Joint Ph.D. Program in Mathematics

UNIVERSITY OF MILANO-BICOCCA
Department of Mathematics and Applications

UNIVERSITY OF PAVIA
Department of Mathematics "Felice Casorati"

SCHUR INDICES OF THE ABSOLUTELY IRREDUCIBLE CHARACTERS OF SOME METACYCLIC GROUPS

Jessica Cologna

Supervisor:
Prof. Andrea Previtali
University of Milano-Bicocca

14 December 2018

Contents

Introduction

Motivation

The notion of Schur index has been introduced by Schur in 1905. Let χ be the character of an irreducible complex representation R of a finite group G. Let F be any algebraic number field. We denote by $F(\chi)$ the field extension of F obtained adjoining $\chi(g)$ for all $g \in G$. Let K be any field extension of $F(\chi)$ such that 1) R can be realized over K and 2) K has minimal degree over $F(\chi)$ with respect to this property. This minimal degree $|K : F(\chi)|$ is denoted by $s_F(\chi)$. The computation of the Schur index has been studied by many authors in the 20^{th} century, some references are [15], [11] [12], [31], [32].

Our interest in this topic arises from the investigation of computational aspects of representation theory. The problem of the construction of a representation of a finite group G affording a given character $\chi \in \mathrm{Irr}(G)$ has no trivial solution but can be approached in some different ways. One possibility is to simplify the complexity of the problem by first constructing a rational representation affording the character $s_{\mathbb{Q}}(\chi)\mathrm{GalSum}_{\mathbb{Q}}(\chi)$ (where $\mathrm{GalSum}_{\mathbb{Q}}(G)$ denotes the sum of the irreducible characters of G that are Galois conjugated to χ in the extension $\mathbb{Q}(\chi)/\mathbb{Q}$) and then decompose such a rational representation into absolutely irreducible components in order to find a suitable representation affording the given character. The complexity of this strategy increases as the Schur index grows. In particular when $s_{\mathbb{Q}}(\chi)$ is greater than 2 no general ways to apply such strategies are known. In order to study this situation we decided to find some small examples to work on. This motivated us to focus our attention on the construction of

irreducible characters with Schur index greater than 2.
A classical example of a group with irreducible characters of Schur index 3, studied also by Lam in [22], is

$$G = \langle a, b \mid a^7, b^9, a^b = a^2 \rangle.$$

This group can by obtained as a semidirect product of two cyclic groups of order 7 and 9, respectively. We decided to investigate whether such a structure can be generalized to obtain other examples of characters with Schur index greather than 2.

Outline

Let p and q be two odd primes such that $p \equiv 1 \mod q^m$ for some positive integer m, where q^m is the maximal power of q w.r.t. this property. In this thesis we study metacyclic groups of the form $G \cong C_p \rtimes_\varphi C_{q^k}$ for some integer k, where the action of C_{q^k} on C_p depends on a parameter l such that $|\varphi(C_{q^k})| = q^l$. From our analysis it arises that any irreducible character of these groups is either linear or it is obtained by induction to G from a faithful character of the abelian subgroup $C_p \times Z(G)$ of G, which has index q^l. As a consequence, non linear characters of G have degree q^l.
Classical results help us to bound the possible values that the Schur index of these non linear character may attain. Let $\chi \in \mathrm{Irr}(G)$ such that $\chi(1) = q^l$ then $s_{\mathbb{Q}}(\chi)\big|\chi(1)$ [19, 10.2], $s_{\mathbb{Q}}(\chi)^2\big||G|$ [10], $s_{\mathbb{Q}}(\chi)\chi(1)\big||G|$ [11].
Let $\psi \in \mathrm{Irr}(C_p \times Z(G))$ be such that $\chi = \psi^G$. Then there is a representation R of G over $\mathbb{Q}(\psi)$ affording χ. We ask if there exists any subfield K of $\mathbb{Q}(\psi)$ with $|K : \mathbb{Q}(\chi)| = s_{\mathbb{Q}}(\chi)$ such that there is a K-representation of G similar to R.
In [17] and [13] a method to find a minimal field for a representation is described. If $X \in \mathrm{GL}_{q^l}(\mathbb{Q}(\psi))$ such that $X^{-1}R(g)X = R(g)^\sigma$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q})$ and for all $g \in G$, then $XX^\tau..X^{\tau^{q^l-1}} = \mu I_{q^l}$ for some μ contained in the subfield K of $\mathbb{Q}(\psi)$ fixed by σ. The representation R is similar to a K-representation if and only if the norm equation $N_{\mathbb{Q}(\psi)/K}(\theta) = \mu$ has a solution. Algebraic number theory provides a way of determinate whether this norm equation is solvable. In our case, the field extension $\mathbb{Q}(\psi)/K$ is a cyclic extension, thus we can use the Hasse Norm Theorem

[26, VI,4.5] and move our problem from global to local norm equations. In particular, the problem to determinate for which subfields K of $\mathbb{Q}(\psi)$ the norm equation is solvable is reduced to the problem to understand when a unique local norm equation has solution. In this thesis we prove for which fields the norm equation is solvable. This allow us to conclude that, in the family of groups we have studied, a stronger bound for the Schur index holds, that is $s_{\mathbb{Q}}(\chi)\big|q^{k-m}$.

In the last chapter of the thesis we discuss the problem of the construction of an absolutely irreducible module affording a given character in the case of Schur index equal 2 and 3. In the first case the problem is reduced to the one of finding a singular element in a quaternion algebra and it can be solved using algorithms due to A. Steel [30] and J. Voight [33]. The situation is more complicated when the Schur index is equal 3 because Dickson algebras are involved and it is necessary to solve an homogeneous quadratic equation in eight variables over a number field.

Notation

$\mathbb{N}$:	the set $\{1, 2, 3, ..\}$
$\mathrm{Irr}_F(G)$:	the set of irreducible characters of a group G over a field F
$\mathrm{Irr}(G)$:	the set of irreducible characters of a group G over $\mathbb{C}$
$\mathrm{Hom}_{FG}(M, N)$:	the group of homorphisms from an FG-module M to N
$\mathrm{End}_{FG}(M)$:	$\mathrm{Hom}_{FG}(M, M)$
$F(\chi)$:	$F\left(\{\chi(g) \ : \ g \in G\}\right)$
$\mathrm{GalSum}_F(\chi)$:	the sum of characters Galois conjugate to χ in $F(\chi)/F$
$s_F(\chi)$:	the Schur index of $\chi \in \mathrm{Irr}(G)$ over a field F
$\mathcal{O}_F$:	the ring of algebraic integers of a number field F
K/F :	K is a field extension of F
$\mathrm{Gal}(K/F)$:	the Galois group of K/F, when K/F is a Galois extension
$\mathrm{Fix}(\sigma)$:	the subfield of K fixed by the subgroup of $\mathrm{Gal}(K/F)$ generated by σ
$e(w/v)$:	the ramification index of a prime ideal w above v
$\mathbb{F}_v$:	the residue field $\mathcal{O}_F/v$
$\mathcal{O}_v^*$:	the group of units of $\mathcal{O}_v$
U_v :	the subgroup of principal units of $\mathcal{O}_v^*$
ζ_n :	a primitive n^{th}-root of unity

Chapter 1

Preliminaries

In this chapter we introduce some basic definitions and results about representation theory which will be strongly used in the rest of the thesis. For those who are familiar with the topic this chapter may be useful in order to fix the notation. For a more complete overview of the topic see [3], [7], [18] and [19].

1.1 Representations, Modules and Characters

Definition 1.1.1. Let G be a group and let F be a field. A *representation* of G over F (or F-representation) is an homomorphism $R : G \longrightarrow \mathrm{GL}_n(F)$, where n is said to be the *degree* of R.

Representations are a very strong tool in group theory because they allow to deal with groups in a concrete way and to study group's proprieties through them.

Definition 1.1.2. Let G be a finite group, F be a field and R be an F-representation of G. The map $\chi : G \longrightarrow F$ defied by $\chi(g) = \mathrm{Tr}(R(g))$ is the *character* of G afforded by R.

It is possible that different F-representations afford the same character, in particular two F-representations R and S of degree n afford the same character if and only if they are similar, that is there exists a matrix $P \in \mathrm{GL}_n(F)$ such that $PR(g) = S(g)P$ for all $g \in G$.

We denote by FG the group algebra of G over the field F. For every F-representation R of G of degree n it is possible to construct an FG-module considering the n-dimensional row vector space M over F where the action of G over M is defined by $g \cdot m = R(g)m$ for every $m \in M$ and $g \in G$. Extending linearly this action to FG we get an FG-module. On the other hand, let M be an n-dimensional FG-module and choose a basis $\mathcal{B}$ of M. For every $g \in G$ it possible to define an homomorphism $\cdot_g : M \longrightarrow M$ such that $\cdot_g(m) = g \cdot m$ for every $m \in M$. As a consequence, for every $g \in G$ there is a matrix $R_g \in \mathrm{GL}_n(F)$ associated to $\cdot_g$ with respect to the basis $\mathcal{B}$. Then $R : G \longrightarrow \mathrm{GL}_n(F)$ defined by $R(g) = R_g$ is a F-representation of G. A classical result in representation theory says that there is a 1-to-1 correspondence between F-representations of G and FG-modules, given by the shown correspondence.

Definition 1.1.3. Let R be a F-representation of G. It is said to be *irreducible* if and only if its associated FG-module M is irreducible, i.e. its only submodules are 0 and M. If so, also the character afforded by R is said to be an irreducible character.

We denote by $\mathrm{Irr}_F(G)$ the set of all irreducible characters afforded by an F-representation of G and by $\mathrm{Irr}(G)$ the set $\mathrm{Irr}_{\mathbb{C}}(G)$. It is a classical result that $|\mathrm{Irr}(G)|$ is equal to the number of conjugacy classes of G.

Let M and N be FG-modules. We denote by $\mathrm{Hom}_{FG}(M, N)$ the set of all linear transformation $\varphi : M \longrightarrow N$ such that $\varphi(x \cdot m) = x \cdot \varphi(m)$ for all $x \in FG$ and $m \in M$. We also denote by $\mathrm{End}_{FG}(M) = \mathrm{Hom}_{FG}(M, M)$ and we call it *endomorphism algebra* of M, $\mathrm{End}_{FG}(M)$ is an F-algebra.

Lemma 1.1.1. *(Schur) Let M and N be irreducible FG-modules. If $M \ncong N$ then* $\mathrm{Hom}_{FG}(M, N) = 0$*, while* $\mathrm{Hom}_{FG}(M, M) = End_{FG}(M)$ *is a division algebra.*

Theorem 1.1.1. *(Maschke) Let G be a finite group and F be field such that its characteristic does not divide the order of G. Then every FG-module is completely reducible (i.e. it is isomorphic to the direct sum of irreducible FG-modules).*

Let M be an FG-module, where F is a characteristic zero field. Then, by Maschke theorem, $M \cong M_1 \oplus M_2 \oplus .. \oplus M_t$ for some irreducible FG-modules $M_1, M_2, .., M_t$. It may also happen that some of these irreducible components are isomorphic within each other, so it is also possible to write M as the direct sum of FG-modules $H_1 \oplus H_2 \oplus .. \oplus H_{t'}$, where each of the H_i components is isomorphic to the direct sum of irreducible isomorphic FG-modules. Such modules H_i are called *homogeneous components* of M.

Among the FG-modules there is a particular one: FG itself, it is called the *regular module*. If the characteristic of F is not a divisor of $|G|$ then, by Maschke theorem, it is a completely reducible module. When an algebra A satisfies the property of being completely irreducible as a module, like FG does, than the algebra is said to be *semisimple*. It is also possible to say something more about the irreducible components of FG:

Proposition 1.1.1. *Let G be a finite group and F a field such that its characteristic does not divide $|G|$. Every irreducible FG-module is isomorphic to a submodule of the regular module FG.*

1.2 Splitting Fields and Character Fields

If R is an F-representation of degree n of a group G and E is a field extension of F then $R(g) \in \mathrm{GL}_n(F) \subseteq \mathrm{GL}_n(E)$, hence R can be seen as an E-representation. In this case we denote it by R^E. If R is an irreducible representation then R^E may not be irreducible.

Definition 1.2.1. Let R be an irreducible F-representation of a group G. If R^E is an irreducible representation for every field extension E of F then R is said to be *absolutely irreducible*.

Definition 1.2.2. A field E is said to be a *splitting field* for G if every irreducible representation of G over E is absolutely irreducible.

Splitting fields for a finite group G are far from being unique. Considering representations over a splitting field is a guarantee that irreducibility will not be lost if we extend our working field. As a consequence, if E is a characteristic zero splitting field for G then $\mathrm{Irr}_E(G) \subseteq \mathrm{Irr}(G)$. But also something stronger is true:

Proposition 1.2.1 (9.11 in [19])**.** *Let $E \subseteq \mathbb{C}$ be a subfield containing $\mathbb{Q}$. It is a splitting field for G if and only if every $\chi \in \mathrm{Irr}(G)$ is afforded by a E-representation of G.*

As a consequence, if E is a characteristic zero splitting field for G then $\mathrm{Irr}_E(G) = \mathrm{Irr}(G)$ and every irreducible $\mathbb{C}$-representation of G is similar to an (absolutely) irreducible E-representation. It follows that, when we are interested in studying representations of a finite group G over the complex number field, we can restrict our working field to any splitting field for G without loosing any information.

Definition 1.2.3. Let G be a finite group, E a splitting field for G, F a subfield of E and $\chi \in \mathrm{Irr}_E(G)$. The minimal subfield of E containing F and $\chi(g)$ for all $g \in G$ is said to be the *character field* of χ over F and it is denoted by $F(\chi)$.

When the field F in the previous definition is the field of rational numbers $\mathbb{Q}$ we refer to $\mathbb{Q}(\chi)$ simply as the character field of χ. In this case $F(\chi)$ is always a subfield of the complex number field independently from the splitting field E.
The character field over some field F of a character χ is a finite degree extension of F, because of the finiteness of G. We need to pay attention about the fact that in general it is not true that there exists an $F(\chi)$-representation of G which affords the character χ. If a field extension K of F is such that there exists a K-representation of G affording χ then it must satisfy $F(\chi) \subseteq K$. Moreover, since we are dealing with finite groups we can say that there is an extension of F of finite degree with such a property.

Definition 1.2.4. Let E be a splitting field for G, F a subfield of E and $\chi \in \mathrm{Irr}_E(G)$. A field K such that $F(\chi) \subseteq K \subseteq E$ is a *minimal field* for χ over F if there exists a K-representation of G affording χ and K has minimal degree over F for such a property.

When the field F is the rational number field we refer to a minimal field of χ over $\mathbb{Q}$ simply as a minimal number field of χ. As we noted above a minimal field K of χ over F is a finite degree extension of $F(\chi)$, hence $|K : F(\chi)| = s$ for some integer s. We would like to have some information about the degree s, some kind of measure of how much one should extend the character field to construct a representation which afford χ.

Let E be a splitting field of a group G containing F as a subfield. Let R be an E-representation of G of degree n and character χ such that $R(g) \in \mathrm{GL}_n(F)$ for all $g \in G$, where F is not necessary a minimal field for

χ over F. If R is irreducible as E-representation then it is irreducible also as F-representation. As a consequence $\chi \in \mathrm{Irr}_F(G)$. Minimal number fields of characters over any field are not unique and there are no standard way to choose one or another.

1.3 Galois conjugation

Starting from an irreducible character $\chi \in \mathrm{Irr}_E(G)$ over a splitting field E of G it is possible to construct other irreducible characters of G.

Proposition 1.3.1 (9.16 in [19]). *Let $\chi \in \mathrm{Irr}_E(G)$ and let F be a subfield of the splitting field E such that $F(\chi) = F$. For every $\tau \in \mathrm{Aut}(F)$ it holds $\chi^\tau \in \mathrm{Irr}_E(G)$.*

The Galois group $\mathrm{Gal}(F(\chi)/F)$ is an abelian finite group because $F(\chi)$ is contained in a cyclotomic extension of F thus, by Webber-Kronecker Theorem, it is an abelian extension of F.
Considering the implications of the previous proposition, it is natural to define an equivalence relation on the set $\mathrm{Irr}_E(\chi)$.

Definition 1.3.1. Let E be a splitting field for G and F be a subfield of E. Two irreducible characters $\chi, \psi \in \mathrm{Irr}_E(G)$ are *Galois conjugated* over F if $F(\chi) = F(\psi)$ and there exists $\tau \in \mathrm{Gal}(F(\chi)/F))$ such that $\chi^\tau = \psi$.

We denote by $\mathrm{GalOrb}_F(\chi)$ the equivalence class of χ and by $\mathrm{GalSum}_F(\chi)$ the sum of all the characters contained in $\mathrm{GalOrb}_F(\chi)$.

Proposition 1.3.2 (9.17 in [19]). *Let E be a splitting field for G and let F be a subfield of E. Then $|\mathrm{GalOrb}(\chi)| = |F(\chi) : F|$.*

Chapter 2

The Schur Index

In 1905 Schur studied the problem that appear considering representations over any field. What he found out is that a special number appears when dealing with these fields.
The aim of this chapter is to introduce the notion of Schur index, introduced by Schur, and to discuss some important results that concern it. In this chapter G will always denote a finite group.

2.1 Schur Index

Let E be a splitting field for a group G and let M be an irreducible EG-module of dimension d. For any subfield F of E such that $|E : F| < \infty$ it is possible to construct an FG-module M' in this way: let $e_1, e_2, .., e_n$ be a basis of E over F and $m_1, m_2, .., m_d$ be a basis of M over E, then M' is the FG-module generated as F-space by $e_1m_1, .., e_1m_d, .., e_nm_1, .., e_nm_d$.
If we consider representations R and S afforded by M and M' respectively then we have $\deg S = \dim M' = nd = n \dim M = n \deg R$.

Example 2.1.1. Let $Q_8 = \langle a, b \mid a^2 = b^2, a^b = a^{-1} \rangle$ be the quaternion group and let $R : G \longrightarrow GL_2(\mathbb{Q}(i))$ given by $R(a) = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$ and $R(b) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Let M be the $\mathbb{Q}(i)G$-module associated to R and m_1, m_2 be a basis for M over $\mathbb{Q}(i)$. Then M' is the $\mathbb{Q}G$-module generated by the basis m_1, m_2, m_1i, m_2i and the corresponding representation is $S : G \longrightarrow GL_4(\mathbb{Q})$ such that $S(a) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$ and $S(b) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$. Both R

and S are irreducible. Let $E = \mathbb{Q}(\varepsilon)$ with $\varepsilon^2 = 1$. Then $M' \otimes_{\mathbb{Q}} E$ is a EG-module. Notice that $S(a) - \varepsilon I_4$ is a zero divisor, hence $M' \otimes_{\mathbb{Q}} E$ is reducible.

In order to simplify the notation we denote M' by M, specifying when it is viewed as an FG-module or an EG-module.

Lemma 2.1.1. *[19, 9.18] Let E be a splitting field for a group G and $F \subseteq E$ be a subfield of E such that $|E : F| = n < \infty$. Let M be an irreducible EG-module, R and S its corresponding representations over E and F, respectively, χ the character afforded by R. Then*

1. *$S \cong \rho \oplus ... \oplus \rho$ where ρ is an irreducible F-representation and R is the unique (up to isomorphism) constituent of ρ^E;*
2. *if $F(\chi) = F$ then $n\chi$ is the character afforded by S.*

As an immediate consequence, for any irreducible F-representation ρ such that R is an irreducible constituent of ρ^E, it holds that $\deg \rho$ divides $n \deg R$.

Lemma 2.1.2. *[19, 9.20] Let E be a splitting field for a group G and $F \subseteq E$ be a subfield of E (not necessary of finite degree), R an irreducible E-representation of G affording χ. Then*

1. *there exists an irreducible F-representation ρ such that R is the unique (up to isomorphism) constituent of ρ^E;*
2. *the character afforded by ρ is $s\chi$ for some integer s. If $|E : F| < \infty$ then s is a divisor of $|E : F|$.*

From Lemma 2.1.2 it follows that for any irreducible E-representation R we can always find an irreducible F-representation ρ such that $\rho^E \cong R \oplus ... \oplus R$ and the multiplicity of R as a constituent of ρ^E does not depend on the choice of ρ. So we are enticed to give the following definition:

Definition 2.1.1. Let E be a splitting field for G, F be a subfield of E and $\chi \in \mathrm{Irr}_E(G)$. Let R be an irreducible E-representation of G affording χ and let ρ be an irreducible F-representation such that R is an irreducible component of ρ^E. The multiplicity of R in ρ^E is called *Schur index* of χ over F and it is denoted by $s_F(\chi)$.

From Lemma 2.1.2 we can also prove the following theorem:

Theorem 2.1.1. *[19, 9.21] Let E be splitting field for G and F be a subfield of E. Let ρ be an irreducible F-representation of G. Then*

1. *the irreducible constituents of ρ^E all occur with equal multiplicity s;*
2. *if E has prime characteristic then $s = 1$;*
3. *let $\{\chi_i\} \subseteq \mathrm{Irr}_E(G)$ be the set of characters afforded by the irreducible constituents of ρ^E. It holds $\{\chi_i\} = \mathrm{GalOrb}_F(\chi)$, for some $\chi \in \mathrm{Irr}_E(G)$;*
4. *the irreducible constituents of $\rho^{F(\chi_i)}$ occur all with multiplicity 1;*
5. *if $\tilde{\rho}$ is any irreducible constituent of $\rho^{F(\chi_i)}$ then $\tilde{\rho}^E$ has a unique irreducible constituent, which has multiplicity 1.*

From *2.* in the previous theorem it follows that Schur indices in prime characteristic are not interesting. For this reason, from now on, we will focus our attention on the characteristic zero case.

Important properties about Schur indices are given by:

Proposition 2.1.1. *[19, 10.2,10.17] Let F be a subfield of $\mathbb{C}$ and $\chi \in \mathrm{Irr}(G)$. Then*

1. *$s_F(\chi) = s_{F(\chi)}(\chi)$;*
2. *$s_F(\chi)$ is the smallest integer s such that $s\chi \in \mathrm{Irr}_{F(\chi)}(G)$;*
3. *$s_F(\chi)\mathrm{GalSum}_F(\chi)$ is a character afforded by an irreducible F-representation of G;*
4. *there exists a field E such that $F(\chi) \subseteq E \subseteq \mathbb{C}$ with $|E : F(\chi)| = s_F(\chi)$ and such that χ is afforded by an irreducible E-representation of G.*

In literature assertion *2.* of the previous proposition is often used as definition for the Schur index. It has been used by Frobenius for the first time and it is completely equivalent to the one we use.

Particularly interesting for us is the last part of the proposition. It gives us a "measure" of how far one has to move from the character field of a given character to have a field big enough to construct a representation of G which affords the given character. Hence, a minimal field K for a character $\chi \in \mathrm{Irr}(G)$ over a field F must satisfy $|K : F(\chi)| \leq s_F(\chi)$. On the other hand $s_F(\chi)$ is the smallest integer such that there exists a representation of G over $F(\chi)$ affording $s_F(\chi)\chi$ so, by Lemma 2.1.2, we have that $|K : F(\chi)|$ is a multiple of $s_F(\chi)$. This allow us to conclude that a minimal field for χ over F must have exactly degree $s_F(\chi)$ over $F(\chi)$. In general, obviously, this is not a sufficient condition.

2.2 Index of Algebras

Every algebra A is an A-module itself with the action given by the multiplication. Such an A-module is called *regular*. An algebra A is said to be *semisimple* if it is completely reducible as A-module.
A classical result due to Wedderburn asserts that:

Theorem 2.2.1. *(Wedderburn) [27, Theorem 3.5] Let A be a finite dimension semisimple algebra over the field F. Then $A \cong M_{m_1}(D_i) \oplus ... \oplus M_{m_t}(D_t)$ for some positive integers $m_1, .., m_t$ and some division algebras $D_1, .., D_t$ over F.*

Let F be any field. A *central simple algebra* over F is an F-algebra A without non-trivial two-side ideals and with center $Z(A) = F$.
As a corollary of Wedderburn's Theorem we have:

Theorem 2.2.2. *Let A be a central simple algebra over the field F. Then there exist a division algebra D with center $Z(D) = F$ and a positive integer n such that $A \cong M_n(D)$.*

Let A and B be central simple algebras over a field F. They are said to be *Brauer equivalent* if and only if there exists a division algebra D over F and two positive integers n and m such that $A \cong M_n(D)$ and $B \cong M_m(D)$. Denote by $\mathfrak{B}(F)$ the set of all the equivalence classes of Brauer equivalent central simple algebras over F. For any field F, $\mathfrak{B}(F)$ form an abelian group, named Brauer group, with respect to multiplication induced by the tensor product. Each element of the Brauer group can be identified with the division algebra over F that realizes the equivalence, that is the division algebra announced in Wedderburn's theorem.

Theorem 2.2.3. *(Corollary 13.1a in [27]) Let A be a central simple algebra over the field F. Then there exists a positive integer s such that $\dim_F A = s^2$ and for any extension field K of F contained in A, $|K : F|$ is a divisor of s.*

The integer s is said to be the *degree* of A over F and it is denoted by $\deg(A)$. Let A be a central simple algebra over F and D be the division algebra that satisfies Wedderburn's theorem (or equivalently the division algebra Brauer equivalent to A). Since division algebras are central simple algebras over their center, then the previous theorem holds also for D, if considered as an algebra over its center $Z(D)$. The positive integer s such that $\dim_{Z(D)}(D) = s^2$ is called the *Schur index* of the central simple algebra A, and it is usually denote by $\mathrm{ind}(A)$. Notice that the Schur index of central simple algebras is invariant under Brauer equivalence, because it depends only on the division algebra D and not on the representative element of the equivalence class of the Brauer group.

How is the definition of Schur index of a central simple algebra related to the one of Schur index of an absolutely irreducible character of a finite group G? In the remaining part of this section we will give an answer to this question.

When the hypotheses of Maschke's theorem are satisfied it is possible, from the decomposition of a module in its irreducible components, to know the structure of the endomorphism algebra of the module, using Wedderburn's theorem.

Theorem 2.2.4. *[3, 1.3.4] Let G be finite group and F be a characteristic zero field. Let M be an FG-module, $H_1, .., H_t$ be its homogeneous components and $S_1, .., S_t$ be irreducible FG-modules such that each $H_i \cong m_i S_i$ for some positive integer m_i. Then, for every $i = 1, .., t$, $D_i = \mathrm{End}_{FG}(S_i)$ is a division algebra, $\mathrm{End}_{FG}(H_i) \cong M_{m_i}(D)$ and $\mathrm{End}_{FG}(M) \cong \oplus_{i=1}^{t} M_{m_i}(D_i)$.*

Let $H_1, .., H_t$ be the homogeneous components of the regular module, $S_1, .., S_t$ be its irreducible components such that $H_i = m_i S_i$ for some positive integer m_i. Then $FG \cong M_{m_1}(D_1) \oplus ... \oplus M_{m_t}(D_t)$ where for each $1 \leq i \leq t$ we have $D_i = \mathrm{End}_{FG}(S_i)$. Let M be an irreducible FG-module, by Proposition 1.1.1 it is isomorphic to S_i for some i, and $D_i = \mathrm{End}_{FG}(M)$. We refer to

$M_{m_i}(D_i)$ as the matrix algebra associated to M (or equivalently to H_i) in the Wedderburn decomposition of FG.

Proposition 2.2.1. *[18, 37.2,37.3] Let G be a finite group and E a splitting field for G. Then $EG \cong \oplus_{i=1}^{t} M_{m_i}(E)$ and $\mathrm{End}_{EG}(M) = E$ for every (absolutely) irreducible EG-module M.*

Let E be a splitting field of G and F a subfield of E. Let M be an irreducible EG-module with character χ. We have seen in Proposition 2.1.1 that $s_F(\chi)\mathrm{GalSum}(\chi)$ is the character afforded by an irreducible FG-module N. Let $M_m(D)$ be the matrix algebra associated to N in the Wedderburn decomposition of FG. Notice that this process does not depend on the choice of N (every irreducible FG-module affording $s_F(\chi)\mathrm{GalSum}(\chi)$ is isomorphic to N so it is associated to the same matrix algebra as N is). As a consequence we can associate to each absolutely irreducible EG-module a matrix algebra in the Wedderburn decomposition of EG and a matrix algebra in the Wedderburn decomposition of FG, both in a unique way.
Another way to look at this association is to think about the representation R associated to the EG-module M as a homomorphism from EG onto $M_{\chi(1)}(E)$. Since $EG \cong FG \otimes_F E \cong \oplus_{i=1}^{t} M_{m_i}(D_i) \otimes_F E$, as a consequence each $R(M_{m_i}(D_i)) \neq 0$ if and only if $M_{m_i}(D_i) \otimes_F E \cong M_{\chi(1)}(E)$ and such a condition is satisfied for exactly one i.

Theorem 2.2.5. *[18, 38.15] Let G be a finite group, F any characteristic zero field and E a splitting field for G, containing F. Let R be an absolutely irreducible E-representation of G with EG-module M and character χ. Let $M_m(D)$ be the matrix algebra in the Wedderburn decomposition of FG such that $R(M_m(D)) \neq 0$, where m is a positive integer and D is a division algebra over F. Then $Z(M_m(D)) \cong Z(D) \cong F(\chi)$ and $s_F(\chi) = \sqrt{\mathrm{dim}_{Z(D)}(D)} = \mathrm{ind}(D)$.*

If we consider an irreducible F-representation ρ in the statement of the previous theorem then for each of its absolute irreducible components (that are the irreducible components of ρ^E) the theorem can be applied and in this case the division algebra D announced in the statement of the theorem is $\mathrm{End}_{FG}(\rho)$. Note that this implies that the Schur indices of conjugate characters are equal, and we already know this to be true.

Definition 2.2.1. Let A be a central simple algebra over F. A field extension K of F is said to be a *splitting field* for A if $A \otimes_F K \cong M_n(K)$ where $n = \deg A$.

A splitting field K for a central simple algebra A is far from being unique, for example any field extension of a splitting field for A is a splitting field. Moreover it is not necessarily contained in A. If we consider a field extension K of F contained in A we have that $|K : F|$ is a divisor of $\deg A$ by Theorem 2.2.3. We say that K is a *strictly maximal subfield* of A if $|K : F| = \deg A$.

Theorem 2.2.6. *Let A be a central simple algebra over F and K be a field extension of F such that $|K : F| = \deg A$. Then K is a splitting field for A if and only if K is isomorphic to a strictly maximal subfield of A as F-algebra.*

Let H be an irreducible $F(\chi)G$-module affording $s_F(\chi)\chi$. The correspondence between Schur indices of absolutely irreducible characters and Schur indices of algebras allows us to conclude that $\mathrm{End}_{F(\chi)G}(H)$ is a division algebra over its center $Z \cong F(\chi)$ and $\mathrm{ind}(\mathrm{End}_{F(\chi)G}(H)) = s_F(\chi)$. The following diagram summarizes the situation:

$$\begin{tikzcd}
\mathrm{End}_{F(\chi)G}(H) \arrow[d, dash, "s_F(\chi)"'] \\
K \arrow[d, dash, "s_F(\chi)"'] \\
F(\chi)
\end{tikzcd}$$

where K is a splitting field for the algebra $\mathrm{End}_{F(\chi)G}(H)$. Moreover,

$$\mathrm{End}_K(H \otimes_{F(\chi)} K) \cong \mathrm{End}_{F(\chi)G}(H) \otimes_{F(\chi)} K \cong M_{s_F(\chi)}(K).$$

If $s_F(\chi) \neq 1$ the matrix algebra $M_{s_F(\chi)}(K)$ is not a division algebra, hence $H^K = H \otimes_{F(\chi)} K$ is a reducible KG-module and its irreducible components are KG-modules affording χ. This proves that a splitting field for the algebra $\mathrm{End}_{F(\chi)G}(H)$ is such that there exists an irreducible K-representation of G affording character χ. In particular when K has degree $s_F(\chi)$ (that is the case when K is isomorphic to a strictly maximal subfield of $\mathrm{End}_{F(\chi)G}(H)$) then it is a minimal field for χ over F.

2.3 Important properties

The aim of this section is to create a brief survey about results concerning the Schur index. Most of these results are consequences of deep results in number theory, their proofs does not give us additional tools useful for our purpose so we do not describe them.

Lemma 2.3.1. *[19, 10.2] Let G be a finite group and F be any subfield of $\mathbb{C}$. For every $\chi \in \mathrm{Irr}(G)$ it holds $s_F(\chi)$ divides $\chi(1)$.*

Even if this lemma is not particularly difficult to prove, it is a very strong bound for the possible values that the index can assume.
A trivial consequence is that any linear character has trivial Schur index. However, this is obvious because any linear character is afforded by a 1-dimensional representation over the character field itself.

Proposition 2.3.1. *(Feit) [11] Let G be a finite group and F be any subfield of $\mathbb{C}$. For every $\chi \in \mathrm{Irr}(G)$ it holds $s_F(\chi)\chi(1)$ divides $|G|$.*

We now introduce as a corollary of this two results a theorem of Fein and Yamada that has been proved before Feit's result.

Theorem 2.3.1. *(Fein-Yamada) [10] Let G be a finite group and F be any subfield of $\mathbb{C}$. For every $\chi \in \mathrm{Irr}(G)$ it holds $s_F(\chi)^2$ divides $|G|$.*

If we are interested in understanding whether and when some integer can occur as a Schur index of a character of some finite group then the following theorem gives us the answer.

Theorem 2.3.2. *(Brauer) [4] For every integer $s \in \mathbb{N}_{>0}$ there exists a finite group G and a field F such that $s = s_F(\chi)$ for some $\chi \in \mathrm{Irr}(G)$.*

So every integer can occur as a Schur index. Anyway, many results shows that most of the times Schur indices have values 1 or 2. The construction of examples of characters with Schur index greater then 2 is not a trivial problem and it has been solved by Brauer in his paper using metacyclic groups. A special situation of what he has shown can be seen by the following:

Proposition 2.3.2. *[19, 10.16] Let p and s be prime integers such that the maximal power of p dividing $s-1$ is 1. Let $G = H \rtimes T$ where H is a cyclic group of order sp, $T \ntrianglelefteq G$ and $|G| = ps^2$. Then there exists $\chi \in \mathrm{Irr}(G)$ such that $s_{\mathbb{Q}}(\chi) = s$.*

A very strong result of Benard and Schacher gives us information about the character field starting from the Schur index.

Theorem 2.3.3. *([2]) Let G be a finite group, $\chi \in \mathrm{Irr}(G)$ and F a characteristic zero field. Then in $F(\chi)$ there is a primitive $s_F(\chi)$-root of unity.*

Since the Schur index tells us how much we need to extend the character field to obtain a field big enough to construct the representation related to the character, it also gives us some information about the splitting fields of the group. An important result in this direction is the Brauer's theorem on splitting fields:

Theorem 2.3.4. *[19, 10.3] Let G be a finite field of exponent n and let ζ_n be a primitive n^{th}-root of unity. Then $\mathbb{Q}(\zeta_n)$ is a splitting field for G.*

Schur indices are also related to norm equations. A very strong connection between these two mathematical objects has been observed by Springer (in a seminar with Cohen), it was picked up by Glasby and Howlett in [17] (as well as by Plesken and Brückner). In [13], Fieker showed that it actually works over number fields. Before going into the details we need to introduce some notation. Given a matrix X with entries in a field K and an automorphism $\sigma \in \mathrm{Aut}(K)$, we denote by X^σ the matrix obtained by applying σ to each entry of X. Moreover we define a norm function as $N(X) = XX^\sigma X^{\sigma^2}..X^{\sigma^{s-1}}$, where s is the order of σ.
Given a representation R of a group G over a number field K and an automorphism $\sigma \in \mathrm{Aut}(K)$, if there exists a matrix $X \in \mathrm{GL}_n(K)$ such that $X^{-1}R(g)X = R(g)^\sigma$ for all $g \in G$ then $N(X)$ is a scalar matrix, hence $N(x) = \mu I_n$ for some $\mu \in \mathrm{Fix}(\sigma)$.
Using the matrix version of Hilbert's Theorem 90 it is possible to prove the following:

Theorem 2.3.5. *[13, Theorem 3] Let R be a representation of a finite group G over a number field K. Let $\sigma \in \mathrm{Aut}(K)$ and $F = \mathrm{Fix}(\sigma)$. Suppose that there exists a matrix $X \in \mathrm{GL}_n(K)$ such that $X^{-1}R(g)X = R(g)^\sigma$ for all $g \in G$ and let μ be such that $N(X) = \mu I_n$. Then R is equivalent to an F-representation of G if and only if there exists some $x \in K$ such that $N_{K/F}(x) = \mu$.*

This result can be used as a tool to calculate the Schur index of a given character. When we have an absolutely irreducible representation over a field

K which affords the character χ, if we are able to find the minimal degree extension F of the character field of χ contained in K such that Theorem 2.3.5 is satisfied, then we can say that $s_{\mathbb{Q}}(\chi) \leq |F : \mathbb{Q}(\chi)|$. Anyway we need to pay attention to the fact that equality may not hold. Indeed, it may happen that no minimal field for χ is contained in a given splitting field. An example for this can be found in [18].

Example 2.3.1. Let Q_8 be the quaternion group. A field K is a splitting field for Q_8 if and only if there exist $a, b \in K$ such that $a^2 + b^2 = -1$. Let p be a prime and $r \geq 1$ such that $2^r + 1 = ps$ for some $s \in \mathbb{N}$. Let ζ_p be a primitive p^{th}-root of unity and $\mathbb{Q}(\zeta_p)$. From $1 = \zeta_p^{2^r+1}$ follows that $\zeta_p^{-1} = \zeta_p^{2^r}$, so ζ_p is a square in K thus ζ_p^m as well, for every $m \in \mathbb{N}$. It holds

$$0 = \left(\sum_{i=0}^{p-1} \zeta_p^i\right)\left(\sum_{j=0}^{s-i} \zeta_p^{ip}\right) = \sum_{i=0}^{2^r} \zeta_p^i = \zeta_p^{-1} + \sum_{i=0}^{2^r-1} \zeta_p^i = \zeta_p^{-1} + \prod_{i=0}^{r-1}(1 + \zeta_p^{2^i}),$$

thus $-1 = \zeta_p \prod_{i=0}^{r-1}(1 + \zeta_p^{2^i})$. Since the product of the sum of two squares is a sum of two squares and $1 + \zeta_p^{2^i}$ is a sum of two squares for every i, then $\prod_{i=0}^{r-1}(1 + \zeta_p^{2^i})$ is the sum of two squares. Hence, $\mathbb{Q}(\zeta_p)$ is a splitting field for Q_8. In $\mathrm{Irr}(Q_8)$ there is a unique character χ such that $\chi(1) = s_{\mathbb{Q}}(\chi) = 2$ and $\mathbb{Q}(\chi) = \mathbb{Q}$. The splitting field $\mathbb{Q}(\zeta_p)$ is not a minimal field for χ. Is there any subfield of $\mathbb{Q}(\zeta_p)$ which is minimal for χ? Choose p to be a multiple of 4. Let $n, m \in \mathbb{N}$ such that $p - 1 = 2^n m$ with $n \geq 2$ and m odd. Since $\mathbb{Q}(\zeta_p)$ is a cyclic extension of $\mathbb{Q}$, there exists a unique maximal subfield K of $\mathbb{Q}(\zeta_p)$ such that $|\mathbb{Q}(\chi) : K| = m$. Let M be an irreducible $\mathbb{Q}G$-module affording $s_{\mathbb{Q}}(\chi)\chi$, then $\dim_{\mathbb{Q}} \mathrm{End}_{\mathbb{Q}G}(M) = 4$. Let $D = \mathrm{End}_{KG}(M^K)$. If K is not a splitting field for $\mathrm{End}_{\mathbb{Q}G}(M)$ then D is a division algebra ([16, 1.1.7]). Since $\mathbb{Q}(\zeta_p)$ is a splitting field for Q_8, we have

$$D \otimes_K \mathbb{Q}(\zeta_p) \cong \mathrm{End}_{\mathbb{Q}(\zeta)G}(M^{\mathbb{Q}(\zeta_p)}) \cong M_2(\mathbb{Q}(\zeta_p)).$$

By Lemma 2.1.2 the degree $|\mathbb{Q}(\zeta_p) : K| = m$ is even, which is a contradiction. Thus K is a splitting field for Q_8. Let F be the unique maximal subfield of K, then $|K : F| = 2$. Since $K \subseteq \mathbb{R}$ so it can not be a splitting field for Q_8. As a conclusion there are no minimal fields for χ contained in the splitting field $\mathbb{Q}(\zeta_p)$.

In [14], Fieker present an algorithm to find a minimal field K for an irreducible character χ starting from a representation over some field E. Using Galois cohomology the algorithm is able to find a field K with the desired properties also if E does not contain it.

When K is a cyclic Galois extension of $\mathbb{Q}(\chi)$ and we want to find the minimal degree over the character field of a subfield of K that affords a representation of character χ, the number of needed checks is minimal because for every integer divisor of the degree of K over the character field we have a unique field and the related automorphism in the Galois group is easy to compute.

Chapter 3

Some Algebraic Number Theory

The aim of this chapter is to introduce algebraic number theory in order to present some tools that will be used in the remaining of the thesis. In particular we are interested in discussing solvability of norm equations over number field. General references for this chapter are [23], [26] and [21].

3.1 Ramification Theory

Let F be an algebraic number field, i.e. a finite extension of the rational field $\mathbb{Q}$. The ring of *algebraic integers* of F is denoted by $\mathcal{O}_F$ and it is defined by

$$\mathcal{O}_F = \{z \in F \mid \exists f \neq 0 \in \mathbb{Z}[x] \text{ monic such that } f(z) = 0\},$$

it is a Dedekind domain ([24, Theorem 14]) and hence every ideal of $\mathcal{O}_F$ factorizes in a unique way as product of prime ideals of $\mathcal{O}_F$. Let K/F be a finite extension of F and let v be a non-zero prime ideal of $\mathcal{O}_F$, then $v\mathcal{O}_K$ is an ideal of $\mathcal{O}_K$ and it has a unique factorization

$$v\mathcal{O}_K = w_1^{e_1} w_2^{e_2} ... w_g^{e_g}$$

where $w_1, w_2, .., w_g$ are distinct prime ideals of $\mathcal{O}_K$ and $g, e_1, e_2, .., e_g$ are positive integers. Prime ideals $w_1, w_2, .., w_g$ are said to *lie above* v and they satisfy $w_i \cap \mathcal{O}_F = v$. Integers e_i are usually denoted as $e_i = e(w_i/v)$ and are called *ramification indices* of w_i over v. In a Dedekind domain every non-zero prime ideal is a maximal ideal, thus we can define two finite fields

$\mathcal{O}_K/w_i$ and $\mathcal{O}_F/v$, both with the same characteristic p, where p is a prime number such that $p\mathbb{Z} = v \cap \mathbb{Z} = w_i \cap \mathbb{Z}$. These fields are called *residue fields* and are denoted by $\mathbb{F}_{w_i}$ and $\mathbb{F}_v$, respectively. The field $\mathbb{F}_{w_i}$ is an extension of $\mathbb{F}_v$, so we define the *residue degree* $f(w_i/v)$ as the field extension degree $[\mathbb{F}_{w_i} : \mathbb{F}_v]$. By [24, Theorem 21], the following relation is always satisfied

$$\sum_{i=1}^{g} f(w_i/v)e(w_i/v) = [K : F].$$

The ideal v is said to be *unramified* in K/F if $e(w_i/v) = 1$ for all i, otherwise it is said to be *ramified.* If $e(w_i/v) = [K : F]$ for some i then v is said to be *totally ramified* in K/F. Note that if $e(w_i/v) = [K : F]$ for one i, then v has a unique prime ideal of $\mathcal{O}_K$ lying above it. If $v\mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$ then v is *inert* in K/F and it is said to *split completely* in K/F if $g = [K : F]$.

If K/F is a Galois extension then the Galois group permutes the ideals w_i transitively (see Proposition 5.11 in [23]). As a consequence $e(w_1/v) = e(w_2/v) = .. = e(w_g/v)$ and $f(w_1/v) = f(w_2/v) = .. = f(w_g/v)$. Hence the prime ideals of $\mathcal{O}_K$ lying above v are all equivalent from the ramification point of view, so we just need to study one of them, say w, to understand what happens in general. We define

$$G_w = \{\sigma \in \mathrm{Gal}(K/F) \text{ s.t. } \sigma(w) = w\}$$

the stabilizer of w under the action of the Galois group. This group is called *decomposition group* of w. It induces an action on $\mathbb{F}_w$ that fixes $\mathbb{F}_v$, thus there is a natural homomorphism from $\phi : G_w \longrightarrow \mathrm{Gal}(\mathbb{F}_w/\mathbb{F}_v)$. Moreover this homomorphism is surjective (Proposition 5.11 in [23]), its kernel is called the *inertia subgroup* and it is denoted by T_w. Note that $[G_w : T_w] = |\mathrm{Gal}(\mathbb{F}_w/\mathbb{F}_v)| = f(w/v)$ and $|T_w| = e(w/v)$. We call *decomposition field* and *inertia field* the subfields of K fixed by G_w and T_w, respectively. If v is unramified in K/F then the inertia group is trivial and ϕ is an isomorphism. Since $\mathbb{F}_w/\mathbb{F}_v$ is a finite extension of finite fields, then its Galois group is cyclic and it is generated by the Frobenius automorphism $\varphi_p : \mathbb{F}_w \longrightarrow \mathbb{F}_w$ such that $\varphi(x) = x^{|\mathbb{F}_v|}$. As a consequence also G_w is cyclic and it is generated by $\phi^{-1}(\varphi_p)$. Such a generator is denoted by $\sigma(w, K/F)$, it is called

Frobenius automorphism at w and it satisfies

$$\alpha^{\sigma(w,K/F)} \equiv \alpha^{|\mathbb{F}_v|} \mod w \qquad \forall \alpha \in \mathcal{O}_K.$$

If the Galois group $\mathrm{Gal}(K/F)$ is abelian then the decomposition group G_w is the same for all prime ideals w of $\mathcal{O}_K$ lying above v. Hence, for unramified primes the Frobenius element of primes above v depends only on v and it is called *Artin automorphism* for v.

Proposition 3.1.1. *(Layer Theorem) [5, 1.3] Let K/F be an abelian extension of number fields. Let v be a prime ideal of $\mathcal{O}_F$ and w a prime ideal of $\mathcal{O}_K$ lying above v. Then v splits completely in $\mathrm{Fix}(G_w)/F$, the primes of $\mathrm{Fix}(G_w)$ above v are inerts in $\mathrm{Fix}(T_w)/\mathrm{Fix}(G_w)$ and they totally ramify in $K/\mathrm{Fix}(T_w)$.*

A particular example of abelian Galois extensions are the cyclotomic extensions of the rational field.

Proposition 3.1.2. *[5, 1.8] Let ζ_m be a primitive m^{th}-root of unity and K be a subfield of the cyclotomic field $\mathbb{Q}(\zeta_m)$. Let H be the subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$ such that $H \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K)$. A prime p not dividing m splits completely in $K/\mathbb{Q}$ if and only if $p \equiv h \mod m$ for some $h \in H$.*

3.2 Completions

An *absolute value* on a field F is a map $\nu : F \longrightarrow \mathbb{R}$ such that

1. $\nu(x) \geq 0$ for all $x \in F$ and $\nu(x) = 0$ if and only if $x = 0$;
2. $\nu(xy) = \nu(x)\nu(y)$ for all $x, y \in F$;
3. $\nu(x + y) \leq \nu(x) + \nu(y)$ for all $x, y \in F$.

If the stronger condition $\nu(x + y) \leq \max(\nu(x), \nu(y))$ is satisfied for all $x, y \in F$ then the absolute value is said to be *non-Archimedean*, otherwise it is said to be *Archimedean*.

Every absolute value defines a distance on F given by $d(x, y) = \nu(y - x)$, thus we can see F as a metric space. Two absolute values are said to be *equivalent* if they define the same topology on F. If ν_1 and ν_2 are equivalent absolute values of F then there exists $\lambda \in F$ such that $\nu_1(x) = \nu_2(x)^\lambda$ for all $x \in F$. A *place* is a class of equivalent absolute values. A metric space F is complete if every Cauchy sequence converges in F. The *completion* of an algebraic number field F with respect to an absolute value ν is obtained as the quotient of the ring of Cauchy sequences in F by the maximal ideal of all the sequences converging to 0. The completion is denoted by F_ν. It is a field complete with respect to the topology induced by ν, it is unique up to isomorphism and the field F is dense in F_ν.

Let v be a prime ideal of $\mathcal{O}_F$ for an algebraic number field F. For every $x \in F^*$ we have that $x\mathcal{O}_F$ is a fractional ideal of $\mathcal{O}_F$ and, since $\mathcal{O}_F$ is a Dedekind domain, $x\mathcal{O}_F$ has a unique factorization into prime ideals. Let $x\mathcal{O}_F = v^\alpha v_1^{\alpha_1}..v_t^{\alpha_t}$ be such a factorization, where $v_1,..,v_t$ are different prime ideals of $\mathcal{O}_F$ (different also from v) and $\alpha, \alpha_1,..,\alpha_t \in \mathbb{Z}$. We denote by $\mathrm{ord}_v(x)$ the integer α_i and we define $\mathrm{ord}_v(0) = \infty$. Then ord_v is a map $F \longrightarrow \mathbb{Z} \cup \{\infty\}$ and it is said to be a *discrete valuation* on F. For any real number $0 < c < 1$ we can define a map $\nu_v : F \longrightarrow \mathbb{R}$ as

$$\nu_v(x) = \begin{cases} c^{\mathrm{ord}_v(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

The map ν_v is a non-Archimedean absolute value of F for every choice of c in the interval $(0,1)$. Moreover the induced topology is independent of c because all the absolute values are equivalent. At same time, if v_1 and v_2 are two different prime ideals of $\mathcal{O}_F$ then ν_{v_1} and ν_{v_2} are not equivalent. Usually the real number c is chosen to be equal to $\frac{1}{p}$ where p is the prime number such that $v \cap \mathbb{Z} = p\mathbb{Z}$. Every non-Archimedean absolute value of F is equivalent to ν_v for some prime ideal v of $\mathcal{O}_F$. For this reason we will usually denote the completion of F with respect to a non-Archimedean absolute value by F_v, where v is the prime ideal of $\mathcal{O}_F$ that realizes the equivalence. Let

$$\mathcal{O}_v = \{x \in F_v \text{ s.t. } \nu_v(x) \leq 1\},$$

this a local ring contained in F_v and it is called the *valuation ring* of v. Let $\mathcal{P}_v$ be its unique maximal ideal, that is $\mathcal{P}_v = \{x \in F_v \text{ s.t. } \nu_v(x) < 1\}$. The field $\mathcal{O}_v/\mathcal{P}_v$ is isomorphic to the residue field $\mathbb{F}_v$ ([26, II,4.3]).

Proposition 3.2.1. *[26, II,4.4] Let R be a set of distinct representatives of $\mathcal{O}_v/\mathcal{P}_v$ in $\mathcal{O}_v$ such that $0 \in R$ and let $\pi \in v - v^2$. Every element $0 \neq$*

$x \in F_v$ may be written as $x = \pi^m \epsilon$ for some integer $m \in \mathbb{Z}$ and some $\epsilon \in \mathcal{O}_v^* = \mathcal{O}_v - \mathcal{P}_v$ (i.e. units of $\mathcal{O}_v$) and it admits a unique representation as a convergent sequence $x = \sum_{i=m}^{\infty} a_i \pi^i$ where $a_i \in R$.

Such a convergent sequence is called *v-adic expansion* of x. The prime element π is called *uniformizer* in F_v and it is such that $\mathcal{P}_v = \pi \mathcal{O}_v$. As a consequence of the previous proposition we have $F_v^* = \langle \pi \rangle \mathcal{O}_v^*$.

Every embedding of an algebraic number field F into the real and complex number fields $\mathbb{R}$ and $\mathbb{C}$ induces an Archimedean absolute value of F (obtained simply by the composition of the embedding with the usual absolute value on $\mathbb{R}$ or the usual norm on $\mathbb{C}$). Different real embeddings induce non-equivalent Archimedean absolute values of F. Two different complex embeddings induce equivalent absolute values of F if and only if they are obtained by conjugation one from the other. Moreover, a real and a complex embedding induce non-equivalent absolute values ([23, 1.2]). Every Archimedean absolute value of F is equivalent to the absolute value induced by some embedding of F into $\mathbb{R}$ or $\mathbb{C}$. The completion of F with respect to an Archimedean absolute value is $\mathbb{R}$ if the embedding is real and is $\mathbb{C}$ if the embedding is complex (see Ostrowski Theorem [26, 4.2]).

Let v be a prime ideal of $\mathcal{O}_F$ and K/F a field extension. Consider the factorization of $v\mathcal{O}_K = w_1^{e_1}..w_g^{e_g}$. The absolute values $\nu_{w_1}, .., \nu_{w_g}$ are pairwise non-equivalent in K and their restriction to F induce the same topology on F as ν_v. Moreover, every completion K_{w_i} is a finite extension of F_v.
At the same time, every finite extension field of F_v is the completion of a finite extension K/F with respect to ν_w for some prime ideal w of $\mathcal{O}_K$ lying above v [26, 8.1,8.2].

Let K/F be a field extension, v be a prime ideal of $\mathcal{O}_F$ and w a prime ideal of $\mathcal{O}_K$ above v. The unique prime ideal $\mathcal{P}_v$ of $\mathcal{O}_v$ generates an ideal $\mathcal{P}_v \mathcal{O}_w$ which has a unique factorization as $\mathcal{P}_w^e$ where e is a non-negative integer called *local ramification index* denoted by $e = e(\mathcal{P}_w/\mathcal{P}_v)$. It holds $e(\mathcal{P}_w/\mathcal{P}_v) = e(w/v)$, $f(\mathcal{P}_w/\mathcal{P}_v) = f(w/v)$ and, for a fixed v, we have

$$\sum_{w \text{ above } v} [K_w : F_v] = [K : F]$$

by [23, 8.3]. Similarly to the number field case, we say that $\mathcal{P}_v$ is *ramified* in K_w/F_v if $e \neq 1$, it is *unramified* in K_w/F_v if $e = 1$ and it is *totally ramified* in K_w/F_v if $e = [K_w : F_v]$.

3.3 Norm equations

Let K/F be a Galois extension of number fields and let v and w be prime ideals of $\mathcal{O}_F$ and $\mathcal{O}_K$ respectively, such that w lies above v. Let p be the characteristic of the residue fields $\mathbb{F}_v$ and $\mathbb{F}_w$ and $N_{K/F} : K \longrightarrow F$ be the norm of the extension K/F, i.e. $N_{K/F}(x) = \prod_{\sigma \in \mathrm{Gal}(K/F)} x^\sigma$ for all $x \in K$. Exactly in the same way we can define the norm of the extension K_w/F_v. Solving a norm equation means finding an element $\theta \in K$ such that $N_{K/F}(\theta) = \lambda$, for some fixed $\lambda \in F$. Understanding if a norm equation has a solution and, eventually, finding one is a problem with no general solution. However things are easier in the case of cyclic extensions, thanks to a well known theorem:

Theorem 3.3.1. *(Hasse Norm Theorem - VI,* 4.5 *in [26]) Let K/F be a cyclic extension of number fields. An element $\lambda \in K^*$ is a norm in K/F if and only if it is a norm in the completion K_w/F_v, for every prime ideals w of $\mathcal{O}_K$ and v of $\mathcal{O}_F$, such that w lies above v.*

Let π_w be an uniformizer in K_w, then $K_w^* = \langle \pi_w \rangle \mathcal{O}_w^*$. Thus

$$N_{K_w/F_v}(K_w^*) = \langle N_{K_w/F_v}(\pi_w) \rangle N_{K_w/F_v}(\mathcal{O}_w^*).$$

In order to understand if a local norm equation has solution, we need to determine $N_{K_w/F_v}(K_w^*)$. It is not obvious how to do it in general, but there are some easy situations that we can handle.

Let $U_w = 1 + \mathcal{P}_w$ be the subgroup of $\mathcal{O}_w^*$ of principal units of $\mathcal{O}_w$. Consider the following sequence

$$0 \longrightarrow U_w \xrightarrow{i} \mathcal{O}_w^* \xrightarrow{\varphi} \mathcal{O}_w^*/U_w \longrightarrow 0,$$

where i is the inclusion map and φ is the canonical quotient map. This is an exact sequence. The quotient $\mathcal{O}_w^*/U_w$ is isomorphic to $\mathbb{F}_w^*$. By [20, 2.3] $\mathcal{O}_w^*$ contains a cyclic subgroup of order $|\mathbb{F}_w^*| = |\mathbb{F}_w| - 1$. Thus there exists a primitive $|\mathbb{F}_w^*|^{th}$-root of unity $\zeta_{|\mathbb{F}_w^*|}$ in $\mathcal{O}_w^*$ and $\mathcal{O}_w^* = \langle \zeta_{|\mathbb{F}_w^*|} \rangle U_w$.

Since we assume K/F to be a cyclic extension, it is also an abelian extension, therefore $[\mathcal{O}_v^* : N_{K_w/F_v}(\mathcal{O}_w^*)] = e(w/v)$, see Corollary of Theorem 3 in [23, XI, §4]. Equivalently,

$$\begin{aligned} e(w/v) =& [\mathcal{O}_v^* : N_{K_w/F_v}(\mathcal{O}_w^*)] = \\ =& [\langle \zeta_{|\mathbb{F}_v^*|} \rangle U_v : N_{\mathbb{F}_w/\mathbb{F}_v}(\langle \zeta_{|\mathbb{F}_w^*|} \rangle) N_{K_w/F_v}(U_w)] = \\ =& [U_v : N_{K_w/F_v}(U_w)], \end{aligned}$$

where the last equality is due to the surjectivity of the norm of finite fields.

If v is unramified in K/F then $\mathcal{P}_w = \mathcal{P}_v$, so π_w is an uniformizer of F_v. In particular $\pi_w \in F_v$ and $N_{K_w/F_v}(\pi_w) = \pi_v^{[K_w:F_v]} = \pi_v^{f(w/v)}$, where the last equality is an easy consequence of $e(w/v)f(w/v) = [K_w : F_v]$ in the unramified case. As a consequence

$$N_{K_w/F_v}(K_w^*) = \langle \pi_v^{f(w/v)} \rangle \mathcal{O}_v^* = \{\pi_v^k x \text{ s.t. } k \in f(w/v)\mathbb{Z} \text{ and } x \in \mathcal{O}_v^*\}.$$

In particular if $\lambda \in \mathcal{O}_v^*$, then it is a local norm of some elements of K_w (more details in Proposition 9.8 in [21]).

If v is ramified in K/F then some more work is needed to determine $N_{K_w/F_v}(K_w^*)$. If we suppose v to be totally ramified in K/F then we have $f(w/v) = 1$ and $|\mathbb{F}_w| = |\mathbb{F}_v|$, so $\zeta_{|\mathbb{F}_w^*|} \in \mathcal{O}_v^*$. Its norm is

$$N_{K_w/F_v}(\zeta_{|\mathbb{F}_w^*|}) = \zeta_{|\mathbb{F}_w^*|}^{[K_w:F_v]} = \zeta_{|\mathbb{F}_w^*|}^{e(w/v)} = \zeta_{|\mathbb{F}_w^*|}^{[K:F]}.$$

As U_v is a pro-p group (see Section 2.2 in [20]) and $N_{K_w/F_v}(U_w)$ is a finite index subgroup of U_v then $[U_v : N_{K_w/F_v}(U_w)]$ is a power of p. With the additional hypothesis of v to be tamely totally ramified in K/F (i.e. $p \nmid e(w/v)$) then it must be $N_{K_w/F_v}(U_w) = U_v$, otherwise $U_v/N_{K_w/F_v}(U_w)$ would contain an element with order a power of p this is a contradiction to the statement $[U_v : N_{K_w/F_v}(U_w)] = e(w/v)$. In conclusion we can characterize the image of the norm for tamely totally ramified extensions as

$$N_{K_w/F_v}(K_w^*) = \langle N_{K_w/F_v}(\pi_w), \zeta_{|\mathbb{F}_w^*|}^{e(w/v)} \rangle U_v.$$

If v is an infinite prime then $F_v = \mathbb{C}$ or $F_v = \mathbb{R}$. If $F_v = \mathbb{C}$ then it must be $K_w = \mathbb{C}$ and trivially $N_{K_w/F_v}(K_w) = F_v = \mathbb{C}$. In a similar way if both F_v and K_w are the field of real numbers then $N_{K_w/F_v}(K_w) = F_v = \mathbb{R}$. It may also happen that $F_v = \mathbb{R}$ and $K_w = \mathbb{C}$. In this case $N_{K_w/F_v}(K_w) = \mathbb{R}_0^+$, where $\mathbb{R}_0^+$ denotes the set of non-negative real numbers.

Here we have decided to discuss only some special cases when we can determine $N_{K_w/F_v}(K_w)$ because in these cases we can have an explicit description of the image of the norm. In [1], Acciaro and Klüners gave an explicit algorithm to test whether a local norm equation is solvable or not in every situation. By their algorithm and using the Hasse Norm Theorem they are able to decide whether a (global) norm equation has a solution.

In the next chapter we will determine a bound for the Schur index of some characters. To do it we will need to determine whether some norm equations have a solution or not. As we will see, in the field extensions that we will meet, every finite prime ideal is unramified or tamely totally ramified. For this reason in this thesis it would be enough to deal with the cases treated in this section to solve the norm equation that we will encounter.

Chapter 4

Schur Indices of Characters of some Metacyclic Groups

In 1930 Brauer proved that every integer can occur as Schur index of some irreducible character of some finite group. Nevertheless, the most frequent situation is to have Schur indices equal to 1 and 2. We are now interested in understanding in which situations Schur indices greater than 2 may occur.

4.1 Groups of order $9p$

Let G be a finite group and consider $\chi \in \mathrm{Irr}(G)$. We know from Proposition 2.3.1 and Theorem 2.3.1 that $s_{\mathbb{Q}}(\chi)$ divides the degree of χ and $s_{\mathbb{Q}}(\chi)^2$ divides $|G|$. If we are interested in characters with Schur index 3 we need $|G|$ to be a multiple of 9 as a necessary condition.

As a first example we focus on groups of order $9p$, with $p > 3$ a prime number. We denote by $n_q(G)$ the number of q-Sylow subgroups of G for every prime number q.

Lemma 4.1.1. *Let G be a finite group of order $9p$ for some odd prime $p > 3$. Then $G = P \rtimes T$ with $|P| = p$ and $T \in Syl_3(G)$.*

Proof. By Sylow Theorems we have four conditions on n_3 and n_p: $n_3 \equiv 1 \mod 3$, $n_3 | p$, $n_p \equiv 1 \mod p$ and $n_p | 9$. The last condition implies n_p equal

$1, 3$ or 9. If n_p is 3 or 9 then p must be 2, because of the third condition. Since p is odd, $p > 3$, then $n_p \big| 9$. Since $n_p \equiv 1 \mod p$, then we have $n_p = 1$. Let P be the normal subgroup of G of order p and T be one of the 3-Sylow subgroups of G. It is sufficient to notice that $G = TP$ and $T \cap P = \{1\}$ to get the conclusion. □

Lemma 4.1.2. *Let G be a finite group of order $9p$ for some prime $p > 3$. If G is non-abelian then $n_3(G) = p$ and $p \equiv 1 \mod 3$.*

Proof. By Sylow theorems we have $n_3 = 1$ or $n_3 = p$. Suppose $n_3 = 1$ then G is abelian, otherwise $n_3 = p$, thus $p \equiv 1 \mod 3$. □

We are interested only in non-abelian groups, since abelian groups have only linear characters and trivial Schur indices.

Corollary 4.1.1. *Let G be a group of order $9p$ for some prime p such that there exists $\chi \in \mathrm{Irr}(G)$ with $s_{\mathbb{Q}}(\chi) = 3$. Then $p \equiv 1 \mod 3$ and $G = T \ltimes_{\varphi} P$ with $T \in \mathrm{Syl}_3(G)$, $n_3(G) = p$ and $\varphi : T \longrightarrow \mathrm{Aut}(P)$ non-trivial.*

From now on we suppose G to be a finite group of order $9p$, for some prime number p, such that there exists $\chi \in \mathrm{Irr}(G)$ with $s_{\mathbb{Q}}(\chi) = 3$. Our aim is to characterize the structure of G, with special attention to its center $Z(G)$. The previous Corollary tells us that $p = |G : N_G(T)|$, where $N_G(T)$ is the normalizer of T in G. At the same time $T \leq N_G(T)$ and $|G : T| = p$, hence $T = N_G(T)$. The center $Z(G)$ is a subgroup of $N_G(T) = T$, but it can not be T itself otherwise T would be normal in G, which is not the case. Hence $|Z| = 1$ or $|Z| = 3$.

Consider the automorphism of the semidirect product $\varphi : T \longrightarrow \mathrm{Aut}(P)$. As P is cyclic of order p then $\mathrm{Aut}(P) \cong C_{p-1}$, hence it has only cyclic subgroups. The image of φ is a cyclic subgroup of $\mathrm{Aut}(P)$ of order that divides $|T| = 9$. We can notice that T is either $T \cong C_9$ or $T \cong C_3 \times C_3$. We analyse the two cases separately. If $T \cong C_9$ then $\varphi(T)$ is isomorphic to C_9 or to C_3 (recall that we are excluding the case where φ is trivial). In the first situation we have the additional condition $p \equiv 1 \mod 9$. If $T \cong C_3 \times C_3$ then $|\varphi(T)| \neq 9$ (because $C_3 \times C_3$ is not cyclic and $\varphi(T)$ is). Hence $\varphi(T) \cong C_3$.

We can summarise the possible presentation of non-abelian groups of order $9p$ with $p \equiv 1 \mod 3$ a prime number as:

1. $C_9 \ltimes C_p = \langle a, b \mid a^p, b^9, a^b = a^r \rangle$ with $o_p(r) = 3$, then $Z = \langle b^3 \rangle$;
2. $C_9 \ltimes C_p = \langle a, b \mid a^p, b^9, a^b = a^r \rangle$ with $o_p(r) = 9$, so $Z = \{1\}$;
3. $(C_3 \times C_3) \ltimes C_p = \langle a, b, c \mid a^p, b^3, c^3, a^b = a^r, a^c = a, b^c = b \rangle$ with $o_p(r) = 3$, so $Z = \langle c \rangle$.

We start our analysis from groups isomorphic to type 2. Recall that the condition on $o_p(r)$ needs $p \equiv 1 \mod 9$ to be satisfied. These groups are Frobenius groups with Frobenius complement the 3-Sylow subgroup T and kernel the normal p-Sylow subgroup P. As a consequence of the Brauer's permutation lemma ([18, 18.5, 18.7]) we have

$$|\mathrm{Irr}(G)| = |\mathrm{Irr}(T)| + \frac{|\mathrm{Irr}(P)| - 1}{|T|} = 9 + \frac{p-1}{9}.$$

In particular irreducible characters of G are either irreducible characters of T, thus linear, or induced by non-trivial characters in $\mathrm{Irr}(P)$ (characters conjugated by elements of T induce the same character on G). If there is any character in $\mathrm{Irr}(G)$ with non-trivial Schur index it has to arise from the second case. Let $\lambda \in \mathrm{Irr}P$, $\lambda \neq 1$. Since λ is linear it is the character of a 1-dimensional K-representation of P, for some field extension K of $\mathbb{Q}(\zeta_p)$, where ζ_p is a p^{th}-root of unity. Let $K = \mathbb{Q}(\zeta_p)$ and let $\pi : P \longrightarrow \mathrm{GL}_1(K)$ be an irreducible K-representation of P of character λ with $\pi(a) = \zeta_p$. The representation R of G induced by π is a degree 9 representation such that

$$R(a) = \begin{pmatrix} \zeta_p & 0 & 0 & \cdots & 0 \\ 0 & \zeta_p^r & 0 & \cdots & 0 \\ 0 & 0 & \zeta_p^{r^2} & \cdots & 0 \\ \vdots & & \vdots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & \zeta_p^{r^8} \end{pmatrix} \qquad R(b) = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix}$$

Notice that $G = PT$, so every $g \in G$ can be written as $g = a^i b^j$ for some $i \in \mathbb{Z}/p\mathbb{Z}$ and some $j \in \mathbb{Z}/9\mathbb{Z}$, hence $R(g)$ is a matrix of the form:

$$R(g) = \left(\begin{array}{c|c} 0 & \mathrm{A} \\ \hline \mathrm{B} & 0 \end{array} \right)$$

with A a diagonal $j \times j$ matrix and B a diagonal $(9-j) \times (9-j)$ matrix.

As a consequence $\chi(a^ib^j) = \mathrm{Tr}(R(a^ib^j)) = 0$ for $j \not\equiv 0 \mod p$ and

$$\chi(a^i) = \mathrm{Tr}(R(a^i)) = \mathrm{Tr}\begin{pmatrix} \zeta_p^i & 0 & \cdots & 0 \\ 0 & \zeta_p^{ir} & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & \zeta_p^{ir^8} \end{pmatrix} = \sum_{j=0}^{8} \zeta_p^{ir^j} = \mathrm{Tr}_{K/F}(\zeta_p^i)$$

where $\mathrm{Tr}_{K/F}$ denotes the field trace of the cyclotomic extension $K = \mathbb{Q}(\zeta_p)$ over its subfield F fixed by the automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\zeta_p) = \zeta_p^r$. Obviously $\mathbb{Q}(\chi) \subseteq F$. Let $\langle r\rangle \leq (\mathbb{Z}/n\mathbb{Z})^*$ and $t_1, t_2, .., t_m$ be a transversal of $\langle r\rangle$ in $(\mathbb{Z}/n\mathbb{Z})^*$, where $m = \frac{p-1}{9}$. For each $k = 1, .., m$ and each $i, j \in t_k\langle r\rangle$ the values of the diagonal on $R(a^j)$ are just a shift permutation of the elements on the diagonal of $R(a^i)$, hence the value of the character $\chi(a^i)$ depends only on the coset to which i belongs. This means that $\mathbb{Q}(\chi) = \mathbb{Q}(\{\sum_{j=0}^{8} \zeta_p^{t_ir^j}\}_{i=1,..,m})$. It is very easy to verify that $\{\sum_{j=0}^{8} \zeta_p^{t_ir^j}\}_{i=1,..,m}$ are linearly independent over $\mathbb{Q}$: let $a_1, .., a_m \in \mathbb{Q}$ be such that

$$0 = \sum_{i=1}^{m} a_i \sum_{j=0}^{8} \zeta_p^{t_ir^j} = \sum_{i=1}^{m}\sum_{j=0}^{8} a_i\zeta_p^{t_ir^j},$$

then $a_i = 0$ for all i, because $\{\zeta_p^{t_ir^j}\}_{i,j}$ is a basis of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$. As a consequence $|\mathbb{Q}(\chi) : \mathbb{Q}| = m$ and $\mathbb{Q}(\chi) = F$.

Denote by R^σ the K- representation of G obtained applying σ to each entry of $R(g)$ for every $g \in G$.

$$R^\sigma(a) = \begin{pmatrix} \zeta_p^r & 0 & \cdots & 0 \\ 0 & \zeta_p^{r^2} & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & \zeta_p \end{pmatrix} \qquad R^\sigma(b) = R(b).$$

It is easy to verify that $R(b)^{-1}R(a)R(b) = R^\sigma(a)$ and, more in general, $R(b)^{-1}R(g)R(b) = R^\sigma(g)$ for every $g \in G$. Consider the norm function $N_{K/F} : K \longrightarrow F$, that sends $x \mapsto xx^\sigma x^{\sigma^2}..x^{\sigma^8}$ for each $x \in K$. We can extend such a norm to a map $N_{K/F} : \mathrm{GL}_8(K) \longrightarrow \mathrm{GL}_8(F)$ by applying $N_{K/F}$ to each entry of the matrices. We have $N_{K/F}(R(b)) = R(b)^9 = I_9$. By Theorem 2.3.5, there exists a representation equivalent to R over $\mathbb{Q}(\chi)$ if and only if there exists some elements in K with field norm equal 1. In this case it is trivial to find a solution for the equation, for example $N_{K/F}(1) = 1$. This allows us to conclude that we can write a representation equivalent to R over $\mathbb{Q}(\chi)$, hence $s_{\mathbb{Q}}(\chi) = 1$.

This shows that groups of type 2 affords only characters with trivial Schur index. Hence, to find some characters of Schur index three, we focus our attention on groups isomorphic to groups of type 1 or 3. These two kind of groups have some properties in common that allow us to prove the following:

Proposition 4.1.1. *Let G be a finite group of order $9p$ for some prime number $p \equiv 1 \mod 3$, such that there exists $\chi \in \mathrm{Irr}(G)$ with $s_{\mathbb{Q}}(\chi) = 3$. Let $Z = Z(G)$ be the center of G. Then*

1. *$|Z| = 3$;*
2. *$\chi(1) = 3$;*
3. *χ is faithful;*
4. *every subgroup of G of order $3p$ is cyclic.*

Proof. The first statement is a direct consequence of the classification of non-abelian groups of order $9p$ and of what we have noticed about groups of type 2.
Let P be the normal p-Sylow subgroup of G, we have $PZ \lhd G$. Hence, by Itô's Theorem ([19, 6.15]), $\chi(1)$ divides $|G : PZ|$. The condition $s_{\mathbb{Q}}(\chi) = 3$ implies $\chi(1) = 3$.
By [18, 38.18] $G/\ker\chi$ has a fixed point free representation over $\mathbb{Q}(\chi)$. Since P is cyclic of order p and $G = T \ltimes P$ for some 3-Sylow subgroup T of G, then the derived group $G' = P$. It is contained in $\ker\chi$ if and only if $\chi \in \mathrm{Irr}(G/G')$, thus linear, which is not the case. Hence $G' \cap \ker\chi = P \cap \ker\chi$ is trivial. Suppose $Z \leq \ker\chi$, then $\chi \in \mathrm{Irr}(G/Z)$ and $s_{\mathbb{Q}}(\chi)^2 \big| |G/Z| = 3p$, that is not true under our hypothesis. Hence $Z \cap \ker\chi = 1$. As a consequence $G/\ker\chi$ has a subgroup isomorphic to $C_3 \ltimes C_p$. Let R be a fixed point free representation of $G/\ker\chi$ over some vector space V, R is a faithful representation. If $G/\ker\chi \cong C_3 \ltimes C_p$ then it acts point-fixed-freely over V and it has order $3p$. By Burnside's lemma [18, 16.11] $G/\ker\chi$ is cyclic and $\ker\chi$ is a normal subgroup of G of order 3, so $\chi \in \mathrm{Irr}(G/\ker\chi)$, hence it is linear with trivial Schur index. This contradicts our hypothesis hence

$\ker \chi = 1$.
Let $H \leq G$ be a subgroup of G of order $3p$, by Burnside's lemma it is cyclic. □

If we consider the group $G = \langle a, b, c \mid a^p, b^3, c^3, a^b = a^r, a^c = a \rangle$, with $o_p(r) = 3$ then it has a subgroup generated by a and b which is not cyclic of order $3p$. By the previous proposition, such a group can not have any irreducible character of Schur Index 3.
In conclusion, groups of order $9p$, with p a odd prime, need to be isomorphic to $\langle a, b \mid a^p, b^9, a^b = a^r \rangle$ with $o_p(r) = 3$ to afford characters of non-trivial Schur index.

With the help of a Magma code, we constructed some example of groups of order $9p$, letting p vary between the primes such that $p \equiv 1 \mod 3$. Consequences of experiments for $p = 7$,19, 109, 163, 487 can be found in the tables in Appendix B for $k = 2$. In particular what is interesting to notice is that the only case where we can find characters of Schur index 3 is when $p = 7$. Further experiments (not reported in the table), shows that we can find non-trivial Schur indices only when $p \not\equiv 1 \mod 9$. Try to find a reason for this behaviour has been the starting point for our considerations about Schur indices of absolutely irreducible characters of metacyclic groups.

4.2 Metacyclic Groups of order $q^k p$

In the previous section we have found some very strong necessary conditions for a group of order $9p$, where p is an appropriate odd prime, to have some characters of Schur index 3. The aim of this section is to study a more general situation in order to understand whether 3 plays a special role.

Proposition 4.2.1. *Let $G = \langle a, b \mid a^p, b^{q^k}, a^b = a^r \rangle$ with $o_p(r) = q^k$, $k \geq 2$, q, p odd primes such that $p \equiv 1 \mod q^k$. Then $s_{\mathbb{Q}}(\chi) = 1$ for all $\chi \in \mathrm{Irr}(G)$.*

Proof. Let P and T be the subgroups of G generated by a and b respectively, P is a normal subgroup of G of order p and $|T| = q^k$. The center of G is trivial. The group G is a Frobenius group with respect to the complement T and with kernel P. By [18, 18.7] G has $|\mathrm{Irr}(T)|$ linear characters with P contained in their kernel and $\frac{|\mathrm{Irr}(P)|-1}{|T|}$ characters induced on G by non-trivial character in $\mathrm{Irr}(P)$. Moreover T acts on $\mathrm{Irr}(P)$ by conjugation, that is

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

Suppose now that $1 \neq \lambda \in \mathrm{Irr}(P)$. Let $\rho = \mathrm{ind}_P^G(\lambda)$ be the representation of G induced by λ. Then $\rho : G \longrightarrow \mathrm{GL}_{q^k}(\mathbb{Q}(\lambda))$ with $\mathbb{Q}(\lambda) = \mathbb{Q}(\zeta_p)$ and ζ_p a primitive p^{th}-root of unity.

$$\rho(a) = \begin{pmatrix} \zeta_p & 0 & \cdots & 0 \\ 0 & \zeta_p^r & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & \zeta_p^{r^{q^k-1}} \end{pmatrix} \qquad \rho(b) = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Consider $X = \rho(b)$. It is such that $\rho(a)X = X\rho(a)^\sigma$ and $\rho(b)X = X\rho(b)^\sigma$ where $\sigma \in \mathrm{Gal}(\mathbb{Q}(\lambda)/\mathbb{Q})$ such that $\sigma(\lambda(a)) = \lambda(a)^r$. We denote by X^{σ^i} the matrix obtained by applying the automorphism σ^i to each entry of X. Since $X \cdot X^\sigma \cdot .. \cdot X^{\sigma^{q^k-1}} = 1 \cdot I_{q^k}$ and the field norm $N_{\mathbb{Q}(\lambda)/\mathbb{Q}}(1) = 1$ then by Theorem 2.3.5 there exists a representation of G over $\mathrm{Fix}(\sigma)$, the subfield of $\mathbb{Q}(\lambda)$ fixed by σ, similar to ρ, thus with character χ. In particular $|\mathbb{Q}(\lambda) : \mathrm{Fix}(\sigma)| = q^k$ and $\mathrm{Fix}(\sigma) = \mathbb{Q}(\chi)$. As a consequence $s_{\mathbb{Q}}(\chi) = 1$. □

Now we introduce a new parameter related to the action of a q-Sylow subgroup of G on the normal p-subgroup. Let $G = \langle a, b \mid a^p, b^{q^k}, a^b = a^r \rangle$ with $o_p(r) = q^l$, $k \geq 2$, q, p odd primes such that $p \equiv 1 \mod q$ and $1 \leq l \leq k$. It is necessary for these parameters to satisfy another condition for G to be well defined: let $m \in \mathbb{N}$ such that q^m is the maximal power of q dividing $p-1$. It must be $1 \leq l \leq m$, because $\langle r \rangle \leq (\mathbb{Z}/p\mathbb{Z})^*$, thus $q^l \mid p-1$.
Let P and T be subgroups of G generated by a and b respectively, then $P \cong C_p$, $T \cong C_{q^k}$ and $G = P \rtimes_\varphi T$ where φ varies according to l. Let $Z = Z(G)$ be the center of the group G. Then $Z = \langle b^{q^l} \rangle$, hence it is a cyclic group of order q^{k-l}.

Definition 4.2.1. Let G be a finite group, H be a subgroup of G and $\lambda \in \mathrm{Irr}(H)$. For every $g \in G$, denote by λ^g the class function $\lambda^g : H \longrightarrow \mathbb{C}$ defined by $\lambda^g(x) = \lambda(g^{x^{-1}})$, for all $x \in H$. By [19, 6.1], $\lambda^g \in \mathrm{Irr}(H)$. Then $I_G(\lambda) = \{g \in G \text{ s.t. } \lambda^g = \lambda\}$ is the *inertia group* of λ in G.

Corollary 4.2.1. *Let $G = \langle a, b \mid a^p, b^{q^k}, a^b = a^r \rangle$ with $o_p(r) = q^l$, $k \geq 2$, q, p odd primes such that $m \geq 1$ is the maximal power of q dividing $p-1$*

and $1 \leq l \leq \min(k,m)$. Let $P = \langle a\rangle$ and $Z = Z(G)$. Then the inertia group of λ in G is $I_G(\lambda) = PZ$ for every $1 \neq \lambda \in \mathrm{Irr}(P)$.

Proof. Since P is a cyclic group of order p then its character table is easy to compute. It contains the trivial character and $p-1$ characters $\{\lambda_i\}$ such that $\lambda_i(a) = \zeta_p^i$ for $i = 1,..,p-1$, where ζ_p is primitive p^{th}-root of unity. Moreover $P \trianglelefteq I_G(\lambda_i)$ and $Z \trianglelefteq I_G(\lambda_i)$. Suppose $b^j \in I_G(\lambda_i)$ for some $1 \leq j < q^k$, then $\lambda_i^{b^j}(a) = \lambda_i(a)$. Hence

$$\zeta_p^i = \lambda_i(a) = \lambda_i^{b^j}(a) = \lambda_i(a^{b^{-j}}) = \lambda_i(a^{r^{-j}}) = \lambda_i(a)^{r^{-j}} = \zeta_p^{ir^{-j}},$$

as a consequence $ir^{-j} \equiv i \mod p$. Since $(i,p) = 1$ then $o_p(r)\big|j$ and $b^j \in Z$, hence $I_G(\lambda) = PZ$. □

Since the inertia group in G of every character in $\mathrm{Irr}(P)$ has been determined, we can make some deductions also on $\mathrm{Irr}(G)$. In particular, in the following proposition, we are able to determine the degrees of the character table of G.

Proposition 4.2.2. *Let $G = \langle a,b \mid a^p, b^{q^k}, a^b = a^r\rangle$ with $o_p(r) = q^l$, $k \geq 2$, q,p odd primes such that $m \geq 1$ is the maximal power of q dividing $p-1$ and $1 \leq l \leq \min(k,m)$. Then G has exactly q^k linear characters, $(p-1)q^{k-2l}$ characters of degree q^l and no other character.*

Proof. Let $P = \langle a\rangle$ and let $\chi \in \mathrm{Irr}(G)$. By Clifford's theorem we have $\chi_P = e\sum_{i=1}^t \lambda_i$ where $\lambda = \lambda_1,..,\lambda_t \in \mathrm{Irr}(P)$ are conjugate.
If $\lambda = 1$ then $\chi_P = e\cdot 1$. Hence $P \leq \ker\chi$, so $\chi \in \mathrm{Irr}(G/P)$. The quotient G/P is isomorphic to T, which is a cyclic group so it affords only linear characters. Hence χ is linear.
If $\lambda \neq 1$ then, by the previous lemma, the inertia group of λ in G is $I_G(\lambda) = PZ$ and $t = |G : I_G(\lambda)| = q^l$. Since λ is linear then $\chi(1) = \chi_P(1) = eq^l$. Consider λ^{PZ} and let $\{\psi_i\}_i \subseteq \mathrm{Irr}(PZ)$ be its irreducible components. Hence $\lambda^{PZ} = \sum e_i\psi_i$ for some positive integers e_i and $(\psi_i)_P = e_i\lambda$. Since both P and PZ are abelian, then ψ_i and λ are both linear. As a consequence $e_i = 1$ for all i and $|PZ : P| = q^{k-l}$. By Gallagher's theorem ([19, Cor6.17]) $\lambda^{PZ} = \sum_{\beta\in\mathrm{Irr}(Z)}\psi_1\beta = \sum_{i=1}^{q^{k-l}}\psi_i$ and $\lambda^G = \sum_{i=1}^{q^{k-l}}\psi_i^G$. Since χ is an irreducible constituent of λ^G then $\chi = \psi_i^G$ for exactly one $i \in \{1,..,q^{k-l}\}$ ([19, Thm 6.11]), let ψ be such a character. Therefore $\chi(1) = |G : PZ|\psi(1) = q^l$ and $e = 1$.

Linear characters of G are in one-to-one correspondence with the irreducible characters of the abelian group G/P, so they are q^k in total. Each non-linear character of G is obtained by induction from an irreducible non-trivial character of PZ such that its restriction to P is a faithful character of P, these are $(p-1)q^{k-l}$. Two irreducible characters of PZ conjugated in G induce the same irreducible character of G. Hence exactly q^l different characters of $\mathrm{Irr}(PZ)$ induce the same character of G, thus the number of non-linear characters of G is $(p-1)q^{k-2l}$.

An additional confirmation that these are all the absolutely irreducible characters of G is given by

$$|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = q^k + (p-1)q^{k-2l}q^{2l} = pq^k.$$

□

We are interested in determining which are the Schur indices of the characters of groups we are dealing with. The conditions about the degrees of these characters, that we have found in the previous proposition, are very strong. Obviously the q^k linear characters have trivial Schur indices, but what about the others $(p-1)q^{k-2l}$ non-linear characters?

The bound of Lemma 2.3.1 tells us that the Schur index of a character is a divisor of its degree. Hence, in our situation, the Schur index of a non-linear character χ is a power of q, say $s_{\mathbb{Q}}(\chi) = q^t$ for some non-negative integer $t \leq l$. While, by Proposition 2.3.1, we have that $s_{\mathbb{Q}}(\chi)\chi(1)\big||G|$, so $t \leq k-l$. It is possible to summarize these two bounds by $0 \leq t \leq \min(l, k-l)$.

In order to have some more precise information about the Schur indices of these characters we decided to compute some examples (see Appendix B). From our analysis it turns out that an additional condition is satisfied: $t \leq \max(0, k-m)$. This bound is stronger then the previous one because $k - l \geq \max(0, k-m)$, by definition of parameters k, l and m.

Conjecture 4.2.1. *Let $G = \langle a, b \mid a^p, b^{q^k}, a^b = a^r \rangle$ with $o_p(r) = q^l$, $k \geq 2$, q, p odd primes such that $q^m \geq 1$ is the maximal power of q dividing $p-1$ and $1 \leq l \leq \min(k, m)$. Then, for all $\chi \in \mathrm{Irr}(G)$, it holds $s_{\mathbb{Q}}(\chi) = q^t$ where $t \leq \min(l, \max(0, k-m))$.*

Moreover, for every integer t such that $0 \leq t \leq \min(l, \max(0, k-m))$, there exists $\chi \in \mathrm{Irr}(G)$ such that $s_{\mathbb{Q}}(\chi) = q^t$.

A first attempt in order to prove the conjecture may be to use the same method used to prove Proposition 4.2.1. Using the information given by Proposition 4.2.2 we have that G has at least q^k characters with trivial Schur index, because they are linear. What is an open question is what are the Schur indices of the $(p-1)q^{k-2l}$ characters of degree q^l. As we have seen in the proof of Proposition 4.2.2 these non-linear characters are obtained by induction on G from the irreducible characters of PZ with faithful restriction on P.

Let $\chi \in \mathrm{Irr}(G)$ and $\psi \in \mathrm{Irr}(PZ)$ be such that $\chi = \psi^G$. In order to determine the Schur index of these characters by looking for the degree over $\mathbb{Q}(\chi)$ of the minimal subfield of $\mathbb{Q}(\psi)$ affording a representation of character χ, we have to convince ourself that there is a minimal field for χ contained in $\mathbb{Q}(\psi)$. To do it we adapt the proof of [8, Theorem(b)] to our situation. Let D be the division algebra central over $\mathbb{Q}(\chi)$ associated to χ. For every prime ideal v of $\mathcal{O}_{\mathbb{Q}(\chi)}$ we can define by m_v the v-local index of D, i.e. $m_v = \mathrm{ind}(D \otimes_{\mathbb{Q}(\chi)} \mathbb{Q}(\chi)_v)$. By [35, Proposition 1], D is similar to a crossed product algebra. Checking the details of Yamada's proof we can see that such an algebra is $(\mathbb{Q}(\psi)/\mathbb{Q}(\chi), \beta)$ where β is a cocycle whose values are 1 and $\zeta_{q^{k-l}}$. As a consequence $m_v = 1$ for all the primes not above q and all the unramified primes in $\mathbb{Q}(\psi)/\mathbb{Q}(\chi)$. The field $\mathbb{Q}(\psi) = \mathbb{Q}(\zeta_{pq^h})$ where ζ_{pq^h} is a primitive $(pq^h)^{th}$-root of unity for some $h \in \mathbb{Z}$ such that pq^h is the exponent of PZ, while $\mathbb{Q}(\psi^G)$ is a subfield such that $|\mathbb{Q}(\psi) : \mathbb{Q}(\psi^G)| = q^l$ and $\zeta_{pq^h}^p \in \mathbb{Q}(\psi^G)$. If v is a prime ideal of $\mathcal{O}_{\mathbb{Q}(\chi)}$ lying above p and w a prime ideal of $\mathcal{O}_{\mathbb{Q}(\psi)}$ above v, by [24, Therem 26] it holds $e(w/p) = \varphi(p) = p-1$. This means that primes above p ramify totally in $\mathbb{Q}(\psi)/\mathbb{Q}(\psi^G)$. Since $s_{\mathbb{Q}}(\chi)$ is a power of q, then we have $m_v = s_{\mathbb{Q}}(\chi)$ if v is above p and $m_v = 1$ otherwise. For the Global Splitting Criterior [28], a field K is a splitting field for D if and only if $m_v \big| [K_w : \mathbb{Q}(\chi)_v]$ for all prime ideals v, w of $\mathcal{O}_{\mathbb{Q}(\chi)}$ and $\mathcal{O}_K$, respectively with $w \big| v$. As a consequence K is a splitting field for D if and only if $s_{\mathbb{Q}}(\chi) \big| [K_w : \mathbb{Q}(\chi)_v]$ for v, w above p. However we have seen that primes above p totally ramify in $\mathbb{Q}(\psi)/\mathbb{Q}(\chi)$ and also in $K/\mathbb{Q}(\chi)$ for every field $\mathbb{Q}(\chi) \subseteq K \subseteq \mathbb{Q}(\psi)$, hence $[K_w : \mathbb{Q}(\chi)_v] = [K : \mathbb{Q}(\chi)]$. Since $\mathbb{Q}(\psi)/\mathbb{Q}(\chi)$ is cyclic, there must be a field K of the desired degree. Thus we can look for minimal fields for χ inside $\mathbb{Q}(\psi)$.

In the next proposition we prove that the value of the Schur indices of χ and φ strongly depends on the their kernel.

Proposition 4.2.3. *Let $\psi, \varphi \in \mathrm{Irr}(PZ)$ such that the restrictions of ψ and φ to P are faithful characters of P. It holds $\psi^G, \varphi^G \in \mathrm{Irr}(G)$ and if $|\ker \psi| = |\ker \varphi|$ then $s_{\mathbb{Q}}(\psi^G) = s_{\mathbb{Q}}(\varphi^G)$.*

Proof. Let $\psi \in \mathrm{Irr}(PZ)$ be such that its restrictions to P is a faithful character, then $\ker \psi \subseteq Z$. Let $|\ker \psi| = q^\delta$, for some $0 \leq \delta \leq l$, then $\ker \psi$ is generated by $b^{q^{k-\delta}}$. It holds that $\psi(a)$ is a primitive p^{th}-root of unity and $1 = \psi(b^{q^{k-\delta}}) = \psi(b^{q^l})^{q^{k-l-\delta}}$, hence $\psi(b^{q^l})$ is a primitive $(q^{k-l-\delta})^{th}$-root of unity. The subgroup PZ of G is generated by a and b^{q^l}, hence $\mathbb{Q}(\psi) = \mathbb{Q}(\zeta_{pq^{k-l-\delta}})$. Since ψ is linear we can consider it as a representation over a 1-dimensional vector space and calculate the induced representation. Let R be such a representation, thus $R : G \longrightarrow \mathrm{GL}_{q^l}(\mathbb{Q}(\psi))$ and

$$R(a) = \begin{pmatrix} \psi(a) & 0 & \cdots & 0 \\ 0 & \psi(a)^r & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & \psi(a)^{r^{q^l-1}} \end{pmatrix} \qquad R(b) = \begin{pmatrix} 0 & \cdots & 0 & \psi(b^{q^l}) \\ 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Let $\sigma \in \mathrm{Gal}\left(\mathbb{Q}(\psi)/\mathbb{Q}(\psi^G)\right)$ be such that $\sigma\left(\psi(a)\right) = \sigma\left(\psi(a)^r\right)$ and $\psi\left(b^{q^l}\right)$ is fixed by σ, then $o(\sigma) = q^l$. The character field of R is

$$\begin{aligned} \mathbb{Q}(\psi^G) =& \mathbb{Q}\left(\mathrm{Tr}(R(a^i))_{i=1,..,p-1}, \psi(b^{q^l})\right) = \\ =& \mathbb{Q}\left(\mathrm{Tr}_{\mathbb{Q}(\psi)/\mathrm{Fix}(\sigma)}(\psi(a)^i)_{i=1,..,p-1}, \psi(b^{q^l})\right) \subseteq \mathrm{Fix}(\sigma). \end{aligned}$$

and it is a subfield of $\mathbb{Q}(\psi)$ of degree $|\mathbb{Q}(\psi) : \mathbb{Q}(\psi^G)| = q^l$, hence $\mathbb{Q}(\psi^G) = \mathrm{Fix}(\sigma)$. To find $s_{\mathbb{Q}}(\psi^G)$ we should find a subfield K of $\mathbb{Q}(\psi)$ minimal with respect to the property of existence of a K-representation of G similar to R. Let K be a subfield of $\mathbb{Q}(\psi)$ and let $t \in \mathbb{N}$ be such that $|K : \mathbb{Q}(\psi^G)| = q^t$, then $\mathrm{Fix}(\tau) = K$ where $\tau = \sigma^{q^t}$. From the Galois correspondence we have

$$\begin{tikzcd}
\mathbb{Q}(\psi) \arrow[d, dash, "q^{l-t}"'] & 1 \arrow[d, dash, "q^{l-t}"'] \\
K \arrow[d, dash, "q^t"'] & \langle\tau\rangle \arrow[d, dash, "q^t"'] \\
\mathbb{Q}(\psi^G) & \langle\sigma\rangle \subseteq \mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q}(\psi^G))
\end{tikzcd}$$

The automorphism τ acts on $\psi(a)$ as b^{q^t} acts on a.
Let $X = R(b^{q^t}) \in \mathrm{GL}_{q^l}(\mathbb{Q}(\psi))$ then

$$X^{-1}R(a)X = R(b^{q^t})^{-1}R(a)R(b^{q^t}) = R(a^{b^{q^t}}) = R(a)^{r^{q^t}} = R(a)^{\tau}$$

$$X^{-1}R(b)X = R(b^{q^t})^{-1}R(b)R(b^{q^t}) = R(b^{b^{q^t}}) = R(b) = R(b)^{\tau}.$$

Using the notation of Theorem 2.3.5 we have

$$N(X) = XX^{\tau}...X^{\tau^{q^{l-t}-1}} = R(b^{q^l})^{q^{l-t}} = R(b^{q^l}) = \psi(b^{q^l})I_{q^l},$$

thus there exists a K-representation of G similar to R if and only if there exists $\theta \in \mathbb{Q}(\psi)$ such that $N_{\mathbb{Q}(\psi)/K}(\theta) = \psi(b^{q^l})$.
Let $\varphi \in \mathrm{Irr}(PZ)$ be another character different from ψ such that its restriction to P is faithful and $|\ker\varphi| = q^{\delta}$. Similarly to what happens for ψ, we have $s_{\mathbb{Q}}(\varphi) = q^t$ for t the minimal integer such that there exists a subfield K of $\mathbb{Q}(\varphi^G)$ that satisfies $|K : \mathbb{Q}(\varphi^G)| = q^t$ and such that $N_{\mathbb{Q}(\varphi)/K}(\theta) = \varphi(b^{q^l})$ has a solution $\theta \in \mathbb{Q}(\varphi)$. Since $\varphi(b^{q^l})$ is a primitive $(q^{k-l-\delta})^{th}$-root of unity, then $\mathbb{Q}(\psi) = \mathbb{Q}(\varphi)$ and $\mathbb{Q}(\psi^G) = \mathbb{Q}(\varphi^G)$. Possibly $\psi(b^{q^l})$ and $\varphi(b^{q^l})$ are two different $(q^{k-l-\delta})^{th}$-roots of unity, anyway there exists a positive integer i such that $\varphi(b^{q^l}) = \psi(b^{q^l})^i$. If there exists $\theta \in \mathbb{Q}(\psi)$ such that $N_{\mathbb{Q}(\psi)/K}(\theta) = \psi(b^{q^l})$ then

$$\begin{aligned}\varphi(b^{q^l}) =& \psi(b^{b^l})^i = \left(N_{\mathbb{Q}(\psi)/K}(\theta)\right)^i = \left(\prod_{\sigma\in\mathrm{Gal}(\mathbb{Q}(\psi)/K)} \theta^{\sigma}\right)^i = \\ &= \left(\prod_{\sigma\in\mathrm{Gal}(\mathbb{Q}(\psi)/K)} (\theta^i)^{\sigma}\right) = N_{\mathbb{Q}(\psi)/K}(\theta^i).\end{aligned}$$

As a consequence, the two norm equations are both solvable or not solvable. Thus $s_{\mathbb{Q}}(\psi^G) = s_{\mathbb{Q}}(\varphi^G)$. □

Let $G = \langle a, b | a^p, b^{q^k}, a^b = a^r \rangle$ with $o_p(r) = q^l$ and let $\psi \in \mathrm{Irr}(PZ)$ with faithful restriction on the normal subgroup P. The character ψ is constant on the cosets of $\ker\psi$ in PZ. The class function $\bar{\psi}$ on $PZ/\ker\psi$ defined by $\bar{\psi}(g\ker\psi) = \psi(g)$ is an irreducible faithful character of $PZ/\ker\psi$. In the proof of Proposition 4.2.3 we have seen that $\ker\psi \leq Z$. Let $\delta \in \mathbb{Z}$ be such that $|\ker\psi| = q^\delta$. The group $G/\ker\psi$ contains $PZ/\ker\psi$ as a subgroup and it has the same metacyclic structure of the groups we are studying. In particular $G/\ker\psi \cong \langle a, \bar{b} | a^p, \bar{b}^{q^{k-\delta}}, a^{\bar{b}} = a^r \rangle$ with $o_p(r) = q^l$. The character $\psi^G \in \mathrm{Irr}(G)$ corresponds to $\bar{\psi}^{(G/\ker\psi)} \in \mathrm{Irr}(G/\ker\psi)$ and thus $s_{\mathbb{Q}}(\psi^G) = s_{\mathbb{Q}}(\bar{\psi}^{(G/\ker\psi)})$. This means that, in order to understand which values the Schur indices can assume in our groups it is enough to study the Schur index of characters induced by faithful characters of PZ.

Summing up what we have said previously we have that, in order to determine the Schur indices of the absolutely irreducible characters of G we have to determine the Schur indices of characters ψ^G such that $\psi \in \mathrm{Irr}(PZ)$ and $\psi_P \in \mathrm{Irr}(P)$ is faithful. We need to find the minimal non-negative integer t such that the norm equation

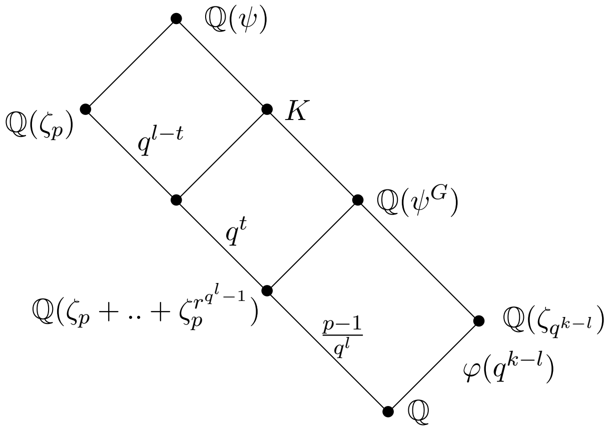
$$N_{\mathbb{Q}(\psi)/\mathrm{Fix}(\tau)}(\theta) = \psi(b^{q^l})$$

has a solution $\theta \in \mathbb{Q}(\psi)$, where $\tau \in \mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q}(\psi^G))$ has order q^{l-t}.

Solving norm equations is in general a difficult problem. However, in this particular situation, we are in a special case for two main reasons. First, we are not interested in finding a solution to the equation but just in understanding whether it has a solution or not. Moreover $\mathbb{Q}(\psi)/\mathbb{Q}(\psi^G)$ is a cyclic extension, thus we can use Hasse Norm Theorem (Theorem 3.3.1) which asserts that there is a solution to the norm equation if and only if there is a local solution everywhere.

In the following analysis we assume $k > l$. We just remember that, for the case $k = l$, we have already found the behaviour of the Schur indices in Proposition 4.2.1.

Passing from global to local norm different behaviour can arise depending on the ramification index of the prime ideal at which we are considering the completion. For this reason, we are now interested in finding which prime ideals of $\mathrm{Fix}(\tau)$ ramify in $\mathbb{Q}(\psi)/\mathrm{Fix}(\tau)$. Since the Galois extension $\mathbb{Q}(\psi)/\mathbb{Q}(\psi^G)$ is cyclic there exists a unique $\tau \in \mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q}(\psi^G))$ such that $|\mathrm{Fix}(\tau) : \mathbb{Q}(\psi^G)| = q^t$. For this reason to every integer $0 \leq t \leq l$ corresponds a unique field $\mathbb{Q}(\psi^G) \subseteq K \subseteq \mathbb{Q}(\psi)$ with $|K : \mathbb{Q}(\psi^G)| = q^t$. We summarize the fields involved in our discussion by the following schema:



where ψ is assumed to be a faithful character of PZ and hence $\psi(b^{q^l}) = \zeta_{q^{k-l}}$, a primitive $(q^{k-l})^{th}$-root of unity.

Let v be a prime ideal of $\mathcal{O}_K$, the ring of algebraic integers in K, and let w be a prime ideal of $\mathcal{O}_{\mathbb{Q}(\psi)}$ lying above v.

Since $\mathbb{Q}(\psi)$ is a cyclotomic extension of $\mathbb{Q}$ of order pq^{k-l} thus, by Corollary 10.4 in [26], the only primes that ramifies in $\mathbb{Q}(\psi)/\mathbb{Q}$ are p and q. As a consequence $e\,(w/v) = 1$ if v does not lie above p or q.

If v lies above q let $\beta = w \cap \mathcal{O}_{\mathbb{Q}(\zeta_{q^{k-l}})}$, then by [24, Theorem 26] it holds $e(\beta/q) = e(w/q) = \varphi(q^{k-l})$, hence

$$e\,(w/\beta) = \frac{e(w/q)}{e(\beta/q)} = 1,$$

thus, also $e\,(w/v) = 1$.

If v lies above p let $\beta = w \cap \mathcal{O}_{\mathbb{Q}(q^{k-l})}$, then by [24, Theorem 26] it holds $e(w/p) = \varphi(p) = p - 1$, hence

$$e\,(w/\beta) = \frac{e(w/p)}{e(\beta/p)} = e(w/p) = p - 1,$$

this means that $e\,(w/v) = q^{l-t}$ and v is totally ramifies in $\mathbb{Q}(\psi)/K$. Moreover p does not divide the ramification index, hence v is tamely ramified in $\mathbb{Q}(\psi)/K$. For more details about the computation of ramification indices in cyclotomic extensions see [6].

According to Section 2.3, if $\mathbb{Q}(\psi)_w$ is an unramified extension of K_v, then every unit of $\mathcal{O}_v$ is the norm of a unit in $\mathbb{Q}(\psi)_w$.
In our case $\zeta_{q^{k-l}}$ is invertible in $\mathcal{O}_v$, thus the local norm equation at every unramified prime v has a solution.
If v is an infinite prime of K then $K_v = \mathbb{C}$ because K can not be embedded into the real numbers. As a consequence also $\mathbb{Q}(\psi)_w = \mathbb{C}$, hence we are considering the trivial norm $N_{\mathbb{C}/\mathbb{C}}$. Any element of $\mathbb{C}$ is the norm of itself, thus also in the infinite case the local norm has a solution.
The only remaining case is when v ramifies in $\mathbb{Q}(\psi)/K$, that is when v lies above p. In this case v totally ramifies in $\mathbb{Q}(\psi)/K$ and, since $e\,(w/v) = q^{l-t}$ and $p \nmid e\,(w/v)$, then $\mathbb{Q}(\psi)_\beta/K_v$ is a totally tamely ramified extension, where $\beta = w \cap \mathcal{O}_{\mathbb{Q}(\zeta_{q^{k-l}})}$.
As a consequence

$$N_{\mathbb{Q}(\psi)_w/K_v}((\mathbb{Q}(\psi)_w)^*) = \langle N_{\mathbb{Q}(\psi)_w/K_v}(\pi), \zeta^{q^{l-t}}_{p^{f(v/p)}-1} \rangle U_{K_v},$$

where π is the uniformizer of $\mathcal{O}_{K_v}$ and $U_{K_v} = 1 + \pi\mathcal{O}_{K_v}$. Since $f(v/\beta) = 1$ then the residue field of $\mathbb{Q}(\psi)_w$ is isomorphic to the residue field of K_v and $f\,(v/p) = f\,(\beta/p)$. Our aim is now to determine the residue degree $f(\beta/v)$. By Proposition 3.1.2 we have that p splits completely in $\mathbb{Q}(\zeta_{q^{k-l}})/\mathbb{Q}$ if and only if $p \equiv 1 \mod q^{k-l}$. This mean that we have to distinguish two different cases:

- if $k - l \leq m$ then $p \equiv 1 \mod q^{k-l}$. Here $f(\beta/p) = 1$ and the residue field of $\mathbb{Q}(\zeta_{q^{k-l}})_\beta$ is isomorphic to the residue field of $\mathbb{Q}_p$. The local norm equation has a solution if and only if

$$\begin{aligned} \zeta_{q^{k-l}} \in N_{\mathbb{Q}(\psi)_w/K_v}((\mathbb{Q}(\psi)_w)^*) &\Leftrightarrow q^{k-l} \mid \frac{p-1}{q^{l-t}} \\ &\Leftrightarrow k - l \leq m - l - t \\ &\Leftrightarrow t \geq k - m. \end{aligned}$$

  The norm equation has a solution exactly for every $t \geq k - m$, in particular the minimal non-negative integer such that the equation has a solution is equal to $\max(0, k-m)$.

- if $k-l \geq m$ then $l \leq k-m$, in particular the minimal non-negative integer such that the equation has a solution is less or equal to $\max(0, k-m)$.

This allow us to conclude the proof of the first part of Conjecture 4.2.1 that we can now announce as a proposition

Proposition 4.2.4. *Let $G = \langle a, b \mid a^p, b^{q^k}, a^b = a^r \rangle$ with $o_p(r) = q^l$, $k \geq 2$, q, p odd primes such that $m \geq 1$ is the maximal power of q dividing $p-1$ and $1 \leq l \leq \min(k, m)$. Then, for all $\chi \in \mathrm{Irr}(G)$ there exists a positive integer $t \leq \min(l, \max(0, k-m))$ such that $s_{\mathbb{Q}}(\chi) = q^t$.*

Proof. By Proposition 4.2.2 G has q^k linear characters with trivial Schur index and $(p-1)q^{k-2l}$ characters of degree q^l. Let $\chi \in \mathrm{Irr}(G)$ have degree q^l. By Proposition 2.3.1 $s_{\mathbb{Q}}(\chi) = q^t$ for some integer $0 \leq t \leq l$. Let P be the subgroup of G generated by a and its center Z. Then $\chi = \psi^G$ for some $\psi \in \mathrm{Irr}(PZ)$ and it can be seen as a faithful character in $\mathrm{Irr}(G/\ker\psi)$. It holds

$$G/\ker\psi \cong \langle a, \bar{b} | a^p, \bar{b}^{q^{k-\delta}}, a^{\bar{b}} = a^l \rangle \text{ with } o_p(r) = q^l.$$

Let $\bar{\psi}$ be the character corresponding to ψ in $PZ/\ker\psi$. From Theorem 2.3.5, t is the minimal non-negative integer such that there exists a subfield K of $\mathbb{Q}(\bar{\psi})$ containing $\mathbb{Q}(\bar{\psi}^G)$ with $|K : \mathbb{Q}(\bar{\psi}^G)| = q^t$ such that there exists a solution to the norm equation

$$N_{\mathbb{Q}(\bar{\psi})/K}(\theta) = \bar{\psi}(b^{q^l}).$$

Let $\delta \in \mathbb{N}$ be such that $|\ker\psi| = q^\delta$. If $k-\delta-l \leq m$ then such a minimal t is $\max(0, k-\delta-m)$, which is trivially less than or equal to $\max(0, k-m)$. If $k-\delta-l > m$ then we can not determine the minimal t but we know it is at most l. □

Let $\delta \in \mathbb{N}$ be such that $|\ker\psi| = q^\delta$. From the proof of Proposition 4.2.4 we can see that, if $k-\delta-l \leq m$ then the Schur index can be calculated explicitly. In particular, a group G as in the statement of Proposition 4.2.4 with the additional condition on the parameters $k-l \leq m$ has q^k linear characters with trivial Schur indices and $\frac{\Delta_\delta(p-1)}{q^l}$ characters of degree q^l and

Schur index $q^{\max(0,k-m-\delta)}$, where $\Delta_{k-l}=1$ and for $\delta \neq k-l$

$$\begin{aligned}\Delta_\delta =&|\{\psi \in \mathrm{Irr}(Z) \text{ s.t. } |\ker\psi| = q^\delta\}| = \\ =&|i=0,..,q^{k-l}-1 \text{ s.t. } v_q(i)=\delta| = \\ =&q^{k-l-\delta-1}(q-1).\end{aligned}$$

This allow us to find explicit formulas for determine how many irreducible characters of G have a given Schur index. In particular the number of character of trivial Schur index is obtained as the sum of the number of linear characters and all of the characters of degree q^l such that $\max(0,k-m-\delta)=0$. As a consequence

$$\left|\{\chi \in \mathrm{Irr}(G) \text{ s.t. } s_{\mathbb{Q}}(\chi)=1\}\right| = q^k + \frac{p-1}{q^l} + \sum_{\delta=k-m}^{k-l-1}(p-1)(q-1)q^{k-2l-\delta-1}.$$

The number of character with Schur index $q^{k-m-\delta}$ is $(p-1)(q-1)q^{k-2l-\delta-1}$. Hence, if $k-m>0$ then for a fixed $0<t\leq k-m$ it holds

$$\left|\{\chi \in \mathrm{Irr}(G) \text{ s.t. } s_{\mathbb{Q}}(\chi)=q^t\}\right| = (p-1)(q-1)q^{t-2l+m-1}.$$

Note that, for every $0 \leq t \leq \max(0,k-m)$ the integer $(p-1)(q-1)q^{t-2l+m-1}$ is non-negative, hence the Schur index assumes every value in the range $[0,\max(0,k-m)]$.

4.3 Metacyclic Groups of order a multiple of a prime

In this section we prove a last generalization of the situation studied previously in this chapter by considering the semidirect product between a normal cyclic group P of prime order p and any other cyclic group K of order k coprime with p. In order to avoid $P \rtimes_\varphi K$ to a be a direct product we want $\varphi(K)$ to be a non-trivial subgroup of $\mathrm{Aut}(P)$. This condition can be seen well if we express $P \rtimes_\varphi K$ by finite group presentation. Thus, let $G=\langle a,b \mid a^p, b^k, a^b=a^r\rangle$ where $o_p(r)=l$, for some integer $l>1$ such that $l\big|(k,p-1)$, where by $(k,p-1)$ we denote the greatest common divisor between k and $p-1$. Let P be the p-Sylow subgroup of G and K be the cyclic subgroup of G generated by b. The center $Z=\langle b^l\rangle$.

Proposition 4.3.1. *Let $\lambda \in \mathrm{Irr}(P)$. Then*

$$I_G(\lambda) = \begin{cases} G & \lambda = 1 \\ PZ & \lambda \neq 1 \end{cases}$$

Proof. Let $\lambda \in \mathrm{Irr}(P)$ be non-trivial, then $\lambda(a) = \zeta_p$ for some primitive p^{th}-root of unity ζ_p. Let $0 \leq i \leq k-1$. If $b^i \in I_G(\lambda)$ then $\lambda^{b^i}(a) = \lambda(a)$. This means that $\zeta_p^{r^{-i}} = \zeta_p$ and $r^{-i} \equiv 0 \mod p$. As a consequence $o_p(r)\big|i$, so $I_G(\lambda) \cap K = Z$. Since $P \lhd I_G(\lambda)$ and $Z \lhd I_G(\lambda)$, we have $I_G(\lambda) = PZ$. □

Let $\chi \in \mathrm{Irr}(G)$ be any irreducible character of G. Combining Clifford's theorem and Proposition 4.3.1 we have $\chi_P = \chi(1) \cdot 1$ or $\chi_P = e \cdot \sum_{i=1}^{l} \lambda_i$ for some non-trivial conjugated characters $\lambda_1, .., \lambda_l \in \mathrm{Irr}(P)$ and some positive integer e. In the first case P is a subgroup of $\ker \chi$, hence $\chi \in \mathrm{Irr}(G/P)$ and it is linear because G/P is cyclic. In the second case we have $I_G(\lambda_i) = PZ$. Let $\lambda = \lambda_1$, then $\lambda^{PZ} = \sum e_i \psi_i$ for some $\psi_i \in \mathrm{Irr}(PZ)$ and some positive integers e_i. Since $(\psi_i)_P = e_i \lambda$ then $e_i = 1$. Using Gallagher's theorem we can conclude that $\lambda^{PZ} = \sum_{i=1}^{kl^{-1}} \psi_i$, hence $\chi_P = \sum_{i=1}^{l} \lambda_i$. . As a consequence $\chi = \psi_i^G$ for some component ψ_i of λ^{PZ} and $\chi(1) = |G : PZ| = l$.

Proposition 4.3.2. *Let $\psi, \varphi \in \mathrm{Irr}(PZ)$ be such that $\ker \psi = \ker \varphi \leq Z$. Then the degree over $\mathbb{Q}(\psi^G)$ of the minimal field for ψ^G contained in $\mathbb{Q}(\psi)$ is equal to the degree over $\mathbb{Q}(\varphi^G)$ of the minimal field for φ^G contained in $\mathbb{Q}(\varphi)$.*

Proof. The center Z is a cyclic group generated by b^l. Let $\delta \in \mathbb{Z}$ be such that $\ker \psi = \ker \varphi = \langle b^{l\delta} \rangle$. Then $\psi(b^l) = \zeta_\delta$ where ζ_δ is some primitive δ^{th}-root of unity. Without loss of generality we can consider $1 \leq \delta \leq kl^{-1}$.
Let $R : G \longrightarrow \mathrm{GL}_l(\mathbb{Q}(\psi))$ be the representation induced by ψ (seen as a one dimensional representation) over G. Then R affords character ψ^G and it is given by

$$R(a) = \begin{pmatrix} \psi(a) & 0 & \cdots & 0 \\ 0 & \psi(a)^r & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & \psi(a)^{r^{l-1}} \end{pmatrix} \qquad R(b) = \begin{pmatrix} 0 & \cdots & 0 & \psi(b^l) \\ 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix}.$$

The character field $\mathbb{Q}(\psi^G)$ corresponds to $\mathbb{Q}(\mathrm{Tr}(R(a)), \psi(b^l))$. Notice that $\mathbb{Q}(\psi)/\mathbb{Q}(\psi^G)$ is a cyclic extension of degree l thus, for every integer $0 \leq t \leq l$ there is a unique field K_t such that $\mathbb{Q}(\psi^G) \subseteq K_t \subseteq \mathbb{Q}(\psi)$ and $|K_t : \mathbb{Q}(\psi^G)| = t$. Let $X = R(b^t)$ and $\tau \in \mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q}(\psi^G))$ be such that $\mathrm{Fix}(\tau) = K_t$. We have $R(g)X = XR(g)^\tau$ for all $g \in G$ and $N_{\mathbb{Q}(\psi)/K}(X) = \psi(b^l)I_l$. By Theorem 2.3.5 the representation R is equivalent to a representation over K if and only if the norm equation $N_{\mathbb{Q}(\psi)/K_t}(\theta) = \psi(b^l)$ has a solution. Let t be the minimum integer such that the norm equation has a solution. Exactly in the same way we can consider the representation induced by φ. Also $\varphi(b^l)$ is a primitive δ^{th}-root of unity, hence $\varphi(b^l) = \zeta_\delta^i$ for some integer i and $\mathbb{Q}(\psi) = \mathbb{Q}(\varphi)$. The degree over $\mathbb{Q}(\varphi^G)$ of the minimal field for φ^G contained in $\mathbb{Q}(\varphi)$ is the minimum integer t such that the norm equation $N_{\mathbb{Q}(\varphi)/K_t} = \varphi(b^l)$ has a solution. The conclusion comes from the observation that the first norm equation is solvable if and only if the second equation is solvable too. □

Proposition 4.3.3. *Let $\chi \in \mathrm{Irr}(G)$ such that $\chi(1) = l$. Let $\psi \in \mathrm{Irr}(PZ)$ be such that $\chi = \psi^G$ and $|\ker\psi| = \delta$ for some $\delta \mid kl^{-1}$. Let s be the degree over $\mathbb{Q}(\chi)$ of the minimal field for χ contained in $\mathbb{Q}(\psi)$. Then*

1. *if $\frac{k}{l\delta} \mid p-1$ then $s \mid \frac{k}{(k,p-1)}$;*
2. *if $\frac{k}{l\delta} \nmid p-1$ then for all prime q such that $v_q\left(\frac{k}{(k,p-1)}\right) > v_q(l)$ it holds $v_q(s) < v_q\left(\frac{k}{(k-p-1)}\right)$.*

Proof. The value of s is the minimum integer t such that the norm equation $N_{\mathbb{Q}(\psi)/K_t}(\theta) = \zeta$ has a solution, where ζ is a primitive $\left(\frac{k}{l\delta}\right)^{th}$-root of unity and K_t is the unique field such that $\mathbb{Q}(\psi^G) \subseteq K_t \subseteq \mathbb{Q}(\psi)$ and $|K : \mathbb{Q}(\psi^G)| = t$. We use Hasse Theorem 3.3.1 to verify the resolvability of the norm equation. Let v be any prime ideal of $\mathcal{O}_{K_t}$ lying above a prime q in $\mathbb{Z}$ and w be a prime ideal of $\mathcal{O}_{\mathbb{Q}(\psi)}$ lying above v. If $q \nmid p\frac{k}{l\delta}$ then $e(w/v) = 1$. If $q \mid \frac{k}{l\delta}$, let $\beta = w \cap \mathcal{O}_{\mathbb{Q}(\zeta)}$.Since p does not divide k, the ramification index $e(w/\beta) = \varphi(\frac{k}{l\delta}) = e(\beta/q)$, hence $e(w/\beta) = 1$. If $q = p$ then $e(w/\beta) = p-1$ and $e(w/v) = \frac{l}{t}$. Moreover $(p, p-1) = 1$, therefore β ramifies tamely totally in $\mathbb{Q}(\psi)/\mathbb{Q}(\zeta)$.

As a consequence ζ is a norm in $\mathbb{Q}(\psi)/K_t$ if and only if it is a local norm for every completion at primes over p. Let v and w be prime ideals of $\mathcal{O}_{\mathbb{Q}(\psi)}$ and K_t respectively, lying above p, and L_w, K_{tv} be their completion. The

extension L_w/K_{tv} is a totally ramified extension, hence the residue field of L_w is isomorphic to the one of K_{tv}, while the residue field of K_{tv} is isomorphic to the one of $\mathbb{Q}(\zeta)_\beta$. In order to determine the residue field of $\mathbb{Q}(\zeta)_\beta$ we need to determine $f(\beta/p)$.
If $\frac{k}{l\delta} \mid p-1$ then, by Proposition 3.1.2 we have $f(\beta/p) = 1$. Thus

$$N_{L_w/K_{tv}}(L_w^*) = \langle \pi_t, \zeta_{p-1}^{\frac{l}{t}} \rangle U_{K_{tv}}$$

where π_t is the uniformizer of $\mathcal{O}_{K_{tv}}$ and $U_{K_{tv}}$ is the group of units of K_{tv}. As a consequence,

$$\begin{aligned} \zeta \text{ is a norm in } L_w/K_{tv} &\Leftrightarrow \frac{k}{l\delta} \mid \frac{t(p-1)}{l} \\ &\Leftrightarrow k \mid t\delta(p-1) \\ &\Leftrightarrow \frac{k}{(p, k-1)} \mid t\delta. \end{aligned}$$

The minimum integer t that satisfies the condition is $t = \frac{k}{(k,p-1)} \frac{1}{(\frac{k}{(k,p-1)}, \delta)}$.
If $\frac{k}{l\delta} \nmid p-1$ then $f(\beta/p) > 1$. Let q be any prime number. If we suppose $v_q\left(\frac{k}{(k,p-1)}\right) > v_q(l)$ then, by $s_{\mathbb{Q}}(\chi) \mid \chi(1)$, follows

$$v_q(s) \leq v_q(l) < v_q\left(\frac{k}{(k,p-1)}\right).$$

We remark that a prime q that satisfies the condition $v_q\left(\frac{k}{(k,p-1)}\right) > v_q(l)$ always exists because the condition $\frac{k}{l\delta} \nmid p-1$ is equivalent to $\frac{k}{(k,p-1)} \nmid l\delta$. Hence, there exists at least one prime number q such that

$$v_q\left(\frac{k}{(k,p-1)}\right) > v_q(l) + v_q(\delta) \geq v_q(l).$$

□

Chapter 5

Construction of Irreducible Modules with assigned Character

One of the first questions to deal with when approaching the problem of constructing a representation of a finite group G affording a given character χ, is about which field is needed to realize the representation.
Let $\chi \in \mathrm{Irr}(G)$, we can see χ as a class function on $\mathbb{C}$ and look for a representation of G over $\mathbb{C}$ of degree $n = \chi(1)$ affording χ. From a computational point of view, and more in general in algebra, working with the complex number field may be very difficult because every complex number must be approximated in computations. Moreover, the construction of a representation affording a given character is a difficult problem because there are many degrees of freedom in the construction due to the fact that given a representation affording χ all the similar representations, obtained by conjugation with any invertible matrix, is again a representation affording χ.

5.1 The splitting strategy

The goal of this section is to discuss the problem of the construction of an irreducible representation starting from its character. We have already introduced the main definitions and results needed to face this problem.

Let G be a finite group and $\chi \in \mathrm{Irr}(G)$ be an absolutely irreducible character of G. The idea is to reduce the complexity of finding a representation over the complex number field to finding a representation of G over some smaller field. We now describe a possible strategy to approach this problem. Any detail and computational aspect will be discussed later.

Let F be any field such that $F \subseteq \mathbb{C}$. In Proposition 2.1.1 we have seen that $\psi = s_F(\chi)\mathrm{GalSum}_F(\chi)$ is the character afforded by an irreducible F-representation of G. Hence, there exists an irreducible FG-module affording character ψ. We now suppose to be able to find an irreducible FG-module M satisfying such a condition. Let K be a minimal field for the character χ containing F. Then $F(\chi) \subseteq K \subseteq \mathbb{C}$ and $|K : F(\chi)| = s_F(\chi)$. Once we have a splitting field we can extend the scalar field of M to K by tensor product. We denote the KG-module $M \otimes_F K$ by M^K. Since K is a minimal field for χ and χ is an irreducible constituent of ψ then some of the irreducible constituents of M^K affords character χ. Our problem now is to find a suitable irreducible component of M^K.

We can illustrate our strategy with the following schema:

$$\begin{tikzcd}
 & \chi \in \mathrm{Irr}(G) \arrow[dl] \arrow[dr] & \\
\psi = s_F(\chi)\mathrm{GalSum}_F(\chi) \arrow[d] & & F(\chi) \subseteq \mathbb{C},\ |F(\chi) : F| = t \arrow[d] \\
M\ FG\text{-module} \longleftrightarrow \psi \arrow[dr] & & \begin{array}{c} K \supseteq F(\chi) \\ |K : F(\chi)| = s_F(\chi) \end{array} \arrow[dl] \\
 & M^K = M \otimes_F K \quad KG\text{-module} \arrow[d] & \\
 & \text{Decomposition of } M^K = \bigoplus_{i=1}^{t} \bigoplus_{j=1}^{s_F(\chi)} S_i &
\end{tikzcd}$$

In particular, by construction of character ψ, the decomposition of M^K is well known:

$$M^K \cong \underbrace{S_1 \oplus ... \oplus S_1}_{H_1} \oplus \underbrace{S_2 \oplus ... \oplus S_2}_{H_2} \oplus \ldots \oplus \underbrace{S_t \oplus ... \oplus S_t}_{H_t}$$

$$H_1 \quad \oplus \quad H_2 \quad \oplus \ldots \oplus \quad H_t$$

where S_i denote the absolutely irreducible components of M^K and H_i are irreducible $F(\chi)G$-modules, hence H_i^K are the homogeneous components of M^K.

From the theoretical point of view this approach will produce the desired result. From the computational point of view not every aspect is clear. We now follow the steps of the procedure in order to understand if the algorithm is reasonable or not.

5.2 Computational aspects

Let $\chi \in \mathrm{Irr}(G)$ be an irreducible character of a finite group G and F be a number field. To calculate the character ψ we need to have a good way to determine both $s_F(\chi)$ and $\mathrm{GalSum}_F(\chi)$. The calculation of the Schur index of a given character in MAGMA uses an algorithm due to Gabi Nebe and Bill Unger [32] and extended by Claus Fieker to the calculation of Schur indices over number fields. The calculation of $\mathrm{GalSum}_F(\chi)$ is very easy. As a consequence the computation of ψ is not a difficult problem. The same holds for the determination of $F(\chi)$: it is immediate once χ is given. Computational problems arise when we want to determine an FG-module of character ψ. As we have already said, the problem of the construction of a representation starting from its character is very difficult and, if we were able to do it in general, we would have solved our problem without any other discussion. In general this problem does not have a good algorithm to be solved. In [30] Allan Kenneth Steel introduced a new algorithm for $F = \mathbb{Q}$ named *IrreducibleRationalRepresentations* (it is used in MAGMA when the function *IrreducibleModules* is called with the rational field as input field). This algorithm takes as input a list of characters in $\mathrm{Irr}_{\mathbb{Q}}(G)$ (possibly the entire list for rational characters) and gives as output a list of $\mathbb{Q}G$-modules affording characters of the input list. The idea behind this algorithm is to create a queue of virtual representations of G sorted by degree, starting with smallest representations. These representations can be constructed as permutation representations, representations induced by representations of subgroups or tensor product of two representations. Following the sort of the queue each $\mathbb{Q}G$-module is decomposed into irreducible modules and non-isomorphic modules affording characters in the input list are given as output.

New representations are added to the queue until a rational module is found for each input character. In general this algorithm can be very slow and it needs a lot of memory, but for groups reasonably large it can be useful. We remark that this algorithm works only for $F = \mathbb{Q}$, which is the most interesting case.

Once we have the irreducible FG-module M affording character ψ we can divide the problem of finding its absolutely irreducible components in two steps: first we find the homogeneous components of M^K and then we split them in absolutely irreducible modules. Homogeneous components of M^K correspond to irreducible components of $M^{F(\chi)}$. To find them we do not need to determine the minimal field K.

Algorithms for finding the homogeneous components of an FG-module are known. From Theorem 2.2.4 and 2.2.5 we have

$$Z(\mathrm{End}_{FG}(M)) \cong \bigoplus_{\bar{\chi} \in \mathrm{GalOrb}_F(\chi)} F(\bar{\chi}).$$

Let $\alpha \in Z(\mathrm{End}_{FG}(M))$ and f be the minimal polynomial of α over F. Then f is irreducible in $F[x]$ and it splits completely in $F(\chi)[x]$. Hence

$$f = \prod_{i=1}^{t} (x - \alpha_i) \text{ for some } \alpha_i \in F(\chi).$$

As a consequence $(\alpha - \alpha_i I)$ are singular elements of $\mathrm{End}_{F(\chi)G}(M^{F(\chi)})$ for each $1 \leq i \leq t$. Thus $\ker(\alpha - \alpha_i I)$ is a proper submodule of $M^{F(\chi)}$ for each i. Iterating this procedure on the found submodules, we get all the homogeneous components of $M^{F(\chi)}$, in particular they are irreducible $F(\chi)$-modules affording characters of the form $s_F(\chi)\bar{\chi}$, where $\bar{\chi} \in \mathrm{Irr}(G)$ is an absolutely irreducible character conjugate to χ and exactly one of them affords character $s_F(\chi)\chi$. Let H be such an irreducible $F(\chi)G$-module. It follows that

$$H^K \cong \underbrace{S \oplus S \oplus ... \oplus S}_{s_F(\chi)}$$

with S an absolutely irreducible component of H. A complete and improved version of this algorithm for rational modules is *HomogeneousComponents* in [30]. In order to apply the algorithm for splitting modules into homogeneous components over any number field F and with the aim of interrupting our computations when an irreducible $F(\chi)G$-module of character $s_F(\chi)$ is found, we used the following code for our computations:

```
Homogeneous_Component:= function(M, chi)
s:=SchurIndex(chi);
Z:=CentreOfEndomorphismRing(M);
d:=Dimension(Z);
B:=Basis(Z);
for b in B do
  f:=MinimalPolynomial(b);
  if (IsIrreducible(f) and Degree(f) eq d) then
    return M;
  end if;
  Fac:=Factorization(f);
  k:=#Fac;
  if (k gt 1) then
    CompOmo:=[];
    for i in [1..k] do
      e:=Evaluate(Fac[i][1]^Fac[i][2],b);
      S:=sub<M|Image(e)>;
      L:=$$(S, chi);
      if Character(L) eq s*chi then
        return L;
      end if;
    end for;
  end if;
end for;
return M;
end function;
```

At this point, the aim is to find the absolutely irreducible components of the $F(\chi)G$-module affording character $s_F(\chi)\chi$. In this case we can not use the same technique used for splitting M because $Z(\mathrm{End}_{F(\chi)G}(H)) \cong F(\chi)$ and the minimal polynomial of each element of the center is a degree one polynomial in $F(\chi)$. Let K be any splitting field of χ, then we can summarize the algebras involved in the splitting process by:

$$\begin{tikzcd}
\mathrm{End}_{FG}(M) \arrow[d, dash, "s_F(\chi)"'] & \mathrm{End}_{F(\chi)G}(H) \arrow[d, dash, "s_F(\chi)"'] & \mathrm{End}_{KG}(S) \cong K \\
K \arrow[d, dash, "s_F(\chi)"'] & K \arrow[d, dash, "s_F(\chi)"'] & \\
F(\chi) \arrow[d, dash, "t"'] & F(\chi) & \\
F & &
\end{tikzcd}$$

Anyway the idea of finding a proper submodule of H looking for singular elements in $\mathrm{End}_{F(\chi)G}(H)$ is still valid, we just need to focus our attention out of the center.

In the particular case of $s_F(\chi) = 1$ the problem is trivial because $F(\chi)$ is also a minimal field for χ over F and the $F(\chi)G$-module H found above is already the wanted output. This means that the described algorithm can successfully be used for finding a representation of G affording a given character $\chi \in \mathrm{Irr}(G)$ when $s_F(\chi) = 1$. Moreover, the representation given by the algorithms is over a minimal field of χ.

If $s_F(\chi) = 2$ then $\mathrm{End}_{F(\chi)G}(H)$ is a division algebra over $F(\chi)$ of degree 4. By Proposition 1.2.1 in [16] the algebra $\mathrm{End}_{F(\chi)G}(H)$ is isomorphic to a generalized quaternion division algebra. To find such a quaternion algebra and an isomorphism from the endomorphism algebra to it we use an algorithm implemented in MAGMA and due to John Voight ([33]), named *IsQuaternionAlgebra*. Let $a, b \in F(\chi)$ be such that $\mathrm{End}_{F(\chi)G}(H)$ is isomorphic to $\langle 1, i, j, ij\rangle_{F(\chi)}$ with $i^2 = a$ and $j^2 = b$. By Proposition 1.3.2 in [16] the conic equation $ax^2 + by^2 = z^2$ has only the zero solution over $F(\chi)$ and it has at least one non-trivial solution over K for every splitting field K of $\mathrm{End}_{F(\chi)G}(H)$. We can use this fact to determine a splitting field K for $\mathrm{End}_{F(\chi)G}(H)$ considering a quadratic extension of $F(\chi)$ such that the equation has a non-zero solution on it. Let $K = F(\chi)(\sqrt{a})$ as Proposition 1.2.3 in [16] suggests (but other choices can be made). Since

$$\mathrm{End}_{KG}(H \otimes_{F(\chi)} K) \cong \mathrm{End}_{\mathrm{F(\chi)G}}(H) \otimes_{F(\chi)} K \cong M_{s_F(\chi)}(K),$$

every element $e \in \mathrm{End}_{KG}(H \otimes_{F(\chi)} K)$ correspondent by the previous isomorphism to a singular matrix is a singular endomorphism of H^K and $\ker e$ is a submodule of H^K. In particular, $\mathrm{End}_{\mathrm{F(\chi)G}}(H) \otimes_{F(\chi)} K$ is isomorphic to $\langle 1, i, j, ij\rangle_K$. We may look for elements e in the quaternion algebra such that $e^2 = 0$. Let $e = t + xi + yj + zij$ for some $t, x, y, z \in K$, then $0 = e^2 = t^2 + 2txi + 2tyj + 2tzij + x^2a + y^2b - z^2ab$. Hence the coordinates of e must satisfy

$$\begin{cases} t = 0 \\ x^2a + y^2b - z^2ab = 0. \end{cases}$$

Since we have chosen K to be $F(\chi)(\sqrt{a})$ then $(0, \sqrt{a}, 1) \in K^3$ is a solution for the second equation in the system. Thus the element corresponding to $e = \sqrt{a}j + ij$ in $\mathrm{End}_{\mathrm{F(\chi)G}}(H) \otimes_{F(\chi)} K$ is singular element and its kernel is a proper submodule of H^K. Schur index equal 2 implies H^K is the sum of two absolutely irreducible modules, hence the submodule that we have found is exactly the module we were looking for.

The following Magma code allow us to construct absolutely irreducible modules over minimal fields affording a given character of Schur index less then 3 using the procedure described above:

```
ConstructModule:= function(G, chi)
irrs:=IrreducibleModules(G, Rationals());
F:=CharacterField(chi);
s:=SchurIndex(chi);
psi:=0;
for x in GaloisOrbit(chi) do
   psi+:=s*x;
end for;
modules:=[M: M in irrs | Dimension(M) eq psi(1)];
modules:=[M: M in modules | Character(M) eq psi];
M:=ChangeRing(modules[1], F);
if  s eq 1 then
   return Homogeneous_Component(M, chi);
elif s eq 2 then
  H:=Homogeneous_Component(M, chi);
  E:=EndomorphismRing(H);
  _,Q,_:=IsQuaternionAlgebra(E);
  K:=ext<F|MinimalPolynomial(Q.2)>;
  HK:=ChangeRing(H,K);
  EK:=EndomorphismRing(HK);
  _,QK,phi:=IsQuaternionAlgebra(EK);
  e:=Inverse(phi)(K.1*QK.3+QK.2*QK.3);
  S:=sub<HK| Image(e)>;
  return S;
else error ''Schur index grather than 2'';
end if;
end function;
```

5.3 Schur Index equal 3

Things are more complicated when $s_F(\chi) > 2$ because the endomorphism algebra has a more complicated structure and the splitting field is no more a quadratic extension of the character field. As a consequence of Albert-Hasse-Brauer-Noether Theorem (see section 18.4 in [27]) we have the following:

Theorem 5.3.1. *(Theorem 18.6 in [27]) Let A be a central simple algebra over a number field F, then A is a cyclic algebra (i.e. there is a strictly maximal subfield K of A such that K is a cyclic extension of F).*

Hence, under our hypothesis, $\mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$ is a cyclic algebra. The structure of a cyclic algebra is somehow a generalization of a quaternion algebra for dimension greater than 4.

Proposition 5.3.1. *(Proposition 15.1 a in [27]) Let A be a cyclic algebra over F, K be a strictly maximal subfield of A and $\mathrm{Gal}(K/F) = \langle\sigma\rangle$, with $o(\sigma) = n$. Then there exists an invertible element $\mu \in A$ such that*

1. *$A = \oplus_{j=1}^{n} u^j K$;*
2. *$x^\mu = x^\sigma$ for all $x \in K$;*
3. *$\mu^n = a \in F^*$.*

Finding a field K and elements u and a in $\mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$ that realize the cyclic algebra is not a trivial problem. In order to lighten our notation, from now on we denote simply by $s = s_F(\chi)$, the degree of the algebra $\mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$. To find a field K with the desired properties we may look for an element $\alpha \in \mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$ such that its minimal polynomial over $F(\chi)$ is of the form $x^s - b$, for some $b \in F(\chi)$. Let K be a splitting field for $x^s - b$ over $F(\chi)$ and let β be a primitive element of the field extension $K/F(\chi)$. The Benard-Schacher Theorem (2.3.3) asserts that $F(\chi)$ contains a primitive s^{th}-root of unity ζ_s, thus let σ be the automorphism of K such that $\sigma(\beta) = \zeta_s\beta$ and $\sigma(x) = x$ for all $x \in F(\chi)$. Then $\mathrm{Gal}(K/F(\chi)) = \langle\sigma\rangle$.

The field K is a normal extension of $F(\chi)$, thus $x^s - b$ splits completely on K as

$$x^s - b = \prod_{i=1}^{s}(x - \beta\zeta_s^i).$$

For each i we have that $\ker\left(\alpha - \beta\zeta_s^i\right)$ is a proper submodule of H^K. If the obtained module is not irreducible we can apply this procedure again until we have an absolutely irreducible module affording character χ. Let us remark that until now we have not used the fact that $\mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$ is a cyclic algebra.

What is still difficult to do is to find an $\alpha \in \mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$ with minimal polynomial of the form $x^s - b$ over $F(\chi)$. We face this problem for the case of $s = 3$. Let $\alpha \in \mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$. Since $\dim_{F(\chi)} H = 3\chi(1)$ then $\mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$ can be considered as a subalgebra of $M_{3\chi(1)}(F(\chi))$. Let $m(x)$ and $p(x)$ be respectively the minimal polynomial of α over $F(\chi)$ and the characteristic polynomial of α. Since $\mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$ has degree 3 then $\deg m$ is equal to 1 or 3. The minimal polynomial is linear if and only if α is a scalar matrix. To avoid this situation we consider only non-scalar elements of $\mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$. Hence, we suppose, $\deg m = 3$, while $\deg p = 3\chi(1)$. The polynomial m is the minimal polynomial of three different elements in $\mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$, that are α, $\zeta_3\alpha$ and $\zeta_3^2\alpha$. Let K be a splitting field for m and $\lambda_1, \lambda_2, \lambda_3 \in K$ be the three different roots of m. The minimal and the characteristic polynomial of α have the same roots, thus $\lambda_1, \lambda_2, \lambda_3$ are eigenvalues of α. The algebraic multiplicity $m_a(\lambda_i)$ of λ_i is such that $\chi(1) \leq m_a(\lambda_i)$ (because the geometric multiplicity of λ_i is $\chi(1)$, the dimension of the absolutely irreducible components of H). On the other hand $\sum_{i=1}^{3} m_a(\lambda_i) = 9$, hence $m_a(\lambda_i) = 3$ for each i. This implies $p(x) = m(x)^{\chi(1)}$.

We now consider the matrix

$$\Lambda = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix}.$$

Its characteristic polynomial coincides with $m(x)$ and it can be determined by Newton's identities as

$$\begin{aligned} m(x) =& x^3 - \mathrm{Tr}(\Lambda)x^2 + \frac{1}{2}\left(\mathrm{Tr}(\Lambda)^2 - \mathrm{Tr}(\Lambda^2)\right)x - \\ &- \frac{1}{6}\left(\mathrm{Tr}(\Lambda)^3 + 2\mathrm{Tr}(\Lambda^3) - 3\mathrm{Tr}(\Lambda)\mathrm{Tr}(\Lambda^2)\right). \end{aligned}$$

The minimal polynomial m is of the desired form if the coefficients of terms of degree 1 and 2 are zero.

$$\begin{cases} -\mathrm{Tr}(\Lambda) = 0 \\ \frac{1}{2}\left(\mathrm{Tr}(\Lambda)^2 - \mathrm{Tr}(\Lambda^2)\right) = 0 \end{cases} \quad \to \quad \begin{cases} \mathrm{Tr}(\Lambda) = 0 \\ \mathrm{Tr}(\Lambda^2) = 0. \end{cases}$$

As we have said the eigenvalues of α are λ_1, λ_2 and λ_3, each with multiplicity $\chi(1)$. This means that $\mathrm{Tr}(\alpha) = \chi(1)\mathrm{Tr}(\Lambda)$ and $\mathrm{Tr}(\alpha^2) = \chi(1)\mathrm{Tr}(\Lambda^2)$. This allow us to conclude that, in order to find elements of $\mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$ with minimal polynomial of the form $x^3 - b$, we have to find an element such that

$$\begin{cases} \mathrm{Tr}(\alpha) = 0 \\ \mathrm{Tr}(\alpha^2) = 0. \end{cases}$$

Let $\mathcal{B} = \{\omega_1, \omega_2, .., \omega_9\}$ be a basis of $\mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$ over $F(\chi)$ and $\{\Gamma^k_{i,j}\}_{1\leq i,j,k\leq 9}$ be the set of structure constants of $\mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$ with respect to $\mathcal{B}$ (that is $\omega_i\omega_j = \sum_k \Gamma^k_{i,j}\omega_k$). Then an element $\alpha \in \mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$ is a linear combination of the basis, thus $\alpha = \sum_{i=1}^9 \alpha_i\omega_i$ for some coefficients $\alpha_i \in F(\chi)$. Hence,

$$\mathrm{Tr}(\alpha) = \sum_{i=1}^{9} \alpha_i \mathrm{Tr}(\omega_i),$$

and

$$\begin{aligned}\mathrm{Tr}(\alpha^2) =&\mathrm{Tr}(\sum_{i=1}^{9}\sum_{j=1}^{9}\alpha_i\alpha_j\omega_i\omega_j) = \\ =&\mathrm{Tr}(\sum_{i=1}^{9}\sum_{j=1}^{9}\alpha_i\alpha_j\sum_{k=1}^{9}\Gamma_{i,j}^{k}\omega_k) = \\ =&\sum_{i=1}^{9}\sum_{j=1}^{9}\sum_{k=1}^{9}\alpha_i\alpha_j\Gamma_{i,j}^{k}\mathrm{Tr}(\omega_k).\end{aligned}$$

Conditions on the first and the second trace of α can be written as

$$\begin{cases}\sum_{i=1}^{9}\alpha_i\mathrm{Tr}(\omega_i) = 0 \\ \sum_{i=1}^{9}\sum_{j=1}^{9}\sum_{k=1}^{9}\alpha_i\alpha_j\Gamma_{i,j}^{k}\mathrm{Tr}(\omega_k) = 0,\end{cases} \tag{5.1}$$

so the problem now is to solve a system of equations in 9 variables $\alpha_1, .., \alpha_9$ in $F(\chi)$. The first equation is linear, the second one is quadratic. Not every element of the basis can have trace zero. We can suppose $w_1 = 1$ so $\mathrm{Tr}(w_1) \neq 0$, thus we have $\alpha_1 = \mathrm{Tr}(\omega_1)^{-1}\sum_{i=2}^{9}\alpha_i\mathrm{Tr}(\omega_i)$. Our aim is now to find a solution to the quadratic equation in 8 variables obtained by substituting α_1 as found in $\sum_{i=1}^{9}\sum_{j=1}^{9}\sum_{k=1}^{9}\alpha_i\alpha_j\Gamma_{i,j}^{k}\mathrm{Tr}(\omega_k) = 0$.

As a first attempt we may try to use a probabilistic approach. Unfortunately the probability to pick randomly an element in $\mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$ such that it is a solution of system 5.1 is zero. In order to prove that, recall that $\mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$ is a cyclic algebra and $\zeta_3 \in F(\chi)$, thus there exists a cyclic extension K of $F(\chi)$ contained in $\mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$ and a basis $\{1, \alpha, \alpha^2\}$ of K over $F(\chi)$. Let $b \in F(\chi)$ be such that $\alpha^3 = b$. The Galois group of K over $F(\chi)$ is generated by the automorphism that sends α to $\zeta_3\alpha$. Moreover there exists an invertible element $\mu \in \mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$ such that $\mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H) = K \oplus \mu K \oplus \mu^2 K$ and $\alpha\mu = \zeta_3\mu\alpha$. Let $a \in F(\chi)$ be such that $\mu^3 = a$. A basis of $\mathrm{End}_{\mathrm{F}(\chi)\mathrm{G}}(H)$ over $F(\chi)$ is given by $\mathcal{B} = \{1, \alpha, \alpha^2, \mu, \mu\alpha, \mu\alpha^2, \mu^2, \mu^2\alpha, \mu^2\alpha^2\}$. We can calculate the product of each element of the basis:

	1	α	α^2	μ	$\mu\alpha$	$\mu\alpha^2$	μ^2	$\mu^2\alpha$	$\mu^2\alpha^2$
1	1	α	α^2	μ	$\mu\alpha$	$\mu\alpha^2$	μ^2	$\mu^2\alpha$	$\mu^2\alpha^2$
α	α	α^2	b	$\zeta_3\mu\alpha$	$\zeta_3\mu\alpha^2$	$\zeta_3 b\mu$	$\zeta_3^2\mu\alpha$	$\zeta_3^2\mu^2\alpha^2$	$\zeta_3^2 b\mu^2$
α^2	α^2	b	$b\alpha$	$\zeta_3^2\mu\alpha^2$	$\zeta_3^2 b\mu$	$\zeta_3^2 b\mu\alpha$	$\zeta_2\mu^2\alpha^2$	$\zeta_3 b\mu^2$	$\zeta_3 b\mu^2\alpha$
μ	μ	$\mu\alpha$	$\mu\alpha^2$	μ^2	$\mu^2\alpha$	$\mu^2\alpha^2$	a	$a\alpha$	$a\alpha^2$
$\mu\alpha$	$\mu\alpha$	$\mu\alpha^2$	$b\mu$	$\zeta_3\mu^2\alpha$	$\zeta_3\mu^2\alpha^2$	$\zeta_3 b\mu^2$	$\zeta_3^2 a\alpha$	$\zeta_3^2 a\alpha^2$	$\zeta_3^2 ab$
$\mu\alpha^2$	$\mu\alpha^2$	$b\mu$	$b\mu\alpha$	$\zeta_3^2\mu^2\alpha^2$	$\zeta_3^2 b\mu^2$	$\zeta_3^2 b\mu^2\alpha$	$\zeta_3 a\alpha^2$	$\zeta_3 ab$	$\zeta_3 ab\alpha$
μ^2	μ^2	$\mu^2\alpha$	$\mu^2\alpha^2$	a	$a\alpha$	$a\alpha^2$	$a\mu$	$a\mu\alpha$	$a\mu\alpha^2$
$\mu^2\alpha$	$\mu^2\alpha$	$\mu^2\alpha^2$	$b\mu^2$	$\zeta_3 a\alpha$	$\zeta_3 a\alpha^2$	$\zeta_3 ab$	$\zeta_3^2 a\mu\alpha$	$\zeta_3^2 a\mu\alpha^2$	$\zeta_3^2 ab\mu$
$\mu^2\alpha^2$	$\mu^2\alpha^2$	$b\mu^2$	$b\mu^2\alpha$	$\zeta_3^2 a\alpha^2$	$\zeta_3^2 ab$	$\zeta_3^2 ab\alpha$	$\zeta_3 a\mu\alpha^2$	$\zeta_3 ab\mu$	$\zeta_3 ab\mu\alpha$

The trace of all the elements of $\mathcal{B}$ is zero, with 1 as unique exception. Indeed, by construction $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\mu) = 0$ and consequently also $\mathrm{Tr}(\alpha^2) = \mathrm{Tr}(\mu^2) = 0$. If we consider $\mu\alpha$ then we have

$$\mathrm{Tr}(\mu\alpha) = \mathrm{Tr}(\alpha\mu) = \mathrm{Tr}(\zeta_3\mu\alpha) = \zeta_3\mathrm{Tr}(\mu\alpha).$$

It follows that $\mathrm{Tr}(\mu\alpha) = 0$. Exactly in the same way we can prove that $\mathrm{Tr}(\mu\alpha^2) = \mathrm{Tr}(\mu^2\alpha) = \mathrm{Tr}(\mu^2\alpha^2) = 0$.

Looking at system 5.1 for the basis $\mathcal{B}$ chosen above, we have

$$\begin{cases} \alpha_1\mathrm{Tr}(1) = 0 \\ \sum_{i=1}^{9}\sum_{j=1}^{9}\alpha_i\alpha_j\Gamma_{i,j}^1\mathrm{Tr}(\alpha) = 0 \end{cases}$$

where the numbering of coefficients $\alpha_1, .., \alpha_9 \in F(\chi)$ corresponds to the numbering used to list the elements of $\mathcal{B}$. From the table of product it is easy to calculate the structure constants $\{\Gamma_{i,j}^k\}$ of $\mathrm{End}_{F(\chi)G}(H)$. This allow us to conclude that

$$\begin{cases} \alpha_1 = 0 \\ b\ \alpha_2\alpha_3 + a\ \alpha_4\alpha_7 + \zeta_3^2 ab\ \alpha_5\alpha_9 + \zeta_3 ab\ \alpha_6\alpha_8 = 0. \end{cases}$$

From a computational point of view we can not solve this conic equation because we do not know the actual values of a and b. However we can note that the anisotropic space of the conic has dimension not greater than 8 over $F(\chi)$, while the dimension $\mathrm{End}_{F(\chi)G}(H)$ over $F(\chi)$ is 9. This shows that a probabilistic approach is not useful.

Solving quadratic equations can be very hard from a computational point of view. There are various methods in literature. One of the main works in this field is [29] of Denis Simon. Here, a possible approach is introduced for quadratic equations over $\mathbb{Q}$, using a generalized LLL-algorithm to reduce the quadratic form. Such an algorithm is implemented in MAGMA when *HasRationalPoints* is called for a conic defined over the rationals. Let q be a positive defined quadratic form over $\mathbb{Z}^n$. Let $Q = (b_i \cdot b_j) \in M_n(\mathbb{R})$ be its symmetric Gram matrix according to a basis $b_1, .., b_n$, where $\cdot$ denotes the scalar product. Then $\det Q \neq 0$ and $q(x) = X^t Q X$, where X is the array of integer coefficients of x respect to $b_1, .., b_n$. Simon's approach consist in applying LLL-reduction on the basis $b_1, .., b_n$ of $\mathbb{Z}^n$ in order to obtain a LLL-reduced basis. Such a procedure may either end when an element b_i^* such that $b_i^* \cdot b_i^* = 0$ is found (in such a case the algorithm finishes returning a zero of q) or it finds a reduced basis.

The major limit of this technique is that the LLL-reduction can be applied only when the quadratic form is defined over the rationals. However, in [25] LLL-reduction is generalized also to Euclidean rings, giving the chance to extend Simon's approach also to quadratic equations defined over imaginary quadratic fields.

This may be helpful for our purpose since the quadratic equations we are dealing with are defined over field extensions of $\mathbb{Q}(\zeta_3)$, because of Benard-Schacher Theorem.

Appendix A

Experimental Data

In order to understand the behaviour of the Schur index of absolutely irreducible characters of the metacyclic groups studied in the previous chapters, we have analysed some example using Magma. We collected the results of our experiments in the tables contained in this Appendix. The output of these experiments helped us to conjecture the bound proved in Proposition 4.2.4. Because of the high computational cost of the created example we have not been able to complete the table via computation. However, the proof of Proposition 4.2.4 is constructive in some cases thus we used these argumentations to complete the table when the cost of the computation was too high (indicated with * in the table).

Let p, q be two odd prime number such that $p \equiv 1 \mod q^m$ for some integer $m \geq 1$ and let $G := \langle a, b \mid a^p, b^{q^k}, a^b = a^r \rangle$ where $o_p(r) = q^l$ for some integer l satisfying $0 \leq l \leq k$. In the next tables q is equal 3, while p is taken equal to $7, 19, 109, 163, 487$, i.e. the smallest primes such that the parameter m assumes value 1, 2, 3, 4 and 5 respectively. The value of the parameter m is explicitly expressed in the table, even if it strictly related to p. The first table reports the degrees of the irreducible characters of the analysed groups. The second one reports their Schur indices. Chosen a column for k and a row for p (or equivalently m) and l, at the intersection between them is reported a list of numbers. The first number in the line corresponds to the number of characters in $\mathrm{Irr}(G)$ of trivial degree (resp. Schur index) when G is constructed with the chosen parameters k, p, l. The value of parameter r is omitted. The second number represents the number of character in $\mathrm{Irr}(G)$ of degree (resp. Schur index) 3, the third is the number of character of degree (resp. Schur index) 9, and so on.

m	p	l	$k=1$		$k=2$			$k=3$				$k=4$					$k=5$					
1	7	1	3	2	6	9	–	27	18	–	–	81	54	–	–	–	243	162	–	–	–	–
2	19	1	3	6	9	18	–	27	54	–	–	81	162	–	–	–	243	486	–	–	–	–
		2			9	–	2	27	–	6	–	81	–	18	–	–	243	–	54	–	–	–
3	109	1	3	36	9	108	–	27	324	–	–	81	972	–	–	–	243	2916	–	–	–	–
		2			9	–	12	27	–	36	–	81	–	108	–	–	243	–	324	–	–	–
		3						27	–	–	27	81	–	–	12	–	243	–	–	36	–	–
4	163	1	3	54	9	162	–	27	486	–	–	81	1458	–	–	–	243*	4374*	–	–	–	–
		2			9	–	18	27	–	54	–	81	–	162	–	–	243*	–	486*	–	–	–
		3						27	–	–	6	81	–	–	18	–	243	–	–	54	–	–
		4										81	–	–	–	2	243	–	–	–	6	–
5	487	1	3	162	9	486	–	27*	1458*	–	–	81*	4374*	–	–	–	243*	13122*	–	–	–	–
		2			9	–	54	27	–	162	–	81*	–	486*	–	–	243*	–	1458*	–	–	–
		3						27	–	–	18	81	–	–	54	–	243	–	–	162	–	–
		4										81	–	–	–	6	243	–	–	–	18	–
		5															243	–	–	–	–	2

Table A.1: Degrees of irreducible characters of metacyclic groups.

m	p	l	$k=1$		$k=2$			$k=3$				$k=4$					$k=5$					
1	7	1	5	–	11	4	–	29	16	–	–	83	52	–	–	–	245	160	–	–	–	–
2	19	1	9	–	27	–	–	45	36	–	–	99	144	–	–	–	261	468	–	–	–	–
		2			11	–	–	29	4	–	–	83	4	12	–	–	245	4	48	–	–	–
3	109	1	39	–	117	–	–	351	–	–	–	405*	648*	–	–	–			–	–	–	–
		2			21	–	–	63	–	–	–	117	72	–	–	–	279	72	216	–	–	–
		3						31	–	–	–	85	8	–	–	–	247	8	24	–	–	–
4	163	1	57	–	171	–	–	513	–	–	–	1539*	–	–	–	–	1701*	2916*	–	–	–	–
		2			27	–	–	81	–	–	–	243	–	–	–	–	405	324	–	–	–	–
		3						33	–	–	–	99	–	–	–	–	261	36	–	–	–	–
		4										83	–	–	–	–	245	4	–	–	–	–
5	487	1	165	–	495	–	–	1485*	–	–	–	4455*	–	–	–	–	13365*	–	–	–	–	–
		2			63	–	–	189	–	–	–	567*	–	–	–	–	1701*	–	–	–	–	–
		3						45	–	–	–	135	–	–	–	–	405	–	–	–	–	–
		4										87	–	–	–	–	261	–	–	–	–	–
		5															245	–	–	–	–	–

Table A.2: Schur indices of irreducible characters of metacyclic groups

Bibliography

[1] V. Acciaro and J. Klueners. Computing local artin maps, and solvability of norm equations. *Journal of Symbolic Computation*, 30(3):239 – 252, 2000.

[2] M. Benard and M. Schacher. The Schur subgroup, II. *Journal of Algebra*, (22):378–385, 1972.

[3] D.J. Benson. *Representations and Cohomology: Volume 1, Basic Representation Theory of Finite Groups and Associative Algebras*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1998.

[4] R. Brauer. Gruppen linearer Substitutionen II. *Math. Z.*, (31):733–747, 1930.

[5] N. Childress. *Class Field Theory*. Universitext. Springer New York, 2008.

[6] H. Cohen, F. Diaz y Diaz, and M. Olivier. Cyclotomic extensions of number fields. *Indagationes Mathematicae*, 14(2):183 – 196, 2003.

[7] C.W. Curtis and I. Reiner. *Methods of Representation Theory*. Number v. 2 in Methods of Representation Theory. Wiley, 1994.

[8] B. Fein. Minimal splitting fields for group representations. *Pacific J. Math.*, 51(2):427 – 431, 1974.

[9] B. Fein. Minimal splitting fields for group representations. ii. *Pacific J. Math.*, 77(2):445 – 449, 1978.

[10] B. Fein and T. Yamada. The Schur index and the order and exponent of a finite group. *Journal of Algebra*, 28(3):496 – 498, 1974.

[11] W. Feit. Some properties of characters of finite groups. *Bulletin of the London Mathematical Society*, 14(2):129–132, 1982.

[12] W. Feit. The computations of some Schur indices. *Israel Journal of Mathematics*, 46(4):274 – 300, Dec 1983.

[13] C. Fieker. Minimizing representations over number fields. *Journal of Symbolic Computation*, 38(1):833 – 842, 2004.

[14] C. Fieker. Minimizing representations over number fields ii: Computations in the Brauer group. *Journal of Algebra*, 322(3):752 – 765, 2009. Special Issue in Honor of John Cannon and Derek Holt.

[15] C. Ford. Groups which determine the Schur index of a representation. *Journal of Algebra*, 57(2):339 – 354, 1979.

[16] P. Gille and T. Szamuely. *Central Simple Algebras and Galois Cohomology.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006.

[17] S.P. Glasby and R.B. Howlett. Writing representations over minimal fields. *Communications in Algebra*, 25(6):1703–1711, 1997.

[18] B. Huppert. *Character Theory of Finite Groups.* De Gruyter Expositions in Mathematics. De Gruyter, 1998.

[19] I.M. Isaacs. *Character Theory of Finite Groups.* AMS Chelsea Publishing Series. AMS Chelsea Pub., 2006.

[20] K. Iwasawa. *Local Classfield Theory.* Oxford mathematical monographs. Clarendon Press, 1982.

[21] N. Jacobson. *Basic Algebra II: Second Edition.* Dover Books on Mathematics. Dover Publications, 2012.

[22] T.Y. Lam. Finite groups embeddable in division rings. *Proceedings of the American Mathematical Society*, 129(11):3161 – 3166, 2001.

[23] S. Lang. *Algebraic Number Theory.* Applied Mathematical Sciences. Springer, 1994.

[24] D.A. Marcus. *Number Fields - 2nd edition.* Universitext. Springer International Publishing, 2018.

[25] H. Napias. A generalization of the LLL-algorithm over euclidean rings or orders. *Journal de théorie des nombres de Bordeaux*, 8(2):387–396, 1996.

[26] J. Neukirch and N. Schappacher. *Algebraic Number Theory.* Verlag Berlin Heidelberg. Springer Berlin Heidelberg, 1999.

[27] R.S. Pierce. *Associative algebras.* Graduate texts in mathematics. Springer-Verlag, 1982.

[28] P. Roquette. *The Brauer-Hasse-Noether Theorem in Historical Perspective.* Schriften der Mathematisch-naturwissenschaftlichen Klasse. Springer Berlin Heidelberg, 2006.

[29] D. Simon. Solving quadratic equations using reduced unimodular quadratic forms. *Mathematics of Computation*, 74(251):1531–1543, 2005.

[30] A.K. Steel. *Construction of Ordinary Irreducible Representations of Finite Groups*. PhD thesis, Pure Mathematics - University of Sydney, 1 2012.

[31] A. Turull. A formula for calculating some Schur indices. *Journal of Algebra*, 227(1):124 – 132, 2000.

[32] W.R. Unger. An algorithm for computing Schur indices of characters. 2017.

[33] J. Voight. *Quadratic forms and quaternion algebras: Algorithms and arithmetic*. PhD thesis, University of California, Berkeley, 2005.

[34] T. Yamada. On the group algebras of metabelian groups over algebraic number fields. i. *Osaka Journal of Mathematics*, 6(1):211–228, 08 1968.

[35] T. Yamada. Characterization of the simple components of the group algebras over the p -adic number field. *J. Math. Soc. Japan*, 23(2):295–310, 04 1971.