q}(\psi^G)\to\mathbb{F}}([A(\psi^G, \mathbb{Q})]) = [(\mathbb{F}(\zeta_m)/\mathbb{F}, \tau')]$ and

$$\frac{\deg(A(\psi^G, F))}{\deg(\mathbb{F}(\zeta_m)/\mathbb{F}, \tau')} = \frac{[G : H]}{[\mathbb{F}(\zeta_m) : \mathbb{F}]} = \frac{n[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\psi^G)]}{[\mathbb{F}(\zeta_m) : \mathbb{F}]} = nd,$$

which yields the isomorphism $A(\psi^G, F) \simeq \mathcal{M}_{nd}(\mathbb{F}(\zeta_m)/\mathbb{F}, \tau')$. □

Remark 2.4. Notice that the description in (2.2) can be given by the numerical information of a 4-tuple:

$$(nd, m, (o_i, \alpha_i, \beta_i)_{1\le i\le l}, (\gamma_{ij})_{1\le i<j\le l}), \tag{2.3}$$

where n, d and m are as in Proposition 2.3 and the tuples of integers $(\alpha_i)_{1\le i\le l}$, $(\beta_i)_{1\le i\le l}$, $(\gamma_{ij})_{1\le i<j\le l}$ satisfy the relations: $x^{g_i} = x^{\alpha_i}, g_i^{o_i} = x^{\beta_i}, [g_j, g_i] = x^{\gamma_{ij}}$, for x a generator of H/K, $g_1, \ldots, g_l \in N/K$ such that $N_1/H = \langle \overline{g_1} \rangle \times \cdots \times \langle \overline{g_l} \rangle$ (with $\overline{g_i}$ the image of $g_i \in N/K$ in N/H), where N_1/H is the image of $\mathrm{Gal}(\mathbb{F}(\zeta_m)/\mathbb{F})$ in N/H under the isomorphism $N/H \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\psi^G))$ and o_i is the order of $\overline{g_i}$, for every $i = 1, \ldots, l$.

Thus $A(\psi^G, F) \simeq M_{nd}(A)$, where A is the algebra defined by the following presentation:

$$A = \mathbb{F}(\zeta_m)(g_1, \ldots, g_l | \zeta_m^{g_i} = \zeta_m^{\alpha_i}, g_i^{o_i} = \zeta_m^{\beta_i}, g_j g_i = g_i g_j \zeta_m^{\gamma_{ij}}, 1 \le i < j \le l). \tag{2.4}$$

Reduction to strongly monomial characters

Let the finite group G have exponent n. For every irreducible character χ of G and every prime p, the *p'-splitting field* of the simple component $A(\chi, F)$ over $\mathbb{F} = F(\chi)$ is the unique field L_p between $\mathbb{F}$ and $\mathbb{F}(\zeta_n)$ such that $[\mathbb{F}(\zeta_n) : L_p]$ is a power of p and

$[L_p : \mathbb{F}]$ is relatively prime to p. That is, the field L_p is the field corresponding to the p-Sylow subgroup of $\mathrm{Gal}(\mathbb{F}(\zeta_n)/\mathbb{F})$ by the Galois correspondence.

Let D be a division algebra central over $\mathbb{F}$ with index m that has the following factorization into prime powers $m = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$. Then D is $\mathbb{F}$-isomorphic to the tensor product $D_1 \otimes D_2 \otimes \cdots \otimes D_s$, where D_i is a division algebra central over $\mathbb{F}$ with index $p_i^{a_i}$ for every i from 1 to s [Pie]. We call the algebra class $[D_i]$ the *p_i-part* of $[D]$ and we denote it by $[D]_{p_i}$. If $p \nmid m$, then let the p-part of $[D]$ be equal to $[\mathbb{F}]$, the identity in the Brauer group of $\mathbb{F}$. Recall that $m_{\mathbb{F}}(\chi)$ denotes the Schur index of χ over $\mathbb{F}$, which coincides with the Schur index of the simple component $A(\chi, F)$ of FG corresponding to χ. Furthermore, $m_{\mathbb{F}}(\chi)_p$ is the p-part of the Schur index of χ over $\mathbb{F}$.

The following proposition from [Yam, Proposition 3.8] gives the reduction part (up to Brauer equivalence) of the computation of a simple p-component $[A(\chi, F)]_p$, for every prime p, to the computation of the p-part corresponding to a suitable subgroup of G and an irreducible character of it that verifies some additional conditions.

Proposition 2.5. *Let G be a finite group of exponent n, χ an irreducible character of G, F a field of characteristic 0 and $\mathbb{F} = F(\chi)$. Let M be a subgroup of G and θ an irreducible character of M such that for each prime p*

$(*)$ *(χ_M, θ) is coprime to p and θ takes values in L_p, the p'-part of $F(\zeta_n)/F(\chi)$.*

Then one has $[A(\chi, F)]_p = [A(\theta, F)]_p$. Moreover, $m_{\mathbb{F}}(\chi)_p = m_{L_p}(\theta)$.

Proof. By Theorem 1.21, $\mathbb{F}(\zeta_n)$ is a splitting field for $\mathbb{F}G$. Thus, $\mathbb{F}(\zeta_n)$ is a splitting field for both $A(\chi, \mathbb{F})$ and $A(\theta, \mathbb{F})$. Let L_p be the p'-splitting field of the simple algebra $A(\chi, \mathbb{F})$. Then the exponents of $A(\chi, L_p)$ and $A(\theta, L_p)$ in $\mathrm{Br}(L_p)$ are both powers of p. Furthermore, if $\overline{\chi}$ is the character given by $\overline{\chi}(g) = \chi(g^{-1})$, for $g \in G$, then

$$[A(\chi \otimes \overline{\chi}, L_p)] = [A(\chi, L_p)] \cdot [A(\overline{\chi}, L_p)] = [L_p].$$

Hence, the character $\chi \otimes \overline{\chi}$ of $G \times G$ is realized in L_p, so the character $(\chi_M) \otimes \overline{\chi}$ of $M \times G$ is also realized in L_p. The character $\theta \otimes \overline{\chi}$ of $M \times G$ is irreducible and by hypothesis $L_p(\theta \otimes \overline{\chi}) \subseteq L_p$. Let $t = (\chi_M, \theta)$ such that $(p, t) = 1$, by hypothesis. Then

$$((\chi_M) \otimes \overline{\chi}, \theta \otimes \overline{\chi})_{M \times G} = (\chi_M, \theta)_M \cdot (\overline{\chi}, \overline{\chi})_G = (\chi_M, \theta) = t.$$

Hence the multiplicity of the character $\theta \otimes \overline{\chi}$ of $M \times G$ in the decomposition as a sum of irreducible characters of $(\chi_M) \otimes \overline{\chi}$ is t and therefore the Schur index $m_{L_p}(\theta \otimes \overline{\chi})$ divides t.

Since $[A(\theta \otimes \overline{\chi}, L_p)] = [A(\theta, L_p)] \cdot [A(\overline{\chi}, L_p)]$ and both exponents of $[A(\theta, L_p)]$ and $[A(\overline{\chi}, L_p)]$ are powers of p, it follows that the exponent of $[A(\theta \otimes \overline{\chi}, L_p)]$ is a power of p.

Furthermore, the exponent of $[A(\theta \otimes \overline{\chi}, L_p)]$ divides the Schur index $m_{L_p}(\theta \otimes \overline{\chi})$ that divides t. Because $(p,t) = 1$, one has $m_{L_p}(\theta \otimes \overline{\chi}) = 1$ and $[A(\theta, L_p)] = [A(\overline{\chi}, L_p)]^{-1} = [A(\chi, L_p)]$. By the injectivity of $\mathrm{Res} : \mathrm{Br}(\mathbb{F})_p \to \mathrm{Br}(L_p)_p$, one obtains that $[A(\chi, \mathbb{F})]_p = [A(\theta, \mathbb{F})]_p$.

Furthermore, $(m_{\mathbb{F}}(\chi))_p = m([A(\chi, \mathbb{F})]_p) = m([A(\chi, L_p)]) = m([A(\theta, L_p)]) = m_{L_p}(\theta)$. □

Existence of suitable strongly monomial characters

Proposition 2.5 states that the p-part of $A(\chi, F)$ is Brauer equivalent to the p-part of $A(\theta, F)$, provided (χ_M, θ) is coprime to p and χ and θ take values in $\mathbb{F}$. If θ is a strongly monomial character then this p-part would be described as explained in Proposition 2.3. Therefore, one would like to show that such a character θ does exist for every prime p dividing the Schur index of χ. However, this is not true. Alternatively, using the following Proposition 2.6, which is a corollary of the Witt–Berman Theorem (Theorem 1.32), one can find such a character θ if $\mathbb{F}$ is replaced by L_p, the p'-splitting field of $A(\chi, F)$.

Proposition 2.6. *Every $\mathbb{F}$-character of G is a $\mathbb{Z}$-linear combination $\sum_i a_i \theta_i^G$, where every $a_i \in \mathbb{Z}$ and each θ_i is an irreducible character of a strongly monomial subgroup of G.*

Proof. By the Witt–Berman Theorem (Theorem 1.32), every $\mathbb{F}$-character of G is a $\mathbb{Z}$-linear combination $\sum_i a_i \theta_i^G$, where the θ_i's are irreducible $\mathbb{F}$-characters of $\mathbb{F}$-elementary subgroups H_i of G. In particular, the H_i's are cyclic-by-p_i-groups for some primes p_i, and by [OdRS1] each H_i is strongly monomial. □

The next proposition establishes the existence of a strongly monomial subgroup and a character with the desired properties that appear in Proposition 2.5, relative to the field L_p, the p'-splitting field of $A(\chi, F)$.

Proposition 2.7. *Let the finite group G have exponent n, $\zeta = \zeta_n$ and χ be an irreducible $\mathbb{F}$-character of G. For every prime p, there exist a strongly monomial subgroup M of G and an irreducible character θ of M satisfying relation $(*)$ for every prime p:*

$(*)$ *(χ_M, θ) is coprime to p and θ takes values in L_p, the p'-part of $F(\zeta_n)/F(\chi)$.*

Proof. Let b be a divisor of $|G|$ such that $|G|/b$ is a power of p and $(p,b) = 1$. Then, by Proposition 2.6, $b1_G = \sum_i c_i \lambda_i^G$, where each λ_i is an $\mathbb{F}$-character of a subgroup M_i of G which is strongly monomial. Furthermore,

$$b\chi = \sum_i c_i \chi \lambda_i^G = \sum_i c_i (\chi_{M_i} \lambda_i)^G.$$

Moreover $\mathbb{F}(\chi_{M_i}) \subseteq \mathbb{F}(\chi) \subseteq \mathbb{F}$, $\mathbb{F}(\lambda_i) \subseteq \mathbb{F}$ for every i and $\mathbb{F}(\zeta)$ is a splitting field of every subgroup of G. Thus, if θ_j is a constituent of $\chi_{M_i}\lambda_i$, that is, θ_j appears in the decomposition of $\chi_{M_i}\lambda_i$ as a sum of irreducible characters, then (θ_j, λ_i) is multiple of $[\mathbb{F}(\theta_j) : \mathbb{F}]$ and therefore

$$b\chi = \sum_j d_j[\mathbb{F}(\theta_j) : \mathbb{F}]\theta_j^G,$$

where each θ_j is an irreducible character in a group M_j' which is strongly monomial. Then

$$b = (\chi, b\chi) = \sum_j d_j[\mathbb{F}(\theta_j) : \mathbb{F}](\chi, \theta_j^G).$$

Since b is not multiple of p, there is j such that if $M = M_j'$ and $\theta = \theta_j$ then $[\mathbb{F}(\theta) : \mathbb{F}](\chi, \theta^G)$ is not multiple of p. Thus (χ, θ^G) is not multiple of p. Since $\mathbb{F} \subseteq \mathbb{F}(\theta) \subseteq \mathbb{F}(\zeta)$ and $[\mathbb{F}(\zeta) : L_p]$ is a prime power, one has that $\mathbb{F}(\theta) \subseteq L_p$. □

Proposition 2.7 proves that, for each prime p, there exists a strongly monomial character θ of a subgroup M of G that takes values in L_p and (χ_M, θ) is coprime to p. Hence, from Proposition 2.5 it follows that $A(\chi, L_p)$ is Brauer equivalent to $A(\theta, L_p)$, because the index of $A(\chi, L_p)$ is a power of p.

Observe that it was proved that the subgroup M in Proposition 2.7 can be taken to be strongly monomial. Moreover, using the Witt–Berman Theorem, one can prove that M could be taken p-elementary. However, for practical reasons, it is better not to impose M to be p-elementary or even strongly monomial, because the role of M, or better said θ, is to use the presentation of $A(\theta, L_p)$ as a cyclotomic algebra given in Proposition 2.3 in order to describe the p-part of $A(\chi, L_p)$, which is Brauer equivalent to $A(\theta, L_p)$ by Proposition 2.5. So, by not imposing conditions on M but on θ, a strongly monomial character in a possibly non-strongly monomial group, the list of possible θ's is larger and it is easier to find the desired strongly monomial character. The proof of Proposition 2.7 does not provide a constructive way to find the character θ, but this is clearly a finite computable searching problem. One only needs to compute L_p, an easy Galois theory problem, and then run through the strongly monomial characters θ of the subgroups M of G computing (χ_M, θ) and $\mathbb{F}(\theta)$ until the character satisfying the hypothesis of Proposition 2.7 is found. The search of the strongly monomial characters of a given group can be performed using the algorithm explained in [OdR1].

Change of field. The corestriction

In this last step we complete the proof of the Brauer–Witt Theorem. Moreover, using an explicit formula for the corestriction $\mathrm{Cor}_{L_p \to \mathbb{F}}$ on 2-cocycles, where L_p is the p'-splitting field of $A(\chi, F)$, and the description of the simple components $A(\chi, L_p)$ as

algebras Brauer equivalent to precise cyclotomic algebras, we obtain a description of the simple algebra $A(\chi, F)$ as Brauer equivalent to a cyclotomic algebra.

The proof of the Brauer–Witt Theorem in standard references like [Yam] does not pay too much attention to effective computations of the corestriction $\mathrm{Cor}_{L_p\to\mathbb{F}}$. Unlikely, we are interested in explicit computations of the cyclotomic form of an element of the Schur subgroup. After decomposing the simple algebra $A(\chi, F)$ in p-parts and describing every simple p-part as Brauer equivalent over L_p to a cyclotomic algebra $[(\mathbb{F}(\zeta)/L_p, \tau)]$, the corestriction allows us to return to the initial field $\mathbb{F}$. Hence, for every prime p, we have

$$\mathrm{Cor}_{L_p\to\mathbb{F}}([(\mathbb{F}(\zeta)/L_p, \tau)]) = [(\mathbb{F}(\zeta)/\mathbb{F}, \mathrm{Cor}_{L_p\to\mathbb{F}}(\tau))].$$

A formula for the action of the corestriction on 2-cocycles is given in [Wei2, Proposition 2-5-2]. This formula takes an easy form in our situation, because we only need to apply $\mathrm{Cor}_{L_p\to\mathbb{F}}$ to a 2-cocycle τ that takes values in a cyclotomic extension $\mathbb{F}(\zeta)$ of $\mathbb{F}$ such that $[L_p : \mathbb{F}]$ and $[\mathbb{F}(\zeta) : L_p]$ are coprimes. In particular, $H = \mathrm{Gal}(\mathbb{F}(\zeta)/L_p)$, the Sylow p-subgroup of the abelian group G, has a complement $H' = \mathrm{Gal}(\mathbb{F}(\zeta)/L_p')$ on $G = \mathrm{Gal}(\mathbb{F}(\zeta)/\mathbb{F})$. We can formulate the following proposition.

Proposition 2.8. *Let $E/\mathbb{F}$ be a finite Galois extension and $\mathbb{F} \le L, L' \le E$ fields such that $L \cap L' = \mathbb{F}$ and $LL' = E$. Let $G = \mathrm{Gal}(E/\mathbb{F})$, $H = \mathrm{Gal}(E/L)$, $H' = \mathrm{Gal}(E/L')$ and $\tau \in H^2(H, E^*)$ a 2-cocycle of H. Then $G \simeq H \times H'$ and*

$$(\mathrm{Cor}_{L\to\mathbb{F}}(\tau))(g_1, g_2) = N_{L'}^{E}(\tau(\pi(g_1), \pi(g_2))), \tag{2.5}$$

where $\pi : G \to H$ denotes the projection, $N_{L'}^{E}$ is the norm function of the extension $L' \le E$ and $g_1, g_2 \in G$. In particular, if $[(E/L, \tau)]$ is a cyclotomic algebra and E is a cyclotomic extension of $\mathbb{F}$, then

$$\mathrm{Cor}_{L\to\mathbb{F}}([(E/L, \tau)]) = [(E/\mathbb{F}, \mathrm{Cor}_{L\to\mathbb{F}}(\tau))]$$

is a cyclotomic algebra.

Proof. By [Spi, Theorem 22.17], $H \simeq \mathrm{Gal}(L'/\mathbb{F})$ and $H' \simeq \mathrm{Gal}(L/\mathbb{F})$ and the mapping $\varphi : G \to \mathrm{Gal}(L'/\mathbb{F}) \times \mathrm{Gal}(L/\mathbb{F})$ given by $\sigma \mapsto (\sigma|_{L'}, \sigma|_L)$ is an isomorphism, hence $G \simeq H \times H'$. Then, using H' as a transversal of H in G, the formula from [Wei2, Proposition 2-5-2] for the corestriction in the particular case of the 2-cocycle $\tau \in H^2(H, E^*)$ takes the following form, where $\pi' : G \to H'$ denotes the projection:

$$\begin{aligned}\mathrm{Cor}_{L\to\mathbb{F}}(\tau)(g_1,g_2) &= \prod_{t\in H'} t^{-1}\tau(tg_1\pi'(tg_1)^{-1}, \pi'(tg_1)g_2\pi'(tg_1g_2)^{-1}) \\ &= \prod_{t\in H'} t^{-1}\tau(\pi(tg_1), \pi(\pi'(tg_1)g_2)) \\ &= \prod_{t\in H'} t^{-1}\tau(\pi(g_1), \pi(g_2)) = N_{L'}^{E}(\tau(\pi(g_1), \pi(g_2))).\end{aligned}$$

□

We now present a proof of the Brauer–Witt Theorem as an easy consequence of the previous steps of the algorithmic proof.

Theorem 2.9 (Brauer–Witt). *If G is a finite group of exponent n, χ is an irreducible character of G, F is a field of characteristic 0 and $\mathbb{F} = F(\chi)$, then the simple component $A(\chi, F)$ is Brauer equivalent to a cyclotomic algebra over $\mathbb{F}$.*

Proof. Let p be an arbitrary prime. Using the restriction homomorphism, we obtain that $\mathrm{Res}_{\mathbb{F}\to L_p}([A(\chi,F)]_p) = [A(\chi, L_p)] = [C]$, that is, a cyclotomic algebra over L_p, the p'-splitting field of $A(\chi, F)$. Proposition 2.8 implies that $\mathrm{Cor}_{L_p\to\mathbb{F}}([C])$ is a class of $\mathrm{Br}(\mathbb{F})$ represented by a cyclotomic algebra over $\mathbb{F}$. Let $[\mathbb{F}(\zeta_n) : L_p] = p^\alpha$ and $[L_p : \mathbb{F}] = m \not\equiv 0 (\mathrm{mod}\ p)$. Let a be an integer such that $am \equiv 1 (\mathrm{mod}\ p^\alpha)$. Then, using the relation between the restriction and the corestriction given by $\mathrm{Cor}_{L_p\to\mathbb{F}} \circ \mathrm{Res}_{\mathbb{F}\to L_p}([A(\chi,F)]_p) = ([A(\chi,F)]_p)^m$, we obtain

$$\begin{aligned}(\mathrm{Cor}_{L_p\to\mathbb{F}}([C]))^a &= (\mathrm{Cor}_{L_p\to\mathbb{F}} \circ \mathrm{Res}_{\mathbb{F}\to L_p}([A(\chi,F)]_p))^a \\ &= ([A(\chi,F)]_p)^{am} = [A(\chi,F)]_p.\end{aligned}$$

Because p is arbitrary and the tensor product of cyclotomic algebras over $\mathbb{F}$ is Brauer equivalent to a cyclotomic algebra by Lemma 1.104, we conclude that the class $[A(\chi, F)]$ is represented by a cyclotomic algebra over $\mathbb{F}$. □

Notice that in the proof of Theorem 2.9 we mentioned that the tensor product of cyclotomic algebras over $\mathbb{F}$ is Brauer equivalent to a cyclotomic algebra. The proof of this claim is also constructible as it appears in Lemma 1.104. Namely, by inflating two cyclotomic algebras, say $C_1 = [(\mathbb{F}(\zeta_{n_1})/\mathbb{F}, \tau_1)]$ and $C_2 = [(\mathbb{F}(\zeta_{n_2})/\mathbb{F}, \tau_2)]$, to a common cyclotomic extension, for example $\mathbb{F}(\zeta_n)$ for n the least common multiple of n_1 and n_2, one may assume that $n_1 = n_2$ and hence $C_1 \otimes C_2 \sim (\mathbb{F}(\zeta_n)/\mathbb{F}, \tau_1\tau_2)$.

This algorithmic proof shows that one may describe $A(\chi, F)$ by making use of Proposition 2.3 to compute its p-parts up to Brauer equivalence. In other words, each p-part of $A(\chi, F)$ can be described in terms of $A_{L_p}(M, H, K)$, where (H, K) is a suitable strong Shoda pair of a subgroup M of G. A *strong Shoda triple* of G is by definition

a triple (M, H, K), where M is a subgroup of G and (H, K) is a strong Shoda pair of G. Notice that the p-part of $A(\chi, F)$ is Brauer equivalent to $\mathrm{Cor}_{L_p \to F(\chi)}(A(\theta, L_p))^{\otimes r}$, where r is an inverse of $[L_p : F(\chi)]$ modulo the maximum p-th power dividing $\chi(1)$. This suggests the algorithm presented in next section.

2.3 A theoretical algorithm

We present a constructive algorithm of the cyclotomic structure of a simple component $A(\chi, F)$ of FG given by the proof of the Brauer–Witt Theorem, which can be used to produce an algorithm for the computation of the Wedderburn decomposition of the group algebra FG.

Algorithm 1. Theoretical algorithm for the computation of the Wedderburn decomposition of FG.

INPUT**:** A group algebra FG of a finite group G over a field F of zero characteristic.

PRECOMPUTATION**:** Compute n, the exponent of G and E, a set of representatives of the F-equivalence classes of the irreducible characters of G.

COMPUTATION**:** For every $\chi \in E$:

(1) Compute $\mathbb{F} := F(\chi)$, the field of character values of χ over F.

(2) Compute $p_1, \ldots, p_r$, the common prime divisors of $\chi(1)$ and $[\mathbb{F}(\zeta_n) : \mathbb{F}]$.

(3) For each $p \in [p_1, \ldots, p_r]$:

  (a) Compute L_p, the p'-part L_p of $\mathbb{F}(\zeta_n)/\mathbb{F}$.

  (b) Search for a strong Shoda triple (M_p, H_p, K_p) of G such that the character θ_p of M_p induced by (H_p, K_p) satisfies:
  $(*)$ (χ_{M_p}, θ_p) is coprime to p and θ_p takes values in L_p.

  (c) Compute $A_p = (L_p(\zeta_{m_p})/L_p, \tau_p = \tau_{L_p})$, as in Proposition 2.3.

  (d) Compute $\tau'_p = \mathrm{Cor}_{L_p \to \mathbb{F}}(\tau_p)$.

  (e) Compute a_p, an inverse of $[L_p : \mathbb{F}]$ modulo the maximum p-th power dividing $\chi(1)$.

(4) Compute m, the least common multiple of $m_{p_1}, \ldots, m_{p_r}$.

(5) Compute $\widehat{\tau_{p_i}} := \mathrm{Inf}_{\mathbb{F}(\zeta_{m_{p_i}}) \to \mathbb{F}(\zeta_m)}(\tau'_{p_i})$, for each $i = 1, \ldots, r$.

(6) Compute $B := (\mathbb{F}(\zeta_m)/\mathbb{F}, \tau)$, where $\tau = \widehat{\tau_{p_1}}^{a_{p_1}} \cdots \widehat{\tau_{p_r}}^{a_{p_r}}$.

(7) Compute $A_\chi := M_{d_1/d_2}(B)$, where d_1, d_2 are the degrees of χ and B respectively.

OUTPUT: $\{A_\chi : \chi \in E\}$, the Wedderburn components of FG.

Remarks 2.10. (i) The basic approach presented in this chapter is still valid for F a field of positive characteristic, provided FG is semisimple (i.e. the characteristic of F is coprime with the order of G) (see [BdR] for the strongly monomial part). On the one hand we have only considered the zero characteristic case for simplicity. On other hand the problem in positive characteristic is somehow simpler, because the Wedderburn components of FG are split, that is, they are matrices over fields.

(ii) In some cases, the algebra A_χ obtained in step (7) of Algorithm 1 is not a genuine matrix algebra, because d_2 does not necessarily divide d_1. This undesired phenomenon cannot be avoided because it is not true, in general, that every Wedderburn component of FG is a matrix algebra of a cyclotomic algebra (see Example 3.6). Luckily, this is a rare phenomenon and, even when it is encountered, the information given by $\frac{d_1}{d_2}$ and B is still useful to describe A_χ (for example, it can be used to compute the index of A_χ).

(iii) From the implementation point of view, a more efficient algorithm is the one used in the `wedderga` package [BKOOdR] that, instead of considering every irreducible character and then searching for some strongly monomial characters of subgroups that give the reduction step, searches for strong Shoda pairs of subgroups that verify the conditions from step (3)(b) of Algorithm 1 running on descending order and analyzes their contribution in step (3)(c) of Algorithm 1 for the different characters and primes. Some of the strong Shoda pairs of subgroups contribute to more than one character or more than one prime. In the next chapter we present a working algorithm and a list of examples that explain how the algorithm works.

Notes on Chapter 2

We give some biographical data about the protagonists of this chapter and some perspectives to be followed in the study of this topic.

Joseph Henry Maclagan Wedderburn (1882–1948) was a Scottish mathematician, who had taught at Princeton University for most of his career. A significant algebraist, he proved that a finite division algebra is a field, and part of the Artin–Wedderburn Theorem on simple algebras. He had also worked in group theory and matrix algebra.

Wedderburn's best known paper is "On hypercomplex numbers", published in the 1907 Proceedings of the London Mathematical Society [Wed1], and for which he was awarded the D.Sc. the following year by the University of Edinburgh. This paper gives a complete classification of simple and semisimple algebras. He then showed that every semisimple algebra can be constructed as a direct sum of simple algebras and that

every simple algebra is isomorphic to a matrix algebra over some division ring. The Artin–Wedderburn Theorem generalizes this result, being a classification theorem for semisimple rings. The theorem states that a semisimple ring R is isomorphic to a finite direct product of matrix rings over division rings D_i, which are uniquely determined up to permutation of the indices i. In particular, any simple left or right Artinian ring is isomorphic to an $n \times n$ matrix ring over a division ring D, where both n and D are uniquely determined. As a direct corollary, the Artin–Wedderburn Theorem implies that every simple ring which is finite dimensional over a division ring (a simple algebra) is a matrix ring. This is Joseph Wedderburn's original result. Emil Artin later generalized it to the case of Artinian rings.

In the structure theorems he presented in his 1907 paper [Wed1], Wedderburn had effectively shown that the study of finite dimensional semisimple algebras reduces to that of division algebras. Thus, the search for division algebras and, in general, the classification of them became a focal point of the new theory of algebras. With Wedderburn's paper from 1907, "On Hypercomplex Numbers", the first chapter in the history of the theory of algebras came to a close. His work neatly and brilliantly placed the theory of algebras in the proper, or at least in the modern, perspective. Later, researchers in the area such as L.E. Dickson, A.A. Albert, R. Brauer and E. Noether, to name only a few, turned to questions concerning more specific types of algebras such as cyclic algebras and division algebras over arbitrary and particular fields like the rational numbers.

The Brauer–Witt Theorem is a result that was independently found in the early 1950's by R. Brauer and E. Witt. It proves that questions on the Schur subgroup are reduced to a treatment of cyclotomic algebras and it can now be said that almost all detailed results about Schur subgroups depend on it.

Richard Brauer (1901–1977) was a leading mathematician, who had worked mainly in abstract algebra, but had made important contributions to number theory. He was also the founder of modular representation theory. Several theorems bear his name, including Brauer's Induction Theorem which has applications in number theory as well as finite groups, and its corollary on Brauer's characterization of characters which is central to the theory of group characters.

Ernst Witt (1911–1991) was a former Ph.D. student of E. Noether, who has taught at the Göttingen and Hamburg Universities. His work was mainly concerned with the theory of quadratic forms and related subjects such as algebraic function fields.

We present now some directions that can be followed by the interested reader in the study of this topic. The description of the Wedderburn components that we presented

in this chapter can be improved by a detailed study of the (local) Schur indices and the Hasse invariants. This is the first natural next step to be followed for future study on this topic, that is, to add local information obtained by using local methods and which complete the previous data. This direction is followed in Chapter 5, where a study of the Schur group of an abelian number field is presented and the maximum of the local Schur indices of the Schur algebras is computed. In order to compute the Schur indices, there can be also used new methods using G-algebras, introduced by A. Turull, as seen in [Her5] or [Tur].

A related topic to the one presented in this chapter is the projective Brauer group. Recently, a projective version of the Brauer–Witt Theorem has been given by Á. del Río and E. Aljadeff [AdR], proving that

Any projective Schur algebra over a field is Brauer equivalent to a radical algebra.

This result was conjectured in 1995 by E. Aljadeff and J. Sonn. In this article it is obtained a characterization of the projective Schur group by means of Galois cohomology. This result provides useful information that can be used to study a similar problem as the one studied in this chapter in the case of twisting group algebras, that is, to describe the simple components of semisimple twisted group algebras given by projective characters of the group as radical algebras in the projective Schur group.

Chapter 3

Implementation: the GAP package `wedderga`

The computational approach and the theoretical algorithm for the computation of the Wedderburn decomposition of semisimple group algebras presented in the previous chapter made possible the implementation and the creation of the functions that are the core of the GAP package `wedderga` [BKOOdR]. These functions upgrade a previous version of the package `wedderga`, enlarging its functionality to the computation of the Wedderburn decomposition and the primitive central idempotents of arbitrary semisimple group algebras of arbitrary finite groups with coefficients in arbitrary number fields or finite fields that are supported by the GAP system [GAP].

What is GAP? The complete name already gives us a clue: *GAP - Groups, Algorithms, Programming - a System for Computational Discrete Algebra.* We cite from its webpage at `http://www.gap-system.org`:

"GAP is a system for computational discrete algebra, with particular emphasis on Computational Group Theory. GAP provides a programming language, a library of thousands of functions implementing algebraic algorithms written in the GAP language as well as large data libraries of algebraic objects. GAP is used in research and teaching for studying groups and their representations, rings, vector spaces, algebras, combinatorial structures, and more."

Many people have helped in different ways to develop the GAP system, to maintain it, and to provide advice and support for users. All of these are nowadays refered to as the *GAP Group.* The concrete idea of GAP as a truly 'open' system for computational group theory was born in 1985 and the GAP system was officially presented in 1988. Since then, the GAP system has continue to grow with the implementation of many functions which are either in the core of the system or inside its packages.

What is a GAP package? We cite again from the GAP webpage:

"Since 1992, sets of user contributed programs, called packages, have been distributed with GAP. For convenience of the GAP users, the GAP Group redistributes packages, but the package authors remain responsible for their maintenance.

Some packages represent a piece of work equivalent to a sizeable mathematical publication. To acknowledge such work there has been a refereeing process for packages since 1996. We call a package an accepted package (with GAP 3 the term share packages was used) when it was successfully refereed or already distributed with GAP before the refereeing process was started. All other packages distributed here and not in this category are called deposited packages, these may be submitted for refereeing or the authors may not want to submit them for various reasons."

The name `wedderga` stands for "`Wedder`burn decomposition of `g`roup `a`lgebras" [1]. This is a GAP package to compute the simple components of the Wedderburn decomposition of semisimple group algebras of finite groups over finite fields and over subfields of finite cyclotomic extensions of the rationals. It also contains functions that produce the primitive central idempotents of these group algebras. Other functions of `wedderga` allow one to construct crossed products over a group with coefficients in an associative ring with identity and the multiplication determined by a given action and twisting. In the light of the previous "definition" of a GAP package, we should call `wedderga` a deposited package, since it is still in refereeing process. However, for briefness we will call it a package.

In the first section of this chapter we give a working algorithm which is closer to the real algorithm than the one presented in section 2.3 and in the second section we give some examples that give a good idea about the process to be followed during the implementation.

More aspects of the implementation and data on the `wedderga` package are given in Appendix that contains the manual of the package. Throughout this chapter we keep the notation from Chapter 2.

3.1 A working algorithm

Algorithm 1 presented in the previous chapter is not the most efficient way to compute the Wedderburn decomposition of a semisimple group algebra FG for several reasons.

Firstly, it is easy to compute the Wedderburn decomposition of FG from the Wed-

[1] The first version of `wedderga` was only computing Wedderburn decomposition of some **rational** group algebras and, in fact, the original name stood for "`Wed`derburn `de`composition of `r`ational `g`roup `a`lgebras".

derburn decomposition of $\mathbb{Q}G$. More precisely, if χ is an irreducible character of G, $\Bbbk = \mathbb{Q}(\chi)$ and $\mathbb{F} = F(\chi)$, then $A(\chi, F) \simeq \mathbb{F} \otimes_{\Bbbk} A(\chi, \mathbb{Q})$. In particular, if $A(\chi, \mathbb{Q})$ is equivalent to the cyclotomic algebra $(\Bbbk(\zeta)/\Bbbk, \tau)$, then $A(\chi, F)$ is equivalent to $(\mathbb{F}(\zeta)/\mathbb{F}, \tau')$, where τ' is the restriction of τ via the inclusion $\mathrm{Gal}(\mathbb{F}(\zeta)/\mathbb{F}) \subseteq \mathrm{Gal}(\Bbbk(\zeta)/\Bbbk)$. Moreover, the degrees of $A(\chi, \mathbb{Q})$ and $A(\chi, F)$ are equal (the degree of χ). This suggests to use the description of the Wedderburn decomposition of $\mathbb{Q}G$ as information to be stored as an attribute of G. (Recall that an attribute of a GAP object is information about the object saved the first time when is computed in a GAP session, to be quickly accessed in subsequent computations). The implemented algorithm computes some data which can be easily used to determine the Wedderburn decomposition of $\mathbb{Q}G$. A small modification will be enough to use this data to produce the Wedderburn decomposition of FG. In this way, the first time that the Wedderburn decomposition of a group algebra FG is calculated by the program it takes more time that the next time it computes the Wedderburn decomposition of LG, a group algebra of the same group over a field L non necessarily equal to F.

```
gap> G:=SmallGroup(512,21);;
gap>FG:=GroupRing(CF(5),G);;
gap>LG:=GroupRing(CF(7),G);;
gap>WedderburnDecomposition(FG);;
gap>time;
11767
gap>WedderburnDecomposition(LG);;
gap>time;
20
```

Secondly, if χ is a strongly monomial character of G, then $A(\chi, F)$ can be computed at once by using Proposition 2.3. That is, there is no need to compute the p-parts separately and merging them together.

Example 3.1. Let p be a prime and consider $\mathbb{Z}_p^*$ acting on $\mathbb{Z}_p$ by multiplication. Let $G = \mathbb{Z}_p \rtimes Z_p^*$ be the corresponding semidirect product. Then $(\mathbb{Z}_p, 1)$ is a strong Shoda pair of G and if χ is the induced strongly monomial character, then $A = A(\chi, F)$ has degree $p-1$. For example, if $p = 31$, then A has degree 30. So according to Algorithm 1, one should describe the cocycles τ_2, τ_3 and τ_5 in step (3) and then perform steps (4)–(6) to compute $\tau = \widehat{\tau_2}^{a_2}\widehat{\tau_3}^{a_3}\widehat{\tau_5}^{a_5}$. Instead, one can compute $A(\chi, \mathbb{F})$ at once using Proposition 2.3. □

In particular, if G is strongly monomial (as so is the group of Example 3.1), then instead of running through the irreducible characters χ of G and looking for some

strong Shoda pairs (H, K) of G such that χ is the character of G induced by (H, K), it is more efficient to produce a list of strong Shoda pairs of G and, at the same time, produce the primitive central idempotents $e(G, H, K)$ of $\mathbb{Q}G$, which helps to control if the list is complete. This was the approach in [OdR1].

Thirdly, even if χ is not strongly monomial and the number r of primes appearing in step (2) of Algorithm 1 is greater than 1, it may happen that one strongly monomial character θ of a subgroup M of G satisfies condition $(*)$ of Proposition 2.5 for more than one prime p.

Example 3.2. Consider the permutation group $G = \langle (3,4)(5,6), (1,2,3)(4,5,7) \rangle$ and its subgroup $M = \langle (1,3,5)(4,6,7), (1,6)(5,7) \rangle$. Then G has an irreducible character χ of degree 6, such that $\mathbb{Q}(\chi) = \mathbb{Q}$ and $(\chi_M, 1_M) = 1$. Clearly 1_M, the trivial character of M, is strongly monomial and satisfies condition $(*)$ for the two possible primes 2 and 3. Using this, it follows at once that $A(\chi, F) = M_6(F)$ for each field F, and so there is no need to consider the two primes separately. □

Fourthly, a strongly monomial character θ of a subgroup of G may satisfy condition $(*)$ for more than one irreducible character χ of G.

Example 3.3. Consider the group $G = \mathrm{SL}(2,3) = \langle a, b \rangle \rtimes \langle c \rangle$ (where $\langle a, b \rangle$ is the quaternion group of order 8 and c has order 3). The group G has one non-strongly monomial character χ_1 of degree 2 with $\mathbb{Q}(\chi_1) = \mathbb{Q}$ and two non-strongly monomial $\mathbb{Q}$-equivalent characters χ_2 and χ_2', also of degree 2, with $\mathbb{Q}(\chi_2) = \mathbb{Q}(\chi_2') = \mathbb{Q}(\zeta_3)$. Then $(M = \langle a, b \rangle, H = \langle a \rangle, 1)$ is a strong Shoda triple. If θ is the strongly monomial character of M induced by $(H, 1)$, then θ satisfies condition $(*)$ for both χ_1 and χ_2 and $p = 2$, the unique prime involved. □

Finally, the weakest part of Algorithm 1 is step $(3)(b)$, where a blind search of a strong Shoda triple of G satisfying condition $(*)$ for each irreducible character of G and each prime $p_1, \ldots, p_r$ may be too costly.

Taking all these into account, it is more efficient to run through the strong Shoda triples of G and for each such triple evaluate its contribution to the p-parts of $A(\chi, F)$ for the different irreducible characters χ of G and the different primes p. This leads to the question of what is the most efficient way to systematically compute strong Shoda triples of G. The first version of `wedderga` included a function `StrongShodaPairs` which computes a list of representatives of the equivalence classes of the strong Shoda pairs of the group given as input. So one can use this function to compute the strong Shoda pairs for each subgroup of G. However, most of the strong Shoda triples of G are not necessary. For example, if G is strongly monomial, we only need to compute the

strong Shoda triples of the form (G, H, K), i.e. in this case one needs to compute only the strong Shoda pairs (H, K) of G. Again, this is the original approach in [OdR1]. This suggests to start by computing the strong Shoda pairs of G and the associated simple components as in Proposition 2.3. If the group is strongly monomial, we are done.

Which are the next natural candidates of subgroups M of G for which we should compute the strong Shoda pairs of M? That is, what are the strong Shoda triples (M, H, K) most likely to actually contribute in the computation? Take any strong Shoda triple (M, H, K) of G. If M_1 is a subgroup of M containing H, then (M_1, H, K) is also a strong Shoda triple of G. Now let ψ be a linear character of H with kernel K and set $\theta = \psi^M$ and $\theta_1 = \psi^{M_1}$. Then, for every irreducible character χ of G, $(\chi_{M_1}, \theta_1) = (\chi, \theta_1^G) = (\chi, \theta^G) = (\chi_M, \theta)$, by Frobenius Reciprocity. So θ satisfies the first part of condition $(*)$ if and only if so does θ_1. However, $F(\theta) \subseteq F(\theta_1)$ and so, the bigger M, the more likely θ to satisfy the second condition of $(*)$ and, in fact, all the contributions of θ_1 are already realized by θ.

Example 3.3. (continuation) Notice that $(H, 1)$ is a strong Shoda pair of M, but it is not a strong Shoda pair of G. In some sense, $(H, 1)$ is very close to be a strong Shoda pair of G, because it is a strong Shoda pair in a subgroup of prime index in G. On the other hand, $(H, H, 1)$ is also a strong Shoda triple of G. However, the strongly monomial character θ of H (in fact linear) induced by $(H, 1)$ does not satisfy condition $(*)$ with respect to either χ_1 or χ_2, because the field of character values of θ contains $i = \sqrt{-1}$. So, G is too big for $(G, H, 1)$ to be a strong Shoda triple of G, while H is too small for $(H, H, 1)$ to contribute in terms of satisfying condition $(*)$. □

Notice also that if M is a subgroup of G and $g \in G$, then the strong Shoda pairs of M and M^g are going to contribute equally in terms of satisfying condition $(*)$ for a given irreducible character χ. This is because if (H, K) is a strong Shoda pair of M, then (H^g, K^g) is a strong Shoda pair of M^g, and if θ is the character of M induced by (H, K), then θ^g is the character induced by (H^g, K^g). Then $(\chi_M, \theta) = (\chi_M, \theta^g)$ and θ and θ^g take the same values. So, we only have to compute strong Shoda pairs for one representative of each conjugacy class of subgroups of G.

Summarizing, we chose the algorithm to run through conjugacy classes of subgroups of G in decreasing order and evaluate the contribution on as many p-parts of as many irreducible characters as possible. In fact, we consider the group $M = G$ separately, because Proposition 2.3 tells us how to compute the corresponding simple algebras without having to consider the p-parts separately. This is called the Strongly Monomial Part of the algorithm and takes care of the Wedderburn components of the form $A(\chi, F)$ for $\chi \in \mathrm{Irr}(G)$ strongly monomial. The remaining components are

computed in the NON-STRONGLY MONOMIAL PART, where we consider proper subgroups M (actually representatives of conjugacy classes). For such an M we use the function `StrongShodaPairs` to compute a set of representatives of strong Shoda pairs (H, K) of M and for each (H, K) we check to which p-parts of the non-strongly monomial characters of G the character θ induced by (H, K) contributes (i.e. condition $(*)$ is satisfied). The algorithm stops when all the p-parts of all the irreducible characters are covered. In most of the cases, only a few subgroups M of G have to be used.

Now we are ready to present the algorithm.

Algorithm 2. Computes data for the Wedderburn decomposition of $\mathbb{Q}G$.

INPUT**:** A finite group G (of exponent n).

STRONGLY MONOMIAL PART:

1. Compute S, a list of representatives of strong Shoda pairs of G.
2. Compute $Data := [[n_x, \Bbbk_x, m_x, \mathrm{Gal}_x, \tau_x] : x \in S]$, where for each $x = (H, K) \in S$:
   - $n_x := [G : N]$, with $N = N_G(K)$;
   - $\Bbbk_x := \mathbb{Q}(\theta_x)$, for θ_x a strongly monomial character of G induced by (H, K);
   - $m_x := [H : K]$;
   - $\mathrm{Gal}_x := \mathrm{Gal}(\Bbbk_x(\zeta_{m_x})/\Bbbk_x)$;
   - $\tau_x := \tau_{\mathbb{Q}}$, the 2-cocycle of Gal_x with coefficients in $\mathbb{Q}(\zeta_{m_x})$ given as in Proposition 2.3.

NON-STRONGLY MONOMIAL PART: If G is not strongly monomial

1. Compute E, a set of representatives of the $\mathbb{Q}$-equivalence classes of the non-strongly monomial irreducible characters of G.
2. Compute $PrimesLps := [PrimesLp_\chi : \chi \in E]$, where $PrimesLP_\chi$ is the list of pairs $[p, L_p]$, with p a prime dividing $\gcd(\chi(1), [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\chi)])$ and L_p is the p'-part of the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\chi)$.
3. Initialize $E' = E$, a copy of E, and
   $Parts := [Parts_\chi := [\,] : \chi \in E]$, a list of length $|E|$ formed by empty lists.
4. For M running in decreasing order over a set of representatives of conjugacy classes of proper subgroups of G (while $E' \neq \emptyset$):
   Compute S_M, the strong Shoda pairs of M and for each $(H, K) \in S_M$:

- Compute θ, a strongly monomial character of M induced by (H, K).
- Compute $Drop := [Drop_\chi : \chi \in E]$, where $Drop_\chi$ is the set of $[p, L_p]$ in $PrimesLps_\chi$, for which $(*)$ holds.
- For each $[p, L_p]$ in $Drop_\chi$, compute m_p, τ'_p and a_p as in Step (3) of Algorithm 1 and add this information to $Parts_\chi$.
- $PrimesLps_\chi := PrimesLps_\chi \setminus Drop_\chi$.
- $E' := E' \setminus \{\chi \in E : PrimesLps = \emptyset\}$.

5. Compute $Data' := [[n_\chi, \Bbbk_\chi, m_\chi, \mathrm{Gal}_\chi, \tau_\chi] : \chi \in E]$, where
   - $\Bbbk_\chi := \mathbb{Q}(\chi)$;
   - $m_\chi :=$ Least common multiple of the m_p's appearing in $Parts_\chi$;
   - $n_\chi := \frac{\chi(1)}{[\Bbbk_\chi(\zeta_{m_\chi}):\Bbbk_\chi]}$;
   - $\mathrm{Gal}_\chi := \mathrm{Gal}(\Bbbk_\chi(\zeta_{m_\chi})/\Bbbk_\chi)$;
   - τ_χ is computed from $m = m_\chi$ and the τ'_p's and a_p's in $Parts_\chi$, as in Steps (3)-(6) of Algorithm 1.

OUTPUT: The list obtained by merging $Data$ and $Data'$.

Notice that the question of whether G is strongly monomial or not, needed to decide whether the NON-STRONGLY MONOMIAL PART of Algorithm 2 should be ran for G, is already answered in the first part because the actual algorithm for the STRONGLY MONOMIAL PART computes at the same time the primitive central idempotents associated to the strongly monomial pairs obtained. The algorithm stops if the sum of the primitive central idempotents at one step is 1.

The output of Algorithm 2 can be used right away to produce the Wedderburn decomposition of $\mathbb{Q}G$. Each entry $[n, \Bbbk, m, \mathrm{Gal}, \tau]$ parameterizes one Wedderburn component of $\mathbb{Q}G$ which is isomorphic to $M_n((\Bbbk(\zeta_m)/\Bbbk, \tau))$.

For an arbitrary field F of zero characteristic, some modifications are needed. The number of 5-tuples, say r, of the output of Algorithm 2 is the number of $\mathbb{Q}$-equivalence classes of irreducible characters of G. Let $\chi_1, \ldots, \chi_r$ be a set of representatives of $\mathbb{Q}$-equivalence classes of irreducible characters of G. Then $\mathbb{Q}G = \oplus_{i=1}^r A(\chi_i, \mathbb{Q})$ and so $FG = F \otimes_{\mathbb{Q}} \mathbb{Q}G = \oplus_{i=1}^r F \otimes_{\mathbb{Q}} A(\chi_i, \mathbb{Q})$. Moreover, if $A = A(\chi, \mathbb{Q})$, then

$$F \otimes_{\mathbb{Q}} A = F \otimes_{\mathbb{Q}} \mathbb{Q}(\chi) \otimes_{\mathbb{Q}(\chi)} A \simeq [F \cap \mathbb{Q}(\chi) : \mathbb{Q}] F(\chi) \otimes_{\mathbb{Q}(\chi)} A = [F \cap \mathbb{Q}(\chi) : \mathbb{Q}] A(\chi, F).$$

Thus, an entry $[n, \Bbbk, m, \mathrm{Gal}, \tau]$ of the output parameterizes $[F \cap \Bbbk : \mathbb{Q}]$ Wedderburn components of FG, each one isomorphic to $\mathbb{F} \otimes_{\Bbbk} M_n((\Bbbk(\zeta_m)/\Bbbk, \tau)) \simeq M_{nd}((\mathbb{F}(\zeta_m)/\mathbb{F}, \tau'))$, where $\mathbb{F}$ is the compositum of $\Bbbk$ and F, $d = \frac{[\Bbbk(\zeta_m):\Bbbk]}{[\mathbb{F}(\zeta_m):\mathbb{F}]} = \frac{|\mathrm{Gal}|}{|\mathrm{Gal}'|}$, $\mathrm{Gal}' = \mathrm{Gal}(\mathbb{F}(\zeta_m)/\mathbb{F})$ and τ' is the restriction of $\tau \in H^2(\mathrm{Gal}, \mathbb{F}(\zeta_m))$ to a 2-cocycle $\tau' \in H^2(\mathrm{Gal}', \mathbb{F}(\zeta_m))$.

If $\zeta_m \in \Bbbk$ then Gal $= 1$ and, in fact, Algorithm 2 only loads the information $[n, \Bbbk]$, which parameterizes the simple component $M_n(\Bbbk)$ of $\mathbb{Q}G$ and $[F \cap \Bbbk : \mathbb{Q}]$ simple components of FG isomorphic to $M_n(\mathbb{F})$. If $\zeta_m \notin \Bbbk$, then the simple component of $\mathbb{Q}G$ is a matrix algebra of size n of a non-commutative cyclotomic algebra. However, if $\zeta_m \in \mathbb{F}$ (equivalently if $\mathrm{Gal}' = 1$), then the simple components of FG given by this entry of the output are isomorphic to $M_{nd}(\mathbb{F})$.

3.2 Examples

In this section we give a list of examples that illustrate the performance of the package `wedderga` and how to use the main functions of the package.

Example 3.4. Consider the group $G = \langle (3,4)(5,6), (1,2,3)(4,5,7) \rangle$ from Example 3.2. This group is the group $(168, 42)$ from the GAP library of small groups and it is isomorphic to $\mathrm{SL}(3,2)$. The Wedderburn decomposition of $\mathbb{Q}G$ can be computed by using the function `WedderburnDecomposition` of `wedderga`.

```
gap> G:=SmallGroup(168,42);;
gap>QG:=GroupRing(Rationals,G);;
gap>WedderburnDecomposition(QG);
[ Rationals, ( Rationals^[ 7, 7 ] ), ( NF(7,[ 1, 2, 4 ])^[ 3, 3 ] ),
  ( Rationals^[ 6, 6 ] ), ( Rationals^[ 8, 8 ] ) ]
```

Thus

$$\mathbb{Q}G \simeq \mathbb{Q} \oplus M_7(\mathbb{Q}) \oplus M_3(\mathbb{Q}(\sqrt{-7})) \oplus M_6(\mathbb{Q}) \oplus M_8(\mathbb{Q}).$$

Notice that the center of the third component is $\mathbb{Q}(\sqrt{-7})$, the subfield of $\mathbb{Q}(\zeta_7)$ consisting of the elements fixed by the automorphism $\zeta_7 \mapsto \zeta_7^2$.

Now we explain how the package obtains this information. As it is explained above, the first part of the algorithm computes a list of representatives of the strong Shoda pairs of G using the function `StrongShodaPairs`. This part of the algorithm provides two strong Shoda pairs and the first two Wedderburn components of $\mathbb{Q}G$, which are calculated as explained in Proposition 2.2.

```
gap> StrongShodaPairs(G);
[ [ Group([ (3,4)(5,6), (1,2,3)(4,5,7) ]),
      Group([ (3,4)(5,6), (1,2,3)(4,5,7) ]) ],
  [ Group([ (3,4)(5,6), (1,7)(5,6), (1,3,5)(4,6,7), (3,6)(4,5) ]),
      Group([ (3,4)(5,6), (1,7)(5,6), (1,3,5)(4,6,7) ]) ] ]
```

The other part of the calculation provides another three Wedderburn components. They correspond to three $\mathbb{Q}$-equivalence classes of non-strongly monomial characters represented by the following characters, where $\alpha = \zeta_7 + \zeta_7^2 + \zeta_7^4 = \frac{-1+\sqrt{-7}}{2}$:

	1	$(3,4)(5,6)$	$(2,3,4)(5,6,7)$	$(2,3,7,5)(4,6)$	$(1,2,3,5,6,7,4)$	$(1,2,3,7,4,6,5)$
χ_1	3	-1	0	1	$-1-\alpha$	α
χ_2	6	2	0	0	-1	-1
χ_3	8	0	-1	0	1	1

So the center of $A_1 := A(\chi_1, \mathbb{Q})$ is $\mathbb{Q}(\chi_1) = \mathbb{Q}(\alpha)$ and the centers of $A_2 := A(\chi_2, \mathbb{Q})$ and $A_3 := A(\chi_3, \mathbb{Q})$ are $\mathbb{Q}(\chi_2) = \mathbb{Q}(\chi_3) = \mathbb{Q}$. Now the program has to compute cyclotomic algebras equivalent to A_1, A_2 and A_3. The degrees of these algebras are 3, 6 and 8 respectively. Since the index of a central simple algebra divides its degree, one has to describe the 3-part of A_1, the 2 and 3-parts of A_2 and the 2-part of A_3. By Proposition 2.5, the 2 and 3-parts of A_2 can be obtained by using two strong Shoda triples of G. However, as we have seen in Example 3.2, $((\chi_2)_M, 1_M) = 1$ for $M = \langle (1,3,5)(4,6,7), (1,6)(5,7) \rangle$. So, there is a unique strong Shoda triple of G, namely (M, M, M), which provides the strongly monomial character 1_M satisfying condition $(*)$ for the two primes involved. It was already explained that $A(\chi_2, \mathbb{Q}) \simeq M_6(\mathbb{Q})$ and this takes care of the fourth entry given as output by `WedderburnDecomposition`.

For the other two characters the algorithm obtains the strong Shoda triple $(M, H = \langle (3,4)(5,6), (1,6,7,5)(3,4) \rangle, K = \langle (1,6,7,5)(3,4) \rangle)$ for both of them. Since $H = N_M(K)$ and $[H : K] = 2$, the algebra $A(M, H, K)$ is Brauer equivalent to $\mathbb{Q}(\zeta_2) = \mathbb{Q}$ (Proposition 2.3). Let θ be the strongly monomial character of M induced by (H, K). If F is the center of $A(\chi_i, \mathbb{Q})$ ($i = 1$ or 3) then $A(\chi_i, \mathbb{Q}) = A(\chi_i, F)$ is Brauer equivalent to $A(\theta, F)$ (Proposition 2.5) and this is isomorphic to $F \otimes_{\mathbb{Q}} A(M, H, K) \simeq F$. So we obtain $A(\chi_1, \mathbb{Q}) \simeq M_3(\mathbb{Q}(\sqrt{-7}))$ and $A(\chi_3, \mathbb{Q}) \simeq M_8(\mathbb{Q})$.

Notice that for all the used strong Shoda triples (L, H, K) of G, the subgroup L is either G (for the Strongly Monomial Part) or M (for the Non-Strongly Monomial Part). The group G has 15 conjugacy classes of subgroups, one formed by G, two classes consisting of subgroups of order 24 and the other classes formed by subgroups of smaller order. The advantage of running through subgroups in decreasing order becomes apparent in this computation, for only the groups M and G have been considered in the search of "useful" strong Shoda triples. This has avoided many unnecessary computations. □

The Wedderburn components of $\mathbb{Q}G$ for the group G of Example 3.4 are matrix algebras over fields. Of course this does not occur always. In general, the Wedderburn components are equivalent to cyclotomic algebras, which `WedderburnDecomposition` presents as matrix algebras over crossed products. In this case it is difficult to use the

output `WedderburnDecomposition` to describe the corresponding factors. The other main function `WedderburnDecompositionInfo` provides a numerical alternative, giving as output a list of tuples of length 2, 4 or 5, with numerical information describing the Wedderburn decomposition of the group algebra given as input. The tuples of length 5 are of the form

$$[n, \Bbbk, m, [o_i, \alpha_i, \beta_i]_{1\leq i\leq l}, [\gamma_{ij}]_{1\leq i<j\leq l}], \tag{3.1}$$

where $\Bbbk$ is a field and $n, k, m, o_i, \alpha_i > 0$ and $\beta_i, \gamma_{ij} \geq 0$ are integers. The data of (3.1) represents the matrix algebra $M_n(A)$ with A the cyclotomic algebra given by the following presentation:

$$A = \Bbbk(\zeta_m)(g_1, \ldots, g_l | \zeta_m^{g_i} = \zeta_m^{\alpha_i}, g_i^{o_i} = \zeta_m^{\beta_i}, g_j g_i = g_i g_j \zeta_m^{\gamma_{ij}}, 1 \leq i < j \leq l). \tag{3.2}$$

The tuples of length 2 and 4 are simplified forms of the 5-tuples and take the forms $[n, \Bbbk]$ and $[n, \Bbbk, m, [o, \alpha, \beta]]$ respectively. They represent the matrix algebras $M_n(\Bbbk)$ and $M_n(A)$, where A has an interpretation as in (3.2) for $l = 1$.

In Example 3.4 each Wedderburn component is described using a unique strong Shoda triple. The next example shows a Wedderburn component which cannot be given by a unique strong Shoda triple.

Example 3.5. Consider the group $G = \langle x, y\rangle \rtimes \langle a, b\rangle$, where $\langle x, y\rangle = Q_8$, the quaternion group of order 8 and $\langle a, b\rangle$ is the group of order 27, with $a^9 = 1$, $a^3 = b^3$ and $ab = ba^4$. The action of a, b on $\langle x, y\rangle$ is given by $(x, a) = (y, a) = 1$, $x^b = y$ and $y^b = xy$. This is the small group $(216, 39)$ from the GAP library.

```
gap> G:=SmallGroup(216,39);;
gap>QG:=GroupRing(Rationals,G);;
gap> WedderburnDecompositionInfo(QG);
[ [ 1, Rationals ], [ 1, CF(3) ], [ 1, CF(3) ], [ 1, CF(3) ],
  [ 1, CF(3) ], [ 3, Rationals ], [ 3, CF(3) ], [ 3, CF(3) ],
  [ 3, CF(9) ], [ 1, Rationals, 4, [ 2, 3, 2 ] ],
  [ 1, CF(3), 12, [ 2, 7, 6 ] ], [ 1, CF(3), 12, [ 2, 7, 6 ] ],
  [ 1, CF(3), 12, [ 2, 7, 6 ] ], [ 1, CF(3), 4, [ 2, 3, 2 ] ],
  [ 1, CF(3), 36, [ 6, 31, 18 ] ] ]
```

Using (3.2) one obtains

$$\mathbb{Q}G = \mathbb{Q} \oplus 4\mathbb{Q}(\zeta_3) \oplus M_3(\mathbb{Q}) \oplus 2M_3(\mathbb{Q}(\zeta_3)) \oplus M_3(\mathbb{Q}(\zeta_9)) \oplus A_1 \oplus 3A_2 \oplus A_3 \oplus A_4,$$

where

$$\begin{aligned} A_1 &= \mathbb{Q}(\zeta_4)[u : \zeta_4^u = \zeta_4^3, u^2 = \zeta_4^2 = -1] \\ A_2 &= \mathbb{Q}(\zeta_{12})[u : \zeta_{12}^u = \zeta_{12}^7, u^2 = \zeta_{12}^6 = -1] \\ A_3 &= \mathbb{Q}(\zeta_3)(\zeta_4)[u : \zeta_4^u = \zeta_4^3, u^2 = \zeta_4^2 = -1] \\ A_4 &= \mathbb{Q}(\zeta_{36})[u : \zeta_{36}^u = \zeta_{36}^{31}, u^6 = \zeta_{36}^{18} = -1] \end{aligned}$$

Recall that $\mathbb{H}(\Bbbk)$ denotes the Hamiltonian quaternion algebra with center $\Bbbk$. Then $A_1 = \mathbb{H}(\mathbb{Q})$ and $A_2 = A_3 = \mathbb{H}(\mathbb{Q}(\zeta_3))$. Moreover, using that -1 belongs to the image of the norm map $N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}$ and Proposition 1.56 one has that $A_2 = A_3 \simeq M_2(\mathbb{Q}(\zeta_3))$ and $A_4 = M_6(\mathbb{Q}(\zeta_3))$.

Now we explain which are the strong Shoda triples that the program discovers and uses to describe the last Wedderburn component A_4. The simple algebra A_4 is $A(\chi, \mathbb{Q})$, where χ is one of the two ($\mathbb{Q}$-equivalent) characters of degree 6 of G. The field $\Bbbk = \mathbb{Q}(\chi)$ of character values of χ is $\mathbb{Q}(\zeta_3)$. It turns out that, unlike in Example 3.4, the factor A_4 of $\mathbb{Q}G$ cannot be given by a unique strong Shoda triple able to cover both primes 2 and 3 in terms of satisfying condition $(*)$. Indeed, if such a strong Shoda triple (M, H, K) exists and θ is a character of M induced by (H, K), then (χ_M, θ) is coprime with 6 and $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\zeta_3)$, because the exponent of G is 36 and $[\mathbb{Q}(\zeta_{36}) : \Bbbk = \mathbb{Q}(\zeta_3)] = 6$. The following computation shows that such a strong Shoda triple does not exist.

```
gap> chi:=Irr(G)[30];;
gap> ForAny(List(ConjugacyClassesSubgroups(G),Representative),
>     M->ForAny(StrongShodaPairs(M),
>         x->
>         Gcd(6,ScalarProduct( Restricted(chi,M) ,
>           LinCharByKernel(x[1],x[2])^M )) = 1 and
>         ForAll(List(ConjugacyClasses(M),Representative),
>           c -> c^(LinCharByKernel(x[1],x[2])^M) in CF(3) )
>        )
>     );
false
```

The function `LinCharByKernel` is a two argument function which, applied to a pair (H, K) of groups with $K \trianglelefteq H$ and H/K cyclic, returns a linear character of H with kernel K.

The two strong Shoda triples of G obtained by the function `WedderburnDecomposition` to describe the 2 and 3-parts of A_4 are

$$(M_2 = \langle a, x, y\rangle, H_2 = \langle a, x\rangle, K_2 = \langle 1\rangle),$$
$$(M_3 = \langle a, x^2, a^2bxy\rangle, H_3 = \langle a^3, x^2, a^2bxy\rangle, K_3 = \langle a^2bxy\rangle).$$

The $2'$ and $3'$-parts of $\mathbb{Q}(\zeta_{36})/\Bbbk$ are $L_2 = \mathbb{Q}(\zeta_9)$ and $L_3 = \mathbb{Q}(\zeta_{12})$, respectively. Following Propositions 2.3, the algorithm computes $A_{L_2}(M_2, H_2, K_2) = (\mathbb{Q}(\zeta_{36})/\mathbb{Q}(\zeta_9), \tau_2)$ and $A_{L_3}(M_3, H_3, K_3) = M_2(\mathbb{Q}(\zeta_{12}))$ (the latter is equivalent to $(\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_{12}), \tau_3 = 1)$). Then the algorithm inflates τ_2 and τ_3 to $\mathbb{Q}(\zeta_{36})$, corestricts to $\mathbb{Q}(\zeta_3)$ and computes the cocycle τ_χ as in steps $(3) - (6)$ of Algorithm 2. This gives rise to the numerical information `[ 1, CF(3), 36, [ 6, 31, 18 ] ] ]` obtained above. We have seen that the interpretation of this data is that A_4 is isomorphic to $M_6(\mathbb{Q}(\zeta_3))$. This may have also been obtained by noticing that $A_{L_2}(M_2, H_2, K_2) = \mathbb{H}(\mathbb{Q}(\zeta_9)) \simeq M_2(\mathbb{Q}(\zeta_9))$. Then the 2 and 3-parts of A_4 are trivial in the Brauer group, and so $A_4 \simeq M_6(\mathbb{Q}(\zeta_3))$. □

Example 3.6. Notice that the size of the matrix A_χ in step (7) of Algorithm 1 is a rational number rather than an integer. The group of smallest order for which this phenomenon occurs is the group $[240, 89]$ in the library of the GAP system. Although this does not make literal sense, still the algorithm provides a lot of information on the Wedderburn decomposition. This example shows how one can use this information. Let G be the mentioned group. Then the output of Algorithm 2 applied to $\mathbb{Q}G$ provides the following numerical information for one of the simple factors of $\mathbb{Q}G$:

```
[ 3/4, 40, [ [ 4, 17, 20 ] , [ 2, 31, 0 ] ] ].
```

Notice that the first entry of this 4-tuple is not an integer and a formal presentation of the corresponding simple algebra is given by

$$A \simeq \mathcal{M}_{3/4}\left(\mathbb{Q}(\zeta_{40})(g, h | \zeta_4^g = \zeta_{40}^{17}, \zeta_4^h = \zeta_{40}^{31}, g^4 = -1, h^2 = 1, gh = hg)\right).$$

Denote $A = \mathcal{M}_{3/4}(B)$. The center of the algebra B is $\mathbb{Q}(\sqrt{2})$ and the algebras $\mathbb{Q}(\zeta_8)(h | \zeta_8^h = \zeta_8^{-1}, h^2 = 1) \simeq M_2(\mathbb{Q}(\sqrt{2}))$ and $\mathbb{Q}(\zeta_5)(g | \zeta_5^g = \zeta_5^2, g^4 = -1)$ are simple algebras in B. Furthermore

$$\begin{aligned} B &= M_2(\mathbb{Q}(\sqrt{2})) \otimes_{\mathbb{Q}(\sqrt{2})} (\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_5)(g | \zeta_5^g = \zeta_5^2, g^4 = -1)) \\ &= M_2(\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_5)(g | \zeta_5^g = \zeta_5^2, g^4 = -1)) \end{aligned}$$

Hence, we can describe the algebra A as

$$M_{3/2}(\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_5)(g | \zeta_5^g = \zeta_5^2, g^4 = -1))$$

and we conclude that the algebra A is isomorphic to either $M_3(D)$ for some division quaternion algebra over $\mathbb{Q}(\sqrt{2})$ or to $M_6(\mathbb{Q}(\sqrt{2}))$. In fact, in order to decide which one of these options is the correct one, one should compute the local Schur indices of the cyclic algebra $C = \mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_5)(g | \zeta_5^g = \zeta_5^2, g^4 = -1) = (\mathbb{Q}(\sqrt{2}, \zeta_5)/\mathbb{Q}(\sqrt{2}), -1)$.

The algebra C has local index 2 at ∞, because $\mathbb{R} \otimes_{\mathbb{Q}(\sqrt{2})} (\mathbb{Q}(\sqrt{2}, \zeta_5)/\mathbb{Q}(\sqrt{2}), -1) \simeq (\mathbb{C}/\mathbb{R}, -1) \simeq \mathbb{H}(\mathbb{R})$. Thus $A \simeq M_3(D)$, for D a division algebra of index 2 and center $\mathbb{Q}(\sqrt{2})$. Notice that D is determined by its Hasse invariants by the Hasse–Brauer–Noether–Albert Theorem. Now we prove that the local indices of A at the finite primes are all 1. By Proposition 1.114, $m_p(A) = 1$ for every finite prime p not dividing 5. Thus, we only have to compute $m_5(A)$. Note that $\zeta_4 \in \mathbb{Q}_5$, so $\mathbb{Q}_5(\sqrt{2}) = \mathbb{Q}_5(\zeta_8)$ is the unique unramified extension of $\mathbb{Q}_5$ of degree 2. Thus $\zeta_8 \in Z(\mathbb{Q}(\sqrt{2})_5 \otimes_{\mathbb{Q}(\sqrt{2})} C)$ and $N_{\mathbb{Q}_5(\sqrt{2},\zeta_5)/\mathbb{Q}_5(\sqrt{2})}(\zeta_8) = -1$. By Proposition 1.112, $m_5(A) = 1$.

Thus, the Hasse invariants of A at the finite primes are all 0 and they are $1/2$ at the two infinite primes. Using these calculations, one deduces that $D = \mathbb{H}(\mathbb{Q}(\sqrt{2}))$ (see also Example 6.13) and $A \simeq M_3(\mathbb{H}(\mathbb{Q}(\sqrt{2})))$.

Remark 3.7. The approach presented in this chapter is still valid for a field F of positive characteristic provided, FG is semisimple (i.e. the characteristic of F is coprime with the order of G). The strongly monomial part has been presented in [BdR] and implemented in the package by O. Broche and Á. del Río. In general, the problem in positive characteristic is somehow simpler because the Wedderburn components of FG are split, that is, they are matrices over fields.

The functionality of the package `wedderga` depends on the capacity of constructing fields in the GAP system. In practice `wedderga` can compute the Wedderburn decomposition of semisimple group algebras over finite abelian extensions of the rationals and finite fields.

Notes on Chapter 3

A useful tool for further study of the description of the Wedderburn decomposition of group algebras of finite groups could be a program able to compute the Schur indices of Schur algebras (see e.g. Example 3.6) using methods that were developed in [Tur, Sch, Her5].

Chapter 4

Group algebras of Kleinian type and groups of units

In this chapter we present some applications of the first part of this work to the study and classification of some special algebras, called of Kleinian type, and applications to the study of units of group rings. The algebras of Kleinian type are finite dimensional semisimple rational algebras A such that the group of units of an order in A is commensurable with a direct product of Kleinian groups. The aim of this chapter is to classify the Schur algebras of Kleinian type and the group algebras of Kleinian type. As an application, we want to characterize the group rings RG, with R an order in a number field and G a finite group, such that the group of units of RG is virtually a direct product of free-by-free groups.

Historically, the study of Kleinian groups, that is discrete subgroups of $\mathrm{PSL}(\mathbb{C})$, goes back to the works of Poincaré and Bianchi and it has been an active field of research ever since. Poincaré described in 1883 a method to obtain presentations of Kleinian groups using fundamental domains [Poi]. In 1892 Bianchi computed fundamental domains for groups of the form $\mathrm{PSL}_2(R)$, where R is a ring of integers of an imaginary quadratic extension [Bia]. These groups are nowadays called *Bianchi groups*. During the last decades, Kleinian groups have been strongly related to the Geometrization Program of Thurston for the classification of 3–manifolds [EGM, MR, Mas, Thu].

The method of studying a group by its action on a topological-geometrical object was first used by Minkowski, then by Dirichlet to prove the Unit Theorem, and later on was generalized by many authors like Eichler, Poincaré, Borel, Harish–Chandra or Siegel. The classical method consists of finding a fundamental domain of the action, that is, a subset of the geometrical object on which the group is acting which is almost equal (in a precise way) to a set of representatives of the orbits of the action, and using

the fundamental domain find presentations of the group. Unfortunately, unless the geometrical object has small dimension and the action is controlable, as in the case of the action of $\mathrm{PSL}_2(\mathbb{Z})$ on the hyperbolic plane, it is very difficult to find a fundamental domain or the problem of finding a presentation of the studied group is computationally unfeasible.

In the case of the Dirichlet Unit Theorem, the group of units of the ring of integers of a number field is included in the Euclidean space using the logarithmic map. In the case of the group $\mathrm{PSL}_2(\mathbb{Z})$, it acts by Möbius transformations discontinuously on the Poincaré's model of the hyperbolic plane $\mathbb{H}^2$. Recall that the Möbius transformation associated to an invertible matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is the map $M_A : \widehat{\mathbb{C}} \to \widehat{\mathbb{C}}$ given by $M_A(z) = \frac{az+b}{cz+d}$, where $\widehat{\mathbb{C}}$ denotes the compactification of the plane (identified with $\mathbb{C}$) by one point. The map $A \mapsto M_A$ defines a group homomorphism from $\mathrm{PSL}_2(\mathbb{C})$ to the bijections of $\widehat{\mathbb{C}}$ on itself. If we identify the hyperbolic plane with the positive semi-plane $\mathbb{H}^2 = \{z = x + yi \in \mathbb{C} : y > 0\}$, then the matrices with real entries leave $\mathbb{H}^2$ invariant and they induce isometries of $\mathbb{H}^2$. In fact, the map $A \mapsto M_A$ induces an isomorphism between $\mathrm{PSL}_2(\mathbb{R})$ and the group of orientations preserving isometries of $\mathbb{H}^2$. Moreover, the set $\{z = x+yi : 2|x| \leq 1, |z| \leq 1\}$ is a fundamental domain of the action of $\mathrm{PSL}_2(\mathbb{Z})$ on $\mathbb{H}^2$. Using this information and classical methods, one can deduce that $\mathrm{PSL}_2(\mathbb{Z})$ is a free product of the free groups C_2 and C_3.

The action of $\mathrm{PSL}_2(\mathbb{C})$ on $\widehat{\mathbb{C}}$ can be extended to an action on the 3–dimensional hyperbolic space $\mathbb{H}^3$, the so-called Poincaré extensions. In fact, $\mathrm{PSL}_2(\mathbb{C})$ is isomorphic via this action to the group of isometries of $\mathbb{H}^3$ that conserve the orientation. The subgroups of $\mathrm{PSL}_2(\mathbb{C})$ that act discontinuously on $\mathbb{H}^3$ are exactly the *discrete subgroups* of $\mathrm{PSL}_2(\mathbb{C})$, that is the projections in $\mathrm{PSL}_2(\mathbb{C})$ of the subgroups of $\mathrm{SL}_2(\mathbb{C})$ having the discrete Euclidean topology induced by $\mathcal{M}_2(\mathbb{C})$ (that we identify with $\mathbb{R}^8 = \mathbb{C}^4$). These groups are called *Kleinian groups* [Bea, Mas].

The use of the methods of Kleinian groups to the study of the groups of units of group rings was started in [Rui] and [PdRR] and led to the notions of algebras of Kleinian type and finite groups of Kleinian type. There it is shown how one can theoretically study $\mathcal{U}(\mathbb{Z}G)$ by considering the action of the simple components of the Wedderburn decomposition of $\mathbb{Q}G$ on the 3–dimensional hyperbolic space if G is a finite group of Kleinian type. These groups have "manageable" simple components S of $\mathbb{Q}G$ that can be fields, or totally definite positive quaternion algebras or quaternion algebras such that the group of units of reduced norm 1 of an order in S is a discrete subgroup of $\mathrm{SL}_2(\mathbb{C})$.

In order to present the main idea of this approach it is convenient to consider a

more general situation that we summarize from [PdRR]. Let A be a finite dimensional semisimple rational algebra and R a $\mathbb{Z}$-order in A. It is well known that R^* is commensurable with the group of units of every order in A and, if A is simple then R^* is commensurable with $Z(R)^* \times R^1$, where R^1 denotes the group of elements of reduced norm 1 of R. Two subgroups of a given group are said to be *commensurable* if their intersection has finite index in both of them. In particular, if $A = \prod_{i\in I} A_i$ with each A_i a simple algebra, then R^* is commensurable with $\prod_{i\in I} Z(R_i)^* \times \prod_{i\in I}(R_i)^1$, where R_i is an order in A_i for each $i \in I$. Since $Z(R_i)^*$ is well understood by the Dirichlet Unit Theorem, the difficulty in understanding R^* up to commensurability relies on understanding the groups of elements of reduced norm 1 of orders in the simple components of the Wedderburn decomposition of A. If each simple component S of A can be embedded in $\mathcal{M}_2(\mathbb{C})$ so that the image of $(R_S)^1$ is a discrete subgroup of $\mathrm{SL}_2(\mathbb{C})$, for R_S an order of S, then one can describe R^* up to commensurability by using methods on Kleinian groups to describe the groups of $(R_S)^1$, for S running through the Wedderburn components of A. In case $A = \mathbb{Q}G$, this method can be used to study the group of units of the integral group ring $\mathbb{Z}G$, which is an order in $\mathbb{Q}G$. This motivates the following definitions that rigorously introduce these objects.

Let K be a number field, A a central simple K-algebra and R an order in A. By order we always mean a $\mathbb{Z}$-order. Let R^1 denote the group of units of R of reduced norm 1. Every embedding $\sigma : K \to \mathbb{C}$ induces an embedding $\overline{\sigma} : A \to M_d(\mathbb{C})$, where d is the degree of A. Namely $\overline{\sigma}(a) = \widetilde{\sigma}\varphi(1 \otimes a)$, where $\varphi : \mathbb{C} \otimes_K A \to M_D(\mathbb{C})$ is a fixed isomorphism and $\widetilde{\sigma} : M_d(\mathbb{C}) \to M_d(\mathbb{C})$ acts componentwise as an automorphism of $\mathbb{C}$ which extends σ. Furthermore, $\overline{\sigma}(R^1) \subseteq \mathrm{SL}_d(\mathbb{C})$.

Definition 4.1. [PdRR] A simple algebra A is said to be of *Kleinian type* if either A is a number field or A is a quaternion algebra over a number field K and $\overline{\sigma}(R^1)$ is a discrete subgroup of $\mathrm{SL}_2(\mathbb{C})$ for some embedding σ of K in $\mathbb{C}$. More generally, an *algebra of Kleinian type* is a finite direct sum of simple algebras of Kleinian type.

Definition 4.2. A finite group G is of *Kleinian type* if the rational group algebra $\mathbb{Q}G$ is of Kleinian type.

If G is a finite group of Kleinian type, then theoretically one can obtain a presentation of a group commensurable with $\mathcal{U}(\mathbb{Z}G)$ as follows: first, compute the Wedderburn decomposition $\prod_i^n A_i$ of the rational group algebra $\mathbb{Q}G$ and an order R_i of A_i for each A_i; second, apply Dirichlet Unit Theorem to obtain presentations of $Z(R_i)^*$; third, compute a fundamental polyhedron of $(R_i)^1$ for every i; fourth, use these fundamental polyhedrons to derive presentations of $(R_i)^1$ for each i; and finally, put all the information together, namely $\mathcal{U}(\mathbb{Z}G)$ is commensurable with the direct product of the groups

for which presentations have been obtained.

The finite groups of Kleinian type have been classified in [JPdRRZ], where it has been also proved that a finite group G is of Kleinian type if and only if the group of units $\mathbb{Z}G^*$ of its integral group ring $\mathbb{Z}G$ is commensurable with a direct product of free-by-free groups. This article was our staring point for the study of this topic and the main reference. Following a suggestion of Alan Reid, we continued the previous work by studying the consequences of replacing the ring of rational integers by another ring of integers. This leads to the following two problems:

> **Problem 1**. Classify the group algebras of Kleinian type of finite groups over number fields.
> **Problem 2**. Given a group algebra of Kleinian type KG, describe the structure of the group of units of the group ring RG for R an order in K.

The simple factors of KG are Schur algebras over their centers. So, in order to solve Problem 1, it is natural to start by classifying the Schur algebras of Kleinian type. This is obtained in Section 4.1. Using this classification and that of finite groups of Kleinian type given in [JPdRRZ] we obtain the classification of the group algebras of Kleinian type in Section 4.2. In Section 4.3 we obtain a partial solution for Problem 2.

4.1 Schur algebras of Kleinian type

Throughout K is a number field. A *cyclic cyclotomic algebra* is a cyclic algebra $(L/K, a)$, where L/K is a cyclotomic extension and a is a root of unity. A cyclic cyclotomic algebra $(L/K, a)$ is a Schur algebra because it is generated over K by the finite metacyclic group $\langle u, \zeta \rangle$, where ζ is a root of unity of L such that $L = K(\zeta)$. Conversely, every algebra generated by a finite metacyclic group is cyclic cyclotomic. Some properties of this type of algebras are studied in Chapter 6.

We will make use several times of the method to compute the Wedderburn decomposition of $\mathbb{Q}G$ for G an arbitrary finite group given in Chapter 2, as well as of the GAP package `wedderga` presented in Chapter 3. Now we quote the following theorem from [JPdRRZ].

Theorem 4.3. *The following statements are equivalent for a central simple algebra A over a number field K.*

(1) *A is of Kleinian type.*

(2) *A is either a number field or a quaternion algebra which is not ramified at at most one infinite place.*

(3) *One of the following conditions holds:*

(a) $A = K$.

(b) *A is a totally definite quaternion algebra.*

(c) $A \simeq M_2(\mathbb{Q})$.

(d) $A \simeq M_2(\mathbb{Q}(\sqrt{d}))$, *for d a square-free negative integer.*

(e) *A is a quaternion division algebra, K is totally real and A ramifies at all but one real embeddings of K.*

(f) *A is a quaternion division algebra, K has exactly one pair of complex (non-real) embeddings and A ramifies at all real embeddings of K.*

We need the following lemmas.

Lemma 4.4. *If $K = \mathbb{Q}(\sqrt{d})$ with d a square-free negative integer then*

(1) *$\mathbb{H}(K)$ is a division algebra if and only if $d \equiv 1 \mod 8$.*

(2) *$\left(\frac{-1,-3}{K}\right)$ is a division algebra if and only if $d \equiv 1 \mod 3$.*

Proof. (1) Writing $\mathbb{H}(K)$ as $(K(\zeta_4)/K, -1)$, one has that $\mathbb{H}(K)$ is a division algebra if and only if -1 is a sum of two squares in K. It is well known that this is equivalent to $d \equiv 1 \mod 8$ [FGS].

(2) Assume first that $A = \left(\frac{-1,-3}{K}\right)$ is not split. Then A is ramified at at least two finite places p_1 and p_2 since $\sum_p \mathrm{Inv}(A_p) = 0$ in $\mathbb{Q}/\mathbb{Z}$ by Hasse–Brauer–Noether–Albert Theorem (see Remark 1.95 (ii)) and A is not ramified at any infinite place. Writing A as $(K(\zeta_3)/K, -1)$ and using Theorem 1.76, one deduces that p_1 and p_2 are divisors of 3. Thus 3 is totally ramified in K and this implies that the Legendre symbol $\left(\frac{D}{3}\right) = 1$, where D is the discriminant of K (see Theorem 1.9). Since $D = d$ or $D = 4d$ and $\left(\frac{p}{3}\right) \equiv p \mod 3$, for each rational prime p, one has $d = \left(\frac{d}{3}\right) = \left(\frac{D}{3}\right) \equiv 1 \mod 3$.

Conversely, assume that $d \equiv 1 \mod 3$. Then 3 is totally ramified in K. Let p be a prime divisor of 3 in K. Then the residue field of K_p has order 3 and $K_p(\zeta_4)/K_p$ is the unique unramified extension of degree 2 of K_p by Theorem 1.77. Since $v_p(-3) = 1$, we deduce from Theorem 1.76 that -3 is not a norm of the extension $K_p(\zeta_4)/K_p$. Thus $K_p \otimes_K A = (K_p(\zeta_4)/K_p, -3)$ is a division algebra, hence so is A. □

Lemma 4.5. *Let D be a division quaternion Schur algebra over a number field K. Then D is generated over K by a metabelian subgroup of D^*.*

Proof. By means of contradiction we assume that D is not generated over K by a metabelian group. Using Amitsur's classification of the finite subgroups of division rings

(see [Ami] or [SW]) we deduce that D is generated by a group G which is isomorphic to one of the following groups: $\mathcal{O}^*$, the binary octahedral group of order 48; $\mathrm{SL}(2,5)$, the binary icosahedral group of order 120; or $\mathrm{SL}(2,3) \times M$, where M is a metacyclic group. Recall that $\mathcal{O}^* = \langle x, y, a, b | x^4 = x^2y^2 = x^2b^2 = a^3 = 1, a^b = a^{-1}, x^y = x^{-1}, x^b = y, x^a = x^{-1}y, y^a = x^{-1} \rangle$. We may assume without loss of generality that G is one of the above groups. Let D_1 be the rational subalgebra of D generated by G. It is enough to show that D_1 is generated over $\mathbb{Q}$ by a metabelian group. So we may assume that D is generated over $\mathbb{Q}$ by G, and so D is one of the factors of the Wedderburn decomposition of $\mathbb{Q}G$.

Computing the Wedderburn decomposition of $\mathbb{Q}(\mathcal{O}^*)$ and $\mathbb{Q}\,\mathrm{SL}(2,5)$ and having in mind that D has degree 2, we obtain that $D \simeq (\mathbb{Q}(\zeta_8)/\mathbb{Q}(\sqrt{2}), -1)$, if $G = \mathcal{O}^*$, and $D \simeq (\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5}), -1)$, if $G = \mathrm{SL}(2,5)$. In both cases D is generated over its center by a finite metacyclic group.

Finally, assume that $G = \mathrm{SL}(2,3) \times M$, with M metacyclic. Then D is a simple factor of $A_1 \otimes_{\mathbb{Q}} A_2$, where A_1 is a simple epimorphic image of $\mathbb{Q}\,\mathrm{SL}(2,3)$ and A_2 is a simple epimorphic image of $\mathbb{Q}M$. Since A_2 is generated by a metacyclic group, it is enough to show that so is A_1. This is clear if A_1 is commutative. Assume otherwise that A_1 is not commutative. Having in mind that D is a division quaternion algebra, one deduces that so is A_1 and, computing the Wedderburn decomposition of $\mathbb{Q}\,\mathrm{SL}(2,3)$, one obtains that A_1 is isomorphic to $\mathbb{H}(\mathbb{Q})$. This finishes the proof because $\mathbb{H}(\mathbb{Q})$ is generated over $\mathbb{Q}$ by a quaternion group of order 8. □

For a positive integer n we set

$$\eta_n = \zeta_n + \zeta_n^{-1} \quad \text{and} \quad \lambda_n = \zeta_n - \zeta_n^{-1}.$$

Observe that $\eta_n^2 - \lambda_n^2 = 4$ and hence $\mathbb{Q}(\eta_n^2) = \mathbb{Q}(\lambda_n^2)$. Furthermore, if $n \geq 3$, then λ_n^2 is totally negative because $\zeta_n^{2i} + \zeta_n^{-2i} \leq 1$, for every $i \in \mathbb{Z}$ prime with n. Therefore, if $\lambda_n^2 \in K$ then $\left(\frac{\lambda_n^2, -1}{K}\right)$ ramifies at every real embedding of K.

We are ready to classify the Schur algebras of Kleinian type.

Theorem 4.6. *Let K be a number field and let A be a non-commutative central simple K-algebra. Then A is a Schur algebra of Kleinian type if and only if A is isomorphic to one of the following algebras:*

(1) *$M_2(K)$, with $K = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{d})$ for d a square-free negative integer.*

(2) *$\mathbb{H}(\mathbb{Q}(\sqrt{d}))$, for d a square-free negative integer, such that $d \equiv 1 \mod 8$.*

(3) *$\left(\frac{-1,-3}{\mathbb{Q}(\sqrt{d})}\right)$, for d a square-free negative integer, such that $d \equiv 1 \mod 3$.*

(4) $\left(\frac{\lambda_n^2,-1}{K}\right)$, *where* $n \geq 3$, $\eta_n \in K$ *and* K *has at least one real embedding and at most one pair of complex (non-real) embeddings.*

Proof. That the algebras listed are of Kleinian type follows at once from Proposition 4.3. Let K be a field. Then $M_2(K)$ is an epimorphic image of KD_8 and if $\lambda_n^2 \in K$ then the algebra $\left(\frac{\lambda_n^2,-1}{K}\right)$ is an epimorphic image of KQ_{2n}. This shows that the algebras listed are Schur algebras because $\mathbb{H}(K) = \left(\frac{\zeta_4^2,-1}{K}\right)$ and $\left(\frac{-3,-1}{K}\right) = \left(\frac{\zeta_6^2,-1}{K}\right)$.

Now we prove that if A is a Schur algebra of Kleinian type then one of the cases (1)–(4) holds. If A is not a division algebra, Proposition 4.3 implies that $A = M_2(K)$ for $K = \mathbb{Q}$ or an imaginary quadratic extension of $\mathbb{Q}$, so (1) holds.

In the remainder of the proof we assume that A is a division Schur algebra of Kleinian type. By Lemma 4.5, A is generated over K by a finite metabelian group G. Then $A = K \otimes_L B$, where B is a simple epimorphic image of $\mathbb{Q}G$ with center L and, by Proposition 2.3, B is a cyclic cyclotomic algebra $(\mathbb{Q}(\zeta_n)/L, \zeta_n^a)$ of degree 2. Since A is of Kleinian type, so is B.

Now we prove that L is totally real. Otherwise, since L is a Galois extension of $\mathbb{Q}$, L is totally complex and therefore K is also totally complex. By Proposition 4.3, both L and K are imaginary quadratic extensions of $\mathbb{Q}$ and so $L = K$ and $\varphi(n) = 4$, where φ is the Euler function. Then either (a) $n = 8$ and $K = \mathbb{Q}(\zeta_4)$ or $K = \mathbb{Q}(\sqrt{-2})$; or (b) $n = 12$ and $K = \mathbb{Q}(\zeta_4)$ or $K = \mathbb{Q}(\zeta_3)$. If $n = 8$, then B is generated over $\mathbb{Q}$ by a group of order 16 containing an element of order 8. Since B is a division algebra, $G = Q_{16}$ and so $B = \mathbb{H}(\mathbb{Q}(\sqrt{2}))$, a contradiction. Thus $n = 12$ and hence $B = (\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_d), \zeta_d^a)$, where $d = 6$ or 4. Since ζ_6 is a norm of the extension $\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_6)$, necessarily $d = 4$. So $A = B = (\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4), \zeta_4^a) = \left(\frac{\zeta_4^a,-3}{\mathbb{Q}(\zeta_4)}\right)$. Since $X = 1 + \zeta_4$, $Y = \zeta_4$ is a solution of the equation $\zeta_4 X^2 - 3Y^2 = 1$, ζ_4 is a norm of the extension $\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)$, and hence so is ζ_4^a, yielding a contradiction.

So L is a totally real field of index 2 in $\mathbb{Q}(\zeta_n)$. Then $L = \mathbb{Q}(\eta_n)$ and necessarily B is isomorphic to $(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\eta_n), -1) \simeq \left(\frac{\lambda_n^2,-1}{L}\right)$. This implies that $A \simeq \left(\frac{\lambda_n^2,-1}{K}\right)$. If K has some embedding in $\mathbb{R}$, then (4) holds. Otherwise $K = \mathbb{Q}(\sqrt{d})$, for some square-free negative integer d. This implies that $L = \mathbb{Q}$. Then $n = 3$, 4 or 6 and so A is isomorphic to either $\mathbb{H}(K)$ or $\left(\frac{-1,-3}{K}\right)$. Since A is a division algebra, Lemma 4.4 implies that, in the first case, $d \equiv 1 \mod 8$ and condition (2) holds, and, in the second case, $d \equiv 1 \mod 3$ and condition (3) holds. □

4.2 Group algebras of Kleinian type

In this section we classify the group algebras of Kleinian type, that is the number fields K and finite groups G such that KG is of Kleinian type. The classification for $K = \mathbb{Q}$ was given in [JPdRRZ].

We start with some notation. The cyclic group of order n is usually denoted by C_n. To emphasize that $a \in C_n$ is a generator of the group, we write C_n either as $\langle a \rangle$ or $\langle a \rangle_n$. Recall that a group G is *metabelian* if G has an abelian normal subgroup N such that $A = G/N$ is abelian. We simply denote this information as $G = N : A$. To give a concrete presentation of G we will write N and A as direct products of cyclic groups and give the necessary extra information on the relations between the generators. By $\overline{x}$ we denote the coset xN. For example, the dihedral group of order $2n$ and the quaternion group of order $4n$ can be given by

$$\begin{array}{rcll} D_{2n} & = & \langle a \rangle_n : \langle \overline{b} \rangle_2, & b^2 = 1, a^b = a^{-1}. \\ Q_{4n} & = & \langle a \rangle_{2n} : \langle \overline{b} \rangle_2, & a^b = a^{-1},\ b^2 = a^n. \end{array}$$

If N has a complement in G then A can be identify with this complement and we write $G = N \rtimes A$. For example, the dihedral group can be also given by $D_{2n} = \langle a \rangle_n \rtimes \langle b \rangle_2$ with $a^b = a^{-1}$ and the semidihedral groups of order 2^{n+2} can be described as

$$\begin{array}{rcll} D^+_{2^{n+2}} & = & \langle a \rangle_{2^{n+1}} \rtimes \langle b \rangle_2, & a^b = a^{2^n+1}. \\ D^-_{2^{n+2}} & = & \langle a \rangle_{2^{n+1}} \rtimes \langle b \rangle_2, & a^b = a^{2^n-1}. \end{array}$$

Following the notation in [JPdRRZ], for a finite group G, we denote by $\mathcal{C}(G)$ the set of isomorphism classes of noncommutative simple quotients of $\mathbb{Q}G$. We generalize this notation and, for a semisimple group algebra KG, we denote by $\mathcal{C}(KG)$ the set of isomorphism classes of noncommutative simple quotients of KG. For simplicity, we represent $\mathcal{C}(G)$ by listing a set of representatives of its elements. For example, using the isomorphisms

$$\mathbb{Q}D^-_{16} \cong 4\mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\sqrt{-2})) \quad \text{and} \quad \mathbb{Q}D^+_{16} \cong 4\mathbb{Q} \oplus 2\mathbb{Q}(i) \oplus M_2(\mathbb{Q}(i))$$

one deduces that $\mathcal{C}(D^+_{16}) = \{M_2(\mathbb{Q}(i))\}$ and $\mathcal{C}(D^-_{16}) = \{M_2(\mathbb{Q}), M_2(\mathbb{Q}(\sqrt{-2}))\}$.

The following groups play an important role in the classification of groups of Kleinian type.

$$\mathcal{W} = \big(\langle t\rangle_2 \times \langle x^2\rangle_2 \times \langle y^2\rangle_2\big) : (\langle \overline{x}\rangle_2 \times \langle \overline{y}\rangle_2), \text{ with } t=(y,x) \text{ and } Z(\mathcal{W}) = \langle x^2, y^2, t\rangle.$$

$$\mathcal{W}_{1n} = \left(\prod_{i=1}^{n} \langle t_i\rangle_2 \times \prod_{i=1}^{n} \langle y_i\rangle_2\right) \rtimes \langle x\rangle_4, \text{ with } t_i=(y_i,x) \text{ and } Z(\mathcal{W}_{1n}) = \langle t_1,\dots,t_n,x^2\rangle.$$

$$\mathcal{W}_{2n} = \left(\prod_{i=1}^{n} \langle y_i\rangle_4\right) \rtimes \langle x\rangle_4, \text{ with } t_i=(y_i,x)=y_i^2 \text{ and } Z(\mathcal{W}_{2n}) = \langle t_1,\dots,t_n,x^2\rangle.$$

$$\mathcal{V} = \big(\langle t\rangle_2 \times \langle x^2\rangle_4 \times \langle y^2\rangle_4\big) : (\langle \overline{x}\rangle_2 \times \langle \overline{y}\rangle_2), \text{ with } t=(y,x) \text{ and } Z(\mathcal{W}) = \langle x^2, y^2, t\rangle.$$

$$\mathcal{V}_{1n} = \left(\prod_{i=1}^{n} \langle t_i\rangle_2 \times \prod_{i=1}^{n} \langle y_i\rangle_4\right) \rtimes \langle x\rangle_8, \text{ with } t_i=(y_i,x) \text{ and}$$
$$Z(\mathcal{V}_{1n}) = \langle t_1,\dots,t_n,y_1^2,\dots,y_n^2,x^2\rangle.$$

$$\mathcal{V}_{2n} = \left(\prod_{i=1}^{n} \langle y_i\rangle_8\right) \rtimes \langle x\rangle_8, \text{ with } t_i=(y_i,x)=y_i^4 \text{ and } Z(\mathcal{V}_{2n}) = \langle t_i,x^2\rangle.$$

$$\mathcal{U}_1 = \left(\prod_{1\le i<j\le 3} \langle t_{ij}\rangle_2 \times \prod_{k=1}^{3} \langle y_k^2\rangle_2\right) : \left(\prod_{k=1}^{3} \langle \overline{y_k}\rangle_2\right), \text{ with } t_{ij}=(y_j,y_i) \text{ and}$$
$$Z(\mathcal{U}_1) = \langle t_{12},t_{13},t_{23},y_1^2,y_2^2,y_3^2\rangle.$$

$$\mathcal{U}_2 = \big(\langle t_{23}\rangle_2 \times \langle y_1^2\rangle_2 \times \langle y_2^2\rangle_4 \times \langle y_3^2\rangle_4\big) : \left(\prod_{k=1}^{3} \langle \overline{y_k}\rangle_2\right), \text{ with } t_{ij}=(y_j,y_i),\ y_2^4=t_{12},$$
$$y_3^4=t_{13} \text{ and } Z(\mathcal{U}_2) = \langle t_{12},t_{13},t_{23},y_1^2,y_2^2,y_3^2\rangle.$$

$$\mathcal{T} = (\langle t\rangle_4 \times \langle y\rangle_8) : \langle \overline{x}\rangle_2, \text{ with } t=(y,x) \text{ and } x^2=t^2=(x,t).$$

$$\mathcal{T}_{1n} = \left(\prod_{i=1}^{n} \langle t_i\rangle_4 \times \prod_{i=1}^{n} \langle y_i\rangle_4\right) \rtimes \langle x\rangle_8, \text{ with } t_i=(y_i,x),\ (t_i,x)=t_i^2 \text{ and}$$
$$Z(\mathcal{T}_{1n}) = \langle t_1^2,\dots,t_n^2,x^2\rangle.$$

$$\mathcal{T}_{2n} = \left(\prod_{i=1}^{n} \langle y_i\rangle_8\right) \rtimes \langle x\rangle_4, \text{ with } t_i=(y_i,x)=y_i^{-2} \text{ and } Z(\mathcal{T}_{2n}) = \langle t_1^2,\dots,t_n^2,x^2\rangle.$$

$$\mathcal{T}_{3n} = \left(\langle y_1^2t_1\rangle_2 \times \langle y_1\rangle_8 \times \prod_{i=2}^{n} \langle y_i\rangle_4\right) : \langle \overline{x}\rangle_2, \text{ with } t_i=(y_i,x),\ (t_i,x)=t_i^2,\ x^2=t_1^2,$$
$$Z(\mathcal{T}_{3n}) = \langle t_1^2,y_2^2,\dots,y_n^2,x^2\rangle \text{ and, if } i\ge 2 \text{ then } t_i=y_i^2,$$

$$\mathcal{S}_{n,P,Q} = C_3^n \rtimes P = (C_3^n \times Q) : \langle \overline{x}\rangle_2, \text{ with } Q \text{ a subgroup of index 2 in } P \text{ and}$$
$$z^x = z^{-1} \text{ for each } z \in C_3^n.$$

We collect the following lemmas from [JPdRRZ].

Lemma 4.7. *Let G be a finite group and A an abelian subgroup of G such that every subgroup of A is normal in G. Let*

$$\mathcal{H} = \{H \mid H \text{ is a subgroup of } A \text{ with } A/H \text{ cyclic and } G' \not\subseteq H\}.$$

Then $\mathcal{C}(G) = \bigcup_{H\in\mathcal{H}} \mathcal{C}(G/H)$.

Lemma 4.8. *Let A be a finite abelian group of exponent d and G an arbitrary group.*

(1) *If $d|2$ then $\mathcal{C}(A \times G) = \mathcal{C}(G)$.*

(2) *If $d|4$ and $\mathcal{C}(G) \subseteq \left\{M_2(\mathbb{Q}), \mathbb{H}(\mathbb{Q}), \left(\frac{-1,-3}{\mathbb{Q}}\right), M_2(\mathbb{Q}(\zeta_4))\right\}$ then $\mathcal{C}(A \times G) \subseteq \mathcal{C}(G) \cup \{M_2(\mathbb{Q}(\zeta_4))\}$.*

(3) *If $d|6$ and $\mathcal{C}(G) \subseteq \left\{M_2(\mathbb{Q}), \mathbb{H}(\mathbb{Q}), \left(\frac{-1,-3}{\mathbb{Q}}\right), M_2(\mathbb{Q}(\zeta_3))\right\}$ then $\mathcal{C}(A \times G) \subseteq \mathcal{C}(G) \cup \{M_2(\mathbb{Q}(\zeta_3))\}$.*

Lemma 4.9. (1) $\mathcal{C}(\mathcal{W}_{1n}) = \{M_2(\mathbb{Q})\}$.

(2) $\mathcal{C}(\mathcal{W}) = \mathcal{C}(\mathcal{W}_{2n}) = \{M_2(\mathbb{Q}), \mathbb{H}(\mathbb{Q})\}$.

(3) $\mathcal{C}(\mathcal{V}), \mathcal{C}(\mathcal{V}_{1n}), \mathcal{C}(\mathcal{V}_{2n}), \mathcal{C}(\mathcal{U}_1), \mathcal{C}(\mathcal{U}_2), \mathcal{C}(\mathcal{T}_{1n}) \subseteq \{M_2(\mathbb{Q}), \mathbb{H}(\mathbb{Q}), M_2(\mathbb{Q}(\zeta_4))\}$.

(4) $\mathcal{C}(\mathcal{T}), \mathcal{C}(\mathcal{T}_{2n}), \mathcal{C}(\mathcal{T}_{3n}) \subseteq \{M_2(\mathbb{Q}), \mathbb{H}(\mathbb{Q}), M_2(\mathbb{Q}(\zeta_4)), \mathbb{H}(\mathbb{Q}(\sqrt{2})), M_2(\mathbb{Q}(\sqrt{-2}))\}$.

(5) *Let $G = \mathcal{S}_{n,P,Q}$.*

   (a) *If $P = \langle x \rangle$ is cyclic of order 2^n then $\mathcal{C}(G) = \mathcal{C}(G/\langle x^2 \rangle) \cup \left\{\left(\frac{\zeta_{2^{n-1}},-3}{\mathbb{Q}(\zeta_{2^{n-1}})}\right)\right\}$. In particular,*

   - *if $P = C_2$ then $\mathcal{C}(G) = \{M_2(\mathbb{Q})\}$,*
   - *if $P = C_4$ then $\mathcal{C}(G) = \left\{M_2(\mathbb{Q}), \left(\frac{-1,-3}{\mathbb{Q}}\right)\right\}$, and*
   - *if $P = C_8$ then $\mathcal{C}(G) = \left\{M_2(\mathbb{Q}), \left(\frac{-1,-3}{\mathbb{Q}}\right), M_2(\mathbb{Q}(\zeta_4))\right\}$.*

   (b) *If $P = \mathcal{W}_{1n}$ and $Q = \langle y_1, \ldots, y_n, t_1, \ldots, t_n, x^2 \rangle$ then $\mathcal{C}(G) = \left\{M_2(\mathbb{Q}), \left(\frac{-1,-3}{\mathbb{Q}}\right), M_2(\mathbb{Q}(\zeta_3))\right\}$.*

   (c) *If $P = \mathcal{W}_{21}$ and $Q = \langle y_1^2, x \rangle$ then $\mathcal{C}(G) = \{M_2(\mathbb{Q}), \mathbb{H}(\mathbb{Q}(\sqrt{3})), M_2(\mathbb{Q}(\zeta_4)), M_2(\mathbb{Q}(\zeta_3))\}$.*

We are ready to present our classification of the group algebras of Kleinian type.

Theorem 4.10. *Let K be a number field and G a finite group. Then KG is of Kleinian type if and only if G is either abelian or an epimorphic image of $A \times H$, for A an abelian group, and one of the following conditions holds:*

(1) *$K = \mathbb{Q}$ and one of the following conditions holds.*

   (a) *A has exponent 6 and H is either $\mathcal{W}$, $\mathcal{W}_{1n}$ or $\mathcal{W}_{2n}$, for some n, or $H = \mathcal{S}_{m,\mathcal{W}_{1n},Q}$ with $Q = \langle y_1, \ldots, y_m, t_1, \ldots, t_m, x^2 \rangle$, for some n and m.*

(b) *A has exponent 4 and H is either $\mathcal{U}_1$, $\mathcal{U}_2$, $\mathcal{V}$, $\mathcal{V}_{1n}$, $\mathcal{V}_{2n}$ or $\mathcal{S}_{n,C_8,C_4}$, for some n.*

(c) *A has exponent 2 and H is either $\mathcal{T}$, $\mathcal{T}_{1n}$, $\mathcal{T}_{2n}$, $\mathcal{T}_{3n}$ or $\mathcal{S}_{n,\mathcal{W}_{21},Q}$ with $Q = \langle y_1^2, x\rangle$, for some n.*

(2) *$K \neq \mathbb{Q}$ and has at most one pair of complex (non-real) embeddings, A has exponent 2 and $H = Q_8$.*

(3) *K is an imaginary quadratic extension of $\mathbb{Q}$, A has exponent 2 and H is either $\mathcal{W}$, $\mathcal{W}_{1n}$, $\mathcal{W}_{2n}$ or $\mathcal{S}_{n,C_4,C_2}$, for some n.*

(4) *$K = \mathbb{Q}(\zeta_3)$, A has exponent 6 and H is either $\mathcal{W}$, $\mathcal{W}_{1n}$ or $\mathcal{W}_{2n}$, for some n, or $H = \mathcal{S}_{m,\mathcal{W}_{1n},Q}$ with $Q = \langle y_1, \ldots, y_m, t_1, \ldots, t_m, x^2\rangle$, for some n and m.*

(5) *$K = \mathbb{Q}(\zeta_4)$, A has exponent 4 and H is either $\mathcal{U}_1, \mathcal{U}_2, \mathcal{V}, \mathcal{V}_{1n}, \mathcal{V}_{2n}, \mathcal{T}_{1n}$ or $\mathcal{S}_{n,C_8,C_4}$, for some n.*

(6) *$K = \mathbb{Q}(\sqrt{-2})$, A has exponent 2 and H is either D_{16}^- or $\mathcal{T}_{2n}$, for some n.*

Proof. To avoid trivialities, we assume that G is non-abelian. The main theorem of [JPdRRZ] states that $\mathbb{Q}G$ is of Kleinian type if and only if G is an epimorphic image of $A \times H$ for A abelian and A and H satisfy one of the conditions (a)–(c) from (1). So, in the remainder of the proof, we assume that $K \neq \mathbb{Q}$.

First we prove that if one of the conditions (2)–(6) holds, then KG is of Kleinian type. For that we compute $\mathcal{C}(KG)$ and check that it consists of algebras satisfying one of the conditions of Theorem 4.6. Since $\mathcal{C}(K\overline{G}) \subseteq \mathcal{C}(KG)$, for $\overline{G}$ an epimorphic image of G, it is enough to compute $\mathcal{C}(KG)$ for $G = A \times H$ and K, A and H satisfying one of the conditions (2)–(6). We use repeatedly Lemmas 4.8 and 4.9 which provide an approximation of $\mathcal{C}(G)$ and $\mathcal{C}(KG) = \{KZ(A) \otimes_{Z(A)} A : A \in \mathcal{C}(G)\}$.

If (2) holds, then $\mathcal{C}(KG) = \{\mathbb{H}(K)\}$.

If (3) holds, then $\mathcal{C}(G) \subseteq \{M_2(\mathbb{Q}), \mathbb{H}(\mathbb{Q}), \left(\frac{-1,-3}{\mathbb{Q}}\right)\}$, and we deduce that $\mathcal{C}(KG) \subseteq \{M_2(K), \mathbb{H}(K), \left(\frac{-1,-3}{K}\right)\}$.

Similarly, if (4) holds then $\mathcal{C}(G) \subseteq \mathcal{C}(H) \cup \{M_2(\mathbb{Q}(\zeta_3))\} \subseteq \{M_2(\mathbb{Q}), \mathbb{H}(\mathbb{Q}), \left(\frac{-1,-3}{\mathbb{Q}}\right), M_2(\mathbb{Q}(\zeta_3))\}$. Hence $\mathcal{C}(KG) = \{M_2(\mathbb{Q}(\zeta_3))\}$, by Lemma 4.4.

Arguing similarly, one deduces that if (5) holds then $\mathcal{C}(KG) = \{M_2(\mathbb{Q}(\zeta_4))\}$.

Finally, assume that (6) holds. If $H = D_{16}^-$ then $\mathcal{C}(G) = \{M_2(\mathbb{Q}), M_2(\mathbb{Q}(\sqrt{-2}))\}$ and so $\mathcal{C}(KG) = \{M_2(\mathbb{Q}(\sqrt{-2}))\}$. Otherwise, $H = \mathcal{T}_{2n}$ for some n. In this case we show that $\mathcal{C}(KG) = \{M_2(\mathbb{Q}(\sqrt{-2}))\}$. For that, we need a better approximation of $\mathcal{C}(G)$ than the one given in Lemma 4.9. Namely, we show that $\mathcal{C}(G) = \{M_2(\mathbb{Q}), \mathbb{H}(\mathbb{Q}), M_2(\mathbb{Q}(\sqrt{-2}))\}$.

Let L be a proper subgroup of H' (the derived subgroup of H) such that H'/L is cyclic. Using that $(y,x)y^2 = 1$, for each $y \in \langle y_1, \ldots, y_n\rangle$, one has that $\mathcal{T}_{2n}/L$ is an epimorphic image of $\mathcal{T}_{21} \times C_2^{n-1}$. Then Lemmas 4.7 and 4.8 imply that $\mathcal{C}(G) = \mathcal{C}(\mathcal{T}_{21})$. So we may assume that $G = \mathcal{T}_{21}$. Now take $B = Z(\mathcal{T}_{21}) = \langle t^2, x^2\rangle \simeq C_2^2$ and L a subgroup of B such that B/L is cyclic. If $t^2 \in L$, then $\mathcal{T}_{21}/L$ is an epimorphic image of $\mathcal{W}$ and therefore $\mathcal{C}(\mathcal{T}_{21}/L) \subseteq \{M_2(\mathbb{Q}), \mathbb{H}(\mathbb{Q})\}$. Otherwise $L = \langle x^2\rangle$ or $L = \langle x^2t^2\rangle$; hence $\mathcal{T}_{21}/L \simeq D_{16}^-$ and so $\mathcal{C}(\mathcal{T}_{21}/L) \subseteq \{M_2(\mathbb{Q}), M_2(\mathbb{Q}(\sqrt{-2}))\}$. Using Lemma 4.7, one deduces that $\mathcal{C}(\mathcal{T}_{2n}) = \{\mathbb{H}(\mathbb{Q}), M_2(\mathbb{Q}), M_2(\mathbb{Q}(\sqrt{-2}))\}$ as claimed.

Conversely, assume that KG is of Kleinian type (and G is non-abelian and $K \neq \mathbb{Q}$). Then $\mathbb{Q}G$ is of Kleinian type, that is G is an epimorphic image of $A \times H$ for A and H satisfying one of the conditions (a)–(c) from (1). Furthermore, K has at most one pair of complex embeddings, by Theorem 4.6. We have to show that K, A and H satisfy one of the conditions (2)–(6). We consider several cases.

Case 1. Every element of $\mathcal{C}(G)$ is a division algebra.

This implies that G is Hamiltonian and so $G \simeq Q_8 \times E \times F$ with E an elementary abelian 2–group and F abelian of odd order [Rob, 5.3.7]. If $F = 1$, then (2) holds. Otherwise, $\mathcal{C}(KG)$ contains $\mathbb{H}(K(\zeta_n))$, where n is the exponent of F. Therefore $n = 3$ and $K = \mathbb{Q}(\zeta_3)$, by Theorem 4.6. Since Q_8 is an epimorphic image of $\mathcal{W}$, condition (4) holds.

In the remainder of the proof we assume that $\mathcal{C}(G)$ contains a non-division algebra B. Then $B = M_2(L)$ for some field L and therefore $M_2(KL) \in \mathcal{C}(KG)$. Since $K \neq \mathbb{Q}$, KL is an imaginary quadratic extension of $\mathbb{Q}$ and $L \subseteq K$. Let E be the center of an element of $\mathcal{C}(G)$. Then KE is the center of an element of $\mathcal{C}(KG)$. If $KE \neq K$, then the two complex embeddings of K extend to more than two complex embeddings of KE, yielding a contradiction. This shows that K contains the center of each element of $\mathcal{C}(G)$.

Case 2. The center of each element of $\mathcal{C}(G)$ is $\mathbb{Q}$.

Then Lemmas 4.8 and 4.9 imply that $\mathcal{C}(G) \subseteq \{M_2(\mathbb{Q}), \mathbb{H}(\mathbb{Q}), \left(\frac{-1,-3}{\mathbb{Q}}\right)\}$. Using this and the main theorem of [LdR] one has that $G = A \times H$, where A is an elementary abelian 2–group and H is an epimorphic image of $\mathcal{W}$, $\mathcal{W}_{1n}$, $\mathcal{W}_{2n}$ or $\mathcal{S}_{n,C_4,C_2}$, for some n. So G satisfies (3).

Case 3. At least one element of $\mathcal{C}(G)$ has center different from $\mathbb{Q}$.

Then the center of each element of $\mathcal{C}(G)$ is either $\mathbb{Q}$ or K. Using Lemmas 4.8 and 4.9 one has: If A and H satisfy condition (1.a) then $K = \mathbb{Q}(\zeta_3)$, hence (4) holds. If either A and H satisfy (1.b) or they satisfy (1.c) with $H = \mathcal{T}_{1n}$, for some n, then $K = \mathbb{Q}(\zeta_4)$ and condition (5) holds.

Otherwise, A has exponent 2 and H is either $\mathcal{T}, \mathcal{T}_{2n}, \mathcal{T}_{3n}$, or $\mathcal{S}_{n,\mathcal{W}_{21},\langle y_1^2,x\rangle}$, for some n. Since A has exponent 2, one may assume that $G = A \times H_1$, for H_1 an epimorphic image of H and H_1 is not an epimorphic image of any of the groups considered above. We use the standard bar notation for the images of $\mathbb{Q}H$ in $\mathbb{Q}H_1$.

Assume first that $H = \mathcal{T}$. Then $(M = \langle y, t\rangle, L = \langle ty^{-2}\rangle)$ is a strong Shoda pair of $\mathcal{T}$ and, by using Proposition 2.3, one deduces that if $e = e(\mathcal{T}, M, L) = \widehat{L}\frac{1-y^4}{2}$, then $\mathbb{Q}Ge \simeq \mathbb{H}(\mathbb{Q}(\sqrt{2}))$. Since $\mathbb{H}(\mathbb{Q}(\sqrt{2}))$ is not of Kleinian type, we have that $\overline{e} = 0$, or equivalently $\overline{y}^4 \in \overline{L}$. Hence either $\overline{y}^4 = 1$, $\overline{t}^2 = 1$ or $\overline{t} = \overline{y}^{-2}$. So H_1 is an epimorphic image of either $\mathcal{T}/\langle y^4\rangle$, $\mathcal{T}/\langle t^2\rangle$ or $\mathcal{T}/\langle ty^2\rangle$. In the first case H_1 is an epimorphic image of $\mathcal{T}_{11}$ and in the second case H_1 is an epimorphic image of $\mathcal{V}$. In both cases we obtain a contradiction with the hypothesis that H_1 is not an epimorphic image of the groups considered above. Thus H_1 is an epimorphic image of $\mathcal{T}/\langle ty^2\rangle \simeq D_{16}^-$. In fact $H_1 = D_{16}^-$, because every proper non-abelian quotient of D_{16}^- is an epimorphic image of $\mathcal{W}$. Then $\mathcal{C}(G) = \mathcal{C}(D_{16}^-) = \{M_2(\mathbb{Q}), M_2(\mathbb{Q}(\sqrt{-2}))\}$ and so $K = \mathbb{Q}(\sqrt{-2})$. Hence condition (6) holds.

Assume now that $H = \mathcal{T}_{2n}$. By the first part of the proof we have $\mathcal{C}(H) = \{\mathbb{H}(\mathbb{Q}), M_2(\mathbb{Q}),$
$M_2(\mathbb{Q}(\sqrt{-2}))\}$. Since we are assuming that one element of $\mathcal{C}(G)$ has center different from $\mathbb{Q}$, then $M_2(\mathbb{Q}(\sqrt{-2})) \in \mathcal{C}(H_1)$ and so $K = \mathbb{Q}(\sqrt{-2})$. Hence condition (6) holds.

In the two remaining options for H we are going to obtain some contradiction.

Suppose that $H = \mathcal{T}_{3n}$. We may assume that n is the minimal positive integer such that G is an epimorphic image of $\mathcal{T}_{3n} \times A$, for A an elementary abelian 2–group. This implies that $\langle \overline{t_1^2}, \overline{t_2}, \ldots, \overline{t_n}\rangle$ is elementary abelian of order 2^n and hence $\langle \overline{y_1}^2, \overline{y_2}, \ldots, \overline{y_n}\rangle \simeq C_4^n$. Let $M = \langle y_1, y_2, \ldots, y_n\rangle$ and $L_1 = \langle t_1 y_1^{-2}, y_2, y_3, \ldots, y_n\rangle$. Then (M, L_1) is a strong Shoda pair of H. By using Proposition 2.3, we obtain that $\mathbb{Q}He(H, M, L_1) \simeq \mathbb{H}(\mathbb{Q}(\sqrt{2}))$. This implies that $\overline{e(H, M, L_1)} = 0$, or equivalently $\overline{t_1^2} = \overline{y_1^4} \in \overline{L_1}$. Since $\overline{t_1^2}$ has order 2 and $\overline{t_1^2} \notin \langle t_2, \ldots, t_n\rangle$ one has $\overline{t_1^2} = \overline{t_1 y_1^{-2} t_2^{\alpha_2} \cdots t_n^{\alpha_n}}$ for some $\alpha_1, \ldots, \alpha_n \in \{0, 1\}$. Since, by assumption, H_1 is not an epimorphic image of $\mathcal{T}_{2n}$, we have $\alpha_i \neq 0$ for some $i \geq 2$. After changing generators one may assume that $\alpha_2 = 1$ and $\alpha_i = 0$ for $i \geq 3$. Thus $\overline{t_1} = \overline{y_1^{-2} t_2}$. Let now $L_2 = \langle t_1 y_1^{-2}, y_2 y_1^{-2}, y_3, \ldots, y_n\rangle$. Then (M, L_2) is also a strong Shoda pair of H and $\mathbb{Q}Ge(H, M, L_2) \simeq \mathbb{H}(\mathbb{Q}(\sqrt{2}))$. The same argument shows that $\overline{y_1}^4 = \overline{t_1^2} \in \overline{L_2} = \langle \overline{t_1 y_1^{-2}}, \overline{y_2 y_1^{-2}}, \overline{y_3}, \ldots, \overline{y_n}\rangle$. This yields a contradiction because $\overline{t_1 y_1^{-2}} = (\overline{y_2 y_1^{-2}})^2 \in \langle \overline{y_2 y_1^{-2}}, \overline{y_3}, \ldots, \overline{y_n}\rangle$ and $\overline{y_1}^4 \notin \langle \overline{y_2 y_1^{-2}}, \overline{y_3}, \ldots, \overline{y_n}\rangle$.

Finally assume that $H = \mathcal{S}_{n,\mathcal{W}_{21},Q}$, with $Q = \langle y_1^2, x\rangle$ and set $y = y_1$. Since, by assumption, G does not satisfy (1.a), one has $\bar{t} = \overline{t_1} \neq 1$. Moreover, as in the previous case, one may assume that n is minimal (for G to be a quotient of $H \times A$, with A elementary abelian 2–group). Let $M = \langle C_3^n, x, t\rangle$ and $L = \langle Z_1, tx^2\rangle$, where

Z_1 is a maximal subgroup of $Z = C_3^n$. Then (M, L) is a strong Shoda pair of H and $\mathbb{Q}He(H, M, L) \simeq \mathbb{H}(\mathbb{Q}(\sqrt{3}))$. Thus $0 = \overline{e(H, M, L)} = \overline{\widehat{L}(1 - \widehat{z})(1 - \widehat{t})}$, where $z \in Z \setminus Z_1$. Comparing coefficients and using the fact that $\overline{t} \neq \overline{z}$, for each $z \in Z$, we have $\overline{\widehat{L}(1 - \widehat{z})} = 0$, that is $\overline{L} = \overline{Z}$ and this contradicts the minimality of n. □

4.3 Groups of units

In this section we study the virtual structure of RG^*, for G a finite group and R an order in a number field K. More precisely, we characterize the finite groups G and number fields K for which RG^* is finite, virtually abelian, virtually a direct product of free groups or virtually a direct product of free-by-free groups.

We say that a group *virtually* satisfies a group theoretical condition if it has a subgroup of finite index satisfying the given condition. Notice that the virtual structure of RG^* does not depend on the order R and, in fact, if S is any order in KG, then S^* and RG^* are commensurable (see Lemma 1.15).

It is easy to show that a group commensurable with a free group (respectively a free-by-free group, a direct product of free groups, a direct product of free-by-free groups) is also virtually free (respectively virtually free-by-free, virtually direct product of free groups, virtually direct product of free-by-free groups).

An important tool is the following lemma.

Lemma 4.11. *Let $A = \prod_{i=1}^n A_i$ be a finite dimensional rational algebra with A_i simple for every i. Let S be an order in A and S_i an order in A_i.*

(1) *S^* is finite if and only if for each i, A_i is either $\mathbb{Q}$, an imaginary quadratic extension of $\mathbb{Q}$ or a totally definite quaternion algebra over $\mathbb{Q}$.*

(2) *S^* is virtually abelian if and only if for each i, A_i is either a number field or a totally definite quaternion algebra.*

(3) *S^* is virtually a direct product of free groups if and only if for each i, A_i is either a number field, a totally definite quaternion algebra or $M_2(\mathbb{Q})$.*

(4) *S^* is virtually a direct product of free-by-free groups if and only if for each i, S_i^1 is virtually free-by-free.*

Proof. We are going to use the following facts:

(a) S^* is commensurable with $\prod_{i=1}^n S_i^*$ and S_i^* is commensurable with $Z(S_i)^* \times S_i^1$. (This is because S and $\prod_{i=1}^n S_i$ are both orders in A.)

(b) S_i^1 is finite if and only if A_i is either a field or a totally definite quaternion algebra (see [Kle1] or [Seh, Lemma 21.3]).

(c) If A_i is neither a field nor a totally definite quaternion algebra and S_i^1 is commensurable with a direct product of groups G_1 and G_2, then either G_1 or G_2 is finite [KdR].

(d) S_i^1 is infinite and virtually free if and only if $A_i \simeq M_2(\mathbb{Q})$ (see [Kle2, page 233]).

(1) By (a), S^* is finite if and only if S_i^* is finite for each i if and only if $Z(S_i)^*$ and S_i^1 are finite for each i. By the Dirichlet Unit Theorem, if A_i is a number field, then S_i^* is finite if and only if A_i is either $\mathbb{Q}$ or an imaginary quadratic extension of $\mathbb{Q}$. Using this and (b), one deduces that, if A_i is not a number field then $Z(S_i)^*$ and S_i^1 are finite if and only if A_i is a totally definite quaternion algebra over $\mathbb{Q}$.

(2) By (a), S^* is virtually abelian if and only if S_i^1 is virtually abelian for each i. If A_i is either a number field or a totally definitive quaternion algebra then S_i^1 is finite and in particular virtually abelian, by (b). Conversely, assume that S_i^1 is virtually abelian. We argue by contradiction to show that A_i is either a number field or a totally definite quaternion algebra. Otherwise, S_i^1 is virtually infinite cyclic by (b) and (c) and the fact that S_i^1 is finitely generated. Then (d) implies that $A_i = M_2(\mathbb{Q})$ and so S_i^1 is commensurable with $\mathrm{SL}_2(\mathbb{Z})$. This yields a contradiction because $\mathrm{SL}_2(\mathbb{Z})$ is not virtually cyclic.

(3) By (a) and [JdR, Lemma 3.1], S^* is virtually a direct product of free groups if and only if so is S_i^1 for each i. As in the previous proof, if A_i is neither commutative nor a totally definite quaternion algebra, then S_i^1 is virtually a direct product of free groups if and only if it is virtually free if and only if $A_i \simeq M_2(\mathbb{Q})$.

(4) Is proved in [JPdRRZ, Theorem 2.1]. □

The characterization of when RG^* is finite (respectively virtually abelian, virtually a direct product of free groups) is an easy generalization of the corresponding result for integral group rings.

Theorem 4.12. *Let R be an order in a number field K and G a finite group. Then RG^* is finite if and only if one of the following conditions holds:*

(1) *$K = \mathbb{Q}$ and G is either abelian of exponent dividing 4 or 6, or isomorphic to $Q_8 \times A$, for A an elementary abelian 2–group.*

(2) *K is an imaginary quadratic extension of $\mathbb{Q}$ and G is an elementary abelian 2–group.*

(3) *$K = \mathbb{Q}(\zeta_3)$ and G is abelian of exponent 3 or 6.*

(4) $K = \mathbb{Q}(\zeta_4)$ *and* G *is abelian of exponent* 4.

Proof. If $K = \mathbb{Q}$, then $R = \mathbb{Z}$ and it is well known that $\mathbb{Z}G^*$ is finite if and only if G is abelian of exponent dividing 4 or 6 or it is isomorphic to $Q_8 \times A$, for A an elementary abelian 2–group [Seh].

If one of the conditions (1)–(4) holds, then KG is a direct product of copies of $\mathbb{Q}$, imaginary quadratic extensions of $\mathbb{Q}$ and $\mathbb{H}(\mathbb{Q})$. Then RG^* is finite by Lemma 4.11.

Conversely, assume that RG^* is finite and $K \neq \mathbb{Q}$. Then $\mathbb{Z}G^*$ is finite and therefore G is either abelian of exponent dividing 4 or 6, or isomorphic to $Q_8 \times A$, for A an elementary abelian 2–group. Moreover, R^* is finite and so $K = \mathbb{Q}(\sqrt{d})$ for d a square-free negative integer. If the exponent of G is 2 then (2) holds. If G is non-abelian, i.e. $G \equiv Q_8 \times A$ with A elementary abelian 2–group, then one of the simple components of KG is $M_2(\mathbb{Q}(\sqrt{d}))$, contradicting the previous paragraph. Thus G is abelian. If the exponent of G is 3 or 6, then one of the simple components of KG is $\mathbb{Q}(\sqrt{d}, \zeta_3)$, hence $d = -3$, and therefore (3) holds. If the exponent of G is 4 then one of the simple components of KG is $\mathbb{Q}(\sqrt{d}, \zeta_4)$ and therefore $d = -1$, that is (4) holds. □

Theorem 4.13. *Let R be an order in a number field K and G a finite group. Then RG^* is virtually abelian if and only if either G is abelian or K is totally real and $G \simeq Q_8 \times A$, for A an elementary abelian 2–group.*

Proof. As in the proof of Theorem 4.12, the sufficient condition is a direct consequence of Lemma 4.11.

Conversely, assume that RG^* is virtually abelian. Then $\mathbb{Z}G^*$ is virtually abelian and therefore it does not contain a non-abelian free group. Then G is either abelian or isomorphic to $G \simeq Q_8 \times A$, for A an elementary abelian 2–group (Theorem 1.35). In the latter case, one of the simple components of KG is $\mathbb{H}(K)$ and hence K is totally real, by Lemma 4.11. □

Theorem 4.14. *Let R be an order in a number field K and G a finite group. Then RG^* is virtually a direct product of free groups if and only if either G is abelian or one of the following conditions holds:*

(1) $K = \mathbb{Q}$ *and* $G \simeq H \times A$, *for A an elementary abelian 2–group and H is either $\mathcal{W}$, $\mathcal{W}_{1n}$, $\mathcal{W}_{1n}/\langle x^2 \rangle$, $\mathcal{W}_{2n}$, $\mathcal{W}_{2n}/\langle x^2 \rangle$, $\mathcal{W}_{2n}/\langle x^2 t_1 \rangle$, $\mathcal{T}_{3n}$ or $H = \mathcal{S}_{n,C_{2t},C_t}$, for some n and $t = 1, 2$ or 4.*

(2) *K is totally real and $G \simeq Q_8 \times A$, for A an elementary abelian 2–group.*

Proof. The finite groups G such that $\mathbb{Z}G^*$ is virtually a direct product of free groups were classified in [JL, JLdR, JdR, LdR] and are the abelian groups and those satisfying

condition (1). So, in the remainder of the proof, one may assume that $R \neq \mathbb{Z}$, or equivalently $K \neq \mathbb{Q}$, and we have to show that RG^* is virtually a direct product of free groups if and only if either G is abelian or (2) holds.

If either G is abelian or (2) holds then RG^* is virtually abelian, hence RG^* is virtually a direct product of free groups, because it is finitely generated.

Conversely, assume that RG^* is virtually a direct product of free groups and G is non-abelian. Since $K \neq \mathbb{Q}$, $M_2(\mathbb{Q})$ is not a simple quotient of KG, hence Lemma 4.11 implies that every simple quotient of KG is either a number field or a totally definite quaternion algebra. In particular, G is Hamiltonian, that is $G = Q_8 \times A \times F$, where A is an elementary abelian 2–group and F is abelian of odd order. If n is the exponent of F then $\mathbb{H}(K(\zeta_n))$ is a simple quotient of KG and this implies that $n = 1$ and K is totally real. □

Now we prove the main result of this section which provides a characterization of when RG^* is virtually a direct product of free-by-free groups.

Theorem 4.15. *Let R be an order in a number field K and G a finite group. Then RG^* is virtually a direct product of free-by-free groups if and only if either G is abelian or one of the following conditions holds:*

(1) *G is an epimorphic image of $A \times H$ with A abelian and K, A and H satisfy one of the conditions (1), (4), (5) or (6) of Theorem 4.10.*

(2) *K is totally real and $G \simeq A \times Q_8$, for A an elementary abelian 2–group.*

(3) *$K = \mathbb{Q}(\sqrt{d})$, for d a square-free negative integer, $SL_2(\mathbb{Z}[\sqrt{d}])$ is virtually free-by-free, and $G \simeq A \times H$ where A is an elementary abelian 2–group and one of the following conditions holds:*

   (a) *H is either $\mathcal{W}_{1n}$, $\mathcal{W}_{1n}/\langle x^2 \rangle$, $\mathcal{W}_{2n}/\langle x^2 \rangle$ or $\mathcal{S}_{n,C_2,1}$, for some n.*

   (b) *H is either $\mathcal{W}$, $\mathcal{W}_{2n}$ or $\mathcal{W}_{2n}/\langle x^2 t_1 \rangle$, for some n and $d \not\equiv 1 \mod 8$.*

   (c) *$H = \mathcal{S}_{n,C_4,C_2}$ for some n and $d \not\equiv 1 \mod 3$.*

Proof. To avoid trivialities we assume that G is not abelian. Along the proof we are going to refer to conditions (1)–(6) of Theorem 4.10 and to conditions (1)–(3) of the theorem being proved. To avoid confusion, we establish the convention that any reference to conditions (1)–(3) refers to condition (1)–(3) of Theorem 4.15.

We first show that if K and G satisfy one of the listed conditions then RG^* is virtually a direct product of free-by-free groups. By Lemma 4.11, this is equivalent to showing that for every $B \in \mathcal{C}(KG)$ and S an (any) order in B, we have that S^1 is virtually free-by-free. By using Lemmas 4.8 and 4.9 and the computation of $\mathcal{C}(KG)$ in

the proof of Theorem 4.10, it is easy to show that if K and G satisfy one of the conditions (1) or (2), then every element of $\mathcal{C}(KG)$ is either a totally definite quaternion algebra or isomorphic to $M_2(K)$ for $K = \mathbb{Q}(\sqrt{d})$, with $d = 0, -1, -2$ or -3. In the first case S^1 is finite and in the second case S^1 is virtually free-by-free (see Lemma 4.11 and [JPdRRZ, Lemma 3.1] or alternatively [Kle1], [MR, page 137] and [WZ]). If K and G satisfy condition (3) then Lemmas 4.4, 4.8 and 4.9 imply that $\mathcal{C}(KG) = \{M_2(\mathbb{Q}(\sqrt{d}))\}$. Since S^1 and $\mathrm{SL}_2(\mathbb{Z}[\sqrt{d}])$ are commensurable and, by assumption, the latter is virtually free-by-free, we have that S^1 is virtually free-by-free.

Conversely, assume that RG^* is virtually a direct product of free-by-free groups. Let B be a simple factor of KG and S an order in B. By Lemma 4.11, S^1 is virtually free-by-free and hence the virtual cohomological dimension of S^1 is at most 2. Then B is of Kleinian type by [JPdRRZ, Corollary 3.4]. This proves that KG is of Kleinian type. Furthermore, B is of one of the types (a)–(f) from Proposition 4.3. However, the virtual cohomological dimension of S^1 is 0, if B is of type (a) or (b); 1 if B is of type (c); 2 if it is of type (d) or (e); and 3 if B is of type (f) [JPdRRZ, Remark 3.5]. Thus B is not of type (f). Since every simple factor of KG contains K, either K is totally real or K is an imaginary quadratic extension of $\mathbb{Q}$ and KG is split.

By Theorem 4.10, G is an epimorphic image of $A \times H$ with A abelian and K, A and H satisfying one of the conditions (1)–(6) of Theorem 4.10. If they satisfy one of the conditions (1), (4), (5) or (6) of Theorem 4.10, then condition (1) (of Theorem 4.15) holds. So, we assume that K, A and H satisfy either condition (2) or (3) of Theorem 4.10. Since A is an elementary abelian 2–group, one may assume that $G = A \times H_1$ with H_1 an epimorphic image of H.

Assume first that K, A and H satisfy condition (2) of Theorem 4.10. Then one of the simple quotient of KG is isomorphic to $\mathbb{H}(K)$. If K is totally real then condition (2) holds. Otherwise $K = \mathbb{Q}(\sqrt{d})$ for d a square-free negative integer and $\mathbb{H}(K)$ is split. By Lemma 4.4, $d \not\equiv 1 \mod 8$. Since $Q_8 \simeq \mathcal{W}_{21}/\langle x^2 t_1 \rangle$, condition (3b) holds.

Secondly assume that K, A and H satisfy condition (3) of Theorem 4.10 and set $K = \mathbb{Q}(\sqrt{d})$ for d a square-free negative integer. Then $\mathcal{C}(G) \subseteq \left\{\mathbb{H}(\mathbb{Q}), M_2(\mathbb{Q}), \left(\frac{-1,-3}{\mathbb{Q}}\right)\right\}$, by Lemma 4.9. By the main theorem of [JdR], H_1 is isomorphic to either $\mathcal{W}$, $\mathcal{W}_{1n}$, $\mathcal{W}_{2n}$, $\mathcal{W}_{1n}/\langle x_1^2 \rangle$, $\mathcal{W}_{2n}/\langle x_1^2 \rangle$, $\mathcal{W}_{2n}/\langle x_1^2 t_1 \rangle$, $\mathcal{S}_{n,C_2,1}$ or $\mathcal{S}_{n,C_4,C_2}$, for some n. If H is either $\mathcal{W}_{1n}$, $\mathcal{W}_{1n}/\langle x_1^2 \rangle$, $\mathcal{W}_{2n}/\langle x_1^2 \rangle$ or $\mathcal{S}_{n,C_2,1}$, then (3a) holds. If H is either $\mathcal{W}$, $\mathcal{W}_{2n}$ or $\mathcal{W}_{2n}/\langle x^2 t_1 \rangle$ then $\mathcal{C}(G) = \{M_2(\mathbb{Q}), \mathbb{H}(\mathbb{Q})\}$ and, arguing as in the previous paragraph, one deduces that $d \not\equiv 1 \mod 8$. In this case condition (3b) holds. Finally, if $G = \mathcal{S}_{n,C_4,C_2}$ then $\mathcal{C}(G) = \left\{M_2(\mathbb{Q}), \left(\frac{-1,-3}{\mathbb{Q}}\right)\right\}$ and using the second part of Lemma 4.4 one deduces that $d \not\equiv 1 \mod 3$, and condition (3c) holds. □

The main theorem of [JPdRRZ] states that a finite group G is of Kleinian type if

and only if $\mathbb{Z}G^*$ is commensurable with a direct product of free-by-free groups. One implication is still true when $\mathbb{Z}$ is replaced by an arbitrary order in a number field. This is a consequence of Theorems 4.10 and 4.15.

Corollary 4.16. *Let R be an order in a number field K and G a finite group. If RG^* is commensurable with a direct product of free-by-free groups then KG is of Kleinian type.*

It also follows from Theorems 4.10 and 4.15 that the converse of Corollary 4.16 fails. The group algebras KG of Kleinian type for which the group of units of an order in KG is not virtually a direct product of free-by-free groups occur under the following circumstances, where $G = A \times H$ for A an elementary abelian 2–group:

(1) K is a number field of degree ≥ 3 over $\mathbb{Q}$ with exactly one pair of complex embeddings and at least one real embedding and $H = Q_8$.

(2) $K = \mathbb{Q}(\sqrt{d})$, for d a square-free negative integer with $d \equiv 1 \mod 8$ and $H = \mathcal{W}$, $\mathcal{W}_{2n}$ or $\mathcal{W}_{2n}/\langle x^2 t_1 \rangle$, for some n.

(3) $K = \mathbb{Q}(\sqrt{d})$ for d a square-free negative integer with $d \equiv 1 \mod 3$ and $H = \mathcal{S}_{n,C_4,C_2}$.

(4) $K = \mathbb{Q}(\sqrt{d})$ and d and H satisfy one of the conditions (3a)–(3c) from Theorem 4.15, but $\mathrm{SL}_2(\mathbb{Z}[\sqrt{d}])$ is not virtually free-by-free.

Resuming, if KG is of Kleinian type, then we have a good description of the virtual structure of RG^* for R an order in K, except for the four cases above. It has been conjectured that $\mathrm{SL}_2(\mathbb{Z}[\sqrt{d}])$ is virtually free-by-cyclic for every negative integer d. This conjecture has been verified for $d = -1, -2, -3, -7$ and -11 (see [MR] and [WZ]). Thus, maybe the last case does not occur and the hypothesis of $\mathrm{SL}_2(\mathbb{Z}[\sqrt{d}])$ being virtually free-by-free in Theorem 4.15 is superfluous.

In order to obtain information on the virtual structure of RG^* in the four cases (1)–(4) above, one should investigate the groups of units S^*, for S an order in the following algebras: $\mathbb{H}(K)$, for K a number field with exactly one pair of complex embeddings and $\mathbb{H}(K)$ is not split, $\mathbb{H}(\mathbb{Q}(\sqrt{d}))$ with $d \equiv 1 \mod 8$, $\left(\frac{-1,-3}{\mathbb{Q}(\sqrt{d})}\right)$ with $d \equiv 1 \mod 3$ and, of course, $M(\mathbb{Q}(\sqrt{d}))$ for d a square-free negative integer. Notice that $K = \mathbb{Q}(\sqrt{-7})$ and $G = Q_8 = \mathcal{W}_{11}/\langle x^2 t_1 \rangle$ is an instance of cases (2) above and, if R is an order in K, then RQ_8^* is commensurable with $\mathbb{H}(R)^*$. A presentation of $\mathbb{H}(R)^*$, for R the ring of integers of $\mathbb{Q}(\sqrt{-7})$ has been computed in [CJLdR].

Notes on Chapter 4

The aim of this chapter was not to give a self-contained presentation about group algebras of Kleinian type, but to continue the work presented in [JPdRRZ] generalizing the results to arbitrary rings of integers. Since we need only selected topics, we are far from presenting a complete picture of them, so that we do not insist on their general history. As already mentioned, our starting point and main reference was the article [JPdRRZ]. The reader is refereed to [Poi, Bia, WZ, Mas] for further information on the topic of Kleinian groups and to [EGM, MR, Mas, Thu] for the applications related to the Geometrization Problem of Thurston for the classification of 3–manifolds.

A more extensive and complete presentation of groups and algebras of Kleinian type can be found in the thesis [Rui] and in the article [PdRR], where these notions were first defined, in the master thesis [Pit, Bar], and in the article [JPdRRZ]. In the latter it has been also given a characterization of finite groups of Kleinian type in terms of the group of units of its integral group ring.

Some possible further development of the results from Section 3 of this chapter can be the generalization of some results to semigroup algebras. It could be interesting to know if the methods developed in [DJ] to reduce problems on semigroup rings to similar problems on group rings and the Wedderburn components of group algebras could be applied here.

Chapter 5

The Schur group of an abelian number field

In this chapter we characterize the maximum r-local index of a Schur algebra over an abelian number field K in terms of global information determined by the field K, for r an arbitrary rational prime. This characterization completes and unifies previous results of Janusz [Jan3] and Pendergrass [Pen2].

Throughout let K be an abelian number field. The existence of the maximum r-local index of a Schur algebra over K is a consequence of the Benard-Schacher Theorem (see Theorem 1.108) which gives a partial characterization of the elements of the Schur group $S(K)$ of the field K. According to this theorem, if n is the Schur index of a Schur algebra A over K, then the group of roots of unity $W(K)$ of K contains an element of order n. Since $S(K)$ is a torsion abelian group, it is enough to compute the maximum of the r-local indices of Schur algebras over K with index a power of p for every prime p dividing the order of $W(K)$. We will refer to this number as $p^{\beta_p(r)}$. In [Jan3], Janusz gave a formula for $p^{\beta_p(r)}$ when either p is odd or K contains a primitive 4-th root of unity. The remaining cases were considered by Pendergrass in [Pen1]. However, some of the calculations involving factor sets in [Pen1] are not correct, and as a consequence the formulas for $2^{\beta_2(r)}$ for odd primes r that appear there are inaccurate. This work was mainly motivated by the problem of finding a correct formula for $p^{\beta_p(r)}$ in this remaining case. Moreover, we need to apply the formula in the next chapter. Since the local index at ∞ will be 2 when K is real and will be 1 otherwise, and for $r = 2$ one has $\beta_p(r) = 0$ unless $p = 2$ and $\zeta_4 \in K$ and $S(K_2) \neq 1$, in which case $\beta_2(r) = 1$, the only remaining case is that of r odd. This is the case considered in this chapter. The characterization of fields K for which $S(K_2)$ is of order 2 is given in [Pen1, Corollary 3.3].

The main result of the chapter (Theorem 5.13) characterizes $p^{\beta_p(r)}$ in terms of the position of K relative to an overlying cyclotomic extension F which is determined by K and p. The formulas for $p^{\beta_p(r)}$ are stated in terms of elements of certain Galois groups in this setting. The main difference between our approach and that of Janusz and Pendergrass is that the field F that we use is slightly larger, which allows us to present some of the somewhat artificial-looking calculations in [Jan3] in a more conceptual fashion. Another highlight of our approach is the treatment of calculations involving factor sets. First we generalize a result from [AS] which describes the factor sets for a given action of an abelian group G on another abelian group W in terms of some data. In particular, we give necessary and sufficient conditions that the data must satisfy in order to be induced by a factor set. Because of the applications we have in mind, extra attention is paid to the case when W is a cyclic p-group.

5.1 Factor set calculations

In this section W and G are two abelian groups and $\Upsilon : G \to \mathrm{Aut}(W)$ is a group homomorphism (later on we will assume that W is a cyclic p-group). A group epimorphism $\pi : \overline{G} \to G$ with kernel W is said to induce Υ if, given $u_g \in \overline{G}$ such that $\pi(u_g) = g$, one has $u_g w u_g^{-1} = \Upsilon(g)(w)$ for each $w \in W$. If $g \mapsto u_g$ is a *crossed section* of π (i.e. $\pi(u_g) = g$ for each $g \in G$) then the map $\alpha : G \times G \to W$ defined by $u_g u_h = \alpha_{g,h} u_{gh}$ is a *factor set* (or 2-*cocycle*) $\alpha \in Z^2(G, W)$. We always assume that the crossed sections are normalized, i.e. $u_1 = 1$ and hence $\alpha_{g,1} = \alpha_{1,g} = 1$. Since a different choice of crossed section for π would be a map $g \mapsto w_g u_g$, where $w : G \to W$, π determines a unique cohomology class in $H^2(G, W)$, namely the one represented by α.

Given a list $g_1, \ldots, g_n$ of generating elements of G, a group epimorphism $\pi : \overline{G} \to G$ inducing Υ, and a crossed section $g \mapsto u_g$ of π, we associate the elements β_{ij} and γ_i of W, for $i, j \leq n$, by the equalities:

$$\begin{aligned} u_{g_j} u_{g_i} &= \beta_{ij} u_{g_i} u_{g_j}, \text{ and} \\ u_{g_i}^{q_i} &= \gamma_i u_{g_1}^{t_1^{(i)}} \cdots u_{g_{i-1}}^{t_{i-1}^{(i)}}, \end{aligned} \tag{5.1}$$

where the integers q_i and $t_j^{(i)}$ for $1 \leq i \leq n$ and $0 \leq j < i$ are determined by

$$q_i = \text{ order of } g_i \text{ modulo } \langle g_1, \ldots, g_{i-1} \rangle, \quad g_i^{q_i} = g_1^{t_1^{(i)}} \cdots g_{i-1}^{t_{i-1}^{(i)}}, \quad 0 \leq t_j^{(i)} < q_j. \tag{5.2}$$

If α is the factor set associated to π and the crossed section $g \mapsto u_g$, and the generating set $g_1, \ldots, g_n$ is clear from the context, then we abbreviate the above by saying that α induces the data (β_{ij}, γ_i). The following proposition gives necessary and sufficient conditions for a list (β_{ij}, γ_i) of elements of W to be induced by a factor set.

Proposition 5.1. *Let W and $G = \langle g_1, \dots, g_n \rangle$ be abelian groups and let $\Upsilon : G \to \mathrm{Aut}(W)$ be an action of G on W. For every $1 \le i, j \le n$, let q_i and $t_j^{(i)}$ be the integers determined by (5.2). For every $w \in W$ and $1 \le i \le n$, let*

$$\Upsilon_i = \Upsilon(g_i), \quad N_i^t(w) = w\Upsilon_i(w)\Upsilon_i^2(w)\cdots\Upsilon_i^{t-1}(w), \quad \text{and} \quad N_i = N_i^{q_i}.$$

For every $1 \le i, j \le n$, let β_{ij} and γ_i be elements of W. Then the following conditions are equivalent:

(1) *There is a factor set $\alpha \in Z^2(G, W)$ inducing the data (β_{ij}, γ_i).*

(2) *The following equalities hold for every $1 \le i, j, k \le n$:*

(C1) $\beta_{ii} = \beta_{ij}\beta_{ji} = 1$.

(C2) $\beta_{ij}\beta_{jk}\beta_{ki} = \Upsilon_k(\beta_{ij})\Upsilon_i(\beta_{jk})\Upsilon_j(\beta_{ki})$.

(C3) $N_i(\beta_{ij})\gamma_i = \Upsilon_j(\gamma_i)N_1^{t_1^{(i)}}(\beta_{1j})\Upsilon_1^{t_1^{(i)}}(N_2^{t_2^{(i)}}(\beta_{2j}))\cdots\Upsilon_1^{t_1^{(i)}}\Upsilon_2^{t_2^{(i)}}\dots\Upsilon_{i-2}^{t_{i-2}^{(i)}}(N_{i-1}^{t_{i-1}^{(i)}}(\beta_{(i-1)j}))$.

Proof. (1) implies (2). Assume that there is a factor set $\alpha \in Z^2(G, W)$ inducing the data (β_{ij}, γ_i). Then there is a surjective homomorphism $\pi : \overline{G} \to G$ and a crossed section $g \mapsto u_g$ of π such that the β_{ij} and γ_i satisfy (5.1). Condition (C1) is clear. Conjugating by u_{g_k} in $u_{g_j}u_{g_i} = \beta_{ij}u_{g_i}u_{g_j}$ yields

$$\beta_{jk}\Upsilon_j(\beta_{ik})\beta_{ij}u_{g_i}u_{g_j} = \beta_{jk}\Upsilon_j(\beta_{ik})u_{g_j}u_{g_i} = \beta_{jk}u_{g_j}\beta_{ik}u_{g_i} = u_{g_k}u_{g_j}u_{g_i}u_{g_k}^{-1} =$$
$$u_{g_k}\beta_{ij}u_{g_i}u_{g_j}u_{g_k}^{-1} = \Upsilon_k(\beta_{ij})\beta_{ik}u_{g_i}\beta_{jk}u_{g_j} = \Upsilon_k(\beta_{ij})\beta_{ik}\Upsilon_i(\beta_{jk})u_{g_i}u_{g_j}.$$

Therefore, we have $\beta_{jk}\Upsilon_j(\beta_{ik})\beta_{ij} = \Upsilon_k(\beta_{ij})\beta_{ik}\Upsilon_i(\beta_{jk})$ and so (C2) follows from (C1).

To prove (C3), we use the obvious relation $(wu_{g_i})^t = N_i^t(w)u_{g_i}^t$. Conjugating by u_{g_j} in $u_{g_i}^{q_i} = \gamma_i u_{g_1}^{t_1^{(i)}}\cdots u_{g_{i-1}}^{t_{i-1}^{(i)}}$ results in

$$N_i(\beta_{ij})\gamma_i u_{g_1}^{t_1^{(i)}}\cdots u_{g_{i-1}}^{t_{i-1}^{(i)}} = N_i^{q_i}(\beta_{ij})u_{g_i}^{q_i} = (\beta_{ij}u_{g_i})^{q_i} = u_{g_j}u_{g_i}^{q_i}u_{g_j}^{-1} = u_{g_j}\gamma_i u_{g_1}^{t_1^{(i)}}\cdots u_{g_{i-1}}^{t_{i-1}^{(i)}}u_{g_j}^{-1}$$
$$= \Upsilon_j(\gamma_i)(\beta_{1j}u_{g_1})^{t_1^{(i)}}\cdots(\beta_{(i-1)j}u_{g_{i-1}})^{t_{i-1}^{(i)}} = \Upsilon_j(\gamma_i)N_1^{t_1^{(i)}}(\beta_{1j})u_{g_1}^{t_1^{(i)}}\cdots N_{i-1}^{t_{i-1}^{(i)}}(\beta_{(i-1)j})u_{g_{i-1}}^{t_{i-1}^{(i)}}$$
$$= \Upsilon_j(\gamma_i)N_1^{t_1^{(i)}}(\beta_{1j})\Upsilon_1^{t_1^{(i)}}(N_2^{t_2^{(i)}}(\beta_{2j}))\cdots\Upsilon_1^{t_1^{(i)}}\Upsilon_2^{t_2^{(i)}}\dots\Upsilon_{i-2}^{t_{i-2}^{(i)}}(N_{i-1}^{t_{i-1}^{(i)}}(\beta_{(i-1)j}))u_{g_1}^{t_1^{(i)}}\cdots u_{g_{i-1}}^{t_{i-1}^{(i)}}.$$

Cancelling on both sides produces (C3). This finishes the proof of (1) implies (2).

Before proving (2) implies (1), we show that if $\pi : \overline{G} \to G$ is a group homomorphism with kernel W inducing Υ, $g \mapsto u_g$ is a crossed section of π and β_{ij} and γ_i are given by (5.1), then $\overline{G}$ is isomorphic to the group $\widehat{G}$ given by the following presentation: the set of generators of $\widehat{G}$ is $\{\widehat{w}, \widehat{g}_i : w \in W, i = 1, \dots, n\}$, and the relations are

$$\widehat{w_1w_2} = \widehat{w_1}\widehat{w_2}, \quad \Upsilon_i(w) = \widehat{g}_i\widehat{w}\widehat{g}_i^{-1}, \quad \widehat{g}_j\widehat{g}_i = \widehat{\beta}_{ij}\widehat{g}_i\widehat{g}_j, \quad \widehat{g}_i^{q_i} = \widehat{\gamma}_i\widehat{g}_1^{t_1^{(i)}}\cdots\widehat{g}_{i-1}^{t_{i-1}^{(i)}}, \tag{5.3}$$

for each $1 \le i, j \le n$ and $w, w_1, w_2 \in W$. Since the relations obtained by replacing $\widehat{w}$ by w and $\widehat{g}_i$ by u_{g_i} in equation (5.3) for each $x \in W$ and each $1 \le i \le n$, hold in $\overline{G}$, there

is a surjective group homomorphism $\phi : \widehat{G} \to \overline{G}$, which associates $\widehat{w}$ with w, for every $w \in W$, and $\widehat{g}_i$ with u_{g_i}, for every $i = 1, \ldots, n$. Moreover, ϕ restricts to an isomorphism $\widehat{W} \to W$ and $|\widehat{g}_i\langle\widehat{W}, \widehat{g}_1, \ldots, \widehat{g}_{i-1}\rangle| = q_i$. Hence $[\widehat{G} : \widehat{W}| = q_1 \cdots q_n = [\overline{G} : W]$ and so $|\widehat{G}| = |\overline{G}|$. We conclude that ϕ is an isomorphism.

(2) implies (1). Assume that the β_{ij}'s and γ_i's satisfy conditions (C1), (C2) and (C3). We will recursively construct groups $\overline{G}_0, \overline{G}_1, \ldots, \overline{G}_n$. Start with $\overline{G}_0 = W$. Assume that $\overline{G}_{k-1} = \langle W, u_{g_1}, \ldots, u_{g_{k-1}}\rangle$ has been constructed with $u_{g_1}, \ldots, u_{g_{k-1}}$ (in the roles of $\widehat{g}_1, \ldots, \widehat{g}_{k-1}$) satisfying the last three relations of (5.3), for $1 \leq i, j < k$, and that these relations, together with the relations in W, form a complete list of relations for $\overline{G}_{k-1}$. To define $\overline{G}_k$ we first construct a semidirect product $H_k = \overline{G}_{k-1} \rtimes_{c_k} \langle x_k\rangle$, where c_k acts on $\overline{G}_{k-1}$ by

$$c_k(w) = \Upsilon_k(w), \quad (w \in W), \qquad c_k(u_{g_i}) = \beta_{ik} u_{g_i}.$$

In order to check that this defines an automorphism of $\overline{G}_{k-1}$ we need to check that c_k respects the defining relations of $\overline{G}_{k-1}$. That it respects the relations of W is clear because Υ_k is an automorphism of W. Now we check that it respects the last three relations in (5.3) for $1 \leq i, j < k$. Using that G is commutative one has $\Upsilon_k\Upsilon_i = \Upsilon_i\Upsilon_k$ and hence

$$c_k(\Upsilon_i(w))c_k(u_{g_i}) = \Upsilon_k(\Upsilon_i(w))\beta_{ik}u_{g_i} = \Upsilon_i(\Upsilon_k(w))\beta_{ik}u_{g_i} = \beta_{ik}u_{g_i}\Upsilon_k(w) = c_k(u_{g_i})c_k(w),$$

which shows that c_k respects the second relation. For the third relation we have

$$\begin{aligned} c_k(u_{g_j})c_k(u_{g_i}) &= \beta_{jk}u_{g_j}\beta_{ik}u_{g_i} = \beta_{jk}\Upsilon_j(\beta_{ik})\beta_{ij}u_{g_i}u_{g_j} = \Upsilon_i(\beta_{jk})\beta_{ik}\Upsilon_k(\beta_{ij})u_{g_i}u_{g_j} \\ &= \Upsilon_k(\beta_{ij})\beta_{ik}u_{g_i}\beta_{jk}u_{g_j} = c_k(\beta_{ij})c_k(u_{g_i})c_k(u_{g_j}). \end{aligned}$$

Finally, for the last relation

$$\begin{aligned} &c_k(u_{g_i})^{q_i} = (\beta_{ik}u_{g_i})^{q_i} = N_i(\beta_{ik})u_{g_i}^{q_i} = N_i(\beta_{ik})\gamma_i u_{g_1}^{t_1^{(i)}} \cdots u_{g_{i-1}}^{t_{i-1}^{(i)}} \\ &= \Upsilon_k(\gamma_i)N_1^{t_1^{(i)}}(\beta_{1k})\Upsilon_1^{t_1^{(i)}}(N_2^{t_2^{(i)}}(\beta_{2k}))\cdots\Upsilon_1^{t_1^{(i)}}\Upsilon_2^{t_2^{(i)}}\ldots\Upsilon_{i-2}^{t_{i-2}^{(i)}}(N_{i-1}^{t_{i-1}^{(i)}}(\beta_{(i-1)k}))u_{g_1}^{t_1^{(i)}}\cdots u_{g_{i-1}}^{t_{i-1}^{(i)}} \\ &= c_k(\gamma_i)(N_1^{t_1^{(i)}}(\beta_{1k})u_{g_1}^{t_1^{(i)}})(N_2^{t_2^{(i)}}(\beta_{2k})u_{g_2}^{t_2^{(i)}})\cdots(N_{i-1}^{t_{i-1}^{(i)}}(\beta_{(i-1)k})u_{g_{i-1}}^{t_{i-1}^{(i)}}) \\ &= c_k(\gamma_i)(\beta_{1k}u_{g_1})^{t_1^{(i)}}\cdots(\beta_{(i-1)k}u_{g_{i-1}})^{t_{i-1}^{(i)}} \\ &= c_k(\gamma_i)c_k(u_{g_1})^{t_1^{(i)}}\cdots c_k(u_{g_{i-1}})^{t_{i-1}^{(i)}}. \end{aligned}$$

Notice that the defining relations of H_k are the defining relations of $\overline{G}_{k-1}$ together with the relations $x_k w = \Upsilon_k(w)x_k$ and $x_k u_{g_i} = \beta_{ik}u_{g_i}x_k$. Using (C3) one deduces $u_{g_i}x_k^{q_k}u_{g_i}^{-1} = u_{g_i}\gamma_k u_{g_1}^{t_1^{(k)}}\cdots u_{g_{k-1}}^{t_{k-1}^{(k)}}u_{g_i}^{-1}$, for each $i \leq k-1$. This shows that $y_k = x_k^{-q_k}\gamma_k u_{g_1}^{t_1^{(k)}}\cdots u_{g_{k-1}}^{t_{k-1}^{(k)}}$ belongs to the center of H_k. Let $\overline{G}_k = H_k/\langle y_k\rangle$ and

$u_{g_k} = x_k\langle y_k\rangle$. Now it is easy to see that the defining relations of G_k are the relations of W and the last three relations in (5.3), for $0 \le i, j \le k$.

It is clear now that the assignment $w \mapsto 1$ and $u_{g_i} \mapsto g_i$ for each $i = 1, \dots, n$ defines a group homomorphism $\pi : \overline{G} = \overline{G}_n \to G$ with kernel W and inducing Υ. If α is the factor set associated to π and the crossed section $g \mapsto u_g$, then (β_{ij}, γ_i) is the list of data induced by α. □

Note that the group generated by the values of the factor set α coincides with the group generated by the data (β_{ij}, γ_i). This observation will be used in the next section.

In the case $G = \langle g_1\rangle \times \cdots \times \langle g_n\rangle$ we obtain the following corollary that one should compare with Theorem 1.3 of [AS].

Corollary 5.2. *If $G = \langle g_1\rangle \times \cdots \times \langle g_n\rangle$ then a list $D = (\beta_{ij}, \gamma_i)_{1\le i,j\le n}$ of elements of W is the list of data associated to a factor set in $Z^2(G, W)$ if and only if the elements of D satisfy* (C1), (C2) *and $N_i(\beta_{ij})\gamma_i = \Upsilon_j(\gamma_i)$, for every $1 \le i, j \le n$.*

In the remainder of this section we assume that $W = \langle\zeta\rangle$ is a cyclic p-group, for p a prime integer. Let p^a and p^{a+b} denote the orders of $W^G = \{x \in W : \Upsilon(g)(x) = x \text{ for each } g \in G\}$ and W respectively. We assume that $0 < a, b$. We also set

$$C = \mathrm{Ker}(\Upsilon) \quad \text{and} \quad D = \{g \in G : \Upsilon(g)(\zeta) = \zeta \text{ or } \Upsilon(g)(\zeta) = \zeta^{-1}\}.$$

Note that D is subgroup of G containing C, G/D is cyclic, and $[D : C] \le 2$. Furthermore, the assumption $a > 0$ implies that if $C \ne D$ then $p^a = 2$.

Lemma 5.3. *There exists $\rho \in D$ and a subgroup B of C such that $D = \langle\rho\rangle \times B$ and $C = \langle\rho^2\rangle \times B$.*

Proof. The lemma is obvious if $C = D$ (just take $\rho = 1$). So assume that $C \ne D$ and temporarily take ρ to be any element of $D \setminus C$. Since $[D : C] = 2$, one may assume without loss of generality that $|\rho|$ is a power of 2. Write $C = C_2 \times C_{2'}$, where C_2 and $C_{2'}$ denote the 2-primary and $2'$-primary parts of C, and choose a decomposition $C_2 = \langle c_1\rangle \times \cdots \times \langle c_n\rangle$ of C_2. By reordering the c_i's if needed, one may assume that $\rho^2 = c_1^{a_1} \dots c_k^{a_k} c_{k+1}^{2c_{k+1}} \dots c_n^{2a_n}$ with $a_1, \dots, a_k$ odd. Then replacing ρ by $\rho c_{k+1}^{-a_{k+1}} \dots c_n^{-a_n}$ one may assume that $\rho^2 = c_1^{a_1} \dots c_k^{a_k}$, with $a_1, \dots, a_k$ odd. Let $H = \langle\rho, c_1, \dots, c_k\rangle$. Then $|\rho|/2 = |\rho^2| = \exp(H \cap C)$, the exponent of $H \cap C$, and so ρ is an element of maximal order in H. This implies that $H = \langle\rho\rangle \times H_1$ for some $H_1 \le H$. Moreover, if $h \in H_1 \setminus C$ then $1 \ne \rho^{|\rho|/2} = h^{|\rho|/2} \in \langle\rho\rangle \cap H_1$, a contradiction. This shows that $H_1 \subseteq C$. Thus $C_2 = (H \cap C_2) \times \langle c_{k+1}\rangle \times \cdots \times \langle c_n\rangle = \langle\rho^2\rangle \times H_1 \times \langle c_{k+1}\rangle \times \cdots \times \langle c_n\rangle$. Then ρ and $B = H_1 \times \langle c_{k+1}\rangle \times \cdots \times \langle c_n\rangle \times C_{2'}$ satisfy the required conditions. □

By Lemma 5.3, there is a decomposition $D = B \times \langle \rho \rangle$ with $C = B \times \langle \rho^2 \rangle$, which will be fixed for the remainder of this section. Moreover, if $C = D$ then we assume $\rho = 1$. Since G/D is cyclic, $G/C = \langle \rho C \rangle \times \langle \sigma C \rangle$ for some $\sigma \in G$. It is easy to see that σ can be selected so that if $D = G$ then $\sigma = 1$, and $\sigma(\zeta) = \zeta^c$ for some integer c satisfying

$$v_p(c^{q_\sigma} - 1) = a + b,\ v_p(c-1) = \begin{cases} a, & \text{if } G/C \text{ is cyclic and } G \neq D, \\ a+b, & \text{if } G/C \text{ is cyclic and } G = D, \text{ and} \\ d \geq 2, & \text{for some integer } d, \text{ if } G/C \text{ is not cyclic,} \end{cases} \tag{5.4}$$

where $q_\sigma = |\sigma C|$ and the map $v_p : \mathbb{Q} \to \mathbb{Z}$ is the classical p-adic valuation. In particular, if G/C is non-cyclic (equivalently $C \neq D \neq G$) then $p^a = 2$, $b \geq 2$, $\rho(\zeta) = \zeta^{-1}$ and $\sigma(\zeta^{2^{b-1}}) = \zeta^{2^{b-1}}$.

For every positive integer t we set

$$V(t) = 1 + c + c^2 + \cdots + c^{t-1} = \frac{c^t - 1}{c - 1}.$$

Now we choose a decomposition $B = \langle c_1 \rangle \times \cdots \times \langle c_n \rangle$ and adapt the notation of Proposition 5.1 for a group epimorphism $f : \overline{G} \to G$ with kernel W inducing Υ and elements $u_{c_1}, \ldots, u_{c_n}, u_\sigma, u_\rho \in \overline{G}$ with $f(u_{c_i}) = c_i$, $f(u_\rho) = \rho$ and $f(u_\sigma) = \sigma$, by setting

$$\beta_{ij} = [u_{c_j}, u_{c_i}], \quad \beta_{i\rho} = \beta_{\rho i}^{-1} = [u_\rho, u_{c_i}], \quad \beta_{i\sigma} = \beta_{\sigma i}^{-1} = [u_\sigma, u_{c_i}], \beta_{\sigma\rho} = \beta_{\rho\sigma}^{-1} = [\beta_\rho, \beta_\sigma].$$

We also set

$$\begin{gathered} q_i = |c_i|, \quad q_\rho = |\rho|, \quad \text{and} \quad \sigma^{q_\sigma} = c_1^{t_1} \ldots c_n^{t_n} \rho^{2t_\rho}, \\ \text{where } 0 \leq t_i < q_i \text{ and } 0 \leq t_\rho < |\rho^2|. \end{gathered} \tag{5.5}$$

With a slightly different notation than in Proposition 5.1, we have, for each $1 \leq i \leq n$, $t_j^{(i)} = 0$ for every $0 \leq j < i$, $t_i^{(\rho)} = 0$, $t_i^{(\sigma)} = t_i$, and $t_\rho^{(\sigma)} = 2t_\rho$. Furthermore, $q_\rho = 1$ if $C = D$ and q_ρ is even if $C \neq D$. Continuing with the adaptation of the notation of Proposition 5.1 we set

$$\gamma_i = u_{c_i}^{q_i}, \quad \gamma_\rho = u_\rho^{q_\rho}, \text{ and } \gamma_\sigma = u_\sigma^{q_\sigma} u_{c_1}^{-t_1} \ldots u_{c_n}^{-t_n} u_\rho^{2t_\rho}.$$

We refer to the list $\{\beta_{ij}, \beta_{i\sigma}, \beta_{i\rho}, \beta_{\sigma\rho}, \gamma_i, \gamma_\rho, \gamma_\sigma : 0 \leq i < j \leq n\}$, which we abbreviate as (β, γ), as the data associated to the group epimorphism $f : \overline{G} \to G$ and choice of crossed section $u_{c_1}, \ldots, u_{c_n}, u_\sigma, u_\rho$, or as the data induced by the corresponding factor set in $Z^2(G, W)$.

Furthermore, for every $w \in W$, $1 \leq i \leq n$ and $t \geq 0$ one has

$$N_i^t(w) = w^t, \quad N_\sigma^t(w) = w^{V(t)} \quad \text{and} \quad N_\rho^t(w) = \begin{cases} w^t, & \text{if } \rho = 1; \\ 1, & \text{if } \rho \neq 1 \text{ and } t \text{ is even;} \\ w, & \text{if } \rho \neq 1 \text{ and } t \text{ is odd.} \end{cases}$$

In particular, for every $w \in W$ one has

$$N_i(w) = w^{q_i}, \quad N_\sigma(w) = w^{V(q_\sigma)}, \quad \text{and} \quad N_\rho(w) = 1.$$

Rewriting Proposition 5.1 for this case we obtain the following.

Corollary 5.4. *Let W be a finite cyclic p-group and let G be an abelian group acting on W with $G = \langle c_1, \dots, c_n, \sigma, \rho \rangle$, $B = \langle c_1 \rangle \times \cdots \times \langle c_n \rangle$, $D = B \times \langle \rho \rangle$ and $C = B \times \langle \rho^2 \rangle$ as above. Let q_i, q_ρ, q_σ and the t_i's be given by (5.5). Let $\beta_{\sigma\rho}, \gamma_\rho, \gamma_\sigma \in W$ and for every $1 \leq i, j \leq n$ let $\beta_{ij}, \beta_{i\sigma}, \beta_{i\rho}$ and γ_i be elements of W. Then the following conditions are equivalent:*

(1) *The given collection $(\beta, \gamma) = \{\beta_{ij}, \beta_{i\sigma}, \beta_{i\rho}, \beta_{\sigma\rho}, \gamma_i, \gamma_\sigma, \gamma_\rho\}$ is the list of data induced by some factor set in $Z^2(G, W)$.*

(2) *The following hold for every $1 \leq i, j \leq n$:*

(C1) $\beta_{ii} = \beta_{ij}\beta_{ji} = 1$.

(C2) (a) $\beta_{ij} \in W^G$.

(b) *If $\rho \neq 1$ then* $\beta_{i\sigma}^2 = \beta_{i\rho}^{1-c}$.

(C3) (a) $\beta_{ij}^{q_i} = 1$.

(b) $\beta_{i\sigma}^{q_i} = \gamma_i^{c-1}$.

(c) $\beta_{i\sigma}^{-V(q_\sigma)} = \beta_{1i}^{t_1} \dots \beta_{ni}^{t_n}$.

(d) $\gamma_\sigma^{c-1} \beta_{1\sigma}^{t_1} \dots \beta_{n\sigma}^{t_n} = 1$.

(e) *If $\rho = 1$ then* $\beta_{i\rho} = \beta_{\sigma\rho} = \gamma_\rho = 1$.

(f) *If $\rho \neq 1$ then* $\beta_{i\rho}^{q_i} \gamma_i^2 = 1$, $\beta_{\sigma\rho}^{V(q_\sigma)} \gamma_\sigma^2 = \beta_{1\rho}^{t_1} \dots \beta_{n\rho}^{t_n}$ *and* $\gamma_\rho \in W^G$.

Proof. By completing the data with $\beta_{\sigma i} = \beta_{i\sigma}^{-1}$, $\beta_{\rho i} = \beta_{i\rho}^{-1}$, $\beta_{\rho\sigma} = \beta_{\sigma\rho}^{-1}$ and $\beta_{\sigma\sigma} = \beta_{\rho\rho} = 1$ we have that (C1) is a rewriting of condition (C1) from Proposition 5.1.

(C2) is the rewriting of condition (C2) from Proposition 5.1 because this condition vanishes when $1 \leq i, j, k \leq n$ and when two of the elements i, j, k are equal. Furthermore, permuting i, j, k in condition (C2) of Proposition 5.1 yields equivalent conditions. So we only have to consider three cases: substituting $i = i$, $j = j$, and $k = \sigma$; $i = i$, $j = j$, and $k = \rho$; and $i = i$, $j = \rho$, and $k = \sigma$. In the first two cases one obtains $\sigma(\beta_{ij}) = \rho(\beta_{ij}) = \beta_{ij}$, or equivalently $\beta_{ij} \in W^G$. For $\rho = 1$ the last case vanishes, and for $\rho \neq 1$ (C2) yields $\beta_{i\sigma}^2 = \beta_{i\rho}^{1-c}$.

Rewriting (C3) from Proposition 5.1 we obtain: condition (C3.a) for $i = i$, $j = j$; condition (C3.b) for $i = i$ and $j = \sigma$; condition (C3.c) for $i = \sigma$ and $j = i$; and condition (C3.d) for $i = \sigma$ and $j = \sigma$.

We consider separately the cases $\rho = 1$ and $\rho \neq 1$ for the remaining cases of rewriting (C3). Assume first that $\rho = 1$. When i is replaced by ρ and j replaced by i (respectively, by σ) we obtain $\beta_{i\rho} = 1$ (respectively $\beta_{\sigma\rho} = 1$). On the other hand, the requirement of only using normalized crossed sections implies $\gamma_\rho = 1$ in this case. When $j = \rho$ the obtained conditions are trivial.

Now assume that $\rho \neq 1$. For $i = i$ and $j = \rho$ one obtains $\beta_{i\rho}^{q_i}\gamma_i^2 = 1$. For $i = \rho$ and $j = i$ one has a trivial condition because $N_\rho(x) = 1$. For $i = \sigma$ and $j = \rho$, we obtain $\beta_{\sigma\rho}^{V(q_\sigma)}\gamma_\sigma^2 = \beta_{1\rho}^{t_1} \dots \beta_{n\rho}^{t_n}$. For $i = \rho$ and $j = \sigma$ one has $\sigma(\gamma_\rho) = \gamma_\rho$, and for $i = \rho$ and $j = \rho$ one obtains $\rho(\gamma_\rho) = \gamma_\rho$. The last two equalities are equivalent to $\gamma_\rho \in W^G$. □

The following result will show to be useful in the proof on the main theorem.

Corollary 5.5. *With the notation of Corollary 5.4, assume that G/C is non-cyclic and q_k and t_k are even for some $k \leq n$. Let (β, γ) be the list of data induced by a factor set in $Z^2(G, W)$. Then the list obtained by replacing $\beta_{k\sigma}$ by $-\beta_{k\sigma}$ and keeping the remaining data fixed is also induced by a factor set in $Z^2(G, W)$.*

Proof. It is enough to show that $\beta_{k\sigma}$ appears in all the conditions of Corollary 5.4 with an even exponent. Indeed, it only appears in (C2.b) with exponent 2; in (C3.b) with exponent q_k; in (C3.c) with exponent $-V(q_\sigma)$; and in (C3.d) and (C3.f) with exponent t_k. By the assumption it only remains to show that $V(q_\sigma)$ is even. Indeed, $v_2(V(q_\sigma)) = v_2(c^{q_\sigma} - 1) - v_2(c-1) = 1 + b - v_2(c-1) \geq 1$ because $c \not\equiv 1 \mod 2^{1+b}$. □

The data (β, γ) induced by a factor set are not cohomologically invariant, because they depend on the selection of π and of the u_{c_i}'s, u_σ and u_ρ. However, at least the β_{ij} are cohomologically invariant. For every $\alpha \in H^2(G, W)$ we associate a matrix $\beta_\alpha = (\beta_{ij})_{1 \leq i,j \leq n}$ of elements of W^G as follows: First select a group epimorphism $\pi : \overline{G} \to G$ realizing α and $u_{c_1}, \dots, u_{c_n} \in \overline{G}$ such that $\pi(u_{c_i}) = c_i$, and then set $\beta_{ij} = [u_{c_j}, u_{c_i}]$. The definition of β_α does not depend on the choice of π and the u_{c_i}'s, because if $w_1, w_2 \in W$ and $\pi(u_1), \pi(u_2) \in C$ then $[w_1u_1, w_2u_2] = [u_1, u_2]$.

Proposition 5.6. *Let $\beta = (\beta_{ij})_{1 \leq i,j \leq n}$ be a matrix of elements of W^G and for every $1 \leq i, j \leq n$ let $a_{ii} = 0$ and $a_{ij} = \min(a, v_p(q_i), v_p(q_j))$, if $i \neq j$.*

Then there is an $\alpha \in H^2(G, W)$ such that $\beta = \beta_\alpha$ if and only if the following conditions hold for every $1 \leq i, j \leq n$:

$$\beta_{ij}\beta_{ji} = \beta_{ij}^{p^{a_{ij}}} = 1. \tag{5.6}$$

Proof. Assume first that $\beta = \beta_\alpha$ for some $\alpha \in Z^2(G, W)$. Then (5.6) is a consequence of conditions (C1), (C2.a) and (C3.a) of Corollary 5.4.

Conversely, assume that β satisfies (5.6). The idea of the proof is that one can enlarge β to a list of data (β, γ) that satisfies conditions (C1)–(C3) of Corollary 5.4. Hence the desired conclusion follows from the corollary.

Condition (C1) follows automatically from (5.6). If $i, j \leq n$ then $\beta_{ij} \in W^G$ follows from the fact that $a \geq a_{ij}$ and so (5.6) implies that $\beta_{ij}^{p^a} = 1$. Hence (C2.a) holds. Also (C3.a) holds automatically from (5.6) because $p^{a_{ij}}$ divides q_i. Hence, we have to select the $\beta_{i\sigma}$'s, $\beta_{i\rho}$'s, γ_i's, $\beta_{\sigma\rho}$, γ_σ, and γ_ρ for (C2.b) and (C3.b)–(C3.f) to hold.

Assume first that $D = G$. In this case we just take $\beta_{i\sigma} = \beta_{i\rho} = \beta_{\sigma\rho} = \gamma_i = \gamma_\sigma = \gamma_\rho = 1$ for every i. Then (C2.b), (C3.b), (C3.d) and (C3.f) hold trivially by our selection. Moreover, in this case $\sigma = 1$ and so $t_i = 0$ for each $i = 1, \ldots, n$, hence (C3.c) also holds.

In the remainder of the proof we assume that $D \neq G$. First we show how one can assign values to $\beta_{\sigma i}$ and γ_i, for $i \leq n$ for (C3.b)–(C3.d) to hold. Let $d = v_p(c-1)$ and $e = v_p(V(q_\sigma)) = a+b-d$. (see (5.4)). Note that $d = a$ if $C = D$ and $a = 1 \leq 2 \leq d \leq b$ if $C \neq D$ (because we are assuming that $D \neq G$). Let X_1, X_2, Y_1 and Y_2 be integers such that $c - 1 = p^d X_1$, $V(q_\sigma) = p^e X_2$, and $X_1 Y_1 \equiv X_2 Y_2 \equiv 1 \mod p^{a+b}$. By (5.6), $\beta_{ij}^{p^{a_{ij}}} = 1$ and so $\beta_{ij} \in W^{p^{a+b-a_{ij}}}$. Therefore there are integers b_{ij}, for $1 \leq i, j \leq n$ such that $b_{ii} = b_{ij} + b_{ij} = 0$ and $\beta_{ij} = \zeta^{b_{ij} p^{a+b-a_{ij}}}$. For every $i \leq n$ set

$$x_i = Y_2 \sum_{j=1}^{n} t_j b_{ji} p^{a-a_{ji}}, \quad \beta_{\sigma i} = \zeta^{x_i p^{d-a}}, \quad y_i = Y_1 Y_2 \sum_{j=1}^{n} t_j b_{ji} \frac{q_i}{p^{a_{ij}}}, \quad \text{and} \quad \gamma_i = \zeta^{y_i}.$$

Then $V(q_\sigma) p^{d-a} x_i = p^e X_2 Y_2 \sum_{j=1}^{n} t_j b_{ji} p^{d-a_{ji}} \equiv \sum_{j=1}^{n} t_j b_{ji} p^{a+b-a_{ji}} \mod p^{a+b}$ and therefore

$$\beta_{\sigma i}^{V(q_\sigma)} = \zeta^{\sum_{j=1}^{n} t_j b_{ji} p^{a+b-a_{ji}}} = \prod_{i=1}^{n} \beta_{ji}^{t_j},$$

that is (C3.c) holds. Moreover $q_i p^{d-a} x_i = p^d Y_2 \sum_{j=1}^{n} t_j b_{ji} \frac{q_i}{p^{a_{ij}}} \equiv p^d X_1 y_i = (c-1) y_i$ and therefore $\beta_{i\sigma}^{q_i} = \gamma_i^{c-1}$, that is (C3.b) holds.

We now compute

$$\begin{array}{rcl} \sum_{i=1}^{n} t_i x_i & = & Y_2 \sum_{1 \leq i,j \leq n} t_i t_j b_{ij} p^{a-a_{ij}} \\ & = & Y_2 \sum_{i=1}^{n+1} t_i^2 b_{ii} p^{a-a_{ii}} + Y_2 \sum_{1 \leq i < j \leq n} t_i t_j (b_{ij} + b_{ji}) p^{a-a_{ij}} = 0. \end{array} \tag{5.7}$$

Then setting $\gamma_\sigma = 1$, one has

$$\gamma_\sigma^{c-1} \prod_{i=1}^{n} \beta_{i\sigma}^{t_i} = \prod_{i=1}^{n} \zeta^{-t_i x_i p^{d-a}} = \zeta^{-p^{d-a} \sum_{i=1}^{n} t_i x_i} = 1$$

and (C3.d) holds. This finishes the assignments of $\beta_{i\sigma}$ and γ_i for $i \leq n$ and of γ_σ.

If $C = D$ then a quick end is obtained assigning $\beta_{i\rho} = \beta_{\sigma\rho} = \gamma_\rho = 1$.

So it only remains to assign values to $\beta_{i\rho}, \beta_{\sigma\rho}$ and γ_ρ under the assumption that $C \neq D$. Set $\beta_{i\rho} = \zeta^{-Y_1 x_i}$. In this case $p^a = 2$ and therefore $2p^{d-a}x_i = p^d x_i \equiv (c-1)Y_1 x_i$ and $q_i Y_1 x_i = 2y_i$. Thus $\beta_{i\sigma}^2 \beta_{i\rho}^{c-1} = \zeta^{2p^{d-a}x_i}\zeta^{(1-c)Y_1 x_i} = 1$, hence (C2.b) holds, and $\beta_{i\rho}^{q_i}\gamma_i^2 = \zeta^{-q_i Y_1 x_i + 2y_i} = 1$, hence the first relation of (C3.f) follows.

Finally, using (5.7) one has

$$\beta_{1\rho}^{t_1} \dots \beta_{n\rho}^{t_n} = (\beta_{1\sigma}^{t_1} \dots \beta_{n\sigma}^{t_n})^{-Y_1} = 1 = \gamma_\sigma^2$$

and the last two relations of (C3.f) hold when $\beta_{\sigma\rho} = \gamma_\rho = 1$. □

Let $\beta = (\beta_{ij})$ be an $n \times n$ matrix of elements of W^G satisfying (5.6). Then the map $\Psi : B \times B \to W^G$ given by

$$\Psi((c_1^{x_1} \dots c_n^{x_n}, c_1^{y_1} \dots c_n^{y_n})) = \prod_{1 \leq i,j \leq n} \beta_{ij}^{x_i y_j}$$

is a *skew pairing* of B over W^G in the sense of [Jan3]; that is, it satisfies the following conditions for every $x, y, z \in B$:

$$(\Psi 1) \quad \Psi(x,x) = \Psi(x,y)\Psi(y,x) = 1, \qquad (\Psi 2) \quad \Psi(x,yz) = \Psi(x,y)\Psi(x,z).$$

Conversely, every skew pairing of B over W^G is given by a matrix $\beta = (\beta_{ij} = \Psi(c_i, c_j))_{1 \leq i,j \leq n}$ satisfying (5.6). In particular, every class in $H^2(G, W)$ induces a skew pairing $\Psi = \Psi_\alpha$ of B over W^G given by $\Psi(x,y) = \alpha_{x,y}\alpha_{y,x}^{-1}$, for all $x, y \in B$, for any cocycle α representing the given cohomology class.

In terms of skew pairings, Proposition 5.6 takes the following form.

Corollary 5.7. *If Ψ is a skew pairing of B over W^G then there is an $\alpha \in H^2(G, W)$ such that $\Psi = \Psi_\alpha$.*

Corollary 5.7 was obtained in [Jan3, Proposition 2.5] for $p^a \neq 2$. The remaining cases were considered in [Pen1, Corollary 1.3], where it is stated that for every skew pairing Ψ of C over W^G there is a factor set $\alpha \in Z^2(G, W)$ such that $\Psi(x,y) = \alpha_{x,y}\alpha_{y,x}^{-1}$, for all $x, y \in C$. However, this is false if $\rho^2 \neq 1$ and B has nontrivial elements of order 2. Indeed, if Ψ is the skew pairing of B over W^G given by the factor set α then $\Psi(x, \rho^2) = 1$ for each $x \in C$. To see this we introduce a new set of generators of G, namely $G = \langle c_1, \dots, c_n, c_{n+1}, \rho, \sigma \rangle$ with $c_{n+1} = \rho^2$. Then condition (C3) of Proposition 5.1, for $i = \rho$ and $j = i$ reads $\beta_{(n+1)i} = 1$ which is equivalent to $\Psi(c_i, \rho^2) = 1$ for all $1 \leq i \leq n$. Using this it is easy to give a counterexample to [Pen1, Corollary 1.3].

Before finishing this section we mention two lemmas that will be needed in the next section. The first one is elementary and so the proof has been omitted.

Lemma 5.8. *Let S be the set of skew pairings of B with values in W^G. If $B = B' \times B''$ and $b_1, b_2 \in B'$ and $b_3 \in B''$ then*

$$\max\{\Psi(b_1 \cdot b_3, b_2) : \Psi \in S\} = \max\{\Psi(b_1, b_2) : \Psi \in S\} \cdot \max\{\Psi(b_3, b_2) : \Psi \in S\}.$$

Lemma 5.9. *Let $\widehat{B} = B \times \langle g \rangle$ be an abelian group and let $h \in B$. If $k = \gcd\{p^a, |g|\}$ and $t = |hB^k|$ then t is the maximum possible value of $\Psi(h, g)$ as Ψ runs over all skew pairings of $\widehat{B}$ over $\langle \zeta_{p^a} \rangle$.*

Proof. Since k divides p^a, the hypothesis $t = |hB^k|$ implies that there is a group homomorphism $\chi : B \to \langle \zeta_{p^a} \rangle$ such that $\chi(B^k) = 1$ and $\chi(h)$ has order t. Let $\Psi : \widehat{B} \times \widehat{B} \to \langle \zeta_{p^a} \rangle$ be given by $\Psi(xg^i, yg^j) = \chi(x^j y^{-i}) = \chi(x)^i \chi(y)^{-j}$, for $x, y \in B$. If $g^i = g^{i'}$, then $i \equiv i' \mod |g|$ and hence $i \equiv i' \mod k$. Therefore, $x^i B^k = x^{i'} B^k$, which implies that $\chi(x)^i = \chi(x)^{i'}$. This shows that Ψ is well defined. Now it is easy to see that Ψ is a skew pairing and $\Psi(h, g) = \chi(h)$ has order t.

Conversely, if Ψ is any skew pairing of $\widehat{B}$ over $\langle \zeta_{p^a} \rangle$ then $\Psi(x, g)^{p^a} = 1$ and $\Psi(x, g)^{|x|} = \Psi(1, g) = 1$ for all $x \in B$. This implies that $\Psi(x^k, g) = \Psi(x, g)^k = 1$ for all $x \in B$, so $\Psi(B^k, g) = 1$. Therefore $\Psi(h, g)^t = \Psi(h^t, g) \in \Psi(B^k, g) = 1$, so the order of $\Psi(h, g)$ divides t. □

5.2 Local index computations

In this section K denotes an abelian number field, p a prime, and r an odd prime. Our goal is to find a global formula for $\beta(r) = \beta_p(r)$, the maximum nonnegative integer for which $p^{\beta(r)}$ is the r-local index of a Schur algebra over K.

We are going to abuse the notation and denote by K_r the completion of K at a (any) prime of K dividing r. If E/K is a finite Galois extension, one may assume that the prime of E dividing r, used to compute E_r, divides the prime of K over r, used to compute K_r. Since E/K is a finite Galois extension, $e(E/K, r)$, $f(E/K, r)$ and $m_r(A)$ do not depend on the selection of the prime of K dividing r (Theorem 1.108). Because $|S(K_r)|$ divides $r - 1$ (Theorem 1.110), if either $\zeta_p \notin K$ or $r \not\equiv 1 \mod p$ then $\beta(r) = 0$ (see Theorem 1.108 and Theorem 1.109). So, to avoid trivialities, we assume that $\zeta_p \in K$ and $r \equiv 1 \mod p$.

Suppose $K \subseteq F = \mathbb{Q}(\zeta_n)$ for some positive integer n and let $n = r^{v_r(n)} n'$. Then $\mathrm{Gal}(F/\mathbb{Q})$ contains a *canonical Frobenius automorphism at r*, which is defined by $\psi_r(\zeta_{r^{v_r(n)}}) = \zeta_{r^{v_r(n)}}$ and $\psi_r(\zeta_{n'}) = \zeta_{n'}^r$. We can then define the *canonical Frobenius automorphism at r in* $\mathrm{Gal}(F/K)$ as $\phi_r = \psi_r^{f(F/K,r)}$. On the other hand, the *inertia subgroup at r in* $\mathrm{Gal}(F/K)$ is by definition the subgroup of $\mathrm{Gal}(F/K)$ that acts as $\mathrm{Gal}(F_r/K_r(\zeta_{n'}))$ in the completion at r. We use the following notation.

Notation 5.10. *First we define some positive integers:*
$m =$ *minimum even positive integer with* $K \subseteq \mathbb{Q}(\zeta_m)$,
$a =$ *minimum positive integer with* $\zeta_{p^a} \in K$,
$s = v_p(m)$ *and*

$$b = \begin{cases} s, & \text{if } p \text{ is odd or } \zeta_4 \in K, \\ s + v_p([K \cap \mathbb{Q}(\zeta_{p^s}) : \mathbb{Q}]) + 2, & \text{if } \mathrm{Gal}(K(\zeta_{p^{2a+s}})/K) \text{ is not cyclic, and} \\ s+1, & \text{otherwise.} \end{cases}$$

We also define

$$L = \mathbb{Q}(\zeta_m), \quad \zeta = \zeta_{p^{a+b}}, \quad W = \langle \zeta \rangle, \quad F = L(\zeta),$$

$$G = \mathrm{Gal}(F/K), \quad C = \mathrm{Gal}(F/K(\zeta)), \quad \text{and} \quad D = \mathrm{Gal}(F/K(\zeta + \zeta^{-1})).$$

Since $\zeta_p \in K$, *the automorphism* $\Upsilon : G \to \mathrm{Aut}(W)$ *induced by the Galois action satisfies the conditions of the previous section and the notation is consistent. As in that section we fix elements* ρ *and* σ *in* G *and a subgroup* $B = \langle c_1 \rangle \times \cdots \times \langle c_n \rangle$ *of* C *such that* $D = B \times \langle \rho \rangle$, $C = B \times \langle \rho^2 \rangle$ *and* $G/C = \langle \rho C \rangle \times \langle \sigma C \rangle$. *Furthermore,* $\sigma(\zeta) = \zeta^c$ *for some integer* c *chosen according to (5.4). Notice that by the choice of* b, $G \neq B$.

We also fix an odd prime r *and set*

$$e = e(K(\zeta_r)/K, r), \quad f = f(K/\mathbb{Q}, r) \quad \text{and} \quad \nu(r) = \max\{0, a + v_p(e) - v_p(r^f - 1)\}.$$

Let $\phi \in G$ *be the canonical Frobenius automorphism at* r *in* G, *and write*

$$\phi = \rho^{j'} \sigma^j \eta, \quad \text{with } \eta \in B, \quad 0 \leq j' < |\rho| \quad \text{and} \quad 0 \leq j < |\sigma C|.$$

For any odd prime q *not dividing* m, *let* $G_q = \mathrm{Gal}(F(\zeta_q)/K)$, $C_q = \mathrm{Gal}(F(\zeta_q)/K(\zeta))$ *(note that by this notation we do not mean the* q*-part of groups* G *or* C*) and let* c_0 *denote a generator of* $\mathrm{Gal}(F(\zeta_q)/F)$. *Finally we fix*

$\theta = \theta_q$, *a generator of the inertia group of* r *in* G_q *and*
$\phi_q = c_0^{s_0} \phi = c_0^{s_0} \eta \rho^{j'} \sigma^j = \eta_q \rho^{j'} \sigma^j$, *the canonical Frobenius automorphism at* r *in* G_q.

Observe that we are considering G as a subgroup of G_q by identifying G with the group $\mathrm{Gal}(F(\zeta_q)/K(\zeta_q))$. Again the Galois action induces a homomorphism $\Upsilon_q : G_q \to \mathrm{Aut}(W)$ and $W^{G_q} = \langle \zeta_{p^a} \rangle$. So this action satisfies the conditions of the previous section and we adapt the notation by setting

$$B_q = \langle c_0 \rangle \times B, \quad C_q = \mathrm{Gal}(F(\zeta_q)/K(\zeta)) = \mathrm{Ker}(\Upsilon_q), \quad D_q = \mathrm{Gal}(F(\zeta_q)/K(\zeta + \zeta^{-1})).$$

Notice that $C_q = \langle c_0 \rangle \times C = B_q \times \langle \rho^2 \rangle$ and $D_q = D \times \langle c_0 \rangle$. Hence $G/C \simeq G_q/C_q$.

If Ψ is a skew pairing of B over W^G then Ψ has a unique extension to a skew pairing Ψ of C over W^G which satisfies $\Psi(B,\rho^2)=\Psi(\rho^2,B)=1$. So we are going to apply skew pairings of B to pairs of elements in C under the assumption that we are using this extension.

Since $p\neq r$, $\theta\in C_q$. Moreover, if $r=q$ then θ is a generator of $\mathrm{Gal}(F(\zeta_r)/F)$ and otherwise $\theta\in C$. Notice also that if G/C is non-cyclic then $p^a=2$ and $K\cap\mathbb{Q}(\zeta_{2^s})=\mathbb{Q}(\zeta_{2^d}+\zeta_{2^d}^{-1})$, where $d=v_p(c-1)$, and so $b=s+d$.

It follows from results of Janusz [Jan3, Proposition 3.2] and Pendergrass [Pen2, Theorem 1] that $p^{\beta(r)}$ always occurs as the r-local index of a cyclotomic algebra of the form $(L(\zeta_q)/L,\alpha)$, where q is either 4 or a prime not dividing m and α takes values in $W(L(\zeta_q))_p$, with the possibility of $q=4$ occurring only in the case when $p^s=2$. By inflating the factor set α to $F(\zeta_q)$ (which will be equal to F when $p^s=2$), we have that $p^{\beta(r)}=m_r(A)$, where

$$\begin{aligned}&A=(F(\zeta_q)/K,\alpha)\text{ (we also write }\alpha\text{ for the inflation)},\\&q\text{ is an odd prime not dividing }m,\text{ and}\\&\alpha\text{ takes values in }\langle\zeta_{p^4}\rangle\text{ if }p^s=2\text{ and in }\langle\zeta_{p^s}\rangle\text{ otherwise.}\end{aligned}\tag{5.8}$$

So it suffices to find a formula for the maximum r-local index of a Schur algebra over K of this form.

Write $A=\bigoplus_{g\in G_q}F(\zeta_q)u_g$, with $u_g^{-1}xu_g=g(x)$ and $u_gu_h=\alpha_{g,h}u_{gh}$, for each $x\in F(\zeta_q)$ and $g,h\in G_q$. After a diagonal change of basis one may assume that if $g=c_0^{s_0}c_1^{s_1}\dots c_n^{s_n}\rho^{s_\rho}\sigma^{s_\sigma}$ with $0\leq s_i<q_i=|c_i|$, $0\leq s_\rho<|\rho|$ and $0\leq s_\sigma<q_\sigma=|\sigma C|$ then $u_g=u_{c_0}^{s_0}u_{c_1}^{s_1}\dots u_{c_n}^{s_n}u_\rho^{s_\rho}u_\sigma^{s_\sigma}$.

It is well known (see [Yam] and [Jan3, Theorem 1]) that

$$m_r(A)=|\xi|,\quad\text{where}\quad\xi=\xi_\alpha=\left(\frac{\alpha_{\theta,\phi_q}}{\alpha_{\phi_q,\theta}}\right)^{r^{v_r(e)}}u_\theta^{r^{v_r(e)}(r^f-1)}.\tag{5.9}$$

This can be slightly simplified as follows. If $r|e$ then $\langle\theta\rangle$ has an element θ^k of order r. Since θ fixes every root of unity of order coprime with r, necessarily r^2 divides m and the fixed field of θ^k in L is $\mathbb{Q}(\zeta_{m/r})$. Then $K\subseteq\mathbb{Q}(\zeta_{m/r})$, contradicting the minimality of m. Thus r does not divide e and so

$$\xi=\frac{\alpha_{\theta,\phi_q}}{\alpha_{\phi_q,\theta}}u_\theta^{r^f-1}=\frac{\alpha_{\theta,\phi_q}}{\alpha_{\phi_q,\theta}}\gamma_\theta^{\frac{r^f-1}{e}}=[u_\theta,u_{\phi_q}]\gamma_\theta^{\frac{r^f-1}{e}},\ \text{where }\gamma_\theta=u_\theta^e.\tag{5.10}$$

With our choice of the $\{u_g:g\in G_q\}$, we have

$$[u_\theta,u_{\phi_q}]=[u_\theta,u_{\eta_q}u_\rho^{j'}u_\sigma^{j}]=\Psi(\theta,\eta_q)[u_\theta,u_\rho^{j'}u_\sigma^{j}],$$

where $\Psi=\Psi_\alpha$ is the skew pairing associated to α. Therefore,

$$\xi=\xi_0\Psi(\theta,\eta_q)\quad\text{ with }\quad\xi_0=\xi_{0,\alpha}=[u_\theta,u_\rho^{j'}u_\sigma^{j}]\gamma_\theta^{\frac{r^f-1}{e}}.$$

Let (β, γ) be the data associated to the factor set α (relative to the set of generators $c_1, \ldots, c_n, \rho, \sigma$).

Lemma 5.11. *Let $A = (F(\zeta_q)/K, \alpha)$ be a cyclotomic algebra satisfying the conditions of (5.8) and use the above notation. Let $\theta = c_0^{s_0} c_1^{s_1} \cdots c_n^{s_n} \rho^{2s_{n+1}}$, with $0 \leq s_i < q_i$ for $0 \leq i \leq n$, and $0 \leq s_{n+1} \leq |\rho^2|$.*

(1) *If G/C is cyclic then $\xi_0^{p^{\nu(r)}} = 1$.*

(2) *Assume that G/C is non cyclic and let $\mu_i = \beta_{i\rho}^{\frac{1-c}{2}} \beta_{i\sigma}^{-1}$. Then $\mu_i = \pm 1$ and $\xi_0^{p^{\nu(r)}} = \prod_{i=0}^{n} \mu_i^{2^{\nu(r)}(j+j')s_i}$.*

Proof. For the sake of regularity we write $c_{n+1} = \rho^2$. Since $e = |\theta|$, we have that q_i divides es_i for each i. Furthermore, $v_p(e)$ is the maximum of the $v_p\left(\frac{q_i}{\gcd(q_i, s_i)}\right)$ for $i = 1, \ldots, n$. Then

$$v_p(e) - v_p(r^f - 1) = \max\left\{ v_p\left(\frac{q_i}{\gcd(q_i, s_i)(r^f - 1)}\right), i = 1, \ldots, n \right\}.$$

Hence

$$\begin{array}{rcl} \nu(r) & = & \max\{0, v_p(e) + a - v_p(r^f - 1)\} \\ & = & \min\left\{ x \geq 0 : p^a \text{ divides } p^x \cdot \frac{s_i(r^f-1)}{q_i}, \text{ for each } i = 1, \ldots, n \right\}. \end{array} \tag{5.11}$$

Now we compute γ_θ in terms of the previous expression of θ. Set $v = u_{c_{n+1}}^{s_{n+1}}$ and $y = u_{c_0}^{s_0} u_{c_1}^{s_1} \cdots u_{c_n}^{s_n}$. Then

$$u_\theta = yv = \gamma vy, \quad \text{with} \quad \gamma = \Psi(c_{n+1}^{s_{n+1}}, c_0^{s_0} c_1^{s_1} \ldots, c_n^{s_n}).$$

Thus $\gamma^e = \Psi(c_{n+1}^{es_{n+1}}, c_0^{s_0} c_1^{s_1} \ldots, c_n^{s_n}) = 1$. Using that $[y, \gamma] = 1$, one easily proves by induction on m that

$$(yv)^m = \gamma^{\binom{m}{2}} y^m v^m.$$

Hence

$$(yv)^e = \gamma^{\binom{e}{2}} y^e v^e = \gamma^{\binom{e}{2}} y^e u_{c_{n+1}}^{es_{n+1}} = \gamma^{\binom{e}{2}} y^e \gamma_\rho^{\frac{es_{n+1}}{q_{n+1}}},$$

and $\gamma^{\binom{e}{2}} = \pm 1$. (If p or e is odd then necessarily $\gamma^{\binom{e}{2}} = 1$.) Now an easy induction argument shows

$$\gamma_\theta = \mu \gamma_0^{\frac{es_0}{q_0}} \gamma_1^{\frac{es_1}{q_1}} \cdots \gamma_n^{\frac{es_n}{q_n}} \gamma_\rho^{\frac{es_{n+1}}{q_{n+1}}}, \quad \text{for some } \mu = \pm 1.$$

Note that $\nu(r) + v_p(r^f - 1) - v_p(e) \geq a \geq 1$, by (5.11). Then $\mu^{p^{\nu(r)} \frac{r^f-1}{e}} = \gamma_\rho^{p^{\nu(r)} \frac{r^f-1}{e}} = 1$, because both μ and γ_ρ are ± 1, and they are 1 if p is odd (see (C3.e) and (C3.f)). Thus

$$\gamma_\theta^{p^{\nu(r)} \frac{r^f-1}{e}} = \prod_{i=0}^{n} \gamma_i^{p^{\nu(r)} \frac{(r^f-1)s_i}{q_i}} \tag{5.12}$$

(1) Assume that G/C is cyclic. We have that $\rho = 1$ and $v_p(c-1) = a$. Note that the β's and γ's are p^b-th roots of unity by (5.8).

Let Y be an integer satisfying $Y\frac{c-1}{p^a} \equiv 1 \mod p^b$. Since $\phi_q = \sigma^j \eta_q$ with $\eta_q \in C_q$, we have $r^f \equiv c^j \mod p^{a+b}$ and so $Y\frac{r^f-1}{p^a} = Y\frac{c-1}{p^a}\frac{c^j-1}{c-1} \equiv V(j) \mod p^b$. Then $\beta_{i\sigma}^{Y\frac{r^f-1}{p^a}} = \beta_{i\sigma}^{V(j)}$.

Using that p^a divides $p^{\nu(r)}\frac{s_i(r^f-1)}{q_i}$ (see (5.11)) and $Y\frac{(c-1)}{p^a} \equiv 1 \mod p^b$ we obtain

$$\gamma_i^{p^{\nu(r)}\frac{s_i(r^f-1)}{q_i}} = \left(\gamma_i^{c-1}\right)^{Y\frac{p^{\nu(r)}s_i(r^f-1)}{p^a q_i}}.$$

Combining this with (C3.b) we have

$$\begin{aligned}
[u_{c_i}^{s_i}, u_\sigma^j]^{p^{\nu(r)}} \gamma_i^{p^{\nu(r)}\frac{s_i(r^f-1)}{q_i}} &= [u_{c_i}, u_\sigma]^{s_i V(j) p^{\nu(r)}} \left(\gamma_i^{c-1}\right)^{Y\frac{p^{\nu(r)}s_i(r^f-1)}{p^a q_i}} \\
&= [u_{c_i}, u_\sigma]^{s_i V(j) p^{\nu(r)}} \beta_{i\sigma}^{Y\frac{p^{\nu(r)}s_i(r^f-1)}{p^a}} \\
&= ([u_{c_i}, u_\sigma]\beta_{i\sigma})^{p^{\nu(r)}s_i V(j)} = 1,
\end{aligned} \tag{5.13}$$

because $\beta_{i\sigma} = [u_\sigma, u_{c_i}] = [u_{c_i}, u_\sigma]^{-1}$. Using (5.12) and (5.13) we have

$$\xi_0^{p^{\nu(r)}} = [u_\theta, u_\sigma^j]^{p^{\nu(r)}} \gamma_\theta^{p^{\nu(r)}\frac{r^f-1}{e}} = \prod_{i=0}^{n} [u_{c_i}^{s_i}, u_\sigma^j]^{p^{\nu(r)}} \gamma_i^{p^{\nu(r)}\frac{s_i(r^f-1)}{q_i}} = 1$$

and the lemma is proved in this case.

(2) Assume now that G/C is non-cyclic. Then $p^a = 2$ and if $d = v_2(c-1)$ then $d \geq 2$ and $b = s + d$. The data for α lie in $\langle\zeta_{2^{s+1}}\rangle \subseteq \langle\zeta_{2^b}\rangle \subseteq \langle\zeta_{2^{1+s+d}}\rangle = W(F)_2$. (C2.b) implies $\mu_i = \pm 1$ and using (C3.b) and (C3.f) one has $\gamma_i^{c+1} = \beta_{i\sigma}^{q_i}\beta_{i\rho}^{-q_i}$. Let X and Y be integers satisfying $X\frac{c-1}{2^d} \equiv Y\frac{c+1}{2} \equiv 1 \mod 2^{1+s+d}$ and set $Z = Y\frac{r^f-1}{2}$.

Recall that $2^a = 2$ divides $2^{\nu(r)}\frac{s_i(r^f-1)}{q_i}$, by (5.11). Therefore,

$$\gamma_i^{2^{\nu(r)}\frac{s_i(r^f-1)}{q_i}} = \left(\gamma_i^{c+1}\right)^{Y\frac{2^{\nu(r)}s_i(r^f-1)}{2q_i}} = \left(\beta_{i\sigma}^{s_i}\beta_{i\rho}^{-s_i}\right)^{2^{\nu(r)}Z}. \tag{5.14}$$

Let $j'' \equiv j' \mod 2$ with $j'' \in \{0,1\}$. Then $\Upsilon(\rho^{j''}) = \Upsilon(\rho^{j'})$ and $N_\rho^{j'}(w) = w^{j''}$. Therefore,

$$\begin{aligned}
[u_\theta, u_\rho^{j'}u_\sigma^j] &= [u_\theta, u_\rho^{j'}]u_\rho^{j'}[u_\theta, u_\sigma^j]u_\rho^{-j'} = \textstyle\prod_{i=0}^n (\beta_{i\rho}^{-s_i})^{j''}(\beta_{i\sigma}^{-s_i})^{V(j)(-1)^{j''}} \\
&= \textstyle\prod_{i=0}^n (\beta_{i\rho}^{-s_i})^{j''}(\beta_{i\sigma}^{-s_i})^{X\frac{c-1}{2^d}V(j)(-1)^{j''}} \\
&= \textstyle\prod_{i=0}^n (\beta_{i\rho}^{-s_i})^{j''}(\beta_{i\sigma}^{-s_i})^{X\frac{c^j-1}{2^d}(-1)^{j''}}.
\end{aligned} \tag{5.15}$$

Using (5.12), (5.14) and (5.15) we obtain

$$\begin{aligned}
\xi_0^{2^{\nu(r)}} &= [u_\theta, u_\rho^{j'}u_\sigma^j]^{2^{\nu(r)}} \gamma_\theta^{2^{\nu(r)}\frac{r^f-1}{e}} \\
&= \left(\textstyle\prod_{i=0}^n \beta_{i\rho}^{-s_i}\right)^{2^{\nu(r)}(Z+j'')} \left(\textstyle\prod_{i=0}^n \beta_{i\sigma}^{s_i}\right)^{2^{\nu(r)}\left(Z - X\frac{c^j-1}{2^d}(-1)^{j''}\right)}.
\end{aligned} \tag{5.16}$$

We claim that $Z + j'' \equiv 0 \mod 2^{d-1}$. On one hand $Y \equiv 1 \mod 2^{d-1}$. On the other hand, $\phi_q = \rho^{j'}\sigma^j\eta_q$, with $\eta_q \in C_q$ and so $r^f \equiv (-1)^{j'}c^j \mod 2^{1+s+d}$. Hence $r^f \equiv (-1)^{j'} = (-1)^{j''} \mod 2^d$ and therefore $Z + j'' = Y\frac{r^f-1}{2} + j'' \equiv \frac{(-1)^{j''}-1}{2} + j'' \mod 2^{d-1}$. Considering the two possible values of $j'' \in \{0, 1\}$ we have $\frac{(-1)^{j''}-1}{2} + j'' = 0$ and the claim follows.

From $d = v_2(c-1)$ one has $c \equiv 1 + 2^{d-1} \mod 2^d$ and hence $Y \equiv 1 + 2^{d-1} \mod 2^d$ and $r^f \equiv (-1)^{j'}c^j \equiv (-1)^{j'}(1 + j2^d) \mod 2^{1+s+d}$. Then

$$\begin{aligned}\frac{Z+j''}{2^{d-1}} &= \frac{Y(r^f-1)+2j''}{2^d} \equiv \frac{Y((-1)^{j''}(1+j2^d)-1)+2j''}{2^d} = \frac{Y(\frac{(-1)^{j''}-1}{2}+(-1)^{j''}j2^{d-1})+j''}{2^{d-1}} \\ &\equiv \frac{(1+2^{d-1})(-j''+(-1)^{j''}j2^{d-1})+j''}{2^{d-1}} = \frac{-j''-j''2^{d-1}+(-1)^{j''}j2^{d-1}+(-1)^{j''}j2^{2(d-1)}+j''}{2^{d-1}} \\ &\equiv -j'' + (-1)^{j''}j \equiv j + j'' \equiv j + j' \mod 2.\end{aligned}$$

Using this, the equality $\beta_{i\rho}^{\frac{1-c}{2}} = \mu_i\beta_{i\sigma}$ and the fact that $\mu_i = \pm 1$ we obtain

$$\beta_{i\rho}^{-(Z+j'')} = \beta_{i\rho}^{-X\frac{c-1}{2^d}(Z+j'')} = \beta_{i\rho}^{-X\frac{c-1}{2}\frac{Z+j''}{2^{d-1}}} = \mu_i^{X\frac{Z+j''}{2^{d-1}}}\beta_{i\sigma}^{X\frac{Z+j''}{2^{d-1}}} = \mu_i^{j+j'}\beta_{i\sigma}^{X\frac{Z+j''}{2^{d-1}}}.$$

Combining this with (5.16) we have

$$\begin{aligned}\xi_0^{2^{\nu(r)}} &= \prod_{i=0}^n \mu_i^{2^{\nu(r)}(j+j')s_i} \prod_{i=0}^n (\beta_{i\sigma}^{s_i})^{2^{\nu(r)}\left[Z - X\frac{c^j-1}{2^d}(-1)^{j''} + \frac{X(Z+j'')}{2^{d-1}}\right]} \\ &= \prod_{i=0}^n \mu_i^{2^{\nu(r)}(j+j')s_i} \prod_{i=0}^n (\beta_{i\sigma}^{s_i})^{2^{\nu(r)}\left[\frac{2^dZ + X(c^j-1)(-1)^{j''} + 2X(Z+j'')}{2^d}\right]}.\end{aligned}$$

To finish the proof it is enough to show that the exponent of each $\beta_{i\sigma}$ in the previous expression is a multiple of 2^{1+s}. Indeed, $2^d \equiv X(c-1) \mod 2^{1+s+d}$ and so

$$\begin{aligned}&2^dZ + X(c^j-1)(-1)^{j''} + 2X(Z+j'') \\ &\equiv ZX(c-1) - X(c^j-1)(-1)^{j''} + 2X(Z+j'') \\ &= X(Y\tfrac{r^f-1}{2}(c+1) + (c^j-1)(-1)^{j''} + 2j'') \\ &= X((r^f-1)Y\tfrac{c+1}{2} - c^j(-1)^{j''} + (-1)^{j''} + 2j'') \\ &\equiv X(r^f - 1 - c^j(-1)^{j''} + 1) \equiv 0 \mod 2^{1+s+d}\end{aligned}$$

as required. This finishes the proof of the lemma in Case 2. □

We need the following Proposition from [Jan3].

Proposition 5.12. *For every odd prime $q \neq r$ not dividing m let $d(q) = \min\{a, v_p(q-1)\}$. Then*

(1) $|c_0^{k_q}C/C^{p^{d(q)}}| \leq |\theta_q^fC/C^{p^a}|$, *and*

(2) *the equality holds if $q \equiv 1 \mod p^a$ and r is not congruent with a p-th power modulo q. There are infinitely many primes q satisfying these conditions.*

Proof. See Proposition 4.1 and Lemma 4.2 of [Jan3]. □

We are ready to prove the main result of the chapter.

Theorem 5.13. *Let K be an abelian number field, p a prime, r an odd prime and let $p^{\beta_p(r)}$ be the maximum r-local index of a Schur algebra over K of index a power of p. If either $\zeta_p \notin K$ or $r \not\equiv 1 \mod p$ then $\beta_p(r) = 0$. Assume otherwise that $\zeta_p \in K$ and $r \equiv 1 \mod p$, and use Notation 5.10 including the decomposition $\phi = \eta\rho^{j'}\sigma^j$ with $\eta \in B$.*

(1) *Assume that r does not divide m.*

   (a) *If G/C is non-cyclic and $j \not\equiv j' \mod 2$ then $\beta_p(r) = 1$.*

   (b) *Otherwise $\beta_p(r) = \max\{\nu(r), v_p(|\eta B^{p^{d(r)}}|)\}$, where $d(r) = \min\{a, v_p(r-1)\}$.*

(2) *Assume that r divides m and let q_0 be an odd prime not dividing m such that $q_0 \equiv 1 \mod p^a$ and r is not a p-th power modulo q_0. Let $\theta = \theta_{q_0}$ be a generator of the inertia group of G_{q_0} at r.*

   (a) *If G/C is non-cyclic, $j \not\equiv j' \mod 2$ and θ is not a square in D then $\beta_p(r) = 1$.*

   (b) *Otherwise $\beta_p(r) = \max\{\nu(r), h, v_p(|\theta^f C^{p^a}|)\}$, where $h = \max_\Psi\{v_p(|\Psi(\theta, \eta)|)\}$ as Ψ runs over all skew pairings of B over $\langle\zeta_{p^a}\rangle$.*

Proof. For simplicity we write $\beta(r) = \beta_p(r)$. We already explained why if either $\zeta_p \notin K$ or $r \not\equiv 1 \mod p$ then $\beta_p(r) = 0$. So in the remainder of the proof we assume that $\zeta_p \in K$ and $r \equiv 1 \mod p$, and so K, p, and r satisfy the condition mentioned at the beginning of the section. It was also pointed out earlier in this section that $p^{\beta(r)}$ is the r-local index of a crossed product algebra A of the form $A = (F(\zeta_q)/K, \alpha)$ with q an odd prime not dividing m and α taking values in $\langle\zeta_{p^s}\rangle$ or in $\langle\zeta_4\rangle$. Moreover, since $p^{\nu(r)}$ is the r-local index of the cyclic Schur algebra $(K(\zeta_r)/K, c_0, \zeta_{p^a})$ [Jan3], we always have $\nu(r) \leq \beta(r)$.

In case 1 one may assume that $q = r$, because $(F(\zeta_q)/K, \alpha)$ has r-local index 1 for every $q \neq r$. Since $\mathrm{Gal}(F(\zeta_r)/F)$ is the inertia group at r in G_r, in this case one may assume that $\theta = \theta_r = c_0$. On the contrary, in case 2, $q \neq r$, and $\theta = c_1^{s_1} \dots c_n^{s_n}\rho^{2s_{n+1}}$, for some $s_1, \dots, s_{n+1}$.

In cases (1.a) and (2.a), G/C is non-cyclic and hence $p^a = 2$. Then $\beta(r) \leq 1$, by the Benard-Schacher Theorem, and hence if $\nu(r) = 1$ then $\beta(r) = 1$. So assume that $\nu(r) = 0$. Furthermore, in case (2.a), s_i is odd for some $i \leq n$, because $\theta \notin D^2$. Now

we can use Corollary 5.5 to produce a cyclotomic algebra $A' = (F(\zeta_q)/K, \alpha')$ so that $\xi_\alpha = -\xi_{\alpha'}$. Indeed, there is such an algebra such that all the data associated to α are equal to the data for A, except for $\beta_{0\sigma}$, in case (1.a), and $\beta_{k\sigma}$, case (2.a). Using Lemma 5.11 and the assumptions $\nu(r) = 0$ and $j \not\equiv j' \mod 2$, one has $\xi_{0,\alpha} = -\xi_{0,\alpha'}$ and $\Psi_\alpha = \Psi_{\alpha'}$. Thus $\xi_\alpha = -\xi_{\alpha'}$, as claimed. This shows that $\beta(r) = 1$ in cases (1.a) and (2.a).

In case (1.b), $\xi = \xi_0\Psi(c_0, \eta)$. By Lemma 5.11, ξ_0 has order dividing $p^{\nu(r)}$ in this case and, by Lemma 5.9, $\max\{|\Psi(\theta, \eta)| : \Psi \in S\} = |\eta B^{p^{d(r)}}|$, where S is the set of skew pairings of B_r with values in $\langle p^a \rangle$. Using this and $\nu(r) \leq \beta(r)$ one deduces that $\beta(r) = \max\{\nu(r), v_p(|\eta B^{p^{d(r)}}|)\}$.

The formula for case (2.b) is obtained in a similar way using the equality $\xi = \xi_0\Psi(\theta, \eta)\Psi(\theta, c_0^{s_0})$ and Lemmas 5.8 and 5.9. □

Remark 5.14. In the previous proof we have cited [Jan3] to show that there is a cyclic Schur algebra $(K(\zeta_r)/K, c_0, \zeta_{p^a})$ of r-local index $p^{\nu(r)}$. In fact, $p^{\nu(r)}$ is the maximum index of a cyclic cyclotomic algebra over K in $S(K)_p$. A proof of this result will be given in the next chapter in Theorem 6.9.

5.3 Examples and applications

The main motivation for Theorem 5.13 is the study the gap between the Schur group of an abelian number field K and its subgroup generated by classes containing cyclic cyclotomic algebras over K, a problem which reduces to studying the gaps between the integers $\nu_p(r)$ and $\beta_p(r)$ for all finite primes p and odd primes r (for details, see next chapter). What Theorem 5.13 really allows one to do is to compute $\beta_p(r)$ in terms of the number of p-th power roots of unity in K and the embedding of $\mathrm{Gal}(F/K)$ in $\mathrm{Gal}(F/\mathbb{Q})$. In this section, we will provide some examples of abelian number fields K to illustrate the computations involved in the various cases of Theorem 5.13. We use the notation of the previous sections in all of these examples.

Example 5.15. Let $K = \mathbb{Q}(\zeta_m)$, with m minimal. Let p be a prime for which $\zeta_p \in K$, and let r be an odd prime which is $\equiv 1 \mod p$. Let a be the maximal integer for which $\zeta_{p^a} \in K$, and let $s = v_p(m)$. If we are not in the case when $b = s$, then $p = 2$, $s = 0$, and $K(\zeta_{p^{2a+s}}) = K(\zeta_4)$, so we will be in the case where $b = s + 1 = 1$. Since $K = L$, we have that $F = K(\zeta_{p^{a+b}})$, so C is trivial. Also, $G = \mathrm{Gal}(K(\zeta_{p^{a+b}})/K)$ will be cyclic for either case of b. Therefore, either case (1b) or (2b) of Theorem 5.13 applies, and it is immediate from $C = B = 1$ that $\beta_p(r) = \nu_p(r)$ for each choice of p and r.

Example 5.16. Let p and r be odd primes with $v_p(r-1) = 2$. Let K be the extension of $\mathbb{Q}(\zeta_p)$ with index p in $L = \mathbb{Q}(\zeta_{pr})$, and consider $\beta_p(r)$. We have $a = s = b = 1$, and $F = \mathbb{Q}(\zeta_{p^2r})$. We have that $G = \langle\theta\rangle \times C$ is elementary abelian of order p^2, so we are in case (2b) of Theorem 5.13. Since $\mathrm{Gal}(F/\mathbb{Q})$ has an element ψ such that ψ^p generates C, letting q_0 and θ be as in Theorem 5.13(2), we find that $v_p(|\psi G|) = 1$. It follows that $p^f = p$, so $\nu_p(r) = 0$ and $v_p(|\theta^f C^{p^a}|) = 1$. Since ϕ generates C, we have that $\phi = \eta$ and so $h = 1$ by Lemma 5.9. So $\beta_p(r) = 1$ in this case.

Example 5.17. Let q be an odd prime greater than 5, and let $K = \mathbb{Q}(\zeta_q, \sqrt{2})$. Let $p = 2$, and let r be any prime for which $r^2 \equiv 1 \mod q$ and $r \equiv 5 \mod 2^6$. In computing $\beta_2(r)$, one sees that $a = 1$ and $L = \mathbb{Q}(\zeta_{8q})$, so $s = 3$. Since $\mathrm{Gal}(K(\zeta_{2^5})/K)$ is not cyclic, we set $b = 5 + v_2([\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]) = 6$, so $F = \mathbb{Q}(\zeta_{64q})$. Since $\mathbb{Q}(\zeta_q) \subset K$, we have $C = \mathrm{Gal}(F/K(\zeta_{64})) = 1$. For our generators of $\mathrm{Gal}(F/K)$, we may choose ρ, σ such that $\rho(\zeta_q) = \zeta_q$, $\rho(\zeta_{64}) = \zeta_{64}^{-1}$, $\sigma(\zeta_q) = \zeta_q$, and $\sigma(\zeta_{64}) = \zeta_{64}^9$. By our choice of r, we have that $\psi_r \notin G$, but $5^2 \equiv 9^3 \mod 64$ implies that $\psi_r^2 = \sigma^3$. This means that we are in case (1a) of Theorem 5.13 with $\nu_p(r) = 0$ and $j \not\equiv j' \mod 2$, so $\beta_2(r) = 1$.

Example 5.18. Let r be an odd prime for which $r \equiv 5 \mod 64$. Let K' be the unique subfield of index 2 in $\mathbb{Q}(\zeta_r)$, and let $K = K'(\sqrt{2})$. Consider $\beta_2(r)$ for the field K. As in the previous example, we have $L = \mathbb{Q}(\zeta_{8r})$ and $F = \mathbb{Q}(\zeta_{64r})$. As in the previous example, choose $\rho, \sigma \in G$ satisfying $\rho(\zeta_{64}) = \zeta_{64}^{-1}$ and $\sigma(\zeta_{64}) = \zeta_{64}^9$. Using Proposition 5.12, choose an odd prime q_0 for which r in not a square modulo q_0. If ψ_r is the Frobenius automorphism in $\mathrm{Gal}(F(\zeta_{q_0})/\mathbb{Q})$, then $\psi_r \notin G_{q_0}$, and $\phi_r = \psi_r^2$ sends ζ_{64} to $\zeta_{64}^{5^2} = \zeta_{64}^{9^3}$. Therefore, $\phi_r = \sigma^3\eta_0$, where $\eta_{q_0} \in C_{q_0}$ fixes ζ_{64r}. Since $\zeta_r \notin K$, $\theta = \theta_{q_0}$ generates a direct factor of G_{q_0} and so it cannot be a square in D. It follows that the conditions of case (2a) of Theorem 5.13 hold, and so we can conclude $\beta_2(r) = 1$.

Example 5.19. Let p be an odd prime and let q and r be primes for which $v_p(q-1) = v_p(r-1) = 2$, $v_q(r^p - 1) = 0$, and $v_q(r^{p^2} - 1) = 1$. The existence of such primes q and r for each odd prime p is a consequence of Dirichlet's Theorem on primes in arithmetic progression. Indeed, given p and q primes with $v_p(q-1) = 2$, there is an integer k, coprime to q such that the order of k modulo q^2 is p^2. Choose a prime r for which $r \equiv k+q \mod q^2$ and $r \equiv 1+p^2 \mod p^3$. Then p, q and r satisfy the given conditions.

Let K be the compositum of K' and K'', the unique subextensions of index p in $\mathbb{Q}(\zeta_{p^2q})/\mathbb{Q}(\zeta_{p^2})$ and $\mathbb{Q}(\zeta_{p^2r})/\mathbb{Q}(\zeta_{p^2})$ respectively. Then $m = p^2rq$, $a = 2$ and $L = \mathbb{Q}(\zeta_m) = K(\zeta_q) \otimes_K K(\zeta_r)$. Therefore, $F = \mathbb{Q}(\zeta_{p^4qr})$, and $G = \mathrm{Gal}(F/K(\zeta_{qr})) \times \mathrm{Gal}(F/K(\zeta_{p^4q})) \times \mathrm{Gal}(F/K(\zeta_{p^4r}))$. We may choose σ so that $\langle\sigma\rangle = \mathrm{Gal}(F/K(\zeta_{qr})) \cong G/C$ has order p^2. The inertia subgroup of r in G is $\mathrm{Gal}(F/K(\zeta_{p^4q}))$, which is generated by an element θ of order p.

Since $K = K' \otimes_{\mathbb{Q}(\zeta_{p^2})} K''$ and $K''/\mathbb{Q}(\zeta_{p^2})$ is totally ramified at r, we have that K'_r is the maximal unramified extension of $K_r/\mathbb{Q}_r$. It follows from $v_q(r^{p^2}-1) = 1$ and $v_q(r^p - 1) = 0$ that $[\mathbb{Q}_r(\zeta_q) : \mathbb{Q}_r] = p^2$, and so $[K'_r : \mathbb{Q}_r] = p = f(K/\mathbb{Q}, r)$. Therefore $v_p(|W(K_r)|) = v_p(|W(\mathbb{Q}_r)|) + f(r) = v_p(r-1) + 1 = 3$, and so we have $\nu(r) = \max\{0, a + v_p(|\theta|) - v_p(|W(K_r)|)\} = 0$. Since $|C| = p$ and θ has order p, we also see that $\theta^{f(r)}C^{p^2}$ is trivial, so $v_p(|\theta^{f(r)}C^{p^2}|) = 0$.

Let ψ_r be the Frobenius automorphism of r in $\mathrm{Gal}(F/\mathbb{Q})$. Then $\psi_r^p = \sigma^p\eta$, where $\eta \in B$ generates $\mathrm{Gal}(F/K(\zeta_{p^4 r}))$. Since $\langle\theta\rangle \cap \langle\eta\rangle = 1$, it follows from Lemma 5.9 that $h = v_p(|\theta|) = 1$. So case (2b) of Theorem 5.13 applies to show that $\beta_p(r) = h = 1$.

Notes on Chapter 5

The problem of the computation of the Schur group of a number field K heavily depends upon the arithmetic structure of K in a way which sometimes defies the intuition. The interested reader may find an exhaustive and technical account of various results related to this topic in Yamada's book [Yam].

The problem of computing $\beta_p(r)$ makes sense for an arbitrary number field K. As far as we know, this has not been treated in the literature. If F is the maximum cyclotomic subfield of K, then the inclusion $F \to K$ induces a homomorphism $S(F) \to S(K)$. Since every element of $S(F)$ is splitted by a cyclotomic extension of F, the values of $\beta_p(r)$ for F and K might be strongly related.

Chapter 6

Cyclic cyclotomic algebras

In this chapter we study some properties of cyclic cyclotomic algebras. These algebras combine properties of both cyclic and cyclotomic algebras and have the advantage of having a form that allows one to apply specific methods for both types of algebras. Cyclic cyclotomic algebras arise naturally as simple components of semisimple group algebras of finite metacyclic groups (see section 1.9).

In this chapter we are interested in two aspects of the cyclic cyclotomic algebras: firstly the ring isomorphism between these algebras, and secondly the subgroup they generate inside the Schur group of a field. In the first section, we show that the invariants that determine the ring isomorphism between cyclic cyclotomic algebras over abelian number fields are essentially the local Schur indices at all rational primes and we give one example showing that this is not the case for arbitrary Schur algebras. The results of this section are collected in [HOdR1]. In the next section we give a characterization of when the subgroup of the Schur group generated by classes containing cyclic cyclotomic algebras over an abelian number field K has finite index in $S(K)$ in terms of the relative position of K in the lattice of cyclotomic extensions of the rationals. The results of this second section are established in [HOdR3].

6.1 Ring isomorphism of cyclic cyclotomic algebras

In this section we show that a ring isomorphism between cyclic cyclotomic algebras over abelian number fields is essentially determined by the list of local Schur indices at all rational primes. As a consequence, a ring isomorphism between simple components of the rational group algebras of finite metacyclic groups is determined by the center, the dimension over $\mathbb{Q}$, and the list of local Schur indices at rational primes. An example is given to show that this does not hold for finite groups in general.

Let KG be a semisimple group algebra. The calculation of the automorphism group of KG reduces to two problems, namely first to compute the Wedderburn decomposition of KG and then to decide which of the Wedderburn components of KG are ring isomorphic (not necessarily isomorphic as algebras) (see [CJP], [Her3] and [OdRS2]). Similarly, deciding whether two semisimple group algebras KG and KH are isomorphic is equivalent to decide if there is a one-to-one correspondence among the Wedderburn components of KG and KH which associate ring isomorphic components. This yields the problem of looking for effective methods to decide whether two Schur algebras are ring isomorphic.

If two Schur algebras $A = A(\chi, K)$ and $B = A(\psi, K)$ are ring isomorphic, for χ and ψ irreducible characters of some finite groups, then A and B have isomorphic centers and the same degrees and indices. However, this information is not always enough, as it can be seen in the next example.

Example 6.1. The dicyclic group $G = C_3 \rtimes C_4$ of order 12 and the quaternion group Q_8 of order 8 have rational valued characters of degree 2 for which the simple components $\mathbb{H}(\mathbb{Q})$ and $\left(\frac{-1,-3}{\mathbb{Q}}\right)$ respectively, are division algebras of index 2 that are not ring isomorphic. This is because the local indices of these characters do not agree at the primes 2 and 3. Both algebras have index 2 at infinity and at finite primes the algebra $\mathbb{H}(\mathbb{Q})$ has non-trivial Schur index only at 2, and $\left(\frac{-1,-3}{\mathbb{Q}}\right)$ has non-trivial index equal at the prime 3. □

Assume now that K is an abelian number field and χ and ψ are irreducible characters of some finite groups. Ring isomorphism between $A(\chi, K)$ and $A(\psi, K)$ forces all local Schur indices $m_p(\chi)$ and $m_p(\psi)$ to be equal for all rational primes p, including the infinite prime. By the result of Benard (see Theorem 1.107), the local index of a simple component of a rational group algebra is the same for all primes of its center that lie over a fixed rational prime. Recall that, by definition, $m_p(\chi)$ is the common Schur index of the $\mathfrak{p}$-local algebra $K(\chi)_{\mathfrak{p}} \otimes_{K(\chi)} A(\chi, K)$ for any prime $\mathfrak{p}$ of $K(\chi)$ lying over the rational prime p.

The conditions that the centers, dimensions, and local indices of $A(\chi, K)$ and $A(\psi, K)$ are respectively equal are not enough to force the two simple components to be ring isomorphic. We give an example of this situation in Example 6.3. Our goal in this section is to give some conditions on the groups G and H which imply that the above conditions are enough to force the two simple components to be ring isomorphic. We will show in Corollary 6.7 that this is the case as long as both of the groups are metacyclic. This is an immediate consequence of Theorem 6.6.

For division algebras whose Brauer classes lie in the Schur subgroup of an abelian number field, a theorem of Spiegel and Trojan [ST] provides a necessary and sufficient

condition for ring isomorphism, which we will apply several times in this section.

Theorem 6.2 (Spiegel-Trojan). *Suppose D and Δ are division algebras of exponent m whose Brauer classes lie in the Schur subgroup of an abelian number field K. Then D and Δ are ring isomorphic if and only if there is an integer s coprime to m for which $[D]^s = [\Delta]$ in $\mathrm{Br}(K)$.*

We now give an example of two simple components of a rational group algebra whose centers, dimensions, and local indices are respectively equal, but they are not ring isomorphic.

Example 6.3. The non-abelian groups $A = C_{11} \rtimes C_{25}$ and $B = C_{31} \rtimes C_{25}$ both have faithful irreducible characters $\phi \in \mathrm{Irr}(A)$, $\theta \in \mathrm{Irr}(B)$ with degree and Schur index 5. The only nontrivial local indices of these characters are $m_{11}(\phi) = 5$ and $m_{31}(\theta) = 5$. Let $K = \mathbb{Q}(\phi, \theta)$, $D = K \otimes A(\phi, \mathbb{Q})$, and $\Delta = K \otimes A(\theta, \mathbb{Q})$. Since $[K : \mathbb{Q}(\phi)]$ and $[K : \mathbb{Q}(\theta)]$ are relatively prime to 5, D and Δ are K-central division algebras of index 5.

Let $G = A \times A \times B \times B$, where the groups A and B are defined as above. Note that G is metabelian, but not metacyclic. Define $\chi, \psi \in \mathrm{Irr}(G)$ by

$$\chi = \phi \otimes 1_A \otimes \theta \otimes \theta, \quad \text{and} \quad \psi = \phi \otimes \phi \otimes 1_B \otimes \theta,$$

where ϕ and θ are the characters defined above. Then the simple components S_χ and S_ψ of KG are central simple K-algebras of the same dimension, whose local indices are equal to 5 at primes of K lying over 11 and 31, and whose local indices are trivial at all other primes of K. However, the class of S_χ in the Brauer group $Br(K)$ is the class $[D][\Delta]^2$, and the class of S_ψ is $[D]^2[\Delta]$. These classes are not powers of one another in $Br(K)$, so by Spiegel and Trojan's Theorem, these two simple components are not ring isomorphic. □

Since a cyclic cyclotomic algebra over K is automatically a cyclotomic algebra over K, the class in the Brauer group of K generated by a cyclic cyclotomic algebra over K always lies in the Schur subgroup of K by the Brauer-Witt Theorem. By Theorem 1.107, this implies that the $\mathfrak{p}$-local index of A is the same value $m_p(A)$ for all primes $\mathfrak{p}$ of K lying over the same rational prime p.

Lemma 6.4. *Let K be an abelian number field. Let $A = (L/K, \sigma, \zeta)$ and $A' = (L/K, \sigma', \zeta')$ be cyclic algebras defined over the same cyclic extension L/K, with ζ and ζ' roots of unity in K. If A and A' have the same exponent in $\mathrm{Br}(K)$ then A is ring isomorphic to A'.*

Proof. Since $\mathrm{Gal}(L/K) = \langle\sigma\rangle = \langle\sigma'\rangle$, there exists some integer r, coprime with $[L:K]$, such that $\sigma' = \sigma^r$. If $rs \equiv 1 \mod [L:K]$, then A' is isomorphic to $(L/K, \sigma, \zeta'^s)$ as an algebra over K by Theorem 1.56. Thus one may assume without loss of generality that $\sigma = \sigma'$.

Let ξ be a root of unity in K such that $\zeta = \xi^n$ and $\zeta' = \xi^{n'}$ for some positive integers n and n'. Let $B = (L/K, \sigma, \xi)$. Then $[B]^n = [A]$ and $[B]^{n'} = [A']$. Hence $[A]$ and $[A']$ are two elements of the same order in a cyclic group and therefore they generate the same cyclic subgroup in $\mathrm{Br}(K)$. Thus A and A' are isomorphic as rings by Spiegel and Trojan's Theorem. □

Note that it is not necessary for $L/\mathbb{Q}$ to be an abelian extension in the above lemma and so L/K may not be a cyclotomic extension.

Lemma 6.5. *Let K be an abelian number field. Let D and D' be two division algebras with center K whose Brauer classes lie in the Schur subgroup of K. Suppose*

$$[D] = [A_1] \otimes_K \cdots \otimes_K [A_n] \text{ and } [D'] = [A_1'] \otimes_K \cdots \otimes_K [A_n'] \text{ in } \mathrm{Br}(K),$$

with $m(A_i) = m(A_i') = p_i^{a_i}$, for $i = 1, \ldots, n$ and $p_1, \ldots, p_n$ distinct rational primes.

If A_i and A_i' are ring isomorphic for all $i = 1, \ldots, n$, then D is ring isomorphic to D'.

Proof. By Spiegel and Trojan's Theorem, for each $i = 1, \ldots, n$ there is an integer r_i coprime to p_i such that $[A_i]^{r_i} = [A_i']$. By the Chinese remainder theorem, there is an integer r such that $r \equiv r_i \mod p_i^{a_i}$ for all i. Therefore,

$$[D]^r = \prod_{i=1}^{n} [A_i]^r = \prod_{i=1}^{n} [A_i]^{r_i} = \prod_{i=1}^{n} [A_i'] = [D'].$$

So by Spiegel and Trojan's Theorem again, D and D' are ring isomorphic. □

The main result of the section is the following theorem.

Theorem 6.6. *Let A and A' be two cyclic cyclotomic algebras over an abelian number field K. Assume that $[A] = [D]$ and $[A'] = [D']$ in $\mathrm{Br}(K)$, for division algebras D and D'.*

If A and A' have the same local Schur indices at every rational prime p (including ∞), then D and D' are ring isomorphic.

Proof. Let $B = (K(\zeta_n)/K, \sigma, \zeta_\ell)$ be a cyclic cyclotomic algebra over K. If $\ell = p_1^{a_1} \cdots p_t^{a_t}$ is the prime factorization of ℓ, then in the Brauer group of K we have

$$[B] = \prod_{i=1}^{t} [(K(\zeta_n)/K, \sigma, \zeta_{p_i^{a_i}})].$$

It is clear that the index of each cyclic algebra $B_i = (K(\zeta_n)/K, \sigma, \zeta_{p_i^{a_i}})$ divides $p_i^{a_i}$ for each i. Therefore, for each rational prime q, the local index of each B_i at the prime q is a power of p_i, and so it follows that $m_q(B) = m_q(B_1) \cdots m_q(B_t)$ for all rational primes q.

Applying this to A and A' and using Lemma 6.5, we may assume that $A = (K(\zeta_n)/K, \sigma, \alpha)$ and $A' = (K(\zeta_{n'})/K, \sigma', \alpha')$ are cyclic cyclotomic algebras such that the common index of A and A', say m, is a power of a single prime p and α and α' are powers of a p^a-th root of unity $\zeta_{p^a} \in K$, where m divides p^a. Since the local indices determine elements of the Schur subgroup of K that are of exponent at most 2, we may assume $m > 2$. By Theorem 1.109, the fact that both A and A' lie in the Schur subgroup of K implies that there is an odd prime r for which $m = m_r(A) = m_r(A') > 2$. Since $\zeta_m \in K$, it follows that $[K(\zeta_{p^b}) : K]$ is a power of p, for every positive integer b.

For every subextension E of $K(\zeta_n)/K$, let E_p denote the maximal subextension of E/K of degree a power of p. Let E and E' be two subextensions of $K(\zeta_n)/K$. We claim that $(EE')_p = E_pE'_p$. The inclusion $E_pE'_p \subseteq (EE')_p$ is clear because

$$[E_pE'_p : K] = [E_pE'_p : E_p][E_p : K] = [E_p : E_p \cap E'_p][E_p : K]$$

and $[E_p : E_p \cap E'_p]$ divides $[E_p : K]$. On the other hand, $[E_pE' : E_pE'_p]$ divides $[E' : E'_p]$ and so $[E_pE' : E_pE'_p]$ is coprime to p. Similarly, $[EE'_p : E_pE'_p]$ is coprime to p. Therefore

$$[EE' : E_pE'_p] = [(EE'_p)(E_pE') : E_pE'_p]$$

is coprime to p. Thus $(EE')_p \subseteq E_pE'_p$ and the claim follows.

Furthermore, either $E_p \subseteq E'_p$ or $E'_p \subseteq E_p$, since $K(\zeta_n)/K$ is cyclic. In particular, if k and k' are two coprime divisors of n, then $K(\zeta_{kk'})_p$ equals either $K(\zeta_k)_p$ or $K(\zeta_{k'})_p$. Therefore, there exists a prime q and a power $d = q^h$ of q that divides n for which $K(\zeta_n)_p = K(\zeta_d)_p$. Moreover, if $q \neq p$ then $K(\zeta_d)_p = K(\zeta_q)_p$, so in this case one may assume that $d = q$.

It follows from Theorem 1.60 that there exists an integer w coprime to p such that

$$[A] = [(K(\zeta_n)/K, \sigma, \alpha)] = [(K(\zeta_d)/K, \overline{\sigma}, \alpha^w)].$$

So one may assume that $n = d$. In a similar fashion, for the algebra A' one may assume that $n' = d' = {q'}^{h'}$ for some prime q' and, if $q' \neq p$ then $h' = 1$. If $K(\zeta_d) = K(\zeta_{d'})$ then it is immediate from Lemma 6.4 that D and D' are ring isomorphic.

Suppose $K(\zeta_d) \neq K(\zeta_{d'})$. Let r be a rational prime for which $m_r(A) = m_r(A') > 2$. The facts pointed out in Theorem 1.109 imply that r must be an odd prime which is not equal to p. By Theorem 1.76 and Theorem 1.56, both of the extensions $K(\zeta_d)/K$ and $K(\zeta_{d'})/K$ must ramify at any prime of K lying above r. However, the only finite

rational prime that ramifies in the extension $\mathbb{Q}(\zeta_{q^h})/\mathbb{Q}$ is q. By Lemma 1.11, it follows that $r = q$. In a similar manner, we can show that $r = q'$. But then $d = d'$, a contradiction. □

Corollary 6.7. *Let K be an abelian number field, G, H finite metacyclic groups and $\chi \in Irr(G)$, $\psi \in Irr(H)$. Suppose*

(1) $K(\chi) = K(\psi)$,

(2) $\chi(1) = \psi(1)$ *and*

(3) $m_p(A(\chi, K)) = m_p(A(\psi, K))$ *for all rational primes p (including ∞).*

Then $A(\chi, K)$ and $A(\psi, K)$ are ring isomorphic.

Proof. Let $\mathbb{K} := K(\chi) = K(\psi)$. Since $\chi(1) = \psi(1)$, $A(\chi, K)$ and $A(\psi, K)$ have the same dimension over $\mathbb{K}$, so it suffices to show that their division algebra parts D_χ and D_ψ are ring isomorphic. Since G is metacyclic, the character χ is induced from a maximal abelian normal subgroup $A/\ker(\chi)$ of $G/\ker(\chi)$, and G/A is cyclic. Suppose that a maximal cyclic subgroup of $A/\ker(\chi)$ has order n and that there is an element $g \in G$ of order ℓ for which $|\langle gA \rangle| = |G/A|$. Then $\mathbb{K} \subseteq K(\zeta_n)$ and $A(\chi, K)$ can be naturally identified with the cyclic cyclotomic algebra $(\mathbb{K}(\zeta_n)/\mathbb{K}, \sigma, \zeta_\ell)$ (see Proposition 2.3). In a similar fashion, we can show that $A(\psi, K)$ can also be expressed as a cyclic cyclotomic algebra. The corollary then follows because Theorem 6.6 can be applied. □

6.2 The subgroup $CC(K)$ of the Schur group $S(K)$ generated by cyclic cyclotomic algebras

Throughout this section K is an abelian number field. It is well known that every element of $Br(K)$ is represented by a cyclic algebra over K and every element of $S(K)$ is represented by a cyclotomic algebra over K by the Brauer–Witt Theorem. However, in general, not every element of $S(K)$ is represented by a cyclic cyclotomic algebra. In fact, as we will see in this section, in general, $S(K)$ is not generated by classes represented by cyclic cyclotomic algebras.

Let $CC(K)$ denote the subgroup of $S(K)$ generated by classes containing cyclic cyclotomic algebras. In other words $CC(K)$ is formed by elements of $S(K)$ represented by tensor products of cyclic cyclotomic algebras. The aim of this section is to study the gap between $S(K)$ and $CC(K)$. More precisely, we give a characterization of when $CC(K)$ has finite index in $S(K)$ in terms of the relative position of K in the lattice of cyclotomic extensions of the rationals.

By Benard-Schacher Theorem (Theorem 1.108), $S(K) = \bigoplus_p S(K)_p$, where p runs over the primes such that $\zeta_p \in K$ and $S(K)_p$ denotes the p-primary part of $S(K)$. Thus $CC(K)$ has finite index in $S(K)$ if and only if $CC(K)_p = CC(K) \cap S(K)_p$ has finite index in $S(K)_p$ for every prime p with $\zeta_p \in K$. Therefore, we are going to fix a prime p such that $\zeta_p \in K$ and our main result gives necessary and sufficient conditions for $[S(K)_p : CC(K)_p] < \infty$, in terms of the Galois group of a certain cyclotomic field F that we are going to introduce next.

Let $L = \mathbb{Q}(\zeta_m)$ be a minimal cyclotomic field containing K, a the minimum positive integer such that $\zeta_{p^a} \in K$, s the minimum positive integer such that $\zeta_{p^s} \in L$ and

$$b = \begin{cases} s, & \text{if } p \text{ is odd or } \zeta_4 \in K, \\ s + v_p([K \cap \mathbb{Q}(\zeta_{p^s}) : \mathbb{Q}]) + 2, & \text{if } \mathrm{Gal}(K(\zeta_{p^{2a+s}})/K) \text{ is not cyclic}, \\ s+1, & \text{otherwise}, \end{cases}$$

where $v_p : \mathbb{Q} \to \mathbb{Z}$ denotes the p-adic valuation. Then we let $\zeta = \zeta_{p^{a+b}}$ and define $F = L(\zeta)$.

The Galois groups of F mentioned above are

$$\Gamma = \mathrm{Gal}(F/\mathbb{Q}),\ G = \mathrm{Gal}(F/K),\ C = \mathrm{Gal}(F/K(\zeta)) \text{ and } D = \mathrm{Gal}(F/K(\zeta + \zeta^{-1})).$$

Notice that $D \neq G$ by the definition of b, and if $C \neq D$ then $p^a = 2$ and $\rho(\zeta) = \zeta^{-1}$ for every $\rho \in D \setminus C$.

As in Chapter 5, we fix elements ρ, σ of G, with $G = \langle \rho, \sigma, C \rangle$, such that $D = B \times \langle \rho \rangle$ and $C = B \times \langle \rho^2 \rangle$ for some subgroup B of C and $G/C = \langle \rho C \rangle \times \langle \sigma C \rangle$. Furthermore, if G/C is cyclic (equivalently $C = D$) then we select $\rho = 1$ and otherwise σ is selected so that $\sigma(\zeta_4) = \zeta_4$. The existence of such ρ and σ in G has been proved in Chapter 5 (see Lemma 5.3).

Finally, to every $\psi \in \Gamma$ we associate two non-negative integers,

$$d(\psi) = \min\{a, \max\{h \geq 0 : \psi(\zeta_{p^h}) = \zeta_{p^h}\}\} \quad \text{and} \quad \nu(\psi) = \max\{0, a - v_p(|\psi G|)\},$$

and a subgroup of C:

$$T(\psi) = \{\eta \in B : \eta^{p^{\nu(\psi)}} \in B^{p^{d(\psi)}}\}.$$

Now we are ready to state the main result of this section.

Theorem 6.8. *Let K be an abelian extension of the rationals, p a prime integer and use the above notation.*

If G/C is cyclic then the following are equivalent:

(1) *$CC(K)_p$ has finite index in $S(K)_p$.*

(2) *For every* $\psi \in \Gamma_p$ *one has* $\psi^{|\psi G|} \in \bigcup_{i=0}^{|\sigma C|-1} \sigma^i T(\psi)$.

(3) *For every* $\psi \in \Gamma_p$ *satisfying* $\nu(\psi) < \min\{v_p(\exp B), d(\psi)\}$, *one has* $\psi^{|\psi G|} \in \bigcup_{i=0}^{|\sigma C|-1} \sigma^i T(\psi)$.

If G/C *is non-cyclic (and in particular* $p = 2$*) then the following are equivalent:*

(1) $CC(K)_2$ *has finite index in* $S(K)_2$.

(2) *For every* $\psi \in \Gamma_2 \setminus G$, *if* $d = v_2([K \cap \mathbb{Q}(\zeta) : \mathbb{Q}]) + 2$ *then*

$$\psi^{|\psi G|} \in \mathrm{Gal}(F/\mathbb{Q}(\zeta_{2^{d+1}})) \bigcap \left(\bigcup_{i=0}^{|\sigma C|-1} \sigma^i \langle \rho, T(\psi) \rangle \right).$$

Notice that conditions (2) and (3) in Theorem 6.8 can be verified by elementary computations in the Galois group Γ.

The subgroup of $S(K)$ generated by cyclic cyclotomic algebras

Now we provide some information on the structure of $CC(K)_p$. We start by introducing some notation and recalling some known facts about local information concerning $S(K)$.

Let $\mathbb{P} = \{r \in \mathbb{N} : r \text{ is prime}\} \cup \{\infty\}$. Given $r \in \mathbb{P}$, we are going to abuse the notation and denote by K_r the completion of K at a (any) prime of K dividing r. If E/K is a finite Galois extension, one may assume that the prime of E dividing r, used to compute E_r, divides the prime of K over r, used to compute K_r.

We also use the following notation, for $\pi \subseteq \mathbb{P}$ and $r \in \mathbb{P}$:

$$\begin{aligned} S(K,\pi) &= \{[A] \in S(K) : m_r(A) = 1, \text{ for each } r \in \mathbb{P} \setminus \pi\}, \\ S(K,r) &= S(K,\{r\}), \\ CC(K,\pi) &= CC(K) \cap S(K,\pi), \\ CC(K,r) &= CC(K) \cap S(K,r), \\ \mathbb{P}_p &= \big\{r \in \mathbb{P} \setminus \{\infty\} : CC(K,\{r,\infty\})_p = CC(K,r)_p \bigoplus CC(K,\infty)_p\big\}. \end{aligned}$$

If p is odd or $\zeta_4 \in K$ then $m_\infty(A) = 1$ for each Schur algebra A and so $\mathbb{P}_p = \mathbb{P} \setminus \{\infty\}$.

Finally, if r is odd then we set

$$\nu(r) = \max\{0, a + v_p(e(K(\zeta_r)/K, r)) - v_p(|W(K_r)|)\}.$$

Notice that the notation for $\nu(r)$ coincides with the one given in Notation 5.10. This is a consequence of the structure of unramified extensions of $\mathbb{Q}_r$ (see Theorem 1.77).

The following theorem provides information on the structure of $CC(K)_p$.

Theorem 6.9. *For every prime p we have*

$$CC(K)_p = \left(\bigoplus_{r \in \mathbb{P}_p} CC(K,r)_p \right) \bigoplus \left(\bigoplus_{r \in \mathbb{P} \setminus \mathbb{P}_p} CC(K, \{r, \infty\})_p \right).$$

Let X_r denote the direct summand labelled by r (of either the first or the second kind) in the previous decomposition.

(1) *If r is odd then X_r is cyclic of order $p^{\nu(r)}$ and is generated by the class of $(K(\zeta_r)/K, \zeta_{p^a})$.*

(2) *X_2 has order 1 or 2 and if it has order 2 then $p^a = 2$ and X_2 is generated by the class of $(K(\zeta_4)/K, -1)$.*

(3) *If $X_\infty \neq 1$, then $p = 2$, $K \subseteq \mathbb{R}$, and X_∞ has exponent 2.*

Proof. Let $A = (E/K, \xi)$ be a cyclic cyclotomic algebra with $[A] \in S(K)_p$. One may assume without loss of generality that $\xi \in W(K)_p$. As in the proof of Lemma 6.4, there is a prime power r^k such that $\ell = [E : K(\zeta_{r^k})]$ is coprime to p. Then $[A^{\otimes \ell}] = [(E/K, \xi^\ell)] = [(K(\zeta_{r^k})/K, \xi)]$ and $m_q(A) = m_q(A^{\otimes \ell}) = m_q(K(\zeta_{r^k})/K, \xi)$, for every $q \in \mathbb{P}$. If $q \notin \{r, \infty\}$ then $K(\zeta_{r^k})/K$ is unramified at q and therefore $m_q(A) = 1$ by Lemma 1.11. Thus $[A] \in CC(K, \{r, \infty\})$. This shows that $CC(K)_p = \sum_{r \in \mathbb{P} \setminus \{\infty\}} CC(K, \{r, \infty\})_p$.

If $\mathbb{P} \setminus \{\infty\} = \mathbb{P}_p$ then this implies that

$$CC(K)_p = \bigoplus_{r \in \mathbb{P}} CC(K,r) = \left(\bigoplus_{r \in \mathbb{P}_p} CC(K,r) \right) \bigoplus CC(K, \infty)$$

as wanted. Assume otherwise that $\mathbb{P} \setminus \{\infty\} \neq \mathbb{P}_p$. If $1 \neq [A] \in CC(K, \infty)$ then for every $r \in \mathbb{P}$ and $[B] \in CC(K, \{r, \infty\}) \setminus CC(K, \infty)$ one has $[B] = [A \otimes B] \cdot [A]$ and $[A \otimes B] \in CC(K, r)$. This implies that $CC(K, \{r, \infty\}) = CC(K, r) \bigoplus CC(K, \infty)$, contradicting the hypothesis. Hence $CC(K, \infty) = 1$ and then

$$CC(K)_p = \left(\bigoplus_{r \in \mathbb{P}_p} CC(K,r)_p \right) \bigoplus \left(\bigoplus_{r \in \mathbb{P} \setminus \mathbb{P}_p} CC(K, \{r, \infty\})_p \right),$$

as desired.

(1) Let $r \in \mathbb{P}$. The map $K_r \otimes_K - : X_r \to S(K_r)$ is an injective group homomorphism. If r is odd then $S(K_r)$ is cyclic of order $e(K(\zeta_r)/K, r)$ and it is generated by the cyclic algebra $(K_r(\zeta_r)/K_r, \zeta_n)$, where $n = |W(K_r)|$ (see e.g. Theorem 1.110 and [Yam]). Therefore X_r is cyclic and hence it is generated by a class containing a cyclic

cyclotomic algebra A. As above we may assume that $A = (K(\zeta_{r^k})/K, \zeta_{p^a}^{\ell})$ for some $k, \ell \geq 1$. Since $[A] = [(K(\zeta_{r^k})/K, \zeta_{p^a})]^{\ell}$, one may assume that $\ell = 1$. Then

$|X_r| = m_r(A) = m_r((K(\zeta_{r^k})'/K, \zeta_{p^a})) = m_r((K(\zeta_r)/K, \zeta_{p^a})) = m((K_r(\zeta_r)/K_r, \zeta_{p^a})) = m((K_r(\zeta_r)/K_r, \zeta_{p^{a+a(r)}})^{\otimes a(r)}) = p^{\nu(r)}$, where $a + a(r) = v_p(n)$. This proves (1).

(2) and (3) follow by similar arguments. □

Remark 6.10. Notice that the proof of Theorem 6.9 shows that if A is a cyclic cyclotomic algebra of index a power of p, then $[A] \in S(K, \{r, \infty\})$ for some prime $r \in \mathbb{P}\backslash\{\infty\}$, and if p is odd or $\zeta_4 \in K$, then $[A] \in S(K, r)$.

By Theorem 6.9, if r is odd then $\nu(r) = \max\{v_p(m_r(A)) : [A] \in CC(K)_p\}$. We can extend the definition of $\nu(r)$ by setting $\nu(2) = \max\{v_p(m_2(A)) : [A] \in CC(K)_p\}$. Notice that $\nu(2) \leq 1$ and $\nu(2) = 1$ if and only if $p^a = 2$ and $(K(\zeta_4)/K, -1)$ is non-split. We will need to compare $\nu(r)$ to $\beta(r) = \max\{v_p(m_r(A)) : [A] \in S(K)_p\}$.

Proposition 6.11. *Let $r \in \mathbb{P}$. Then*

(1) *$CC(K)_p = S(K)_p$ if and only if $\nu(r) = \beta(r)$ for each $r \in \mathbb{P} \setminus \{\infty\}$.*

(2) *$CC(K)_p$ has finite index in $S(K)_p$ if and only if $\nu(r) = \beta(r)$ for all but finitely many primes r.*

Proof. We prove (2) and let the reader to adapt the proof to show (1).

Assume that $CC(K)_p$ has finite index in $S(K)$ and let $[A_1], \ldots, [A_n]$ be a complete set of representatives of cosets modulo $CC(K)_p$. Then $\pi = \{r \in \mathbb{P} : m_r(A_i) \neq 1 \text{ for some } i\}$ is finite and $\nu(r) = \beta(r)$ for every $r \in \mathbb{P} \setminus \pi$. Conversely, assume that $\nu(r) = \beta(r)$ for every $r \in \mathbb{P} \setminus \pi$, with π a finite subset of $\mathbb{P}$ containing ∞. Then $S(K, \pi)_p$ is finite and we claim that $S(K)_p = S(K, \pi)_p + CC(K)_p$. Let $[B] \in S(K)_p$. We prove that $[B] \in S(K, \pi)_p + CC(K)_p$ by induction on $h(B) = \prod_{r \in \mathbb{P}\setminus\pi} m_r(B)$. If $h(B) = 1$ then $[B] \in S(K, \pi)_p$ and the claim follows. Assume that $h(B) > 1$ and the induction hypothesis. Then there is a cyclic cyclotomic algebra A and $r \in \mathbb{P} \setminus \pi$ such that $m_r(B) = m_r(A) > 1$. Since $S(K_r)$ is cyclic, there is a positive integer ℓ coprime to $m_r(B)$ such that $(A^{\otimes \ell}) \otimes_K K_r \cong B \otimes_K K_r$ as K_r-algebras. Let $C = (A^{\mathrm{op}})^{\otimes \ell} \otimes B$. Since $A^{\otimes \ell} \in CC(K, \{r, \infty\})_p$, it follows that $h(C) = \frac{h(B)}{m_r(A)} < h(B)$, and hence $[C] \in S(K, \pi)_p + CC(K)_p$, by the induction hypothesis. Therefore, $[B] = [A]^{\ell}[C] \in S(K, \pi)_p + CC(K)_p$, as required. □

Notice that for p odd Proposition 6.11 is a straightforward consequence of the decomposition of $CC(K)_p$ given in Theorem 6.9 and the Janusz Decomposition Theorem [Jan3].

Examples

Now we present several examples comparing $S(K)$ and $CC(K)$ for various fields.

Example 6.12. $K = \mathbb{Q}$.

It follows from the Hasse–Brauer–Noether–Albert Theorem (see Remark 1.95 (ii)) that $S(\mathbb{Q}, r)$ is trivial for all primes r and hence so is $CC(\mathbb{Q}, r)$. The cyclic cyclotomic algebra $\mathbb{H}_{2,\infty} = \mathbb{H}(\mathbb{Q}) = (\mathbb{Q}(\zeta_4)/\mathbb{Q}, -1)$ is a rational quaternion algebra which lies in $CC(\mathbb{Q}, \{2, \infty\})$. When r is odd, the cyclic algebra $\mathbb{H}_{r,\infty} = (\mathbb{Q}(\zeta_r)/\mathbb{Q}, -1)$ has real completion $\mathbb{R} \otimes_{\mathbb{Q}} \mathbb{H}_{r,\infty} \simeq M_n(\mathbb{H}(\mathbb{R}))$, for $n = \frac{r-1}{2}$, so $m_\infty(\mathbb{H}_{r,\infty}) = 2$. The extension $\mathbb{Q}_r(\zeta_r)/\mathbb{Q}_r$ is unramified at primes other than r, so $[\mathbb{H}_{r,\infty}] \in CC(\mathbb{Q}, \{r, \infty\})$ (and $m_r(\mathbb{H}_{r,\infty})$ must be 2). If r and q are distinct finite primes, then $[\mathbb{H}_{r,\infty}][\mathbb{H}_{q,\infty}]$ is an element of $CC(\mathbb{Q}, \{r, q\})$, and it follows from Remark 6.10 that this element cannot be represented by a cyclic cyclotomic algebra. Nevertheless, it is easy to see at this point that $S(\mathbb{Q}) = CC(\mathbb{Q})$.

The smallest example of an algebra representing an element in $CC(\mathbb{Q}, \{2, 3\})$ is the generalized quaternion algebra $\left(\frac{-3,2}{\mathbb{Q}}\right)$. The algebra of 2×2 matrices over $\left(\frac{-3,2}{\mathbb{Q}}\right)$ is isomorphic to a simple component of the rational group algebra of the group of order 48 that has the following presentation $\langle x, y, z : x^{12} = y^2 = z^2 = 1, x^y = x^5, x^z = x^7, [y, z] = x^9 \rangle$. □

Example 6.13. $CC(K, \infty) \neq 1$.

It is also possible that $CC(K, \infty)$ is non-trivial. For example, the quaternion algebra $\mathbb{H}(\mathbb{Q}(\sqrt{2})) = (\mathbb{Q}(\zeta_8)/\mathbb{Q}(\sqrt{2}), -1)$ is homomorphic to a simple component of the rational group algebra of the generalized quaternion group of order 16. It has real completion isomorphic to $\mathbb{H}(\mathbb{R})$ at both infinite primes of $\mathbb{Q}(\sqrt{2})$, so $m_\infty(\mathbb{H}(\mathbb{Q}(\sqrt{2}))) = 2$. If r is an odd prime then $m_r(\mathbb{H}(\mathbb{Q}(\sqrt{2}))) = 1$. Since $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$ is ramified and the sum of the local invariants at infinite primes is an integer, we deduce that $m_2(\mathbb{H}(\mathbb{Q}(\sqrt{2}))) = 1$, so it follows that $[\mathbb{H}(\mathbb{Q}(\sqrt{2}))] \in CC(\mathbb{Q}(\sqrt{2}), \infty)$. □

Example 6.14. *Cyclotomic fields.*

Suppose $K = \mathbb{Q}(\zeta_m)$ for some positive integer $m > 2$. Assume that either m is odd or 4 divides m. The main theorem of [Jan2] shows that if p is a prime dividing m and $m = p^n m_0$ with m_0 coprime to p, then

$$S(\mathbb{Q}(\zeta_m))_p = \{[A \otimes_{\mathbb{Q}(\zeta_{p^n})} \mathbb{Q}(\zeta_m)] : [A] \in S(\mathbb{Q}(\zeta_{p^n}))_p\}.$$

When $p^n > 2$, we know by [BeS, Theorem 3] that $S(\mathbb{Q}(\zeta_{p^n}))_p$ is generated by the Brauer classes of characters of certain metacyclic groups, which, in their most natural crossed product presentation, take the form of cyclic cyclotomic algebras. Therefore, $S(\mathbb{Q}(\zeta_{p^n}))_p = CC(\mathbb{Q}(\zeta_{p^n}))_p$. Since it is easy to see that when K is an extension of a field

E, $\{[A\otimes_E K] : [A] \in CC(E)\} \subseteq CC(K)$, we can conclude that $S(\mathbb{Q}(\zeta_m)) = CC(\mathbb{Q}(\zeta_m))$ for all positive integers m. □

Combining Proposition 6.11 with the results of [Jan3] one can obtain examples with $S(K)_p \neq CC(K)_p$.

Example 6.15. *$CC(K)_p \neq S(K)_p$, p odd.*

By Theorem 6.9, if $CC(K)_p = S(K)_p$ then $S(K)_p = \bigoplus_{r\in\mathbb{P}} S(K,r)_p$. However, Proposition 6.2 of [Jan3] shows that for every odd prime p there are infinitely many abelian extensions K of $\mathbb{Q}$ such that $S(K)_p \neq \bigoplus_{r\in\mathbb{P}} S(K,r)_p$. Thus for such fields K one has $S(K)_p \neq CC(K)_p$. □

Example 6.16. *$CC(K)_2 \neq S(K)_2$ with $\zeta_4 \in K$.*

Let q be a prime of the form $1+5\cdot 2^9 t$ with $(t,10)=1$. In the last section of [Jan3] one constructs a subfield K of $\mathbb{Q}(\zeta_{2^9\cdot 5\cdot q})$ such that $\max\{m_q(A) : [A] \in S(K)_2\} = 4$ (in particular $\zeta_4 \in K$), and for every $[A] \in S(K)_2$ with $m_q(A) = 4$, one has $m_r(A) \neq 1$, for some prime r not dividing $10q$. In the notation of Proposition 6.11 this means that $v_2(|S(K,q)|) < \beta(q) = 4$ (for $p = 2$). Then $S(K)_2 \neq \bigoplus_{r\in\mathbb{P}} S(K,r)_2$ and, as in Example 6.15, this implies that $CC(K)_2 \neq S(K)_2$. □

Example 6.17. *$CC(K)_2 \neq S(K)_2$ with $\zeta_4 \notin K$.*

An example with $S(K)_2 \neq CC(K)_2$ and $\zeta_4 \notin K$ can be obtained using Theorem 5 of [Jan1]. This result gives necessary and sufficient conditions for $S(k)$ to have order 2 when k is a cyclotomic extension of $\mathbb{Q}_2$. This is the maximal 2-local index for a Schur algebra. If $|S(k)| = 2$ then $\zeta_4 \notin k$. If, moreover, $\mathbb{H} = (k(\zeta_4)/k, -1)$ is not split then $CC(k)_2 = S(k)_2$, because $\mathbb{H}$ is a cyclic cyclotomic algebra. However, there are some fields k for which $|S(k)| = 2$ and $\mathbb{H}$ is split. In that case $S(k)$ is generated by the class of a cyclotomic algebra A and we are going to show that $CC(k) \neq S(k)$. Then for any algebraic number field with $K_2 = k$ we will also have $CC(K)_2 \neq S(K)_2$.

Indeed, if $CC(k) = S(k)$ then A is equivalent to a cyclic cyclotomic algebra $(k(\zeta_m)/k, \zeta)$. One may assume that $\zeta \in W(k)_2 \setminus \{1\}$ and hence $\zeta = -1$, because $\zeta_4 \notin k$. Write $m = 2^{v_2(m)}m'$, with m' odd. Since $k(\zeta_m)/k$ must be ramified, $v_2(m) \geq 2$. If $k(\zeta_{m'})/k$ has even degree then this would contradict the fact that $k(\zeta_m)/k$ is cyclic. So $k(\zeta_{m'})/k$ has odd degree and therefore $(k(\zeta_m)/k, -1)$ is equivalent to $(k(\zeta_{2^{v_p(m)}})/k, -1)$ by Theorem 1.60. Then A is equivalent to $(k(\zeta_4)/k, -1)$ by [Jan1, Theorem 1], yielding a contradiction. □

Finiteness of $S(K)_p/CC(K)_p$

The main idea of the proof of Theorem 6.8 is to compare $\nu(r)$ and $\beta(r)$ for odd primes r not dividing m. We will use the notation introduced at the beginning of the section

including the Galois groups Γ, G, C, D, and B, the elements $\rho, \sigma \in G$, and the decompositions $D = \langle\rho\rangle \times B$ and $C = \langle\rho^2\rangle \times B$.

We also use the following numerical notation for every odd prime r not dividing m:

$$\begin{aligned} a + a(r) &= v_p(|W(K_r)|), \\ d(r) &= \min\{a, v_p(r-1)\}, \\ f_r &= f(K/\mathbb{Q}, r), \\ f(r) &= v_p(f_r), \end{aligned}$$

and introduce $\psi_r \in \Gamma$ and $\phi_r \in G$ as follows:

$$\psi_r(\varepsilon) = \varepsilon^r \text{ for every root of unity } \varepsilon \in F, \quad \text{and} \quad \phi_r = \psi_r^{f_r}.$$

The order of ψ_r modulo G is f_r, and ψ_r and ϕ_r are Frobenius automorphisms at r in Γ and G respectively. By the uniqueness of an unramified extension of a local field of given degree, one has $v_p(|W(K_r)|) = v_p(|W(\mathbb{Q}_r)|) + f(r) = v_p(e(K(\zeta_r)/K, r)) + f(r)$. Thus

$$\nu(r) = \max\{0, a - f(r)\}. \tag{6.1}$$

This gives $\nu(r)$ in terms of the numerical information associated to r. The value of $\beta(r)$ was computed in Theorem 5.13. We will need the following lemma.

Lemma 6.18. *$\nu(r)$ and $\beta(r)$ depend only on $d(r)$ and the element $\psi_r \in \Gamma$.*

Proof. $\nu(r)$ is determined by $f(r)$ (see (6.1)), and $f(r)$ by $f_r = |\psi_r G|$. So $\nu(r)$ is determined by ψ_r. On the other hand, $\psi_r = \rho^{j'}\sigma^j\eta$ for uniquely determined integers $0 \le j' < |\rho|$, $0 \le j < |\sigma C|$ and $\eta \in B$. Therefore, ψ_r determines whether or not $j \equiv j' \bmod 2$, and also the element η required in Theorem 5.13. So knowing ψ_r and $d(r)$ will allow one to compute $\beta(r)$. □

We can now give a necessary and sufficient condition, in local terms, for $CC(K)_p$ to have finite index in $S(K)_p$.

Theorem 6.19. *$CC(K)_p$ has finite index in $S(K)_p$ if and only if $\nu(r) = \beta(r)$ for all odd primes r not dividing m.*

Proof. The sufficiency is a consequence of Proposition 6.11.

Suppose that there is an odd prime r not dividing m for which $\nu(r) < \beta(r)$. By Dirichlet's Theorem on primes in arithmetic progression there are infinitely many primes r' such that $r' \equiv r \mod \operatorname{lcm}(m, p^{a+b}, p^{v_p(r-1)+1})$. For such an r' one has $\psi_{r'} = \psi_r$ and $v_p(r'-1) = v_p(r-1)$. Then $\beta(r') = \beta(r) > \nu(r) = \nu(r')$ for infinitely many primes r', by Lemma 6.18, and hence $[S(K)_p : CC(K)_p] = \infty$, by Proposition 6.11. □

When p is odd, this result can be interpreted in terms of the local subgroups of $S(K)_p$ and $CC(K)_p$.

Theorem 6.20. *Let K be a subfield of $\mathbb{Q}(\zeta_n)$, p an odd prime and n a positive integer. Then the following conditions are equivalent:*

(1) *$CC(K)_p$ has finite index in $S(K)_p$.*

(2) *$CC(K,r)_p = S(K,r)_p$, for almost all $r \in \mathbb{P}$.*

(3) *$CC(K,r)_p = S(K,r)_p$, for every prime r not dividing n.*

Proof. By the Janusz Decomposition Theorem [Jan3], we have

$$S(K)_p = S(K,\pi)_p \bigoplus \left(\bigoplus_{r \notin \pi} S(K,r)_p \right),$$

where π is the set of prime divisors of m, the smallest integer for which $K \subseteq \mathbb{Q}(\zeta_m)$. This shows that $\beta(r) = v_p(|S(K,r)|_p)$, whenever r is a prime that does not divide m and hence, for such primes $\nu(r) = \beta(r)$ if and only if $CC(K,r)_p = S(K,r)_p$. Now the results follow from Proposition 6.11 and Theorem 6.19. □

An obvious consequence of Theorem 6.20 is the following:

Corollary 6.21. *If K is a subfield of $\mathbb{Q}(\zeta_n)$ and p is an odd prime then the order of the group $\bigoplus_{r \in \mathbb{P}, r \nmid n} S(K,r)_p / CC(K,r)_p$ is either 1 or infinity.*

We now proceed with the proof of the main theorem of the section.

Proof of Theorem 6.8. For each $\psi \in \Gamma$ we put $h(\psi) = \max\{0 \leq h \leq a+b : \psi(\zeta_{p^h}) = \zeta_{p^h}\}$. Clearly $d(\psi) = \min\{a, h(\psi)\}$. By Dirichlet's Theorem on primes in arithmetic progression, for every $\psi \in \Gamma$ there exists an odd prime r not dividing m such that $\psi = \psi_r$. For such a prime one has $h(\psi) = \min\{a+b, v_p(r-1)\}$. This prime r can be selected so that $h(\psi) = v_p(r-1)$, because otherwise we would have $h(\psi) = a+b < v_p(r-1)$, and we could replace r by a prime r' satisfying $r' \equiv r \mod m$ and $r' \equiv 1 + p^{a+b} \mod p^{a+b+1}$. For such an r', one has $d(r) = d(r')$, and thus $\nu(r) = \nu(r')$ and $\beta(r) = \beta(r')$ by Lemma 6.18.

Let $q = |\sigma C|$. We now consider the case when G/C is cyclic. Then $D = C = B$ and $\rho = 1$. We set $t = v_p(\exp(B))$. If $t = 0$, then $T(\psi) = B$ for every $\psi \in \Gamma_p$, so that (2) and (3) obviously hold. Furthermore $|\eta B^{p^{d(r)}}| = 1$ and so $\nu(r) = \beta(r)$ for all odd primes r not dividing m, by Theorem 5.13. So (1) holds by Theorem 6.19. So to avoid trivialities we assume that $t > 0$.

(1) implies (2). Suppose K does not satisfy condition (2) and let $\psi \in \Gamma_p$ with $\psi^{|\psi G|} \notin \bigcup_{j=0}^{q-1} \sigma^i T(\psi)$. Let r be an odd prime not dividing m for which $\psi = \psi_r$ and $h(\psi) = v_p(r-1)$. Then $d(r) = d(\psi)$ and $p^{f(r)} = f_r = |\psi G|$, so $\nu(r) = \nu(\psi)$. The assumption $\psi^{|\psi G|} \notin \bigcup_{j=0}^{q-1} \sigma^i T(\psi)$, means that when we express $\psi^{|\psi G|}$ as $\sigma^j \eta$ with $0 \leq j < q$ and $\eta \in B$, the order of $\eta B^{p^{d(\psi)}}$ in $B/B^{p^{d(\psi)}}$ is strictly greater than $p^{\nu(\psi)} = p^{\nu(r)}$. By Theorem 5.13, we have $\beta(r) > \nu(r)$ for this odd prime r not dividing m, and so Theorem 6.19 implies that (1) fails.

(2) implies (3) is obvious.

(3) implies (1). Assume that (1) fails. Then, by Theorem 6.19, there exists a prime r not dividing m for which $\beta(r) > \nu(r)$. As above, we may select such an r so that $v_p(r-1) \leq a+b$.

Let $\psi = \psi_r$. Our choice of r implies that $d(\psi) = d(r)$. We claim that one can assume $\psi \in \Gamma_p$. If $\psi \notin \Gamma_p$, then let ℓ be the least positive integer such that ψ^ℓ lies in Γ_p. Let r' be a prime integer such that $r' \equiv r^\ell \mod \operatorname{lcm}(m, p^{a+b})$. Since ℓ is coprime to p, we have $v_p(r'-1) = v_p(r^\ell - 1) = v_p(r-1)$ and therefore $d(\psi^\ell) = d(r') = d(r) = d(\psi)$. Since $\psi_{r'} = \psi_r^\ell$ and ℓ is coprime to p, we also have $f(r') = f(r) = f(\psi)$. It follows from Lemma 6.18 that $\beta(r) = \beta(r')$ and $\nu(r) = \nu(r')$. So by replacing r by r' if necessary, one may assume that $\psi \in \Gamma_p$ and $d(\psi) = d(r)$.

For this prime r and element $\psi = \psi_r \in \Gamma_p$, the assumption $\beta(r) > \nu(r)$ and Theorem 5.13 imply that, when we write $\phi_r = \psi^{f_r} = \sigma^j \eta$, with $0 \leq j < q$ and $\eta \in B$, the order of $\eta B^{p^{d(r)}}$ in $B/B^{p^{d(r)}}$ is precisely $p^{\beta(r)}$. Then $\eta^{p^{\nu(r)}} \notin B^{p^{d(r)}}$, equivalently $\eta \notin T(\psi)$ and hence $\psi^{|\psi G|} \notin \bigcup_{j=0}^{q-1} \sigma^i T(\psi)$.

Since the exponent of $B/B^{p^{d(r)}}$ is precisely p^k, where $k = \min\{t, d(r)\}$, this can only be possible if $\nu(\psi) = \nu(r) < k = \min\{t, d(\psi)\}$. This shows that if condition (1) fails, then condition (3) also fails. This completes the proof in the case that G/C is cyclic.

Now suppose G/C is non-cyclic. In particular, $p^a = 2$ and $\sigma(\zeta_4) = \zeta_4$. Let $d = v_2([K \cap \mathbb{Q}(\zeta) : \mathbb{Q}]) + 2$ and let c be an integer such that $\sigma(\zeta) = \zeta^c$. Then $v_p(c-1) = d$ and $d(\psi) = 1$ for all $\psi \in \Gamma_2$.

(1) implies (2). Suppose (2) fails. Then there exists a $\psi \in \Gamma_2 \setminus G$ such that either $\psi^{|\psi G|} \notin \operatorname{Gal}(F/\mathbb{Q}(\zeta_{2^{d+1}}))$ or $\psi^{|\psi G|} \notin \bigcup_{i=0}^{q-1} \sigma^i \langle \rho, T(\psi) \rangle$.

As above, there exists an odd prime r not dividing m such that $\psi = \psi_r$, $|\psi G| = f_r$, and $\nu(\psi) = \nu(r)$. Since $\psi \notin G$ we have $f(r) > 0$ and so $\nu(r) = 0$, by (6.1). Also from $f(r) > 0$ one deduces that $\phi_r = \psi^{f_r}$ fixes ζ_4 and so when we write $\phi_r = \rho^{j'} \sigma^j \eta$ with $0 \leq j' < |\rho|$, $0 \leq j \leq q$, $\eta \in B$, we have that j' is even.

If $\phi_r \notin \operatorname{Gal}(F/\mathbb{Q}(\zeta_{2^{d+1}}))$, then j is odd, and we are in the case of Theorem 5.13, part (1), with $\nu(r) = 0$ and $\beta(r) = 1$. Otherwise, j is even and $\psi^{|\psi G|} \notin \bigcup_{i=0}^{q-1} \sigma^i \langle \rho, T(\psi) \rangle$. Then $\eta \notin T(\psi)$, or equivalently, $\nu(r) < v_2(|\eta B^2|)$ (observe that $d(r) = 1$). By Theo-

rem 5.13, we have $\beta(r) = v_2(|\eta B^2|) > \nu(r)$. Therefore, in all cases in which (2) fails, we have $\nu(r) < \beta(r)$. So (1) fails by Theorem 6.19.

(2) implies (1). Suppose (1) fails. By Theorem 6.19, there exists an odd prime r not dividing m such that $0 = \nu(r) < \beta(r) = 1$. Since $\nu(r) = 0$, we must have $f(r) > 0$, so $\psi = \psi_r \notin G$. As above, we may adjust ψ_r by an odd power and make a different choice of r without changing $\nu(r)$ or $\beta(r)$ in order to arrange that $\psi \in \Gamma_2$. Write $\phi_r = \psi^{f_r} = \psi^{|\psi G|} = \rho^{j'}\sigma^j\eta$, with $0 \le j' < |\rho|$, $0 \le j < q$ and $\eta \in B$. As above, j' is even because $f(r) > 0$. If j is odd, then $\psi^{|\psi G|} \notin \mathrm{Gal}(F/\mathbb{Q}(\zeta_{2^{d+1}}))$ and so (2) fails. Suppose now that j is even, so we have $\psi^{|\psi G|} \in \mathrm{Gal}(F/\mathbb{Q}(\zeta_{2^{d+1}}))$. Then the fact that $\beta(r) = 1$ implies by Theorem 5.13 that $|\eta B^{2^{d(r)}}| = 2$. Since $d(r) \le a = 1$, we have $d(\psi) = d(r) = 2$ and so $\eta \notin B^2$ and $\eta \notin T(\psi)$. Then $\psi^{|\psi G|} \notin \prod_{i=0}^{q-1} \sigma^i\langle\rho, T(\psi)\rangle$ and so (2) fails. □

Some obvious consequences of Theorem 6.8 are the following.

Corollary 6.22. *If $\psi^{|\psi G|} \notin \langle\sigma, \rho, T(\psi)\rangle$, for some $\psi \in \Gamma_p$, then $CC(K)_p$ does not have finite index in $S(K)_p$.*

Corollary 6.23. *If G/C is cyclic and $\nu(\psi) \ge \min\{v_p(\exp B), d(\psi)\}$ for all $\psi \in \Gamma_p$, then $CC(K)_p$ has finite index in $S(K)_p$.*

Corollary 6.24. *If G/C is cyclic and $v_p(\exp B) + v_p(\exp(\mathrm{Gal}(K/\mathbb{Q}))) \le a$ then $CC(K)_p$ has finite index in $S(K)_p$.*

Proof. If $\psi \in \Gamma_p$ then $v_p(|\psi G|) \le v_p(\exp(\mathrm{Gal}(K/\mathbb{Q}))) \le a - v_p(\exp B)$, by assumption. Therefore $\nu(\psi) = \max\{0, a - v_p(|\psi G|)\} \ge v_p(\exp B)$ and Corollary 6.23 applies. □

Example 6.25. *A simple example with $[S(K)_p : CC(K)_p] = \infty$.*

Let p and q be odd primes with $v_p(q-1) = 2$. Let K be the subextension of $L = \mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_p)$ with index p in $\mathbb{Q}(\zeta_{pq})$. Then $F = \mathbb{Q}(\zeta_{p^2q})$, $G \cong \langle\theta\rangle \times C$ is elementary abelian of order p^2, and Γ_p has an element ψ such that ψ^p generates C. Then $a = v_p(|\psi G|) = 1$ and so $\nu(\psi) = 0$ and $d(\psi) = 1$. Therefore, $T(\psi) = 1$ and hence $\langle\sigma, T(\psi)\rangle = \langle\sigma\rangle$. However, $\langle\sigma\rangle \cap C = 1$ and hence $\psi^{|\psi G|} = \psi^p \notin \langle\sigma, T(\psi)\rangle$. So it follows from Corollary 6.22 that $CC(K)_p$ has infinite index in $S(K)_p$. □

The reader may check using Theorem 6.8 that $[S(K)_p : CC(K)_p] = \infty$ for the fields K constructed by Janusz that were mentioned in Example 6.15. The same holds for the field of Example 6.16. This can be verified using the arguments in the proofs of Lemmas 4.2 and 6.4 and Proposition 6.5 in [Jan3], where it is proved that $0 = v_p(|S(K,q)|) < \beta(q)$ for all the primes q such that $q \equiv 1 \mod 16$ and r is not a square modulo q.

In all the examples shown so far, the index of $CC(K)_p$ in $S(K)_p$ is either 1 or infinity. This, together with Corollary 4.5, may lead one to believe that the quotient

group $S(K)_p/CC(K)_p$ is either trivial or infinite for every field K and every prime p. By Corollary 2.3 and Theorem 4.3, $S(K)_p/CC(K)_p$ is both finite and non-trivial if and only if $\nu(r) = \beta(r)$ for every odd prime not dividing m and $\nu(r) \neq \beta(r)$ for r either 2 or an odd prime dividing m. In the following example we show that for every odd prime p there exists a field K satisfying these conditions.

Example 6.26. *An example with $CC(K)_p \neq S(K)_p$ and $[S(K)_p : CC(K)_p] < \infty$.*

Let p be an arbitrary odd prime and let q and r be primes for which $v_p(q-1) = v_p(r-1) = 2$, $v_q(r^p - 1) = 0$, and $v_q(r^{p^2} - 1) = 1$. The existence of such primes q and r for each odd prime p is a consequence of Dirichlet's Theorem on primes in arithmetic progression. Indeed, given p and q primes with $v_p(q-1) = 2$, there is an integer k, coprime to q such that the order of k modulo q^2 is p^2. Choose a prime r for which $r \equiv k + q \mod q^2$ and $r \equiv 1 + p^2 \mod p^3$. Then p, q and r satisfy the given conditions.

Let K be the compositum of K' and K'', the unique subextensions of index p in $\mathbb{Q}(\zeta_{p^2q})/\mathbb{Q}(\zeta_{p^2})$ and $\mathbb{Q}(\zeta_{p^2r})/\mathbb{Q}(\zeta_{p^2})$ respectively. Then $m = p^2rq$, $a = 2$ and $L = \mathbb{Q}(\zeta_m) = K(\zeta_q) \otimes_K K(\zeta_r)$. Therefore, $F = \mathbb{Q}(\zeta_{p^4qr})$, and $G = \mathrm{Gal}(F/K(\zeta_{qr})) \times \mathrm{Gal}(F/K(\zeta_{p^4q})) \times \mathrm{Gal}(F/K(\zeta_{p^4r}))$. We may choose σ so that $\langle\sigma\rangle = \mathrm{Gal}(F/K(\zeta_{qr})) \cong G/C$ has order p^2. The inertia subgroup of r in G is $\mathrm{Gal}(F/K(\zeta_{p^4q}))$, which is generated by an element θ of order p. Note that $B = C$ and $v_p(\exp(\mathrm{Gal}(K/\mathbb{Q}))) = v_p(\exp B) = 1 < a = 2$. Hence K satisfies the conditions of Corollary 6.24 and so $CC(K)_p$ has finite index in $S(K)_p$.

Since $K = K' \otimes_{\mathbb{Q}(\zeta_{p^2})} K''$ and $K''/\mathbb{Q}(\zeta_{p^2})$ is totally ramified at r, we have that K'_r is the maximal unramified extension of $K_r/\mathbb{Q}_r$. It follows from $v_q(r^{p^2} - 1) = 1$ and $v_q(r^p - 1) = 0$ that $[\mathbb{Q}_r(\zeta_q) : \mathbb{Q}_r] = p^2$, and so $[K'_r : \mathbb{Q}_r] = p = f(K/\mathbb{Q}, r)$. Therefore $v_p(|W(K_r)|) = v_p(|W(\mathbb{Q}_r)|) + f(r) = v_p(r-1) + 1 = 3$, and so we have $\nu(r) = \max\{0, a + v_p(|\theta|) - v_p(|W(K_r)|)\} = 0$.

Let ψ_r be the Frobenius automorphism of r in $\mathrm{Gal}(F/\mathbb{Q})$. Then $\psi_r^p = \sigma^p\eta$, where $\eta \in B$ generates $\mathrm{Gal}(F/K(\zeta_{p^4r}))$. Since $\langle\theta\rangle \cap \langle\eta\rangle = 1$, there exists a skew pairing $\Psi : B \times B \to W(K)_p$ such that $\Psi(\theta, \eta)$ has order p. By Theorem 5.13, it follows that $\beta(r) \geq 1$, and so $S(K)_p \neq CC(K)_p$. □

We finish with an example which shows that, when G/C is noncyclic, it is possible for $CC(K)_2$ to have infinite index in $S(K)_2$ even when $t = v_2(\exp B) = 0$. It also is a counterexample to [Pen1, Theorem 2.2].

Example 6.27. An example with $[S(K)_2 : CC(K)_2] = \infty$ and $C = 1$.

Let q be an odd prime greater than 5 and set $K = \mathbb{Q}(\zeta_q, \sqrt{2})$. We compute $[S(K)_2 : CC(K)_2]$. In the notation of this section, we have $a = 2$, $m = 8q$, so $s = 3$ and $a + b = 1 + 3 + v_2([K \cap \mathbb{Q}(\zeta_{2^3}) : \mathbb{Q}]) + 2 = 6$. Hence $F = \mathbb{Q}(\zeta_{64q})$. Since $\mathbb{Q}(\zeta_q) \subset K$,

we have $C = \mathrm{Gal}(F/K(\zeta_{64})) = 1$. For our generators of $\mathrm{Gal}(F/K)$, we may choose ρ, σ such that $\rho(\zeta_q) = \zeta_q$, $\rho(\zeta_{64}) = \zeta_{64}^{-1}$, $\sigma(\zeta_q) = \zeta_q$, and $\sigma(\zeta_{64}) = \zeta_{64}^{9}$. Let r be any prime for which $r^2 \equiv 1 \mod q$ and $r \equiv 5 \mod 2^6$. Then $\psi_r \notin G$, but $5^2 \equiv 9^3 \mod 64$ implies that $\psi_r^2 = \sigma^3$. This means that we are in the case of Theorem 5.13, where $\nu(r) = 0$ and j is odd, so $\beta(r) = 1$. So $[S(K)_2 : CC(K)_2]$ is infinite. □

Notes on Chapter 6

Even if the problem of the computation of the automorphism group of group algebras and the Isomorphism Problem for group algebras of metacyclic groups do not appear explicitly as a studied topic, we gathered the main ingredients, namely the computation of the Wedderburn components of group algebras and a criterion to decide which components are isomorphic as rings. Note that the Wedderburn decomposition of a rational group algebra of a metacyclic group has been computed in [OdRS2], so the first part of the problem has been solved for metacyclic groups. The second problem, that of deciding which simple components are ring isomorphic, can be attacked using the results of the first section.

The computation of the index $[S(K) : CC(K)]$ when this is finite is more complicated than the computation of $\beta(r)$ and $\nu(r)$ and depend on a more detailed analysis of the position of K among the cyclotomic fields.

Conclusions and perspectives

The present book was mainly concerned with the computational aspect of the Wedderburn decomposition of group algebras and some of its applications, with the aim of giving explicit presentations of the Wedderburn components.

The main idea in our approach was the use of the Brauer-Witt Theorem, that gives a presentation of the simple components seen as Schur algebras over their centers as cyclotomic algebras, up to Brauer equivalence. This method led us to the necessity of finding a constructive proof of the Brauer-Witt Theorem and an algorithm to describe the Wedderburn components using it, which was studied in Chapter 2.

This theoretical algorithm allowed us to elaborate a "working" algorithm which made possible its implementation in a package called `wedderga` for the computer system GAP. This is an improvement with respect to a previous version of `wedderga`, which was only capable to compute the Wedderburn decomposition of some rational group algebras. Some aspects of the implementation were presented in Chapter 3. The numerical description of some Wedderburn components, given by the outputs of some functions of the `wedderga` package, has some limitations when identifying the simple algebras as matrices over precise division algebras. This was illustrated by examples when presenting the functionality of `wedderga`.

The main motivation for our search for an explicit computation of the Wedderburn components of group algebras was given by its applications, mainly to the study of units of group rings and automorphisms of algebras. The second part of the book presented some applications to the classification of group algebras of Kleinian type with further applications to groups of units, the characterization of ring automorphisms of simple components of rational group algebras and the study of a special subgroup of the Schur group of an abelian number field.

In Chapter 4 we presented an application of a good knowledge and description of the Wedderburn components of group algebras of finite groups over number fields. A classification of the group algebras of Kleinian type over a number field was given, continuing the work from [JPdRRZ]. Moreover, we characterized the group rings RG,

with R an order in a number field and G a finite group, such that the group of units of RG is virtually a direct product of free-by-free groups.

The information provided by our description of the Wedderburn components can be completed with extra data given by the Schur index and the Hasse invariants of the simple algebras. This requires computation of local Schur indices, a research direction followed in Chapter 5, where we characterized the maximum p-local index of a Schur algebra over an abelian number field, for p an arbitrary prime number.

In Chapter 6 we defined the notion of cyclic cyclotomic algebra, a type of algebra which was useful for our purposes. These algebras arise naturally as simple components of rational group algebras of metacyclic groups. Moreover, another reason that suggested us the study of the algebras having this cyclic and cyclotomic presentation was the fact that methods for the computation of the local Schur indices and the Hasse invariants are classically presented for cyclic algebras. The first section of this chapter was dedicated to the study of these algebras and their applications to the study of the ring isomorphism between them. In the second section we presented the subgroup generated by the cyclic cyclotomic algebras inside the Schur group and we gave a characterization of when $CC(K)$ has finite index in $S(K)$ in terms of the relative position of K in the lattice of cyclotomic extensions of the rationals.

Some further developments of this topic can be done in different directions. As we have already mentioned above, the limitations of our description of the Wedderburn components can be surpassed by a detailed study of the (local) Schur indices and the Hasse invariants. Thus, as we have already started in Chapter 5, an option for future study on this topic is to add local information obtained by local methods and which completes the previous data. New methods using G-algebras can also be used in order to compute Schur indices.

Recently, a projective version of the Brauer-Witt Theorem was given in [AdR]. More precisely, it was proved that any projective Schur algebra over a field is Brauer equivalent to a radical algebra. This can provide useful information that can be used to study a similar problem in the case of twisting group algebras, that is to describe its simple components given by projective characters of the group as radical algebras in the projective Schur group.

Another possible interesting idea to be studied is the generalization of some results from Chapter 4 to semigroup algebras, since it seems that it can be reduced to the knowledge of the Wedderburn components of some group algebras. There are also other interesting problems that rely on the description of the Wedderburn components of group algebras, such as the Isomorphism Problem or the study of error correcting codes (when the group algebra is over a finite field).

Bibliography

[AH] A.A. Albert and H. Hasse, *A determination of all normal division algebras over an algebraic number field*, Trans. Amer. Math. Soc. **34** (1932), 171–214.

[AdR] E. Aljadeff and Á. del Río, *Every projective Schur algebra is Brauer equivalent to a radical abelian algebra*, Bull. London Math. Soc., to appear.

[Ami] S.A. Amitsur, *Finite subgroups of division rings*, Trans. Amer. Math. Soc. **80** (1955), 361–386.

[AS] S.A. Amitsur and D. Saltman, *Generic abelian crossed products and p-algebras*, J. Algebra **51** (1978), 76–87.

[Ban] B. Banieqbal, *Classification of finite subgroups of* 2×2 *matrices over a division algebra of characteristic zero*, J. Algebra **119** (1988), 449–512.

[Bar] D. Bardyn, *Presentations of units of integral group rings*, Master Thesis, Vrije Universiteit Brussels, 2006.

[Bas] H. Bass, *The dirichlet unit theorem, induced characters, and Whitehead groups of finite groups*, Topology **4** (1966), 391–410.

[Bea] A.F. Beardon, *The geometry of discrete groups*, Graduate Texts in Mathematics **91**, Springer–Verlag, New York, 1983.

[Ben] M. Benard, *The Schur subgroup I*, J. Algebra **22** (1972), 374–377.

[BeS] M. Benard and M.M. Schacher, *The Schur subgroup II*, J. Algebra **22** (1972), 378–385.

[Bia] L. Bianchi, *Sui gruppi dei sustituzioni lineari con coefficienti appartenenti a corpi quadratici immaginari*, Math. Ann. **40** (1892), 332–412.

[BH] A.A. Borel and Harish Chandra, *Arithmetic Subgroups Of Algebraic Groups*, Ann. of Math. **75** (1962), 485–535.

[BoS] Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Academic Press, 1966.

[BKRS] V. Bovdi, A. Konovalov, R. Rossmanith and C. Schneider. LAGUNA – Lie AlGebras and UNits of group Algebras, Version 3.3.3; 2006 (`http://ukrgap.exponenta.ru/laguna.htm`).

[Bra1] R. Brauer, *On the representation of a group of order g in the field of the g-th roots of unity*, Amer. J. Math. **67** (1945), 461–471.

[Bra2] R. Brauer, *On the algebraic structure of group rings*, J. Math. Soc. Japan **3** (1951), 237–251.

[BHN] R. Brauer, H. Hasse and E. Noether, *Beweis eines Hauptsatzes in der Theorie der Algebren*, J. Reine Angew. Math. **167** (1932), 399–404.

[BKOOdR] O. Broche Cristo, A. Konovalov, A. Olivieri, G. Olteanu and Á. del Río, *Wedderga – Wedderburn Decomposition of Group Algebras, Version 4.0;* 2006 (`http://www.gap-system.org/Packages/wedderga.html` and `http://www.um.es/adelrio/wedderga.htm`).

[BP] O. Broche Cristo and C. Polcino Milies, *Central Idempotents in Group Algebras*, Contemp. Math. (to appear).

[BdR] O. Broche Cristo and Á. del Río, *Wedderburn decomposition of finite group algebras*, Finite Fields Appl. **13** (2007), 71–79.

[Bro] K.S. Brown, *Cohomology of Groups*, Graduate Text in Mathematics **87**, Springer–Verlag, 1982.

[CJP] S. Coelho, E. Jespers and C. Polcino Milies, *The automorphism group of the group algebra of certain metacyclic groups*, Comm. Algebra **24** (1996), 4135–4145.

[CJLdR] C. Corrales, E. Jespers, G. Leal and Á. del Río, *Presentations of the unit group of an order in a non-split quaternion algebra*, Adv. Math. **186** (2004), 498–524.

[CR] Ch.W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Wiley–Interscience, New York, 1962.

[DJ] A. Dooms and E. Jespers, *Generators for a subgroup of finite index in the unit group of an integral semigroup ring*, J. Group Theory, **7** (2004), 543–553.

[EGM] J. Elstrodt, F. Grunewald and J. Mennicke, *Groups Acting on Hyperbolic Space*, Harmonic Annalysis and Number Theory, Springer–Verlag, 1998.

[FD] B. Farb, R.K. Dennis, *Noncommutative algebra*, Graduate Texts in Mathematics **144**, Springer–Verlag, 1993.

[FGS] B. Fein, B. Gordon and J.H. Smith, *On the representation of -1 as a sum of two squares in an algebraic number field*, J. Number Theory **3** (1971), 310–315.

[FS] D.D. Fenster and J. Schwermer, *A delicate collaboration: Adrian Albert and Helmut Hasse and the Principal theorem in division algebras in the early 1930's*, Arch. Hist. Exact Sci. **59** (2005), 349–379.

[FH] K.L. Fields and I.N. Herstein, *On the Schur subgroup of the Brauer group*, J. Algebra **20** (1972), 70–71.

[GAP] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*; 2006, (`http://www.gap-system.org`).

[Gru] W. Grunwald, *Ein allgemeines Existenztheorem für algebraische Zahlkörper*, J. Reine Angew. Math. **169** (1933), 103–107.

[Has1] H. Hasse, *Theory of cyclic algebras over an algebraic number field*, Trans. Amer. Math. Soc. **34** (1932), 171–214.

[Has2] H. Hasse, *Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper*, Math. Ann. **107** (1933), 731–760.

[HP] B. Hartley and P.F. Pickel, *Free subgroups in the unit group of integral group rings*, Canad. J. Math. **32** (1980), 1342–1352.

[Her1] A. Herman, *Metabelian groups and the Brauer–Witt theorem*, Comm. Alg. **23** (1995), 4073–4086.

[Her2] A. Herman, *A constructive Brauer–Witt theorem for certain solvable groups*, Canad. J. Math. **48** (1996), 1196–1209.

[Her3] A. Herman, *On the automorphism group of rational group algebras of metacyclic groups*, Comm. Algebra **25** (1997), 2085–2097.

[Her4] A. Herman, *Using character correspondences for Schur index computations*, J. Algebra **259** (2003), 353–360.

[Her5] A. Herman, *Using G-algebras for Schur index computation*, J. Algebra **260** (2003), 463–475.

[HOdR1] A. Herman, G. Olteanu and Á. del Río, *Ring isomorphism of cyclic cyclotomic algebras*, Algebr. Repres. Theory, accepted paper.

[HOdR2] A. Herman, G. Olteanu and Á. del Río, *The Schur group of an abelian number field*, J. Pure Appl. Algebra, accepted paper. (`arXiv:0710.1026`)

[HOdR3] A. Herman, G. Olteanu and Á. del Río, *The gap between the Schur group and the subgroup generated by cyclic cyclotomic algebras*, submitted. (`arXiv:0710.1027`)

[HS] P.J. Hilton, U. Stammbach, *A Course in Homological Algebra*, 2nd ed., Graduate Text in Mathematics **4**, Springer–Verlag, 1997.

[Hum] J.E. Humphreys, *Arithmetic groups*, Lecture Notes in Mathematics **789** Springer, Berlin, 1980.

[Hup] B. Huppert, *Character Theory of Finite Groups*, de Gruyer Expositions in Mathematics **25**, Walter de Gruyer, 1998.

[Isa] I.M. Isaacs, *Character Theory of Finite Groups*, Academic Press, 1976.

[Jan1] G.J. Janusz, *Generators for the Schur Group of Local and Global Number Fields*, Pacific J. Math. **56** (1975), 525–546.

[Jan2] G.J. Janusz, *The Schur group of cyclotomic fields*, J. Number Theory **7** (1975), 345–352.

[Jan3] G.J. Janusz, *The Schur group of an algebraic number field*, Ann. of Math. **103** (1976), 253–281.

[Jan4] G.J. Janusz, *Automorphism groups of simple algebras and group algebras*, in "Representation Theory of Algebras", Philadelphia, 1976, Lecture Notes in Pure and Applied Mathematics **37**, 381–388.

[Jan5] G.J. Januzs, *Algebraic Number Field*, 2nd ed., Graduate Studies in Mathematics **7**, 1996.

[Jes] E. Jespers, *Free normal complements and the unit group in integral group rings*, Proc. Amer. Math. Soc. **122** (1994), 59–66.

[JL] E. Jespers and G. Leal *Generators of large subgroups of the unit group of integral group rings*, Manuscripta Math. **78** (1993), 303–315.

[JLPa] E. Jespers, G. Leal and A. Paques, *Central idempotents in rational group algebras of finite nilpotent groups*, J. Algebra Appl. **2** (2003), 57–62.

[JLPo] E. Jespers, G. Leal and C. Polcino Milies, *Units of integral group rings of some metacyclic groups*, Can. Math. Bull. **37** (1994), 228–237.

[JLdR] E. Jespers, G. Leal and Á. del Río, *Products of free groups in the unit group of integral group rings*, J. Algebra **180** (1996), 22–40.

[JPdRRZ] E. Jespers, A. Pita, Á. del Río, M. Ruiz and P. Zalesski, *Groups of units of integral group rings commensurable with direct products of free-by-free groups*, Adv. Math. **212** (2007), 692–722.

[JdR] E. Jespers and Á. del Río, *A structure theorem for the unit group of the integral group ring of some finite groups*, J. Reine Angew. Math. **521** (2000), 99–117.

[KS] A.V. Kelarev and P. Solé, *Error correcting codes as ideals in group rings*, Contemp. Math. **273** (2001), 11–18.

[Kle1] E. Kleinert, *A theorem on units of integral group rings*, J. Pure Appl. Algebra **49** (1987), 161–171.

[Kle2] E. Kleinert, *Units of classical orders: a survey*, L'Enseignement Mathématique **40** (1994), 205–248.

[KdR] E. Kleinert and Á. del Río, *On the indecomposability of unit groups*, Abh. Math. Sem. Univ. Hamburg **71** (2001), 291–295.

[LdR] G. Leal and Á. del Río, *Products of free groups in the unit group of integral group rings II*, J. Algebra **191** (1997), 240–251.

[LR] F. Lorenz and P. Roquette, *The theorem of Grunwald–Wang in the setting of valuation theory*, Fields Institute Communications Series **35** (2003), 175–212.

[MR] C. Maclachan and A.W. Reid, *The Arithmetic of Hyperbolic* 3*-Manifolds*, Springer–Verlag, 2002.

[Mar] D. Marcus, *Number fields*, Springer–Verlag, 1977.

[Mas] B. Maskit, *Kleinian groups*, Springer–Verlag, 1988.

[Mol] R.A. Mollin, *Algebras with uniformly distributed invariants*, J. Algebra **44** (1977), 271–282.

[Mon] S. Montgomery, *Fixed rings of finite automorphisms groups of associative rings*, LNM **818**, 1980.

[Mos] C. Moser, *Représentation de* -1 *comme somme de carrés dans un corps cyclotimique quelconque*, J. Number Theory **5** (1973), 139–141.

[Neu1] J. Neukirch, *Algebraic number theory*, Fundamental Principles of Mathematical Sciences **322**, Springer–Verlag, 1999.

[Neu2] J. Neukirch, *Cohomology of number fields*, Fundamental Principles of Mathematical Sciences **323**, Springer–Verlag, 2000.

[Oli] A. Olivieri, *Unidades Bicíclicas y Descomposición de Wedderburn de Anillos de Grupo*, Tesis Doctoral, Universidad de Murcia, Departamento de Matemáticas, 2002.

[OdR1] A. Olivieri and Á. del Río, *An algorithm to compute the primitive central idempotents and the Wedderburn decomposition of a rational group algebra*, J. Symbolic Comput. **35** (2003) 673–687.

[OdRS1] A. Olivieri, Á. del Río and J.J. Simón *On monomial characters and central idempotents of rational group algebras*, Comm. Algebra **32** (2004), 1531–1550.

[OdRS2] A. Olivieri, Á. del Río and J.J. Simón *The group of automorphisms of a rational group algebra of a finite metacyclic group*, Comm. Algebra **34** (2006), 3543–3567.

[Olt1] G. Olteanu, *El teorema de Brauer–Witt*, Publicaciones del Departamento de Matemáticas, Universidad de Murcia, Número **52**, 2005.

[Olt2] G. Olteanu, *Computing the Wedderburn decomposition of group algebras by the Brauer–Witt theorem*, Math. Comp. **76** (2007), 1073–1087.

[Olt3] G. Olteanu, *Wedderburn decomposition of group algebras. A computational approach with applications to and Schur groups and units*, Ph.D. Thesis, University of Murcia, Spain, 2007.

[Olt4] G. Olteanu, *Wedderburn decomposition of group algebras and Schur groups*, Mini-Workshop: Arithmetik von Gruppenringen, Mathematisches Forschungsinstitut Oberwolfach, Oberwolfach Report No. 55/2007.

[OdR2] G. Olteanu and Á. del Río, *An algorithm to compute the Wedderburn decomposition of semisimple group algebras implemented in the GAP package* `wedderga`, J. Symbolic Comput., accepted paper.

[OdR3] G. Olteanu and Á. del Río, *Group algebras of Kleinian type and groups of units*, J. Algebra (2007), **318** 2007, 856–870.

[Park] A. E. Parks, *A group–theoretic characterization of M-groups*, Proc. Amer. Math. Soc. **95** (1985), 209–212.

[Pars1] K.H. Parshall, *Joseph H.M. Wedderburn and the structure theory of algebras*, Arch. Hist. Exact Sci. **32** (1985), 223–349.

[Pars2] K.H. Parshall, *Defining a mathematical research school: the case of algebra at the University of Chicago, 1892–1945*, Historia Math. **31** (2004), 263–278.

[Pas1] D.S. Passman, *The algebraic structure of group rings*, Pure and Applied Mathematics, Wiley–Interscience, 1977.

[Pas2] D.S. Passman, *Infinite Crossed Products*, Pure and Applied Mathematics **135**, Academic Press, Inc., Boston, MA, 1989.

[Pen1] J.W. Pendergrass, *The* 2*-part of the Schur Group*, J. Algebra **41** (1976), 422–438.

[Pen2] J.W. Pendergrass, *The Schur subgroup of the Brauer group*, Pacific J. Math. **69** (1977), 477–499.

[Pie] R.S. Pierce, *Associative Algebras*, Graduate Texts in Mathematics **88**, Springer–Verlag, 1982.

[Pit] A. Pita, *Grupos Kleinianos, aplicación al estudio de grupos de unidades*, Tesina de Licenciatura, Universidad de Murcia, 2003.

[PdRR] A. Pita, Á. del Río and M. Ruiz, *Groups of units of integral group rings of Kleinian type*, Trans. Amer. Math. Soc. **357** (2004), 3215–3237.

[PH] V.S. Pless and W.C. Huffman, *Handbook of Coding Theory*, Elsevier, New York, 1998.

[Poi] H. Poincaré, *Mémoires sur les groups kleinéens*, Acta Math. **3** (1883) 49–92.

[Pol-Seh] C. Polcino Milies and S.K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers, 2002.

[Rei] I. Reiner, *Maximal orders*, Academic Press 1975, reprinted by LMS 2003.

[RieS] U. Riese, P. Schmid, *Schur Indices and Schur Groups, II*, J. Algebra **182** (1996), 183–200.

[dRR] Á. del Río and M. Ruiz, *Computing large direct products of free groups in integral group rings*, Comm. Algebra **30** (2002), 1751–1767.

[RitS1] J. Ritter and S.K. Sehgal, *Generators of subgroups of $\mathcal{U}(\mathbb{Z}G)$*, Representation theory, groups rings and coding theory 331–347, Contemp. Math. **93**, Amer. Math. Soc., Providence, 1989.

[RitS2] J. Ritter and S.K. Sehgal, *Construction of units in integral group rings of finite nilpotent groups*, Trans. Amer. Math. Soc. **324** (1991), 603–621.

[RitS3] J. Ritter and S.K. Sehgal, *Construction of units in integral group rings of monomial and symmetric groups*, J. Algebra **142** (1991), 511–526.

[Rob] D.J.S. Robinson, *A course in the theory of groups*, Springer–Verlag, 1982.

[Roq] P. Roquette, *The Brauer–Hasse–Noether theorem in historical perspective*, Schriften der Mathematisch–Naturwissenschaftlichen Klasse der Heidelberger Akademie der Wissenschaften [Publications of the Mathematics and Natural Sciences Section of Heidelberg Academy of Sciences] **15**, Springer–Verlag, 2005.

[Rui] M. Ruiz, *Buscando estructura en el grupo de las unidades de un anillo de grupo con coeficientes enteros*, Tesis Doctoral, Universidad de Murcia, 2002.

[Sal] D.J. Saltman, *Lectures on Division Algebras*, Regional Conference Series in Mathematics, Number **94**, 1999.

[Sch] P. Schmid, *Schur indices and Schur groups*, J. Algebra **169** (1994), 226–247.

[Seh] S.K. Sehgal, *Units of integral group rings*, Longman Scientific and Technical Essex, 1993.

[Ser] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics **67**, Springer–Verlag, 1979.

[Shi] M. Shirvani, *The structure of simple rings generated by finite metabelian groups*, J. Algebra **169** (1994), 686–712.

[SW] M. Shirvani and B.A.F. Wehrfritz, *Skew Linear Groups*, Cambridge University Press, 1986.

[Sho] K. Shoda, *Über die monomialen Darstellungen einer endlichen Gruppe*, Proc. Phys. Math. Soc. Jap. **15** (1933), 249–257.

[ST] E. Spiegel and A. Trojan, *Schur algebras and isomorphic division algebras*, Portugal. Math. **46** (1989), 189–192.

[Spi] K. Spindler, *Abstract algebra with applications*, Vol. II. Rings and Fields, Marcel Dekker, Inc., New York, 1994.

[Thu] W. Thurston, *The geometry and topology of 3-manifolds*, Lecture notes, Princeton, 1980.

[Tur] A. Turull, *Clifford theory with Schur indices*, J. Algebra **170** (1994), 661–677.

[Wan] Sh. Wang, *On Grunwald's theorem*, Ann. of Math. **51** (1950), 471–484.

[Wed1] J.H.M. Wedderburn, *On hypercomplex number systems*, Proc. London Math. Soc. **6** (1907), 77–118.

[Wed2] J.H.M. Wedderburn, *On division algebras*, Trans. Amer. Math. Soc. **22** (1921), 129–135.

[Wei1] E. Weiss, *Algebraic number theory*, Dover Publications, Inc., Mineola, NY, 1998.

[Wei2] E. Weiss, *Cohomology of Groups*, Pure and Applied Mathematics **34**, Academic Press, New York–London, 1969.

[WZ] J.S. Wilson and P.A. Zalesski, *Conjugacy separability of certain Bianchi groups and HNN-extensions*, Math. Proc. Cambridge Philos. Soc. **123** (1998), 227–242.

[Wit] E. Witt, *Die Algebraische Struktur des Gruppenringes einer Endlichen Gruppe Über einem Zahlkorper*, J. Reine Angew. Math. **190** (1952), 231–245.

[Yam] T. Yamada, *The Schur Subgroup of the Brauer Group*, Lecture Notes in Math. **397**, Springer–Verlag, 1974.

Index