G-theory of group rings for finite groups

Dissertation

zur

Erlangung des Doktorgrades (Dr. rer. nat.)

der

Mathematisch-Naturwissenschaftlichen Fakultät

der

Rheinischen Friedrich-Wilhelms-Universität Bonn

vorgelegt von

Iuliia Semikina

aus

Kiew, Ukraine

Bonn 2018

Angefertigt mit Genehmigung der Mathematisch-Naturwissenschaftlichen Fakultät
der Rheinischen Friedrich-Wilhelms-Universität Bonn

1. Gutachter: Prof. Dr. Wolfgang Lück
2. Gutachter: Prof. Dr. Catharina Stroppel
Tag der Promotion: 04.10.2018
Erscheinungsjahr: 2018

Acknowledgements

I would like to thank my advisor, Wolfgang Lück, for his help, support and interesting mathematical discussions we had. I am grateful to Bonn International Graduate School and Max-Planck-Gesellschaft for providing a scholarship for the period of my studies. I would like to thank the Max Planck Institute for Mathematics in Bonn for the atmosphere and the opportunity to meet so many talented people from all areas of mathematics.

Thanks to all the mathematicians who were helping me during these years. I express my gratitude towards to all the professors whose courses I attended, particularly Günter Harder, Matthias Kreck, Wolfgang Lück, Catharina Stroppel, Peter Teichner, and Don Zagier. Many thanks to Elba Garcia Failde, Fabian Henneke, Thorge Jensen, Daniel Kasprowski, Achim Krause, Malte Lackmann, Alessandro Malusà, Anna Mkrtchyan, Timm von Puttkamer, Geordie Williamson, Christoph Winges, and many others. I would also like to thank Sergiy Kolyada, who was the one who motivated me to come to Bonn for a Master program. Special thanks to Danylo for his help, care, and encouragement. Finally, thanks to my family for their continuous support throughout the years.

Contents

Acknowledgements **1**

Introduction **5**

1 Modular representation theory background **11**
1.1 Definitions . . . 11
1.1.1 Language of representations and modules . . . 11
1.1.2 Change of the base ring . . . 12
1.2 Modular representations vs ordinary representations . . . 14
1.3 Reduction modulo p: the passage from char 0 to char p . . . 15
1.4 Brauer characters . . . 17
1.5 Projective modules . . . 20
1.6 Example: p-groups . . . 22
1.7 The cde triangle . . . 23
1.8 Blocks . . . 25
1.9 Blocks of defect 0 . . . 28
1.10 p-blocks of a group . . . 31

2 K- and G-theory prerequisites **33**
2.1 First definitions and examples of groups K_0 and G_0 . . . 33
2.1.1 Definitions and properties . . . 33
2.1.2 Examples of explicit computations . . . 37
2.2 K_1 and G_1 . . . 41
2.2.1 Definitions . . . 41
2.2.2 The reduced norm . . . 43
2.2.3 Maximal orders . . . 44
2.3 Higher K-groups and classical tools to compute them . . . 46
2.3.1 Q-construction . . . 46
2.3.2 Fundamental theorems in K-theory . . . 48
2.4 Keating's computation of $G_1(\mathbb{Z}G)$ . . . 51

3 The decomposition conjecture for G-theory of group rings **53**
3.1 Hambleton-Taylor-Williams Conjecture . . . 53
3.1.1 The statement and the state of the Conjecture . . . 53
3.1.2 The map in the Conjecture . . . 54
3.1.3 A motivation . . . 56
3.2 The comparison of ranks of G_0-groups . . . 57
3.3 The computation of torsions for G_0-groups . . . 59
3.3.1 The computation of tors $G_0(\mathbb{Z}G)$ . . . 59

3.3.2 The computation of the predicted torsion 62
3.4 The comparison of ranks for G_1-groups 63
3.4.1 The description of $R(G)$ 63
3.4.2 The description of $P(G)$ 64
3.4.3 A solvable counterexample 66
3.4.4 Counting modular representations in terms of rational 68
3.5 The comparison of torsions for G_1-groups 74
3.5.1 Schur indices 74
3.5.2 SK_1 of maximal orders 76
3.6 The comparison of ranks for higher degrees 77
3.7 Jacobinski conductor formula 78
3.8 The known results for higher G-groups 82

Introduction

The subject of algebraic K-theory takes its roots in the 1950's, when Grothendieck introduced the notion of a group K associated to an abelian category $\mathcal{A}$ to reformulate the Riemann-Roch theorem. The letter "K" stands for the German word "Klassen" (classes). Nowadays it is denoted by $K_0(\mathcal{A})$ and is called the Grothendieck group of $\mathcal{A}$.

Nearly at the same time another topic that influenced the development of K-theory was growing. Namely, Whitehead in his work on simple homotopy theory constructed an obstruction for a homotopy equivalence f between CW-complexes to be built up from expansions and contractions. This obstruction, denoted $\tau(f)$, is an element of a group, nowadays called Whitehead group $\mathrm{Wh}(\pi)$, that depends only on the fundamental group of the CW-complex considered. The Whitehead group is given as a quotient of $K_1(\mathbb{Z}\pi)$, where $\mathbb{Z}\pi$ denotes the group ring of π. Among other topological applications of the lower K-groups we should mention h-cobordisms, pseudo-isotopies, and Wall's finiteness obstruction. These important connections were motivating the interest in computing the algebraic K-groups of an integral group ring.

In his fundamental work [Q] Quillen united the existing foundations of K_0, K_1 and introduced K-theory of an exact category $\mathcal{C}$ using the Q-construction. Namely, he defined higher K-groups as homotopy groups of the classifying space of the associated Quillen category $Q\mathcal{C}$

$$K_i(\mathcal{C}) = \pi_{i+1}(BQ\mathcal{C}), \; i \geq 0.$$

If R is a ring with 1, then applying the Q-construction to the category $\mathcal{P}(R)$ of finitely generated projective left R-modules we obtain the classical algebraic K-theory of a ring $K_i(R) = K_i(\mathcal{P}(R))$. The computation of K-groups is an extremely difficult task, the Quillen-Lichtenbaum and the Vandiver Conjecture give the prediction for the groups $K_n(\mathbb{Z})$, but the verification of these conjectures remains an open problem.

If we let $\mathrm{Mod}_{fg}(R)$ to be the category of all finitely generated left R-modules we get the so called G-theory

$$G_i(R) = K_i(\mathrm{Mod}_{fg}(R)), \; i \geq 0.$$

There is a canonical map $K_i(R) \to G_i(R)$, called the Cartan map, which is an isomorphism if R is regular. The computation of G-groups of a ring is usually an even harder problem than determining the K-groups. One of the difficulties that arises when dealing with G-theory is a lack of functoriality.

The following interesting conjecture formulated by Lück in [Lü] was one of the motivations for us to study G-theory of group rings. The conjecture says that the amenability of a group G (we allow infinite groups here) can be detected by the element $[\mathbb{C}G] \in G_0(\mathbb{C}G)$. Using the machinery developed for the group von Neumann algebras Lück showed that if G is amenable then $[\mathbb{C}G]$ is an element of infinite order in $G_0(\mathbb{C}G)$ and in particular is non-zero. The direction of showing that $[\mathbb{C}G] \neq 0 \in G_0(\mathbb{C}G)$ implies amenability of a group G is an open problem.

As in the situation with K-theory, the interest in studying G-theory of integral group rings for finite groups was motivated by the following obstruction problem coming from dynamical systems. Given a smooth compact manifold M and a diffeomorphism $f\colon M \to M$, determine when f is isotopic to a Morse-Smale diffeomorphism. The isotopy classes of Morse-Smale diffeomorphisms have particularly well-behaved dynamical properties and such dynamical systems were objects of considerable research. Franks and Shub constructed an obstruction, the Lefschetz invariant $L(f)$, that vanishes if and only if f is isotopic to a Morse-Smale diffeomorphism. These obstructions lie in a universal group SSF, which was described by Lenstra in terms of Grothendieck groups $G_0(\mathbb{Z}C_n)$ with cyclic groups C_n. In his work Lenstra showed more, he proved a beautiful decomposition of a Grothendieck group of an integral group ring for any finite abelian group G

$$G_0(\mathbb{Z}G) \cong \bigoplus_{C \in C(G)} G_0\Big(\mathbb{Z}[\xi_{|C|}, \frac{1}{|C|}]\Big), \tag{1}$$

where $C(G)$ denotes the set of all cyclic quotients of G (isomorphic quotients coming from different subgroups of G are considered to be different), $|C|$ is the order of a cyclic group C, and $\xi_{|C|}$ is a primitive $|C|$-th root of unity.

It was a natural next step to consider the higher groups $G_n(\mathbb{Z}G)$ for an arbitrary finite group G. This question was independently studied by Webb [We1], [We2] and Hambleton, Taylor and Williams [HTW]. In [We1] Webb adapted the methods of Lenstra and obtained explicit decomposition formulas for $G_0(\mathbb{Z}G)$ in case of dihedral groups D_{2n} and quaternion groups Q_{4m}.

In [We2] Webb proved the same Lenstra formula (1) for higher groups $G_n(RG)$ for all $n > 0$ with R a noetherian ring and G a finite abelian group. Let Γ denote a maximal $\mathbb{Z}$-order in $\mathbb{Q}G$ containing $\mathbb{Z}G$. Then Γ is Morita equivalent to the product of maximal orders Γ_C in the corresponding simple algebras A_C of $\mathbb{Q}G$, $C \in C(G)$. Denote by $\mathcal{U}$ the product of $\Gamma_C[\frac{1}{|C|}]$ taken over $C(G)$. Then the Lenstra formula is saying that $G_0(\mathbb{Z}G) \cong \bigoplus_{C\in C(G)} G_0(\Gamma_C[\frac{1}{|C|}])$. Webb defined the Lenstra functor on the level of classifying spaces and proved that the constructed map carries certain homotopy fibers to the required homotopy fibers, mimicking Lenstra's observation for G_0. The original Lenstra map is carrying the relations R_1 in the Heller-Reiner presentation $G_0^t(\Gamma)/R_1$ of $G_0(\mathbb{Z}G)$ to the relations R_2 of the presentation $G_0^t(\Gamma)/R_2$ of $G_0(\mathcal{U})$ obtained from the localization sequence $\Gamma \to \mathcal{U}$, we will discuss these presentations in detail in Section 3.3. With the same approach in [We5] Webb obtained an analogous decomposition formula for $G_n(RG)$ for G a finite nilpotent group with some restrictions on its 2-Sylow subgroups and R a noetherian ring.

Using a completely different argument Hambleton, Taylor, and Williams in [HTW] proved the same result for all nilpotent groups and conjectured a general decomposition formula for $G_n(RG)$ for all finite groups G. This formula will be the main focus of the thesis.

For a finite group G consider the Wedderburn decomposition of the rational group algebra

$$\mathbb{Q}G \cong \prod_{\rho \in X(G)} M_{n_\rho}(D_\rho^{op}), \tag{2}$$

where $X(G)$ denotes the set of isomorphism classes of rational irreducible representations of G, and D_ρ is the division algebra $\mathrm{End}_{\mathbb{Q}G}(V_\rho)$ associated to $\rho\colon G \to \mathrm{Aut}(V_\rho)$.

For a representation $\rho \in X(G)$ let k_ρ be the order of the kernel of ρ and let d_ρ be the dimension of any of the irreducible complex constituents of $\mathbb{C} \otimes_{\mathbb{Q}} \rho$. Define $\omega_\rho = \frac{|G|}{k_\rho d_\rho}$. Let Λ_ρ be a maximal $\mathbb{Z}[1/\omega_\rho]$-order in D_ρ. Hambleton, Taylor and Williams conjectured the following decomposition formula, which we call the HTW-decomposition.

Conjecture (Hambleton-Taylor-Williams)**.** *Let G be a finite group and R a noetherian ring. Then*

$$G_n(RG) \cong \bigoplus_{\rho \in X(G)} G_n(R \otimes \Lambda_\rho), \quad \forall n \geq 0. \tag{3}$$

Note that the isomorphism of groups is only conjectured abstractly without providing a candidate map for the isomorphism. There is no obvious map between the two sides of the conjectured decomposition since unlike for K-theory here we are lacking functoriality. Hence constructing the map is a part of the conjecture. We discuss this point in the Subsection 3.1.2.

In [We4] Webb showed the HTW-decomposition for groups of square-free order and for all $n \geq 0$. In [LaWe] Laubenbacher and Webb proved the conjecture for $n = 0$ and G a group with cyclic Sylow subgroups. Webb and Yao [WeY] found out that in general the Hambleton-Taylor-Williams Conjecture fails to be true, and the symmetric group S_5 is a counterexample in degree $n = 1$. Using Keating's result on the rank of $G_1(\mathbb{Z}G)$ and the fact that $\mathbb{Q}$ is a splitting field for the group S_5 Webb and Yao explicitly computed the ranks of both sides of the HTW-decomposition, and the ranks did not agree. Nevertheless, Webb and Yao remarked it is reasonable to expect that the HTW-Conjecture might hold for finite solvable groups. In Section 3.4 we provide a solvable counterexample to the Hambleton-Taylor-Williams Conjecture.

Theorem A. *The group* $\mathrm{SL}(2, \mathbb{F}_3)$ *does not satisfy the HTW-decomposition.*

To prove this we use the same source of contradiction as in [WeY], namely, the rank of $G_1(\mathbb{Z}G)$. For a finite group G we consider the following two numbers: $R(G)$ ("R" stands for "rank"), the rank of $G_1(\mathbb{Z}G)$, and $P(G)$ ("P" stands for "prediction"), the rank of $\bigoplus_{\rho \in X(G)} G_1(\Lambda_\rho)$. We give a computable description of $R(G)$ and $P(G)$ and then apply this description to compute the difference $P(G) - R(G)$ for the solvable group $G = \mathrm{SL}(2, \mathbb{F}_3)$. The difference turns out to be non-zero and therefore we conclude that the group $\mathrm{SL}(2, \mathbb{F}_3)$ is a counterexample to the Hambleton-Taylor-Williams Conjecture.

In the same Section 3.4 we prove a general inequality estimating the number of modular irreducible representations of a finite group G in terms of the rational irreducible representations of G. Let E_ρ be the center of D_ρ and let $\mathcal{O}_\rho$ be the ring of algebraic integers in E_ρ.

Theorem B. *Let G be any finite group and let p be a prime integer that divides the order of G. Then*

$$\#\{\textit{irreducible } \mathbb{F}_p\textit{-representations of } G\} \geq \sum_{\rho \in I_p} t_\rho,$$

where I_p is the set of rational irreducible representations ρ of G for which the corresponding number ω_ρ is not divisible by p, and t_ρ is the number of different prime ideals in $\mathcal{O}_\rho$ that divide the principal ideal (p).

As a corollary of Theorem B we obtain that $P(G) \geq R(G)$ for any finite group G. The proof of the inequality gives an explanation of the failure of the HTW-decomposition for $G_1(\mathbb{Z}G)$ and sheds some light on the meaning of the number ω_ρ. Namely, in the language of modular representation theory, the condition that the number ω_ρ is not divisible by a prime p exactly means that the complex constituents of the representation ρ are p-blocks of defect zero for the quotient group of G they faithfully represent and that they remain irreducible after reduction mod p. Strict inequality may occur, because in general not every irreducible $\mathbb{F}_p$-representation of G is obtained from such a representation. Theorem A and Theorem B are contained in our paper [S]. The inequality obtained $P(G) \geq R(G)$ leads to the natural guess that a weaker version of the HTW-Conjecture may hold. Namely, instead of asking for the isomorphism in the HTW-decomposition, one might conjecture that there exists either an injective homomorphism $G_n(\mathbb{Z}G) \hookrightarrow \bigoplus_{\rho \in X(G)} G_n(\Lambda_\rho)$ or a surjective homomorphism $\bigoplus_{\rho \in X(G)} G_n(\Lambda_\rho) \twoheadrightarrow G_n(\mathbb{Z}G)$. Since we still don't have any map that would work for all groups G we have to consider both of these options.

On a positive side of results that confirm the HTW-decomposition (and hence the weaker versions of it) we checked in Section 3.2 and Section 3.6 using the result of Kuku that in all degrees other than 1 the rank predicted by the HTW-decomposition is the correct one. Let $R_n(G)$ be the rank of $G_n(\mathbb{Z}G)$ and $P_n(G)$ the rank of $\bigoplus_{\rho \in X(G)} G_n(\Lambda_\rho)$.

Theorem C. *Let G be a finite group, then for all $n \geq 2$ and $n = 0$ it holds*

$$P_n(G) = R_n(G).$$

Furthermore, using the results of Keating and some analysis of Schur indices in Section 3.5 we were able to compare the torsion part of $G_1(\mathbb{Z}G)$ with the one predicted by the HTW-decomposition. Surprisingly, in this case the HTW-decomposition gives a correct answer for all finite groups G.

Theorem D. *Let G be a finite group, then* $\operatorname{tors} G_1(\mathbb{Z}G) \cong \bigoplus_{\rho \in X(G)} \operatorname{tors} G_1(\Lambda_\rho)$.

The thesis is organized as follows. Chapter 1 is meant to be an introduction to modular representation theory. There we include all the facts needed to prove Theorem B, in particular the Brauer-Nesbitt theorem on blocks of defect zero. In Chapter 2 we introduce K- and G-groups and consider examples showing that in general these groups are very different. In Chapter 2 we state all the main tools needed for treating the HTW-decomposition. In Section 2.4 we present the result of Keating on $G_1(\mathbb{Z}G)$. Chapter 3 is the core of this thesis. In Section 3.1 we review the Hambleton-Taylor-Williams Conjecture and explain the initial motivation behind Lenstra's result. In Sections 3.2 and 3.3 we present the computations for rank and torsion of G_0 predicted by the HTW-decomposition. Section 3.4 is based on the author's paper [S] and is devoted to the comparing $P(G)$ and $R(G)$ as defined above. In particular the counterexample $\mathrm{SL}(2, \mathbb{F}_3)$ is treated in detail. The inequality $P(G) \geq R(G)$ is obtained as a corollary from Theorem B of this Section. Next in Section 3.5 Theorem D confirming the Hambleton-Taylor-Williams Conjecture for the torsion part of G_1 is obtained. The results of Kuku and Theorem C are the content of Section 3.6. The numbers ω_ρ being inverted in the HTW-decomposition are exactly the same as those appearing in the Jacobinski conductor formula, which we discuss in Section 3.7. Finally, in Section 3.8 we present the proof due to Hambleton, Taylor, and Williams of the HTW-decomposition for finite nilpotent groups.

Chapter 1

Modular representation theory background

In this Chapter we introduce all the terminology and important statements from the theory of modular representations that are needed for the investigation of G-theory later in Chapter 3. In the situation when representations of a group are considered over a field of characteristic dividing the order of the group, the theory becomes very different and much more difficult then the classical case of characteristic zero. The main sources we used for this Chapter are the classical book by C. Curtis and I. Reiner [CuRe1], the book by P. Webb [W], and the book by J.-P. Serre [Se].

1.1 Definitions

1.1.1 Language of representations and modules

This subsection is devoted to stating basic definitions in representation theory of finite groups. All representations and all modules are understood to be finite dimensional.

Let G be a finite group and F be an arbitrary field. A *representation* of G over a field F, or an F*-representation* of G, is a pair (V, ϕ), where V is a finite dimensional F-vector space and $\phi\colon G \to \mathrm{GL}(V)$ is a group homomorphism. Given such a representation (V, ϕ) we may turn V into a left FG-module by defining $g \cdot v = \phi(g)v$, for all $g \in G,\ v \in V$. And vice versa, given a finite dimensional FG-module V, we have an action of G on V by F-linear invertible endomorphisms. This gives a homomorphism $G \to \mathrm{GL}(V)$ and hence a representation of G over F. In other words, a representation of G over F is the same as an FG-module having a finite F-basis. We will use both languages of representations and modules interchangeably.

Using the language of modules the classical notion of a representation of a group G over a field can be carried over unchanged to define a representation of G over a commutative ring. All rings we consider are always meant to be unital rings. Given a commutative ring R, an R*-representation* of G is an RG-module V that has a finite R-basis.

Suppose that V is free as an R-module (which is the case if R is a field). Then we may choose an R-basis $\{v_1, \dots, v_n\}$ of V and write the action of each $g \in G$ as a matrix $\phi_g \in \mathrm{GL}_n(R)$. The rank n of the free R-module V is called the *degree* of the representation. This way we obtain a *matrix representation* of G, i.e., a group homomorphism $\phi\colon G \to \mathrm{GL}_n(R)$. It is easy to check that the result of selecting a different basis $\{v_1', \ldots, v_n'\}$ in V is an *equivalent* matrix representation of G, meaning that there exists a matrix $A \in \mathrm{GL}_n(R)$, such that $\phi_g' = A\phi_g A^{-1}$ for all $g \in G$.

1.1.2 Change of the base ring

A natural question to ask is how representations of the same group over different base fields are related. Most frequently the representations of a group G over algebraically closed fields such as $\mathbb{C}$ or $\bar{\mathbb{Q}}$ are considered. For us it will be important to look at representations of G over fields that are not algebraically closed, and to study the behavior of these representations when passing to field extensions, in particular to the algebraic closure of the base field. An inverse question will be of importance as well, namely, whether a representation can be defined over a smaller field or a subring. This subsection is devoted to setting the terminology and basic facts concerning the change of the base ring.

Let R be a commutative ring and V an RG-module. Let R' be another commutative ring and $f\colon R \to R'$ be a ring homomorphism. Then we may consider $U = R' \otimes_R V$, which is a module over $R' \otimes_R RG \cong R'G$ in a clear way. This easy construction will be extremely useful for us, especially in the following two situations.

1. If R is a subring of a commutative ring R', then we say that an $R'G$-module $U = R' \otimes_R V$ is obtained from V by *extending the scalars from R to R'*. If an $R'G$-module U is isomorphic to $R' \otimes_R V$ for some RG-module V, then we say that U can be *written in R*.

2. Let $R' = R/I$, where I is an ideal in R. Then $U = R' \otimes_R V \cong V/IV$. In terms of matrix representation the resulting representation U is obtained from V by reducing coefficients of matrices modulo I. We say that U is a *reduction of V modulo I*. In case an $R'G$-module W is of the form $R' \otimes_R V$ for some RG-module V, we say that W *can be lifted to* V, and V is a lift of W. In general a lift V is not uniquely determined up to an R-equivalence.

Suppose that V is a free R-module with an R-basis $\{v_1, \ldots, v_n\}$. Then an $R'G$-module $U = R' \otimes_R V$ is also free as an R'-module and $1 \otimes_R v_1, \ldots, 1 \otimes_R v_n$ is its R'-basis. With such a choice of basis the group G acts on U by matrices with coefficients in R. Vice versa, if we can choose an R'-basis $\{u_1, \ldots, u_n\}$ of an $R'G$-module U in a way that the action of G with respect to this basis is given by the matrices with coefficients in R, then $V := R\langle u_1, \ldots, u_n\rangle$ is an RG-submodule of U and $U = R' \otimes_R V$.

Let G a finite group. An RG-module L is called an *RG-lattice* if it is finitely generated and projective as an R-module. If R is a Dedekind domain the condition for L being an RG-lattice becomes easier, namely, L should be finitely generated and torsion-free as an R-module. In the situation when R is a PID, the definition reduces to requiring L to be finitely generated and free as an R-module.

Let us assume for now that R is a PID with field of fractions F. We are going to examine the relation between RG- and FG-modules. Given an RG-module U we can extend the scalars to obtain an FG-module $V = F \otimes_R U$, and we may view U as a subset of V. The other way around, starting with an FG-module V we call an RG-submodule $U \subseteq V$ a *full RG-lattice in V*, if U is an RG-lattice and has an R-basis which is also an F-basis of V. It is clear that if U is a full RG-lattice in V, then $V \cong F \otimes_R U$. The following lemma implies that every finitely generated FG-module contains a full RG-lattice, and hence can be written in R.

Lemma 1. *Let R be a PID with field of fractions F. Let V be a finite dimensional vector space over F. Then any finitely generated R-submodule U that contains an F-basis of V is a full R-lattice in V.*

Proof. Let U be a finitely generated R-submodule that contains an F-basis of V. Since U is a subset of an F-vector space it is R-torsion free. The fact that R is a PID implies that U is a free R-module. Therefore, U is an R-lattice. Let $\{u_1, \ldots, u_n\}$ be an R-basis of U. We will show that it is also an F-basis of V. Since U contains an F-basis of V, it follows that $\{u_1, \ldots, u_n\}$ span V over F. Suppose that we have a non-trivial linear relation $\lambda_1 u_1 + \ldots + \lambda_n u_n = 0$, for some $\lambda_i \in F$. Since F is a field of fractions of R we may write $\lambda_i = \frac{x_i}{y_i}$, $x_i, y_i \in R$. After clearing the denominators we will obtain a linear dependence of $\{u_1, \ldots, u_n\}$ over R, which is a contradiction. Thus, we have shown that U is a full R-lattice in V. □

Corollary 2. *Let R be a PID with field of fractions F. For any finite dimensional FG-module V there exists a full RG-lattice in V.*

Proof. Let $\{v_1, \ldots, v_n\}$ be an F-basis for V. Consider an R-submodule U in V generated by $\{gv_i \mid g \in G,\ i = \overline{1, n}\}$. Clearly, U is an RG-submodule and it is finitely generated as an R-module. Moreover, it contains an F-basis of V. Hence by Lemma 1 U is a full RG-lattice in V, which finishes the proof. □

Remarks.

1. The Corollary 2 will play an important role later in the procedure of passing from a representation over a field of characteristic zero to a modular representation.

2. The existence of a full RG-lattice for a given FG-module V is guaranteed by the Corollary 2, but in general such a lattice does not have to be unique up to an R-isomorphism.

3. Let $R \subseteq R'$ be commutative rings. Let V be an $R'G$-module that is free as R'-module and can be written in R. In general this does not imply that V contains a full RG-lattice. Nevertheless, in the situation when R' is noetherian Smith normal form guarantees the existence of a full RG-lattice.

1.2 Modular representations vs ordinary representations

Let G be a finite group and p be a prime integer dividing the order of the group $|G|$. *Modular representations* are representations of G over a field of positive characteristic. When the characteristic of the ground field does not divide $|G|$ the representation theory is the same as in ordinary (characteristic zero) case. In the situation when characteristic divides $|G|$ the representation theory becomes much more sophisticated. Before we describe a procedure of reduction modulo p, which will allow us to pass from characteristic 0 to characteristic p, let us discuss the major differences between ordinary representation theory and the one over a field of characteristic p.

Semisimplicity By Maschke's theorem the group algebra FG is semisimple if and only if $\mathrm{char}F$ does not divide the order $|G|$. As a corollary we have that in case of $\mathrm{char}F \nmid |G|$ every representation of G over F is a direct sum of irreducible representations, which essentially reduces ordinary representation theory to the study of simple FG-modules. In the situation of $\mathrm{char}F = p$ we don't have this powerful tool, but since FG is Artinian we still can use a weaker alternative, namely, Jordan-Hölder decomposition. Recall, that Jordan-Hölder theorem guarantees, that for every finitely generated FG-module V there is a series of modules, called *composition series*

$$0 = V_0 \subseteq V_1 \subseteq \ldots \subseteq V_{n-1} \subseteq V_n = V,$$

such that all composition factors V_i/V_{i-1} are simple FG-modules. Moreover, Jordan-Hölder theorem ensures that the set of composition factors and multiplicities with which they occur do not depend on the choice of composition series. Of course, just knowing the set of composition factors with multiplicities does not recover the initial module, but still will be important for us in the sequel.

Characters Let (V, ϕ) be a representation of G over a field F. Recall that the character of (V, ϕ) is a function $\chi\colon G \to F$ given by $\chi(g) = \mathrm{Tr}(\phi(g))$. If F is a field of characteristic 0, then representation is uniquely determined up to isomorphism by its character. The analogous statement fails in any positive characteristic q, since the direct sum of q copies of trivial representation and the direct sum of $2q$ copies of trivial representation are obviously non-isomorphic, but have the same character, which is zero for all elements of G. This problem can be fixed by the so called Brauer character, which will be introduced later in Section 1.4. However, Brauer character determine representation only up to composition factors, not up to isomorphism.

Number of irreducible representations If F is algebraically closed and $\mathrm{char}F \nmid |G|$, then the number of irreducible representations of G equals the number of conjugacy classes of elements in G. In the situation when F

is algebraically closed and $\text{char}F = p$ the number of irreducible representations is equal to the number of conjugacy classes of elements in G with order coprime to p. Therefore, we always have more simple modules when $\text{char}F \nmid |G|$ compared to the case of $\text{char}F \mid |G|$.

1.3 Reduction modulo p: the passage from char 0 to char p

Let G be a finite group and let p be a prime integer that divides the order of G. We are going to describe the procedure, called the reduction modulo p, which takes a representation of G over a field of characteristic zero as an input, and returns a representation of G over a field of characteristic p instead. We remark that the resulting modular representation will not be uniquely determined up to isomorphism, but only up to composition factors, which we will discuss in greater details later in this section.

A *p-modular system* is a triple (F, R, k), where F is a field of characteristic zero with a discrete (additive) valuation v, $R = \{x \in F \mid v(x) \geq 0\}$ is a valuation ring of F with a unique maximal ideal (π), and $k = R/(\pi)$ is a field of characteristic p. All further discussion will be held in a general setting of an arbitrary p-modular system, but for our purposes the theory developed later on will only be applied to the following important case.

Example 3. *Let K be an algebraic number field.*

- *R the ring of integers in K*
- *$\mathfrak{p}$ fixed prime ideal in R lying above $p \in \mathbb{Q}$, i.e. $p \in \mathfrak{p}$*
- *$R_{\mathfrak{p}}$ localization of R at $\mathfrak{p}$*
- *$\mathfrak{P} = \mathfrak{p}R_{\mathfrak{p}} = (\pi)$ unique maximal ideal in $R_{\mathfrak{p}}$*
- *$\overline{K} := R/\mathfrak{p} \cong R_{\mathfrak{p}}/\mathfrak{P}$ finite field of characteristic p*

Let us note that the ring $R_{\mathfrak{p}}$ is a PID with field of fractions K. The unique maximal ideal $\mathfrak{P} = \mathfrak{p}R_{\mathfrak{p}}$ is principal, which justifies our notation $\mathfrak{p}R_{\mathfrak{p}} = (\pi)$, $\pi \in R_{\mathfrak{p}}$.

We claim that $(K, R_{\mathfrak{p}}, \overline{K})$ is a p-modular system. Since $R_{\mathfrak{p}}$ is a PID and therefore a unique factorization domain, each element $x \in R_{\mathfrak{p}}$ can be written uniquely up to units in a form

$$x = \pi^{\alpha}\pi_1^{\alpha_1} \ldots \pi_k^{\alpha_k},$$

where $\alpha, \alpha_i \in \mathbb{Z}_{\geq 0}$ and $\pi_i \in R_{\mathfrak{p}}$ are prime elements not associated to π. We put $v(x) := \alpha$. The $\mathfrak{p}$-adic valuation on K is defined by

$$v(x/y) := v(x) - v(y),\ x, y \in R \setminus \{0\},$$

and $v(0) := \infty$. It is easy to check that it is indeed a valuation on K and it does not depend on the choice of a generating element π of the ideal $\mathfrak{p}R_{\mathfrak{p}}$. It is also *evident that $R_\mathfrak{p}$ is a valuation ring of K, and $\overline{K} = R_\mathfrak{p}/(\pi)$ is a field of characteristic p. Therefore, $(K, R_\mathfrak{p}, \overline{K})$ is a p-modular system.*

From now on let (F, R, k) be a p-modular system. Let (V, ϕ) be an F-representation of G, and let us fix some F-basis $\{v_1, \ldots, v_d\}$ of V. The procedure of the reduction modulo p goes in two steps.

Step 1. Replace ϕ by an F-equivalent R-representation ϕ', or in other words choose a full RG-lattice U in V. This is possible due to Corollary 2. In terms of representations it guarantees that we can find a base change $A \in GL_d(F)$ such that $\phi'(g) := A\phi(g)A^{-1} \in GL_d(R)$ for all $g \in G$. In general the choice of the matrix A is not unique and ϕ' is not determined up to an R-equivalence.

Step 2. Reduce the representation ϕ' modulo (π). In our terminology for modules this means that we reduce a full RG-lattice U modulo ideal (π). We call the resulting kG-module $\overline{V} = U/\pi U$ *a reduction modulo p of an FG-module V*. In terms of a matrix representation the reduction $\overline{\phi}\colon G \to GL_d(k)$ is a composition of ϕ' with the quotient map $GL_d(R) \to GL_d(k)$. We call this new k-representation $\overline{\phi}$ *the reduction modulo p of ϕ*, and say that ϕ *is a lift of* $\overline{\phi}$.

As we emphasized in the beginning the result of reduction modulo p of an FG-module does not have to be uniquely defined up to k-isomorphism, because of the choice involved in the first step. Nevertheless, the following theorem shows that the composition factors counted with multiplicities in Jordan-Hölder decomposition of the resulting module $\overline{V}$ are independent of the choice being made during the reduction modulo p.

Theorem 4 (Brauer-Nesbitt)**.** *Let (F, R, k) be a p-modular system, let G be a finite group, and let V a finitely generated FG-module. Let U_1, U_2 be full R-lattices in V. Then the kG-modules $\overline{U}_1 = U_1/\pi U_1$ and $\overline{U}_2 = U_2/\pi U_2$ have the same composition factors counted with multiplicities.*

Proof. The sum $U_1 + U_2$ is a full RG-lattice in V, by Lemma 1, and contains both modules U_1, U_2. Therefore it is enough to prove the claim for the case if $U_1 \subseteq U_2$. Since an RG-module U_2/U_1 has finite composition length, without loss of generality we may assume that U_2/U_1 is simple or equivalently that U_1 is a maximal kG-submodule in U_2. Hence the kG-submodule $\pi U_2/U_1 \subseteq U_2/U_1$ must be either trivial or the whole U_2/U_1. The latter case is impossible since $\mathrm{Rad}R = (\pi)$ and by Nakayama's lemma $M = \mathrm{Rad}R \cdot M$ implies $M = 0$.

Therefore we have the following chain of inclusions $\pi U_1 \subseteq \pi U_2 \subseteq U_1 \subseteq U_2$. It is left to show that the kG-modules U_2/U_1 and $\pi U_2/\pi U_1$ have the same composition factors. The multiplication by π gives an isomorphism of RG-modules $U_2/U_1 \cong \pi U_2/\pi U_1$, which implies that these modules are also isomorphic over kG. □

Recall that by $G_0(A)$, where A is a finite dimensional algebra over a field, we mean a Grothendieck group with a basis indexed by simple A-modules. Given (F, R, k) a splitting p-modular system for G the reduction modulo p induces a map on Grothendieck groups $d\colon G_0(FG) \to G_0(kG)$ which we call *the decomposition map*. We define *the decomposition matrix D* to be the matrix with rows indexed by the simple FG-modules and columns indexed by the simple kG-modules with entries given by

$$d_{VS} = \text{multiplicity of } S \text{ as a composition factor of } \overline{V},$$

where S is a simple kG-module, V is a simple FG-module, and $\overline{V}$ is a reduction of V modulo p. The coefficients d_{VS} are called *decomposition numbers.* Directly from the definition we have that for a simple FG-module V

$$d(V) = [\overline{V}] = \sum_S d_{VS}[S] \in G_0(kG),$$

where sum runs over all simple kG-modules. Brauer-Nesbitt theorem guarantees that the multiplicity of composition factors does not depend on the choice of a reduction $\overline{V}$, and hence the decomposition map and the decomposition matrix are well-defined.

To avoid confusion of having several decomposition matrices the condition of being splitting is added to (F, R, k). Also we will need this assumption later to show the relation of the decomposition matrix to the Cartan matrix, which is not fulfilled without splitting assumption for (F, R, k). A computation of a decomposition matrix is in general a very hard task, since when trying to do it from scratch one has to construct all simple representations in characteristic zero, then find full RG-lattices inside those, reduce the lattices modulo maximal ideal in R, and finally determine the composition factors. The problem might be a bit simplified by using Brauer characters instead of directly dealing with representations, which is discussed in the next section. Nevertheless, the problem of finding the decomposition numbers remains widely open in general, for instance, it is still open for symmetric groups.

1.4 Brauer characters

Let G be a finite group, let F be an arbitrary field and V be an FG-module. The definition of an F-character makes sense for any field, namely, $\chi\colon G \to F$ given by $\chi(g) = \mathrm{Tr}(g)$ is always well-defined. The F-characters can be used to distinguish simple modules because of the following theorem [CuRe1, Theorem 17.3].

Theorem 5 (Frobenius-Schur)**.** *For a finite group G and an arbitrary field F the F-characters afforded by a set of inequivalent simple FG-modules are F-linearly independent.*

However, as was mentioned before if F is a field of positive characteristic two FG-modules can have the same F-characters without even having the same set of composition factors. Brauer found a clever way to fix this issue by introducing Brauer characters, which he was calling "modular characters" at that time. Given (F, R, k) a splitting p-modular system, Brauer associated to each kG-module L a function $\lambda\colon G_{p'} \to F$, where $G_{p'}$ is the set of p-regular elements of G, and this function λ determines L up to composition factors. In this section we briefly review the definition and main properties of Brauer characters. Even though everything will be stated in the general context of a p-modular system, for the purposes of our work this machinery will be only applied to the case of F being an algebraic number field.

We start by stating some facts from group theory needed for the construction of Brauer character. Recall, that an element of a group is called *p-singular* (or *p-element*) if its order is a power of p. An element of a group is called *p-regular* (or *p'-element*) if its order is coprime to p. The set of p-elements in G is denoted by G_p and the set of p'-elements is denoted by $G_{p'}$. It is clear that the intersection of G_p and $G_{p'}$ consists of one element, namely the identity element.

Lemma 6 ([CuRe], Lemma 40.3)**.** *Every element $g \in G$ has unique decomposition $g = g_{p'} g_p$, where $g_{p'}, g_p$ commute and $g_{p'} \in G_{p'}$, $g_p \in G_p$.*

The elements $g_{p'}$ and g_p are called the *p'-part* (or *p-regular part*) of g, and the *p-part* (or *p-singular part*) of g, respectively.

Remark 7. *Let k be a field of characteristic p, then the values of k-characters on G_p do not provide new information. Namely, given any representation of G its k-character satisfies $\chi(g) = \chi(1)$, for all $g \in G_p$.*

Proof. Let $g \in G_p$. Since the order of g is p^r for some $r \in \mathbb{Z}_{\geq 0}$ all the eigenvalues of the action of g are p^r-th roots of unity (to have roots of unity we may pass to an algebraic closure of the field), which can only be 1 in characteristic p. The value of the character $\chi(g)$ equals the sum of eigenvalues of the action of g, and hence, equals $\chi(1)$. □

Let $|G| = p^d m$, where $(p, m) = 1$. Let (F, R, k) be a splitting p-modular system for G with $\mathrm{char} F = 0$. The condition of splitting is needed since we want F and k to contain a primitive m-th root of unity, which we denote by ω. If we would like to define Brauer character for F not containing m-th root of unity, then first we need to extend the scalars to achieve this property. Since the valuation of roots of unity is 0 it follows that $\omega \in R$. Denote by $f: R \to k$ the quotient map. It is not difficult to show that the image $\overline{\omega} = f(\omega) \in k$ is also a primitive m-th root of unity in k and the restriction $f_{|\langle\omega\rangle}: \langle\omega\rangle \to \langle\overline{\omega}\rangle$ is an isomorphism of cyclic groups. Let L be a finitely generated kG-module and let $x \in G_{p'}$. All the eigenvalues of the action of x on L are m-th roots of unity, that we denote by $\xi_1, \ldots, \xi_d$. Put

$$\lambda(x) := \sum_{i=1}^{d} f^{-1}(\xi_i).$$

We call $\lambda: G_{p'} \to F$ defined as above *the Brauer character of L.* Let us emphasize that it is only defined on p-regular elements of G and takes values in a field F of characteristic 0.

Example 8. *Let G be an arbitrary finite group and V_1 a direct sum of p copies of a trivial representation of G over $\mathbb{F}_p$, i. e. $V_1 = \bigoplus_{i=1}^{p} \mathbb{F}_p$. Then for any $x \in G_{p'}$ all the eigenvalues are 1 and hence the corresponding Brauer character takes value $\lambda_1(x) = p$. Analogously, for $V_2 = \bigoplus_{i=1}^{2p} \mathbb{F}_p$ the corresponding Brauer character takes value $\lambda_2(x) = 2p$, for all $x \in G_{p'}$.*

This example shows that opposed to the ordinary character Brauer character can distinguish representations V_1 and V_2. Let us state the elementary properties of Brauer characters.

Proposition 9. *Let (F, R, k) be a p-modular system with $\mathrm{char}F = 0$, and let U be a kG-module. Then*

1. $\lambda_U(1) = \dim_k(U)$.
2. *λ is a class function on the set of conjugacy classes of p-regular elements.*
3. *If $0 \to U_1 \to U_2 \to U_3 \to 0$ is a short exact sequence of kG-modules, then $\lambda_{U_2} = \lambda_{U_1} + \lambda_{U_3}$. In particular, Brauer character depends only on composition factors of a module.*
4. *If U can be lifted to an RG-lattice $\hat{U}$, i. e. $U \cong \hat{U}/(\pi)\hat{U}$, then the values of the ordinary character of $\hat{U}$ coincide with the Brauer character of U on the set of p-regular elements of G.*

As one would expect by analogy with the ordinary characters the Brauer characters of the simple kG-modules are linearly independent. Namely, let us denote by $cc_p(G)$ the set of conjugacy classes of p-regular elements in G, and by $F^{cc_p(G)}$ the vector space of functions $cc_p(G) \to F$.

Theorem 10. *Let $U_1, \ldots, U_n$ be a full set of non-isomorphic simple kG-modules. Then the corresponding Brauer characters $\lambda_1, \ldots, \lambda_n$ form a basis of $F^{cc_p(G)}$.*

Theorem 10 together with Proposition 9 imply that the Brauer character precisely characterizes the composition factors of a module, but in general cannot detect its equivalence-type.

Corollary 11. *Let L and M be kG-modules with Brauer characters λ and μ, respectively. Then $\lambda = \mu$ if and only if L and M have the same set of composition factors (counted with multiplicities), or equivalently $[L] = [M] \in G_0(kG)$*

As we already mentioned the Brauer character gives us a tool for computing the decomposition matrix. Namely, given an FG-module V and its ordinary character χ_V we immediately obtain from Proposition 9 that

$$\chi_V(g) = \sum_S d_{VS}\lambda_S(g), \text{ for all } g \in G_{p'}.$$

Linear independence of Brauer characters $\{\lambda_S\}_S$ guarantees that the coefficients d_{VS} are uniquely determined. Hence, in the situation when the ordinary characters of simple FG-modules and the Brauer characters of simple kG-modules are known, we may easily compute the decomposition numbers just by expressing an ordinary character as a linear combination of simple Brauer characters.

1.5 Projective modules

Let us switch for a moment to a more general setting of A being a finite dimensional algebra over a field, bearing in mind our main example of a group algebra. All modules are finitely generated unless explicitly stated otherwise. Even though an algebra A, viewed as a module over itself, does not necessarily decompose into a direct sum of simple A-modules, we still can write it as a direct sum of indecomposable A-modules. The Krull-Schmidt theorem guarantees that indecomposable components are uniquely determined up to isomorphism. The following properties, which we state without proofs, show the importance of the role indecomposable projective modules play in modular representation theory.

1. The decompositions of A into a direct sum of submodules $A = A_1 \oplus A_2 \oplus \ldots \oplus A_n$ biject with expressions of 1 as a sum of orthogonal idempotents $1 = e_1 + e_2 + \ldots + e_n$, $e_i \in A$. The submodule corresponding to the idempotent e_i is determined by $A_i = Ae_i$ and A_i is indecomposable if and only if e_i is primitive.

2. Every simple A-module S has a projective cover P_S, which is uniquely determined up to isomorphism. It is given by $P_S = Ae_S$, where e_S is a primitive idempotent in A satisfying $e_S S \neq 0$.

3. Isomorphism classes of indecomposable projective A-modules are in bijection with isomorphism classes of simple A-modules. The correspondence is given as follows.

$$\left\{ \begin{array}{c} \text{Iso classes of indecomposable} \\ \text{projective } A\text{-modules} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Iso classes of} \\ \text{simple } A\text{-modules} \end{array} \right\}$$

$$P \longmapsto S = P/\mathrm{Rad}P$$
$$P_S \longleftarrow S,$$

where P_S is the projective cover of S. In other words, every indecomposable projective A-module is isomorphic to a projective cover P_S of some simple module S, and $P_S \cong P_T$ if and only if $S \cong T$.

4. Every indecomposable projective A-module P_S occurs as a direct summand of the module A and we have the following decomposition

$$A \cong \bigoplus_S P_S^{n_S},$$

where the sum runs over all simple modules S and $n_S = \dim_{D_S}(S)$, $D_S = \mathrm{End}_A(S)$. Let us note that n_S equals multiplicity of S appearing as a summand in $A/\mathrm{Rad}A$.

5. Every projective A-module (not necessarily finite dimensional) decomposes into a direct sum of indecomposable projective submodules, the summands are uniquely determined up to isomorphism.

6. Let (F, R, k) be a splitting p-modular system for G. Given a projective RG-module P its reduction $P/(\pi)P$ is a projective kG-module. Moreover, every projective kG-module can be uniquely lifted to a projective RG-module. This means that reduction homomorphism $K_0(RG) \to K_0(kG)$ is an isomorphism. On the contrary, the reduction of a simple RG-module does not have to be a simple kG-module; in general, not every simple kG-module can be lifted to an RG-module

In the situation when FG is a group algebra with coefficient field of characteristic zero all finitely generated modules are projective by Maschke theorem, and being simple is the same as being projective indecomposable, while in positive characteristic simple modules are mostly non-projective. Comparing ordinary and modular representation theory, we see that even though properties, we are used to have for simple modules in characteristic 0, do not pass through to the modular case, some of them do still hold for the indecomposable projective modules. Namely, if $A = FG$ with $\text{char} F = 0$ the properties $(1) - (5)$ translate into the standard statements about irreducible representations.

One of the important applications of the projective modules is a computation of the multiplicity of a simple module as a factor in a Jordan-Hölder decomposition of an arbitrary module. For a simple A-module S and an A-module M, we denote by $[M : S]$ the multiplicity of S as a composition factor of M.

Proposition 12. *Let S be a simple A-module with projective cover P_S.*

1. *Let T be a simple A-module, then*

$$\dim \text{Hom}_A(P_S, T) = \begin{cases} \dim \text{End}_A(S), & \text{if } T \cong S \\ 0, & \text{otherwise.} \end{cases}$$

2. *Let M be an A-module, then*

$$[M : S] = \dim \text{Hom}_A(P_S, M)/ \dim \text{End}_A(S).$$

Proof. (1) From the condition that $P_S/\text{Rad}P_S \cong S$ is simple and the fact that $\text{Rad}P_S$ is the smallest submodule in P_S, such that the quotient $P_S/\text{Rad}P_S$ is semisimple, we immediately conclude that if $f : P_S \to T$ is a non-zero homomorphism, then $T \cong S$. Any homomorphism $f : P_S \to S$ factors through the quotient $P_S/\text{Rad}P_S$, and any homomorphism $P_S/\text{Rad}P_S \to S$ is either an isomorphism or a zero map, which implies $\text{Hom}_A(P_S, T) \cong \text{End}_A(S)$.

(2) Let $0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_n = M$ be a composition series for M. We prove the claim by induction on n. For $n = 1$ the result follows from part (1). To conclude the induction step suppose that $n > 1$ and $[M_{n-1} : S] = \dim \text{Hom}_A(P_S, M_{n-1})/ \dim \text{End}_A(S)$ and consider the short exact sequence

$$0 \to M_{n-1} \to M \to M/M_{n-1} \to 0,$$

which after applying $\mathrm{Hom}_A(P_S, -)$ becomes

$$0 \to \mathrm{Hom}_A(P_S, M_{n-1}) \to \mathrm{Hom}_A(P_S, M) \to \mathrm{Hom}_A(P_S, M/M_{n-1}) \to 0.$$

Therefore,

$$\begin{aligned}\dim \mathrm{Hom}_A(P_S, M) = \mathrm{Hom}_A(P_S, M_{n-1}) + \dim \mathrm{Hom}_A(P_S, M/M_{n-1}) = \\ = \dim \mathrm{End}_A(S)([M_{n-1} : S] + [M/M_{n-1} : S]),\end{aligned}$$

where the last equality follows from part (1). Dividing both sides by $\dim \mathrm{End}_A(S)$ completes the induction step and the proof is finished. □

We now introduce the Cartan matrix for a group G in characteristic p. Let (F, R, k) be a splitting p-modular system for G. *The Cartan matrix* C is the matrix with rows and columns indexed by the simple kG-modules with entries defined by

$$c_{ST} = [P_T : S] = \text{multiplicity of } S \text{ as a composition factor in } P_T,$$

where S and T are simple kG-modules. The coefficients c_{ST} are called *Cartan invariants.* Later we will see how the Cartan matrix is related to the decomposition matrix and it will be shown that the Cartan matrix is symmetric.

1.6 Example: p-groups

Let G be a finite p-group and let k be a field of characteristic p. In this situation it is very easy to describe all simple and projective kG-modules. Nevertheless, this example will be of a great use for us later on.

Proposition 13. *Let G be a p-group and k a field of characteristic p. The trivial module k is the unique simple kG-module.*

Proof. Let S be a simple kG-module. If $k = \mathbb{F}_p$, then S is a finite set. The cardinality of S is divisible by p, since it is a vector space over the field with p elements. The group G acts on S and each orbit has size a power of p (can be 1), since G is a p-group. The zero element in S has orbit of size 1. Therefore, since the sum of sizes of all orbits in S equals to the cardinality of S there must exist a non-zero element $x \in S$ with an orbit of size 1. This means that x is fixed by G and hence generates a trivial kG-submodule in S. Consequently $S \cong k$. In a general situation of k being an arbitrary field of characteristic p, consider a nonzero element $s \in S$ and let S' be an $\mathbb{F}_pG$-submodule in S generated by $\{gs \mid g \in G\}$. By the previous argument S' contains a non-zero vector x fixed by G, and again by simplicity of S we conclude that $S \cong k$. □

Lemma 14. *Let G be a p-group and k a field of characteristic p. Then* $\mathrm{Rad}(kG)$ *coincides with the augmentation ideal* $I(kG) = \{\sum \alpha_g g \in kG \mid \sum \alpha_g = 0\}$.

Proof. It is straightforward from the definition that the augmentation ideal $I(kG)$ is precisely the set of those elements in kG that act by zero on the trivial kG-module k. Using the characterization of a radical as $\mathrm{Rad}(kG) = \{x \in kG \mid xS =$

0 for every simple kG-module $S\}$ and that k is the only simple kG-module we conclude the claim $\mathrm{Rad}(kG) = I(kG)$. □

Proposition 15. *Let G be a p-group and k a field of characteristic p. Then the regular representation is the only indecomposable projective kG-module.*

Proof. The uniqueness follows from Proposition 13 and the bijection between isomorphism classes of indecomposable projective modules and simple modules. Let us show that kG is indecomposable. If $kG = V_1 \oplus V_2$, where V_i are non-zero kG-submodules, then $\mathrm{Rad}(kG) = \mathrm{Rad}(V_1) \oplus \mathrm{Rad}(V_2)$ with $\mathrm{Rad}(V_i) \neq V_i$. Hence, the codimension of $\mathrm{Rad}kG$ in kG is at least two, but as we have shown in Lemma 14 $kG/\mathrm{Rad}(kG) = kG/I(kG) \cong k$, which leads to a contradiction. □

Note that we have just proved that kG is a projective cover of k, since by Nakayama Lemma $kG \to kG/\mathrm{Rad}(kG)$ is an essential epimorphism.

Corollary 16. *For a p-group G and a field k of characterisitc p any projective kG-module is free.*

Proof. Any projective kG-module decomposes into a direct sum of indecomposable projective kG-modules, hence by Proposition 15 it should a free module. □

1.7 The cde triangle

The goal of this section is to prove the relation between the decomposition matrix and the Cartan matrix, namely $C = D^T D$. Later on this will be used to deduce the significant properties of blocks of defect zero, which are the essential tools in our work. We start by introducing the cde triangle. Let (F, R, k) be a splitting p-modular system for G. The *cde triangle* is the following triangular-shaped diagram.

$$\begin{array}{ccc} & G_0(FG) & \\ {\scriptstyle e}\nearrow & & \searrow{\scriptstyle d} \\ K_0(kG) & \xrightarrow{\quad c \quad} & G_0(kG) \end{array}$$

Homomorphisms:

c We choose a basis of $K_0(kG)$ given by the classes of indecomposable projective kG-modules $[P_S]$. Any such module P_S can be viewed as an element in $G_0(kG)$ and the homomorphism c called *the Cartan map* is given on the basis elements by
$$c([P_S]) = [P_S].$$

d A basis of $G_0(FG)$ is given by the classes of simple FG-modules $[V]$. The decomposition map d was already defined as a reduction modulo p. Namely, given a simple FG-module V we put
$$d([V]) = [\overline{V}].$$

e An indecomposable projective kG-module P_S can be lifted to a projective RG-module $\hat{P}_S$, which is uniquely determined up to isomorphism and hence we have a well-defined the map

$$e([P_S]) = [F \otimes_R \hat{P}_S].$$

Proposition 17. *The homomorphisms above satisfy $c = de$.*

Proof. Let P_S be an indecomposable kG-module, then $e([P_S]) = [F \otimes_R \hat{P}_S]$. To reduce $F \otimes_R \hat{P}_S$ modulo p we need to choose a full RG-sublattice, which may be taken $\hat{P}_S$, and then reduce it modulo maximal ideal (π). Since $\hat{P}_S$ is a lift of P_S we obtain that

$$de(P_S) = d([F \otimes_R \hat{P}_S]) = [\hat{P}_S/\pi\hat{P}_S] = [P_S] = c([P_S]).$$

□

It is easy to see that in the chosen bases the Cartan map c is given by the Cartan matrix C and the decomposition map d is given by D^T the transpose of the decomposition matrix. Our next goal is to determine the matrix of e. For this we will need the following lemma, relating the homomorphisms between lattices and homomorphisms between reductions of those lattices.

Lemma 18. *Let (F, R, k) be a p-modular system. Let U, V be FG-modules and U_0, V_0 be the corresponding full RG-lattices.*

1. $\mathrm{Hom}_{RG}(U_0, V_0)$ *is a full R-lattice in* $\mathrm{Hom}_{FG}(U, V)$.

2. *Assume that additionally U_0 is projective as an RG-module, then*

$$\mathrm{Hom}_{RG}(U_0, V_0)/\pi\mathrm{Hom}_{RG}(U_0, V_0) \cong \mathrm{Hom}_{kG}(U_0/\pi U_0, V_0/\pi V_0).$$

Proof. (1) We may identify $\mathrm{Hom}_{RG}(U_0, V_0)$ with a subset of $\mathrm{Hom}_{FG}(U, V)$, since R-bases in U_0 and V_0 are at the same time F-bases of U and V, respectively, and an RG-homomorphism $U_0 \to V_0$ written as a matrix in the chosen basis has coefficients in $R \subseteq F$, hence it determines an FG-homomorphism $U \to V$. Since $\mathrm{Hom}_{RG}(U_0, V_0)$ is a subset of a free finitely generated R-module $\mathrm{Hom}_R(U_0, V_0)$ and R is a PID, then $\mathrm{Hom}_{RG}(U_0, V_0)$ is an R-lattice.

It is left to show that $\mathrm{Hom}_{RG}(U_0, V_0)$ spans $\mathrm{Hom}_{FG}(U, V)$ over F. Let $f : U \to V$ be an FG-homomorphism, let us write it in terms of the bases chosen in U_0 and V_0, we get a matrix M_f with entries in F. By clearing denominators we can choose $r \in R \setminus \{0\}$ such that rM_f has coefficients in R, and hence $rf \in \mathrm{Hom}_{RG}(U_0, V_0)$.

(2) Firstly, let us observe that $\pi\mathrm{Hom}_{RG}(U_0, V_0) = \mathrm{Hom}_{RG}(U_0, \pi V_0)$, since the multiplication by π on the left induces an RG-isomorphism $V_0 \to \pi V_0$. Next, consider the map $q : \mathrm{Hom}_{RG}(U_0, V_0) \to \mathrm{Hom}_{RG}(U_0, V_0/\pi V_0)$ induced by the quotient $V_0 \to V_0/\pi V_0$. Because of projectivity of U_0 the map q is surjective with kernel $\mathrm{Hom}_{RG}(U_0, \pi V_0)$. Therefore,

$$\mathrm{Hom}_{RG}(U_0, V_0)/\pi\mathrm{Hom}_{RG}(U_0, V_0) \cong \mathrm{Hom}_{RG}(U_0, V_0/\pi V_0).$$

Moreover, every RG-homomorphism $U_0 \to V_0/\pi V_0$ must vanish on πU_0 and hence factors through $U_0/\pi U_0$, which implies

$$\mathrm{Hom}_{RG}(U_0, V_0/\pi V_0) \cong \mathrm{Hom}_{kG}(U_0/\pi U_0, V_0/\pi V_0).$$

□

Theorem 19. *Let (F, R, k) be a splitting p-modular system for G and assume that R is complete with respect to its valuation. Let S be a simple kG-module and let V be a simple FG-module, then*

$$[(F \otimes_R \hat{P}_S) : V] = [\overline{V} : S].$$

In particular with respect to the chosen bases the matrix of e is D.

Proof. Since FG is a semisimple algebra we have that

$$[(F \otimes_R \hat{P}_S) : V] = \dim_F \mathrm{Hom}_{FG}(F \otimes_R \hat{P}_S, V)/\dim_F \mathrm{End}_{FG}(V).$$

Let V_0 be a full RG-lattice in V. Applying Lemma 18 we obtain

$$\begin{aligned}\dim_F \mathrm{Hom}_{FG}(F \otimes_R \hat{P}_S, V) &= \dim_R \mathrm{Hom}_{RG}(\hat{P}_S, V_0) \\ &= \dim_k \mathrm{Hom}_{kG}(P_S, \overline{V}).\end{aligned}$$

As we have shown in Proposition 12

$$[\overline{V} : S] = \dim_k \mathrm{Hom}_{kG}(P_S, \overline{V})/\dim_k \mathrm{End}_{kG}(S).$$

Since we assumed that both F, k are splitting fields for G the dimensions of $\mathrm{End}_{FG}(V)$ and $\mathrm{End}_{kG}(S)$ are both 1, which yields the desired formula

$$[(F \otimes_R \hat{P}_S) : V] = [\overline{V} : S].$$

The matrix of the homomorphism e is determined by

$$e([P_S]) = [F \otimes_R \hat{P}_S] = \sum_V e_{VS}[V],$$

hence $e_{VS} = [F \otimes_R \hat{P}_S : V] = [\overline{V} : S] = d_{VS}$, which completes the proof. □

From Proposition 17 and Theorem 19 we get an immediate corrolary which allows to easily determine the Cartan matrix from the knowledge of the decomposition matrix.

Corollary 20. *Let (F, R, k) be a splitting p-modular system for G. Then $C = D^T D$, in particular the Cartan matrix C is symmetric.*

1.8 Blocks

The theory of blocks plays a crucial role in the modular representation theory. Even though for our purposes only the so-called blocks of defect zero are needed, let us first introduce the general notion of a block. In the literature one may find different equivalent approaches to define what a block is. Here we will provide several definitions of a block and see how they are equivalent. After that we will examine blocks of defect zero in more detail.

Blocks as idempotents. Let A be a ring with 1. A *block* of a ring A is a primitive idempotent in the center $Z(A)$, i.e., $e \in Z(A)$ such that $e^2 = e$ and if $e = e_1 + e_2$ with $e_i \in Z(A)$ orthogonal idempotents, then one of e_i is 0. The following proposition shows how central idempotents of A determine decompositions of A into a direct sum of 2-sided ideals (compare to the property (1) from Section 1.5).

Proposition 21. *The decompositions of a ring A into a direct sum of 2-sided ideals*

$$A = A_1 \oplus \ldots \oplus A_n$$

biject with expressions of 1 as a sum of orthogonal central idempotents

$$1 = e_1 + \ldots + e_n.$$

The central idempotent e_i corresponding to A_i is determined as identity element of A_i. In opposite direction the 2-sided ideal corresponding to e_i is $A_i = Ae_i$. The A_i is indecomposable as a ring if and only if the corresponding e_i is a primitive central idempotent.

The proof is straightforward and we don't include it here. The decomposition of A as a direct sum of indecomposable 2-sided ideals is unique in a very strong sense, namely, the summands A_i are uniquely determined as subsets of A, and automatically the corresponding primitive central idempotents e_i are also uniquely determined. For the comparison the statement about decomposition of A into a direct sum of indecomposable A-modules only guarantees the uniqueness of summands up to isomorphism. From the Proposition 21 we immediately get the following equivalent definition of a block.

Blocks as ring summands. A *block* of a ring A is an indecomposable 2-sided ideal in A that is a direct summand of A.

We proceed by showing that each block determines an equivalence class of indecomposable A-modules. Let V be an A-module and let

$$1 = e_1 + \ldots + e_n,$$

where $e_i \in Z(A)$ are orthogonal primitive central idempotents. We can decompose V into a direct sum of A-submodules as

$$V = e_1V \oplus \ldots \oplus e_nV.$$

If V is an indecomposable A-module we obtain that $V = e_iV$ for some i, and $e_jV = 0$ for $j \neq i$. We say that a module V belongs to a block e if $eV = V$. This defines an equivalence relation on indecomposable A-modules, It is clear that each indecomposable A-module belongs to a unique block, and each block e is non-empty, since it contains all indecomposable Ae-modules viewed as A-modules.

Therefore, we see that a block e is uniquely determined by modules that belong to it, and we obtain the following equivalent description of a block.

Blocks as equivalence classes of indecomposable modules. A *block* of a primitive central idempotent e consists of all indecomposable A-modules V, such that $eV = V$.

So far all the descriptions of a block directly involved primitive central idempotents of A. The next characterization of a block differs from previous and is given in terms of an equivalence relation on simple A-modules.

We say that simple A-modules S, T are *linked* if there exists a non-split short exact sequence of A-modules $0 \to X \to Y \to Z \to 0$ with $\{X, Z\} = \{S, T\}$, which is equivalent to the condition that at least one of the groups $\mathrm{Ext}^1_A(S, T)$, $\mathrm{Ext}^1_A(T, S)$ is non-trivial. We call simple A-modules S, T *equivalent* $S \sim T$ if either $S \cong T$ or there is a sequence of simple A-modules $S = S_1, S_2, \ldots, S_n = T$ such that the consecutive modules S_i, S_{i+1} are linked.

Proposition 22. *Let A be a finite dimensional algebra over a field, and let S, T be simple A-modules. The following are equivalent.*

1. *$S \sim T$.*
2. *There exists a sequence of simple A-modules $S = S_1, S_2, \ldots, S_n = T$ such that the consecutive modules S_i and S_{i+1} are composition factors of the same indecomposable projective A-module.*
3. *S and T belong to the same block.*

Proof. (1) $\Rightarrow$ (2) It is enough to prove that if two simple A-modules S and T are linked, then there is an indecomposable projective A-module having S, T among its composition factors. Let

$$0 \longrightarrow S \xrightarrow{\ i\ } X \xrightarrow{\ q\ } T \longrightarrow 0 \qquad (1.1)$$

be a non-split short exact sequence. Let $\pi_T \colon P_T \to T$ be a projective cover of T. By projectivity of P_T there exists a homomorphism $f \colon P_T \to X$ making the following diagram commute

$$\begin{array}{ccccc} & & & & P_T \\ & & & \overset{f}{\swarrow} & \downarrow \pi_T \\ S & \hookrightarrow & X & \xrightarrow{\ q\ } & T \end{array}$$

We claim that f is surjective. Suppose that $\mathrm{im}\, f$ is a proper submodule of X. Since X has only 2 composition factors $\mathrm{im}\, f$ must be simple. Since T is a composition factor of $\mathrm{im}\, f$, we conclude that $q_{|\mathrm{im}\, f} \colon \mathrm{im}\, f \to T$ is an isomorphism, which forces the sequence (1.1) to split and leads to a contradiction. Hence, $f \colon P_T \to X$ is surjective and therefore, both S and T are composition factors of the indecomposable projective A-module P_T.

(2) $\Rightarrow$ (3) The claim immediately follows from an easy observation that if $0 \to X \to Y \to Z \to 0$ is a short exact sequence of A-modules, then Y belongs to a block e if and only if X, Z belong to e.

(3) ⇒ (1) Let us decompose the set of equivalence classes of simple A-modules into two parts: $\mathcal{C}_1$ consisting of all simple modules that are equivalent to S, and $\mathcal{C}_2$ being the set of all the rest simple A-modules. We claim that every A-module V can be uniquely written as $V = V_1 \oplus V_2$, where V_i is a submodule in V having all its composition factors in $\mathcal{C}_i$, $i = 1, 2$. The idea behind the proof of this claim is an observation that it is possible to find a composition series $0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_n = V$ such that for some index i all the composition factors of M_i belong to $\mathcal{C}_1$ and composition factors of V/M_i belong to $\mathcal{C}_2$. This can be achieved by "interchanging" consecutive composition factors from $\mathcal{C}_2$ and $\mathcal{C}_1$ in the composition series. Then we put $V_1 = M_i$, which is the submodule of V carrying $\mathcal{C}_1$ composition factors of V. Repeating the same procedure with roles of $\mathcal{C}_1$ and $\mathcal{C}_2$ interchanged we get V_2. For more details see Lemma 12.1.6 in [W].

Decompose A into a direct sum of submodules $A = A_1 \oplus A_2$, such that decomposition factors of A_i lie in $\mathcal{C}_i$. Apart from being a left ideal A_i is also a right ideal, since for any $a \in A$ multiplication by a on the right induces a surjective homomorphism of A-modules $A_i \to A_i \cdot a$, which means that the composition factors of $A_i \cdot a$ belong to $\mathcal{C}_i$. Hence A_1 is a direct sum of blocks. Since S and T belong to the same block in A_1, we conclude that $T \in \mathcal{C}_1$ and $S \sim T$. □

Blocks as equivalence classes of simple modules. A *block* of A is an equivalence class of simple A-modules given by the equivalence relation generated by $S \sim T$ if $\mathrm{Ext}^1_A(S, T) \neq 0$.

1.9 Blocks of defect 0

A notable role in this thesis is played by the blocks of defect 0. So far we have not explained what a "defect of a block" is, but blocks of defect zero are particularly easy to describe. Here we are going to use the characterization of a block in terms of equivalence classes of simple modules. Let G be a finite group and let (F, R, k) be a splitting p-modular system. We call a block e of kG *a block of defect zero* if it contains a simple projective kG-module.

Lemma 23. *If a block of kG contains a simple kG-module S that is at the same time projective, then S is the only simple kG-module in this block.*

Proof. We claim that any short exact sequence $0 \to X \to Y \to Z \to 0$ of kG-modules with $S \in \{X, Z\}$ splits. If $Z = S$, then it must split by projectivity of S. At the same time we know that any projective kG-module is injective, so in case $X = S$ the sequence splits because of injectivity of S. Therefore, S is the only simple module in its equivalence class, which finishes the proof. □

We have just shown that a block of defect zero consists of precisely one simple module. Let S be a simple kG-module from a block of defect zero. Since S is projective it can be uniquely lifted to a simple projective RG-module $\hat{S}$ by Property 6 in Section 1.5, which is in general not the case for an arbitrary simple kG-module. Therefore, a simple FG-module $V = F \otimes_R \hat{S}$ is the unique lift of S. By abuse of notation both simple modules S and V will be called blocks of defect zero of kG

and FG, respectively. Note that for FG we defined blocks of defect zero as lifts of defect zero blocks in kG. In this section we characterize defect zero blocks in FG and show that complex characters of those vanish outside p-regular elements of G.

Theorem 24. *Let G be a finite group of order $p^\alpha m$, where $p \nmid m$, and let (F, R, k) be a splitting p-modular system. Let V be an FG-module with a full RG-sublattice U. The following are equivalent.*

1. *A kG-module $\overline{V} = U/\pi U$ is simple and projective.*
2. *V is a simple FG-module and $p^\alpha | \dim_F(V)$.*
3. *V is a simple FG-module and U is a projective RG-module.*

Proof. (1) $\Rightarrow$ (2) Let us first show that V is a simple FG-module. Assume on the contrary that $V = V_1 \oplus V_2$, where V_i are FG-submodules in V. Then we can find full RG-sublattices U_i in V_i, $i = 1, 2$ and obtain that composition factors of $\overline{V}$ are the same as of $U_1 \oplus U_2$, which is contradicting to simplicity of $\overline{V}$.

Next we explain how projectivity of $\overline{V}$ implies that the dimension of V is a multiple of p^α. It is clear that $\dim_F V = \text{rank}\,_R U = \dim_k \overline{V}$. Let H be a Sylow p-subgroup in G. Since $\overline{V}$ is a projective kG-module its restriction $\text{Res}^G_H \overline{V}$ is also projective as a kH-module (see e.g. [W, Lemma 8.1.2]). By Corollary 16 all finitely generated projective kH-modules are free, since H is a p-group and $\text{char} k = p$. Therefore, the dimension of $\overline{V}$ is divisible by order of H, which is exactly p^α. Hence, $p^\alpha | \dim_F(V)$.

(2) $\Rightarrow$ (3) Denote by $n = \dim_F(V) = \text{rank}\,_R(U)$. Let us view U as a module over $\text{End}_R(U) \cong M_n(R)$. Then U is projective, since it is isomorphic to an $M_n(R)$-module of column vectors $\{(u_1, \dots, u_n)^T \mid u_i \in R\}$, that is obviously a direct summand in $M_n(R)$.

Our next claim is that the homomorphism $RG \to \text{End}_R(U)$ given by the action of RG identifies $\text{End}_R(U) \cong M_n(R)$ with a direct summand of RG. It is easy to see that this claim implies that U is a projective RG-module.

Let us consider the primitive central idempotent in FG associated with V

$$e = \frac{n}{|G|} \sum_{g \in G} \chi_V(g) g^{-1}.$$

Since $p^\alpha \mid n$ we have $n/|G| \in R$. As $\chi_V(g)$ is a sum of roots of unity, which all have valuation 1, we conclude that $\chi_V(g) \in R$ and thus get $e \in R$. Therefore

$$RG = eRG \oplus (1 - e)RG.$$

The homomorphism $\rho \colon FG \to \text{End}_F(V)$ given by the action of FG on V has kernel $(1 - e)FG$ and identifies eFG with $\text{End}_F(V) \cong M_n(F)$. Since U is a full RG-lattice in V we conclude that the restriction of ρ to RG has image in $\text{End}_R(U) \cong M_n(R)$ and has kernel $(1 - e)RG$. Now it is left to show that $\rho_{|RG} \colon RG \to \text{End}_R(U)$ is surjective. Let us check that the following homomorphism is a section for $\rho\colon FG \to \mathrm{End}_F(V)$

$$s\colon \mathrm{End}_F(V) \to FG$$
$$s(\phi) = \tfrac{n}{|G|} \sum_{g\in G} \mathrm{Tr}(\rho(g^{-1})\phi)\cdot g.$$

It is enough to check $\rho s(\rho(h)) = \rho(h)$ for $h \in G$, since $\mathrm{End}_F(V)$ is generated by $\rho(h)$.

$$s(\rho(h)) = \frac{n}{|G|}\sum_{g\in G}\mathrm{Tr}(\rho(g^{-1})\rho(h))\cdot g = \frac{n}{|G|}\sum_{g'\in G}\mathrm{Tr}(\rho(g'^{-1}))\cdot hg' = he.$$

Therefore,

$$\rho s(\rho(h)) = \rho(he) = \rho(h)\rho(e) = \rho(h).$$

We see that the image of $\mathrm{End}_R(U) \subseteq \mathrm{End}_F(V)$ under the section s lies in RG, hence $\rho_{|RG}\colon RG \to \mathrm{End}_R(U)$ is a surjective homomorphism, which finishes the proof.

(3) $\Rightarrow$ (1) Since U is a direct summand of a free RG-module, its reduction $\overline{V} = U/\pi U$ is a direct summand of a free kG-module. Hence $\overline{V}$ is a projective kG-module.

We proceed by showing that $\overline{V}$ is indecomposable. Suppose on the contrary that $\overline{V} \cong P_{S_1} \oplus \ldots \oplus P_{S_r}$, where P_{S_i} is an indecomposable projective module, and due to characterization provided in Section 1.5 is a projective cover of some simple kG-module S_i. Hence $U \cong \hat{P}_{S_1} \oplus \ldots \oplus \hat{P}_{S_r}$ and $V \cong (F\otimes_R \hat{P}_{S_1}) \oplus \ldots \oplus (F\otimes_R \hat{P}_{S_r})$, which implies $r = 1$ and $\overline{V} \cong P_{S_1}$. Let us examine the multiplicity of S_1 as a composition factor in $\overline{V} \cong P_{S_1}$. On one hand $P_{S_1}/\mathrm{Rad}(P_{S_1}) \cong S_1$ and $\mathrm{Soc}(P_{S_1}) \cong S_1$, hence if $P_{S_1} \not\cong S_1$ the multiplicity of S_1 as a composition factor in P_{S_1} is at least 2. On the other hand by Theorem 19 we have that for any simple FG-module W it holds

$$[\overline{W} : S_1] = [(F\otimes_R \hat{P}_{S_1}) : W] = [V : W] = \begin{cases} 1, & \text{if } W \cong V \\ 0, & \text{otherwise.} \end{cases}$$

In other words it means that the column of decomposition matrix corresponding to S_1 consists of zeroes apart from the only entry in the row of a simple FG-module V. Using the fact that $C = D^T D$ we conclude that $[P_{S_1} : S_1] = 1$. Therefore, $P_{S_1} \cong S_1$ and $\overline{V}$ is simple as claimed. □

Proposition 25. *Let P be a projective RG-module. Then the character of $F\otimes_R P$ vanishes on the elements of order divisible by p.*

Proof. Let $g \in G$ be an element of order divisible by p. Consider a cyclic subgroup $C = \langle g\rangle$ generated by g. Then P is still projective viewed as an RC-module. Let us write $g = g_p g_{p'}$, where $g_p, g_{p'}$ are p-singular and p-regular components of g, respectively. Since g_p and $g_{p'}$ commute it is clear that $C = \langle g_p\rangle \times \langle g_{p'}\rangle$.

The reduction $P/(\pi)P$ is a projective kC-module. Any projective kC-module can be written as a tensor product over k of a projective $k\langle g_p\rangle$-module and a projective $k\langle g_{p'}\rangle$-module. By Corollary 16 all projective $k\langle g_p\rangle$-modules are free, since $\langle g_p \rangle$ is a p-group, and we deduce that

$$P/(\pi)P \cong (k\langle g_p \rangle)^a \otimes P',$$

where P' is a projective $k\langle g_{p'} \rangle$-module. Let a projective $R\langle g_{p'} \rangle$-module $\hat{P}'$ be the lift of a $k\langle g_{p'} \rangle$-module P'. Hence by the uniqueness of lifts

$$P \cong (R\langle g_p \rangle)^a \otimes \hat{P}', \text{ for some } a \in \mathbb{Z}_{\geq 0},$$

$$F \otimes_R P \cong (F\langle g_p \rangle)^a \otimes (F \otimes_R \hat{P}').$$

The property of characters that $\chi_{M \otimes N} = \chi_M \chi_N$ implies that the character of $F \otimes_R P$ is the product of $a \cdot \chi_{F\langle g_p \rangle}$ and $\chi_{F \otimes_R \hat{P}'}$. It is clear that the character of the regular representation $\chi_{F\langle g_p \rangle}$ is zero outside the elements of $\langle g_{p'} \rangle$, which concludes the proof. □

Proposition 26. *Let F be a splitting field for G of characteristic* 0, *and let V be a simple FG-module. Let p be a prime integer and $|G| = p^\alpha m$, where $p \nmid m$. If $p^\alpha | \dim_F V$, then $\chi_V(g) = 0$ for any element $g \in G$ of order divisible by p.*

Proof. As we have shown in Theorem 24, V is a block of defect zero in FG, hence is of the form $F \otimes_R P_S$, where P_S is an indecomposable projective RG-module. Hence by Proposition 25 χ_V vanishes on the elements of order divisible by p, which finishes the proof. □

1.10 p-blocks of a group

Let G be a finite group and (F, R, k) be a splitting p-modular system. If we apply the theory of blocks to a semisimple algebra FG, then the Artin-Wedderburn decomposition

$$FG \cong \prod_i M_{n_i}(F)$$

will be the same as a decomposition of FG into a direct sum of blocks, and each block will contain exactly one simple FG-module. On the other hand, we may obtain much more interesting partition of simple FG-modules into blocks as follows. Let V be a simple FG-module, it may be viewed as an RG-module, since RG is a subring in FG. Let $e \in RG$ be a block in RG, then e is also a central idempotent in FG. We say that *an FG-module V belongs to a block e* if $eV = V$. Evidently each simple FG-module V belongs to a unique block, and if U is a full RG-lattice in V, then U belongs to the same block as V. Hence we have just defined a partition of simple FG-modules into blocks consistent with that for RG. Next proposition shows that blocks of RG biject with blocks of kG under the reduction modulo the ideal (π).

Proposition 27. *Let G be a finite group and (F, R, k) be a splitting p-modular system, such that R is complete. Then the reduction modulo (π) induces a bijection*

$$\{\textit{idempotents in } Z(RG)\} \leftrightarrow \{\textit{idempotents in } Z(kG)\},$$

where primitive idempotents correspond to primitive ones.

From this we immediately conclude that the decomposition of RG into blocks after reduction modulo π becomes the decomposition of kG into blocks; and an RG-module V belongs to a block $e \in RG$ if and only if $V/\pi V$ belongs to a block $\overline{e} \in kG$.

In the same manner as with the notion of a block, a p-block of a group G is any of the following objects (with the passage from one object to another explained above).

- A block of RG, i.e., an indecomposable central idempotent e in RG, keeping in mind corresponding indecomposable two-sided ideal eRG in RG, and RG-modules that belong to e.
- A block in kG, i.e., an indecomposable central idempotent $\overline{e}$ in kG, indecomposable two-sided ideal ekG in kG; kG-modules that belong to $\overline{e}$.
- Block of simple FG-modules $\{V - \text{simple } FG\text{-module} \mid eV = V\}$, for e indecomposable central idempotent in RG.

For the sake of completeness let us introduce the notion of the defect of a block. Let G be a group of order $|G| = p^\alpha m$, with $(p, m) = 1$. ***The defect** d **of a** p**-block** e* of G is the smallest integer such that $p^{\alpha-d}$ divides the dimensions of all simple FG-modules in this block. Denote by $\text{ord}_p(n)$ the biggest power of p that divides n. Let V be a simple FG-module. From the fact that over a splitting field F of characteristic zero the dimensions of irreducible representations divide the order of G, we get that $\text{ord}_p(\dim_F V) \leq \alpha$, and hence automatically $d \geq 0$.

In the situation if the defect of a block e is zero the definition says that all simple FG-modules in e have dimensions divisible by p^{α}. Let V be a simple FG-module in e. By Theorem 24 the reduction $\overline{V}$ is simple and projective kG-module and by Lemma 23 $\overline{V}$ is the only simple kG-module in a block $\overline{e}$. Hence our definition is consistent with the one given in Section 1.9. Therefore, V is the only simple FG-module in a block e, since another simple FG-module V' in e would give rise to a non-isomorphic simple kG-module $\overline{V}'$ in a block $\overline{e}$, which is impossible.

Chapter 2

K- and G-theory prerequisites

This Chapter serves as an introduction to an algebraic K- and G-theory. Here we explain all the prerequisites needed later for the Conjecture of Hambleton, Taylor, and Williams. Since we are aiming to discuss the decomposition of G-groups of a group ring into G-groups of certain maximal orders in Chapter 3 here we will be paying a special attention to group rings and maximal orders.

2.1 First definitions and examples of groups K_0 and G_0

2.1.1 Definitions and properties

Historically the motivation to study algebraic K-groups has several origins. Firstly, K-groups host interesting topological invariants. For instance, the group K_1 gives rise to a Whitehead group, which in turn contains the so-called Whitehead torsion that is an obstruction for a homotopy equivalence of finite CW-complexes to be simple. Secondly, similar construction appeared in Grothendieck's proof of Riemann-Roch theorem and in the topological K-theory of Atiyah-Hirzebruch. The analogy between projective modules and vector bundles led to the development of the algebraic K-theory of rings.

Definition 28. *Let R be a ring. Define $K_0(R)$ to be an abelian group given by the following presentation.*

- **Generators:** *isomorphism classes of finitely generated projective R-modules, where the class represented by a module P is denoted by $\bar{P}$;*
- **Relations:** $\bar{P}_0 + \bar{P}_2 = \bar{P}_1$ *for every exact sequence* $0 \to P_0 \to P_1 \to P_2 \to 0$ *of finitely generated R-modules P_0, P_1, P_2.*

Since every short exact sequence of projective R-modules splits, $K_0(R)$ is just a group completion of an abelian monoid formed by the isomorphism classes of projective R-modules together with the direct sum operation. The group $K_0(R)$ is also called the *Grothendieck group* of R. A natural question to ask is what kind of a group we get if we drop the adjective 'projective'. If we add an extra restriction on R asking it to be a left noetherian ring, then the defined object will have very nice properties, which in general are lost if we allow arbitrary rings. We will return to this point when stating the main properties of K- and G-theory.

Definition 29. *Let R be a ring. Define $G_0(R)$ to be an abelian group given by the following presentation.*

- **Generators:** *isomorphism classes $\bar{M}$ of finitely generated R-modules M;*
- **Relations:** $\bar{M}_0 + \bar{M}_2 = \bar{M}_1$ *for every exact sequence $0 \to M_0 \to M_1 \to M_2 \to 0$ of finitely generated R-modules M_0, M_1, M_2.*

The following lemma gives a criterion for two modules to represent the same element in $G_0(R)$.

Lemma 30. *Let R be a ring. Let M_1, M_2 be finitely generated R-modules. Then $[M_1] = [M_2] \in G_0(R)$ if and only if there exist finitely generated R-modules A, B, C and short exact sequences of the form*

$$0 \to A \to M_1 \oplus B \to C \to 0,$$
$$0 \to A \to M_2 \oplus B \to C \to 0.$$

Proof. The sufficiency is obvious and we only need to show the necessity. Suppose $[M_1] = [M_2] \in G_0(R)$. The group $G_0(R)$ is defined as a quotient of the free abelian group with generators given by isomorphism classes of finitely generated R-modules by the subgroup generated by the expressions $\bar{M} - \bar{M}' - \bar{M}''$ coming from the short exact sequences. Therefore

$$\bar{M}_1 - \bar{M}_2 = \sum_{i \in I} (\bar{X}_i - \bar{X}_i' - \bar{X}_i'') - \sum_{j \in J} (\bar{Y}_j - \bar{Y}_j' - \bar{Y}_j''),$$

where the index sets I, J are finite, and modules X_i, X_i', X_i'' fit into an exact sequence $0 \to X_i' \to X_i \to X_i'' \to 0$, and the same for modules Y_j, Y_j', Y_j''. Hence,

$$\bar{M}_1 + \sum_{i \in I} (\bar{X}_i' + \bar{X}_i'') + \sum_{j \in J} \bar{Y}_i = \bar{M}_2 + \sum_{j \in J} (\bar{Y}_j' + \bar{Y}_j'') + \sum_{i \in I} \bar{X}_i.$$

Consider $X = \oplus_{i \in I} X_i$, $Y = \oplus_{j \in J} Y_j$ and analogously define X', X'', Y', Y''. Then there are short exact sequences

$$\begin{aligned} 0 \to X' \to X \to X'' \to 0, \\ 0 \to Y' \to Y \to Y'' \to 0 \end{aligned} \tag{2.1}$$

and an R-module $B = M_1 \oplus X' \oplus X'' \oplus Y$ is isomorphic to $M_2 \oplus Y' \oplus Y'' \oplus X$. From (2.1) there is a short exact sequence

$$0 \to X' \oplus Y' \to B \oplus M_2 \to M_1 \oplus X'' \oplus Y'' \oplus M_2 \to 0.$$

Doing the same for $M_2 \oplus Y' \oplus Y'' \oplus X \cong B$ we obtain a short exact sequence

$$0 \to X' \oplus Y' \to B \oplus M_1 \to M_1 \oplus X'' \oplus Y'' \oplus M_2 \to 0,$$

which finishes the proof. □

The corresponding condition for two finitely generated projective modules to represent the same element in $K_0(R)$ is much easier.

Lemma 31. *Let R be a ring and let P_1, P_2 be finitely generated projective R-modules. Then $[P_1] = [P_2] \in K_0(R)$ if and only if P_1 is stably isomorphic to P_2, i.e., $P_1 \oplus R^n \cong P_2 \oplus R^n$ for some $n \in \mathbb{N}$.*

In some literature in the situation when R is a non-noetherian ring $G_0(R)$ is defined differently. Namely, instead of all finitely generated R-modules one considers pseudo-coherent modules, i.e., those modules that admit an infinite resolution by finitely generated projective R-modules. In this work we will denote such a group by $G'_0(R)$. If R is noetherian then every finitely generated R-module is pseudo-coherent, which yields $G_0(R) \cong G'_0(R)$. Both groups $K_0(R)$ and $G_0(R)$ are instances of the following general construction.

Definition 32. *Let $\mathcal{C}$ be a small exact category. Define $K_0(\mathcal{C})$ to be an abelian group with generators $[C]$, $C \in \mathrm{Obj}(\mathcal{C})$ and relations $[C_1] = [C_0] + [C_2]$ for every short exact sequence $0 \to C_0 \to C_1 \to C_2 \to 0$ in $\mathcal{C}$.*

Examples.

1. If $\mathcal{P}_R$ is a category of finitely generated projective R-modules, then $K_0(\mathcal{P}_R) = K_0(R)$.
2. If $\mathrm{Mod}_{fg}(R)$ is a category of all finitely generated R-modules, then $K_0(\mathrm{Mod}_{fg}(R)) = G_0(R)$.
3. If $\mathcal{M}_R$ is a category of pseudo-coherent R-modules, then $K_0(\mathcal{M}_R) = G'_0(R)$.
4. Let $\mathcal{H}_R$ be a category of all R-modules having a finite length resolution by finitely generated projective R-modules. The category $\mathcal{H}_R$ is an exact subcategory of $\mathrm{Mod}(R)$ and it is closed under taking kernels of surjections. Therefore, $K_0(\mathcal{H}_R) \cong K_0(R)$.

One of the crucial differences between K_0 and G_0 is that K_0 is functorial while G_0 is not. Namely, given rings R, S any ring homomorphism $f\colon R \to S$ induces a homomorphism of groups $f_*\colon K_0(R) \to K_0(S)$ via $[P] \mapsto [S \otimes_R P]$. Since any short exact sequence of projective R-modules splits, the tensor product $S \otimes_R -$ preserves exactness and the map f_* is well-defined. Clearly, the same procedure would not work for G_0 since exactness of the short exact sequences is not necessarily preserved after tensoring with S. Nevertheless, with some additional assumptions a ring homomorphism $f\colon R \to S$ will induce the following maps on G_0.

- If S is finitely generated as an R-module, in particular this holds if the ring homomorphism $f\colon R \to S$ is surjective, then we may view each finitely generated S-module as an R-module via $r \cdot m = f(r) \cdot m$ for $r \in R, m \in M$ and the resulting R-module will be finitely generated. The defined functor $\mathrm{Mod}_{fg}(S) \to \mathrm{Mod}_{fg}(R)$ is exact and therefore induces a group homomorphism $res_f\colon G_0(S) \to G_0(S)$, which we call a *transfer* or a *a restriction homomorphism*.

- If S is flat as an R-module, then the functor $\mathrm{Mod}_{fg}(R) \to \mathrm{Mod}_{fg}(S)$ sending M to $S \otimes_R M$ is exact, and hence induces a group homomorphism $f_*\colon G_0(R) \to G_0(S)$, which we call *a base change homomorphism*. It is possible to extend the definition of f_* to the situation when S has a finite resolution by flat right R-modules. In this case Serre's formula gives an explicit expression $f_*([M]) = \sum(-1)^i[\mathrm{Tor}_i^R(S, M)]$.

Let us explain how to define a base change homomorphism f_* when S, viewed as a right R-module, admits a finite resolution by flat R-modules

$$0 \to F_n \to F_{n-1} \to \ldots \to F_0 \to S.$$

Let $\mathcal{F}$ be a full subcategory of $\mathrm{Mod}_{fg}(R)$ consisting of R-modules M such that $\mathrm{Tor}_i(S, M) = 0$ for all $i \neq 0$, i.e., precisely the category for which the functor $S \otimes_R -\colon \mathcal{F} \to \mathrm{Mod}_{fg}(S)$ is exact. It is clear that $\mathcal{F}$ contains $\mathcal{P}(R)$. Moreover, every finitely generated R-module M has a finite resolution by modules from $\mathcal{F}$ because of the following. Let

$$\ldots \to P_{n+1} \to P_n \to P_{n-1} \to \ldots \to P_0 \to M \to 0$$

be a projective resolution of M. The kernel $K_n = \ker(P_{n-1} \to P_{n-2})$ is a finitely generated module which has a projective resolution that consists of truncated at n-th place projective resolution of M

$$\ldots \to P_{n+2} \to P_{n+1} \to K_n \to 0.$$

From this $\mathrm{Tor}_i(S, K_n) = \mathrm{Tor}_{n+i+1}(S, M) = 0$ for $i > 0$, since S admits length n flat resolution. Therefore, $K_n \in \mathcal{F}$ and M admits a finite resolution by modules from $\mathcal{F}$. Moreover, the category $\mathcal{F}$ is closed under taking kernels of epimorphisms by a long exact sequence for Tor. Hence $K_0(\mathcal{F}) \cong G_0(R)$ and the tensor product $S \otimes_R -$ induces a map

$$f_*\colon G_0(R) \cong K_0(\mathcal{F}) \to G_0(S).$$

Serre's formula

$$f_*([M]) = \sum(-1)^i[\mathrm{Tor}_i^R(S, M)] \tag{2.2}$$

follows immediately from the fact that for a bounded chain complex C_* we have (see e.g. [Wei] Proposition II.7.5)

$$\chi(C_*) = \sum_i(-1)^i[C_i] = \sum_i(-1)^i[H_i(C_*)].$$

For any ring R there is a canonical homomorphism $i\colon \mathbb{Z} \xrightarrow{1 \mapsto 1} R$ which induces a group homomorphism $i_*\colon K_0(\mathbb{Z}) \to K_0(R)$.

Definition 33. *The cokernel of i_* is called the reduced K_0-group of R*

$$\tilde{K}_0(R) = K_0(R)/\mathrm{im}\ i_*.$$

2.1.2 Examples of explicit computations

The following examples of computations show that in general the groups $K_0(R), G_0(R), G_0'(R)$ are very different.

1. Let $R = k[x_1, x_2, \dots, x_n, \dots]/\big(x_i x_j \mid i, j \in \mathbb{Z}_{>0}\big)$, where k is a field and $k[x_1, x_2, \dots, x_n, \dots]$ denotes a polynomial ring in variables x_i. It is clear that the ideal $\mathfrak{m}$ generated by the images of x_i's in R satisfies $\mathfrak{m}^2 = 0$ and $R/\mathfrak{m} \cong k$. Moreover, $\mathfrak{m}$ is the unique maximal ideal in R, because any element outside $\mathfrak{m}$ is of the form $\alpha_0 + \sum_{i\geq 1} \alpha_i \overline{x}_i$, $\alpha_0 \in k^\times$ and has an inverse $\alpha_0^{-2}(\alpha_0 - \sum_{i\geq 1} \alpha_i \overline{x}_i)$. Therefore, R is a local ring with a maximal ideal $\mathfrak{m}$. Since $\mathfrak{m}$ is a nilpotent ideal in R we obtain (see e.g. [Wei] Lemma II.2.2)

$$K_0(R) \cong K_0(R/\mathfrak{m}) \cong \mathbb{Z}.$$

The following argument due to Swan [Sw] shows that

$$G_0(R) = 0.$$

Firstly, by induction on the number of generators it is easy to show that the class $[M] \in G_0(R)$ of any finitely generated R-module M can be written as a finite sum $\sum_i [R/J_i]$, for some ideals J_i in R. Hence, it is enough to show that $[R/J] = 0$ for any ideal J in R. We consider separately the cases of J being of finite and infinite dimension over k.

Case 1: $\dim_k(J) = \infty$. Denote by $\overline{x}_i$ the image of x_i in R. Then $\{\overline{x}_1, \overline{x}_2, \dots, \overline{x}_n, \dots\}$ is a k-basis of $\mathfrak{m}$. Let $\{j_1, j_2, \dots, j_n, \dots\}$ be a k-basis of J and let $j_n = \sum_i \lambda_{in} \overline{x}_i$, $\lambda_{in} \in k$. Consider a finitely generated R-module M, that has a k-basis $\{a, b, c_i\}_{i=1}^{\infty}$ and the action of R is given by $\overline{x}_n \cdot a = c_n$, $\overline{x}_n \cdot b = \sum_i \lambda_{in} c_i$, $\overline{x}_n \cdot c_i = 0$. Then we have the following exact sequences

$$0 \longrightarrow R \xrightarrow[1\mapsto a]{\alpha} M \longrightarrow \operatorname{coker}(\alpha) \cong k \longrightarrow 0,$$

$$0 \longrightarrow R \xrightarrow[1\mapsto b]{\beta} M \longrightarrow \operatorname{coker}(\beta) \cong R/J \longrightarrow 0,$$

which imply that $[R/J] = [k]$. Now let us take an infinite dimensional ideal $J' = (\overline{x}_2, \dots, \overline{x}_n, \dots)$ in R and consider a map $\gamma\colon k \to R/J'$ which sends 1 to the image of $\overline{x}_1$. This gives an exact sequence

$$0 \longrightarrow k \xrightarrow[1\mapsto \overline{x}_1]{\gamma} R/J' \longrightarrow k \longrightarrow 0,$$

from which we conclude $2[k] = [R/J'] = [k] = 0$. Consequently, $[R/J] = 0$.

Case 2: $\dim_k(J) = m < \infty$. Then $[J]$ is itself a finitely-generated R-module and $[J] = m[k] = 0$ by the result from Case 1. An obvious exact sequence

$$0 \to J \to R \to R/J \to 0$$

implies that $[R/J] = [R]$. Similarly to the previous case, let us consider an R-module M' with a k-basis $\{a, b, c_i\}_{i=1}^{\infty}$ and the action of R given by

$$\overline{x}_n \cdot a = c_n, \ \overline{x}_n \cdot c_i = 0,$$

and

$$\overline{x}_{2n} \cdot b = c_{2n}, \ \overline{x}_{2n-1} \cdot b = 0.$$

This provides us the following exact sequences

$$0 \longrightarrow R \xrightarrow[1 \mapsto a]{\alpha'} M' \longrightarrow k \longrightarrow 0,$$

$$0 \longrightarrow R/\big(\overline{x}_{2n-1} \mid n \in \mathbb{Z}_{>0}\big) \xrightarrow[1 \mapsto b]{\beta'} M' \longrightarrow R/\big(\overline{x}_{2n} \mid n \in \mathbb{Z}_{>0}\big) \longrightarrow 0.$$

It yields $[R] = [M'] = 0$, where the last equality follows from the conclusion of the previous case. This finishes the proof of the claim that $[R/J] = 0$.

Finally, we prove that

$$G_0'(R) \cong \mathbb{Z}$$

by showing that every pseudo-coherent R-module M is isomorphic to R^n for some n. We call a free resolution

$$\ldots \xrightarrow{\alpha_3} P_2 \xrightarrow{\alpha_2} P_1 \xrightarrow{\alpha_1} P_0 \xrightarrow{\alpha_0} M \longrightarrow 0$$

of M *minimal* if every P_i has a free R-basis that is mapped to a minimal set of generators of the image $\alpha_i(P_i) = \ker(\alpha_{i-1})$. Similarly, the existence of a projective resolution is proved, one may show the existence of a minimal resolution. If all the terms P_i in a free resolution of M are finitely generated R-modules then it is minimal if and only if the image of each P_{i+1} is contained in $\mathfrak{m}P_i$. This is so since the set of generators is minimal if and only if there are no relations between them with one of the coefficients being a unit, and the image of P_{i+1} consists of exactly those elements in P_i that give relations between generators of $\ker(\alpha_{i-1})$.

Let us take a minimal free resolution of M. Since M is pseudo-coherent $\mathrm{Tor}_i(M, k)$ are finite dimensional vector spaces, and the dimension of $\mathrm{Tor}_i(M, k)$ equals the rank of P_i in a minimal free resolution of M. Therefore, $\alpha_1(P_1) \subseteq \mathfrak{m}P_0$ and hence $\mathfrak{m}P_1 \subseteq \ker(\alpha_1)$, since $\mathfrak{m}^2 = 0$. On the other hand, $\ker(\alpha_1) = \mathrm{im}\ (\alpha_2) \subseteq \mathfrak{m}P_1$, and, consequently, $\ker(\alpha_1) = \mathfrak{m}P_1$. But unless $P_1 = 0$ an R-module $\mathfrak{m}P_1$ is not finitely generated, which contradicts to the fact that it is an image of a finitely generate module P_2. Hence, $M \cong P_0 = R^n$ for some $n \in \mathbb{N}$, which finishes the proof.

2. Let G be a finite group and let $R = \mathbb{Z}G$ be the group ring of G. Swan showed [[Sw2] Theorem 8.1 and Proposition 9.1] that in this case the reduced projective class group $\tilde{K}_0(\mathbb{Z}G)$ is finite and hence

$$\mathrm{rank}\ K_0(\mathbb{Z}G) = \mathrm{rank}\ (\mathbb{Z} \oplus \tilde{K}_0(\mathbb{Z}G)) = 1.$$

On the other hand, if G is a cyclic group C_n the Lenstra decomposition, which we discuss in much greater detail later, gives

$$G_0(\mathbb{Z}C_n) \cong \bigoplus_{d|n} (\mathbb{Z} \oplus \mathrm{Cl}(\mathbb{Z}[\xi_d, 1/d])),$$

where ξ_d is a primitive dth root of unity and $\mathrm{Cl}(\mathbb{Z}[\xi_d, 1/d])$ denotes the ideal class group of the Dedekind ring $\mathbb{Z}[\xi_d, 1/d]$. Therefore, we immediately conclude that $K_0(\mathbb{Z}C_n) \not\cong G_0(\mathbb{Z}C_n)$ for any $n > 1$. Since for a finite group G the group ring $\mathbb{Z}G$ is noetherian we have that

$$G'_0(\mathbb{Z}G) \cong G_0(\mathbb{Z}G).$$

3. If G is an infinite group it is much harder to obtain any information about $G_0(\mathbb{Z}G)$. Let $F_2 = \langle a, b\rangle$ be the free group on two generators a, b and let $R = \mathbb{Z}F_2$ be the group ring. Lück [Lü] computed that

$$0 = [\mathbb{Z}F_2] \in G_0(\mathbb{Z}F_2)$$

The argument goes as follows. Consider a short exact sequence of $\mathbb{Z}F_2$-modules

$$0 \longrightarrow (\mathbb{Z}F_2)^2 \xrightarrow[\substack{(0,1)\mapsto(a-1)\\(1,0)\mapsto(b-1)}]{} \mathbb{Z}F_2 \xrightarrow[1\mapsto 1]{} \mathbb{Z} \longrightarrow 0$$

coming from the cellular chain complex of the universal cover of $S^1 \vee S^1$, where $\mathbb{Z}$ is a trivial $\mathbb{Z}F_2$-module. It implies that $[\mathbb{Z}F_2] = -[\mathbb{Z}]$ in $G_0(\mathbb{Z}F_2)$. Now it is enough to show that $[\mathbb{Z}] = 0 \in G_0(\mathbb{Z}[\mathbb{Z}])$, since there exists a surjective group homomorphism $F_2 \to \mathbb{Z}$ which induces a restriction map $G_0(\mathbb{Z}[\mathbb{Z}]) \to G_0(\mathbb{Z}F_2)$ that takes the trivial $\mathbb{Z}[\mathbb{Z}]$-module $\mathbb{Z}$ to the trivial $\mathbb{Z}F_2$-module $\mathbb{Z}$. Denote by x a generator of the group $\mathbb{Z}$. Now we may consider a short exact sequence of $\mathbb{Z}[\mathbb{Z}]$-modules

$$0 \longrightarrow \mathbb{Z}[\mathbb{Z}] \xrightarrow[1\mapsto(x-1)]{} \mathbb{Z}[\mathbb{Z}] \xrightarrow[1\mapsto 1]{} \mathbb{Z} \longrightarrow 0,$$

coming from the cellular chain complex of the universal cover of S^1. It yields $[Z] = 0 \in G_0(\mathbb{Z}[\mathbb{Z}])$, which finishes the proof.

It is an open question whether the whole group $G_0(\mathbb{Z}F_2)$ is trivial. Furthermore, there is the following related conjecture (see [Lü], Conjecture 9.67).

Conjecture. *The group G is amenable if and only if* $[\mathbb{C}G] \neq 0 \in G_0(\mathbb{C}G)$.

It would be also interesting to know whether the stronger version of the conjecture holds, namely if a group G is non-amenable then $G_0(\mathbb{C}G) = 0$.

On the other hand, Gersten (see [Ge], Theorem 5.1) showed that

$$K_0(\mathbb{Z}F_2) \cong \mathbb{Z}.$$

Moreover, every finitely presented $\mathbb{Z}F_2$-module has a finite resolution by finitely generated projective $\mathbb{Z}F_2$-modules. Therefore,

$$G'_0(\mathbb{Z}F_2) \cong K_0(\mathbb{Z}F_2) \cong \mathbb{Z}.$$

This example shows that in the situation of a non-noetherian group ring the groups $G_0(\mathbb{Z}G)$ and $G_0'(\mathbb{Z}G)$ become different even though they coincide in the case of a finite G.

4. Combining the first two examples and taking $R = R_1 \times R_2$, where $R_1 = k[x_1, x_2, \dots, x_n, \dots]/\big(x_i x_j \mid i, j \in \mathbb{Z}_{>0}\big)$ and $R_2 = \mathbb{Z}C_n$ with n a non-prime integer, we obtain an example of a ring R for which all three groups $K_0(R), G_0(R)$, and $G_0'(R)$ are pairwise distinct.

5. Even though in general the groups $K_0(R)$ and $G_0(R)$ are different we may allocate a nice class of rings, namely regular rings (for properties and characterization of regular rings see [Se3]), for which they appear to be the same.

Definition 34. *A noetherian ring R is called regular, if R has finite global homological dimension.*

In particular every finitely generated module over a regular ring has a finite resolution by finitely generated projective R-modules. Therefore, for a regular ring R the Cartan map is an isomorphism and

$$K_0(R) \xrightarrow{\cong} G_0(R) \cong G_0'(R)$$

The class of regular rings includes Dedekind domains (in particular fileds). If a ring R is regular, then so is a polynomial ring $R[x]$, and any localization of R. The group rings of non-trivial finite groups are not regular. Another class of rings that will be important for us are hereditary rings.

Definition 35. *A ring R is called left hereditary if every left ideal of R is a projective R-module.*

By the characterization in [Re] Theorem 2.44 for a left hereditary ring R all the submodules of a free module are projective. In particular if additionally R is noetherian every finitely generated R-module has a resolution by finitely generated projective R-modules of length at most 1. Consequently, a noetherian hereditary ring R is regular and we have $K_0(R) \cong G_0(R) \cong G_0'(R)$.

6. If R is a Dedekind domain, then

$$G_0(R) \cong K_0(R) \cong \mathbb{Z} \oplus \tilde{K}_0(R)$$

and it is well known that

$$\tilde{K}_0(R) \cong \mathrm{Cl}(R),$$

where $\mathrm{Cl}(R)$ is the class group of R.

7. The following results answer the natural question how the groups K_0 and G_0 change when passing from a ring R to a polynomial ring $R[t]$ or to a ring of Laurent polynomials $R[t, t^{-1}] \cong R[\mathbb{Z}]$. First notice that the obvious map $f\colon R[t] \xrightarrow{t \mapsto 0} R$ is not flat, but R admits a finite resolution by projective (hence flat) right $R[t]$-modules

$$0 \to R[t] \xrightarrow{\cdot t} R[t] \xrightarrow{t \mapsto 0} R \to 0$$

Therefore, we may define $f_*\colon G_0(R[t]) \to G_0(R)$ via Serre's formula 2.2

$$f_*([M]) = [R \otimes_{R[t]} M] - [\mathrm{Tor}_1^{R[t]}(R, M)].$$

Analogously, the exact sequence of right $R[t, t^{-1}]$-modules

$$0 \to R[t, t^{-1}] \xrightarrow{\cdot(t-1)} R[t, t^{-1}] \xrightarrow{t \mapsto 1} R \to 0$$

yields a map $g_*\colon G_0(R[t, t^{-1}]) \to G_0(R)$ given by Serre's formula 2.2. For the proof of the following theorem see ([R], Chapter 3).

Theorem 36 (Fundamental Theorem for G_0). *Let R be a noetherian ring. Then the maps f_* and g_* are isomorphisms*

$$G_0(R) \cong G_0(R[t]) \cong G_0(R[t, t^{-1}]).$$

If a ring R is regular, then both $R[t]$ and $R[t, t^{-1}]$ are also regular and Theorem 36 gives

$$K_0(R) \cong K_0(R[t]) \cong K_0(R[t, t^{-1}]).$$

For an arbitrary ring R the structure of $K_0(R[t, t^{-1}])$ is more complicated and involves the so called nil-terms (see [R], Theorem 3.3.2).

Theorem 37 (Fundamental Theorem for K_0). *Let R be an arbitrary ring. Then*

$$K_0(R[t, t^{-1}]) \cong K_0(R) \oplus K_{-1}(R) \oplus NK_0(R) \oplus NK_0(R).$$

2.2 K_1 and G_1

2.2.1 Definitions

Before proceeding with the general framework of higher K-groups let us first examine the groups K_1 and G_1, since they are much better understood than the general case.

Definition 38. *Let $\mathcal{C}$ be a small exact category. Define $K_1(\mathcal{C})$ to be an abelian group with generators $[(C, \alpha)]$, where $C \in \mathrm{Obj}(\mathcal{C})$ and $\alpha \in \mathrm{Aut}(C)$, and relations*

- $[(C, \alpha\beta)] = [(C, \alpha)] + [(C, \beta)]$ *for all* $\alpha, \beta \in \mathrm{Aut}(C)$;
- $[(C_1, \alpha_1)] = [(C_0, \alpha_0)] + [(C_2, \alpha_2)]$ *for every commutative diagram in $\mathcal{C}$ with exact rows of the form*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & C_0 & \xrightarrow{i} & C_1 & \xrightarrow{q} & C_2 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha_0} & & \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \\
0 & \longrightarrow & C_0 & \xrightarrow{i} & C_1 & \xrightarrow{q} & C_2 & \longrightarrow & 0.
\end{array}$$

As before we define $K_1(R) := K_1(\mathcal{P}_R)$ and $G_1(R) := K_1(\mathcal{M}_R)$, where $\mathcal{P}_R$ is a category of finitely generated projective R-modules and $\mathcal{M}_R$ is a category of finitely generated R-modules.

The group $K_1(R)$ has another interesting characterization. Let $\mathrm{GL}(R)$ be the infinite general linear group given as a direct limit of inclusions

$$\mathrm{GL}_1(R) \subseteq \mathrm{GL}_2(R) \subseteq \ldots \subseteq \mathrm{GL}_n(R) \subseteq \mathrm{GL}_{n+1}(R) \subseteq \ldots$$

where $A \in \mathrm{GL}_n(R)$ is mapped to $\left(\begin{smallmatrix} A & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_{n+1}(R)$. Let $E_n(R) \subseteq \mathrm{GL}_n(R)$ be a subgroup generated by the elementary matrices $\{E_{ij}(x) \mid x \in R\}$. Let $E(R) = \varinjlim_n E_n(R)$. Then it is not difficult to show that

$$[\mathrm{GL}(R), \mathrm{GL}(R)] = E(R). \tag{2.3}$$

Theorem 39. *There is an isomorphism*

$$K_1(R) \cong \mathrm{GL}(R)/[\mathrm{GL}(R), \mathrm{GL}(R)] = \mathrm{GL}(R)_{ab}.$$

Sketch of the proof. First note, that we may replace the group $K_1(R)$ by the group $K_1^f(R)$, which is defined in the same way but whose generators are (F, α), where F are finitely generated free R-modules and $\alpha \in \mathrm{Aut}(F)$. An isomorphism $\phi\colon K_1(R) \to K_1^f(R)$ is given as follows. If P is a finitely generated projective R-module, then we may find a finitely generated R-module Q such that $P \oplus Q \xrightarrow[g]{\cong} R^n$ for some n. Then we define $\phi([P, \alpha]) = [R^n, g \circ (\alpha \oplus id_Q) \circ g^{-1}]$. It is not difficult to check that the homomorphism $\varphi\colon \mathrm{GL}(R)_{ab} \to K_1^f(R)$ sending $A \in \mathrm{GL}_n(R)$ to $[R^n, r_A]$, where r_A denotes the right multiplication by A, is well-defined and induces an isomorphism of abelian groups. □

For any ring R there is an obvious homomorphism of abelian groups

$$i\colon R^\times_{ab} \to K_1(R),\ x \mapsto [R, r_x],$$

where r_x denotes a right multiplication by an element x. In general the homomorphism i is neither surjective nor injective. In the situation when a ring R is commutative the determinant map induces a surjective homomorphism

$$\det\colon K_1(R) \to R^\times,\ [R^n, f] \mapsto \det(f)$$

which satisfies $\det \circ i = \mathrm{id}_{R^\times}$, and hence in this case i is injective and $R^\times$ appears as a direct summand in $K_1(R)$.

Definition 40. *If R is commutative we define $SK_1(R) := \ker(\det\colon K_1(R) \to R^\times)$.*

Hence for a commutative ring R it holds $K_1(R) \cong SK_1(R) \oplus R^\times$ and $SK_1(R)$ is the "interesting part" of $K_1(R)$. From Theorem 39, equality 2.3, and an observation that every elementary matrix has determinant 1 we immediately conclude that

$$SK_1(R) \cong SL(R)/E(R)$$

and hence $SK_1(R)$ may be viewed as an obstruction for $SL(R)$ to be generated by the elementary matrices. The proof of the first part of the following result can be found in [R, Corollary 2.3.7]. The second part is the famous Bass-Milnor-Serre theorem and for its proof see [BMS] or [Mil].

Theorem 41.

1. *If R is a Dedekind domain such that $R/\mathfrak{p}$ is finite for every non-zero prime ideal $\mathfrak{p}$ in R, then $SK_1(R)$ is a torsion group.*
2. *If $\mathcal{O}_F$ is the ring of algebraic integers of a number field F, then $SK_1(\mathcal{O}_F)$ vanishes.*

Therefore, for the ring of integers $\mathcal{O}_F$ it holds

$$K_1(\mathcal{O}_F) \cong G_1(\mathcal{O}_F) \cong \mathcal{O}_F^\times$$

and consequently $K_1(\mathcal{O}_F)$ is completely determined by the classical Dirichlet's unit theorem.

Theorem 42 (Dirichlet's unit theorem)**.** *Let F be a number field and let $\mathcal{O}_F$ be the ring of algebraic integers in F. Then the abelian group $\mathcal{O}_F^\times$ is finitely generated with torsion subgroup equal to the cyclic subgroup of roots of unity in F and*

$$\text{rank } (\mathcal{O}_F^\times) = r_1 + r_2 - 1,$$

where r_1 is the number of real embeddings of F and r_2 is the number of conjugate pairs of complex embeddings of F.

In the following subsection we present the description of K_1 of a finite dimensional central division algebra due to Wang and Hasse-Schilling-Maass. This result will be needed later in Keating's computation of $G_1(\mathbb{Z}G)$ for a finite group G.

2.2.2 The reduced norm

Let D be a finite dimensional division algebra over its center $Z(D) = F$, let $d = \dim_F(D)$. Let E be a maximal subfield in D and let $n = [E : F]$, then $E \otimes_F D \cong M_n(E)$ and hence, $d = n^2$ (see e.g. [La]). The integer n is called *the Schur index* of D. Schur indices will be treated in more detail in Section 3.5. The inclusion $D \hookrightarrow M_n(E)$ gives rise to a map

$$N_{\text{red}} \colon D^\times \hookrightarrow \mathrm{GL}_n(E) \xrightarrow{\det} E^\times,$$

whose image lies in $F^\times$. This map $N_{\text{red}} \colon D^\times \to F^\times$ is called *a reduced norm* of D and is independent of the choice of E. If A is a finite dimensional simple algebra, then by Artin-Wedderburn theorem A is isomorphic to a matrix algebra $M_k(D)$ for some division algebra D with center F, and then for each $m > 0$ it holds $M_m(A) \cong M_{mk}(D)$. We call the induced map $N_{\text{red}} \colon \mathrm{GL}_m(A) \cong \mathrm{GL}_{mk}(D) \to F^\times$ *the reduced norm* for A. We define $SK_1(A)$ to be the kernel of the induced map

$$N_{\text{red}} \colon K_1(A) \cong K_1(D) \to K_1(F) \cong F^\times.$$

Suppose that F is a number field. Wang proved that in this case $SK_1(D) = 1$. Moreover, the Hasse-Schilling-Maass norm theorem (see e.g. [Re], §33 for more details) gives a description of the image of N_{red} in $F^\times$, and hence determines the whole $K_1(D)$. For every real embedding $\sigma\colon F \to \mathbb{R}$ we have that $\mathbb{R} \otimes_F D$ is a matrix algebra over $\mathbb{R}$ or $\mathbb{H}$. D is called *ramified at* σ if $\mathbb{H}$ occurs.

Theorem 43 (Hasse-Schilling-Maass)**.** *Let F be a number field and let D be a division ring with center F, then*

$$N_{\mathrm{red}}\colon K_1(D) \xrightarrow{\cong} F_+ := \{x \in F \mid \sigma(x) > 0 \textit{ in } \mathbb{R} \textit{ for all ramified } \sigma\}.$$

Let A be a finite dimensional semisimple algebra over a field F. Then we may extend the definition of the reduced norm as follows. Let $A = A_1 \oplus \ldots \oplus A_l$, where A_i are simple algebras, and let F_i denote the center of A_i. Let E be a splitting field for A, i.e., $E \otimes_F A$ is a direct sum of matrix algebras over E. The reduced norm of A is defined as a direct product of reduced norms on A_i

$$N_{\mathrm{red}}\colon K_1(A) \cong \bigoplus_{i=1}^{l} K_1(A_i) \to \bigoplus_{i=1}^{l} F_i^\times.$$

Let A be a finite-dimensional semisimple algebra over a number field F, let R be the ring of integers in F, and let Λ be an R-order in A. The inclusion $\Lambda \hookrightarrow A$ induces a map $K_1(\Lambda) \to K_1(A)$ and composing it with the reduced norm map we obtain *a reduced norm* defined for Λ

$$N_{\mathrm{red}}\colon K_1(\Lambda) \to K_1(A) \to \bigoplus_{i=1}^{l} F_i^\times.$$

We define $SK_1(\Lambda)$ to be the elements of $K_1(\Lambda)$ with the reduced norm 1.

2.2.3 Maximal orders

Since the main focus of this work is the investigation of the decomposition of G-groups of a group ring into direct sum of G-groups of some maximal orders let us introduce orders here and discuss what is known for them. For the exposition in this subsection we will mainly follow [Re] and [AG].

Definition 44. *Given a commutative domain R with field of fractions k and a finite dimensional k-algebra A we call a subset $\Lambda \subseteq A$ an R-order in A if*

(i) Λ is a finitely generated R-submodule in A;

(ii) $k\Lambda = A$;

(iii) Λ is a subring of A.

If additionally Λ is not properly contained in any other R-order of A, then we say that it is a maximal R-order. A subset $\Lambda \subseteq A$ satisfying only the first two conditions $(i), (ii)$ is called a full R-lattice in A.

Examples.

1. Let G be a finite group, then RG is an R-order in kG.
2. The ring of integers $\mathcal{O}_F$ in an algebraic number field F is the unique maximal $\mathbb{Z}$-order in F.
3. Let $A = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ be the quaternion algebra, then $\mathbb{Z}$-submodule Λ generated by $1, i, j, k$ is a $\mathbb{Z}$-order which is contained in the maximal $\mathbb{Z}$-order Γ generated by $i, j, k, (1 + i + j + k)/2$.
4. $M_2(\mathbb{Z})$ is the maximal $\mathbb{Z}$-order in $M_2(\mathbb{Q})$.
5. Let R be a complete discrete valuation ring with field of fractions k and let D be a division k-algebra. Then the integral closure of R in D is the unique maximal R-order in D. In general a maximal order does not have to be unique.

In the next proposition we state without the proof some properties of the maximal orders that will be needed later.

Proposition 45 (Properties of maximal orders)**.**

(i) Let Λ be a maximal R-order in a central simple k-algebra A and let $S \subseteq R$ be a multiplicative subset. Then $\Lambda[S^{-1}]$ is a maximal $R[S^{-1}]$-order in A (see e.g. [AG], Proposition 1.1).

(ii) Assume that R is noetherian and integrally closed, let A be a central simple k-algebra. Then any R-order in A is contained in a maximal order (see e.g. [AG], Proposition 1.1).

(iii) Let R be a Dedekind ring and A be a separable k-algebra. Let Λ be an R-order in A. Then Λ is maximal if and only if for each prime ideal P in R, the localization Λ_P is a maximal R_P-order in A, which is equivalent to $\hat{\Lambda}_P$ being a maximal $\hat{R}_P$-order in $\hat{A}_P$ ([Re], §11).

(iv) Let R is a Dedekind ring and A be a separable k-algebra, then every maximal R-order Λ in A is left and right hereditary (see [Re], Theorem 21.4). Furthermore, Λ is noetherian. Therefore, for such Λ it holds $G_i(\Lambda) = K_i(\Lambda)$ for all $i \geq 0$.

From now on we assume that R is a Dedekind domain with field of fractions k. Let A be a separable finite dimensional algebra over k. Let

$$A \cong \prod_i A_i,$$

where A_i are simple k-algebras. Then every maximal R-order Λ in A is a direct product of maximal R-orders Λ_i in the simple components A_i. Hence the problem of understanding maximal orders in separable algebras reduces to the one for separable simple algebras. The following lemma shows that it suffices to work with simple central algebras.

Lemma 46. *Let A be a separable simple k-algebra. Let k' be the center of A and R' the integral closure of R in k'. If Λ is a maximal R'-order in A, then Λ is at the same time a maximal R-order in A, and vice versa.*

Proof. Λ is a maximal R'-order in A. Since k' is a separable extension of k it follows that R' is a finitely generated module over R. It is clear that Λ is finitely generated as an R-module. Now since $k \otimes_R R' = k'$ we get that $k \otimes_R \Lambda = k \otimes_R (R' \otimes_{R'} \Lambda) = A$ and hence Λ is an R-order in A. The task is now to show that it is a maximal R-order. Suppose on the contrary that there exists an R-order Γ such that $\Lambda \subsetneq \Gamma$. Then it is easy to see that $R' \cdot \Gamma$ is an R'-order in A and $R' \cdot \Lambda = \Lambda \subsetneq \Gamma \subseteq R' \cdot \Gamma$, which contradicts the maximality of Λ.

In the other direction if Λ is a maximal R-order, then since R' is finitely generated over R we immediately conclude that Λ is also a maximal R'-order. This finishes the proof. □

Let A be a separable simple central k-algebra. Then

$$A \cong \mathrm{Hom}_D(V, V)$$

for some uniquely determined division algebra D and V a right D-vector space. Let Γ be a maximal R-order in D. Then using the above notation Theorem 21.6 in [Re] implies the following.

Proposition 47. *Every maximal R-order Λ in A is Morita equivalent to Γ.*

This allows us to talk about G-groups of a maximal R-order in A without specifying the order, since they are all Morita equivalent.

Let us now switch to the situation when R is the ring of integers in a number field F. Let A be a separable F-algebra. The following theorem due to Lam ([La3], Theorem 3.3) which is the analogue of the similar result of Bass-Milnor-Serre for K_1 of ring of integers allows to estimate the rank of G_1 for an arbitrary R-order in A.

Theorem 48 (Lam)**.** *Let Λ be an R-order in A. Then*

(i) $G_1(\Lambda) \to G_1(A)$ has finite kernel.

(ii) If $\Lambda' \subseteq \Lambda$ is another R-order in A, then $G_1(\Lambda') \to G_1(\Lambda)$ has finite kernel and cokernel.

(iii) $K_1(\Lambda) \to G_1(\Lambda)$ has finite kernel and cokernel.

In the next section we will outline main tools used for the computation of K- and G-groups.

2.3 Higher K-groups and classical tools to compute them

2.3.1 Q-construction

So far we only talked about K_0 and K_1 groups and did not mention higher K-groups. In this section we define higher K-groups of an exact category using the classical Quillen's Q-construction (see the original Quillen's paper [Q]). The idea is to define higher K-groups as homotopy groups of a classifying space of a category. To obtain the desired properties the trick is to modify the initial category $\mathcal{C}$ and consider the category $Q\mathcal{C}$ instead.

Definition 49. *Let $\mathcal{C}$ be a category with exact sequences.*

- *A morphism $A \to B$ in $\mathcal{C}$ is called an admissible monomorphism if it can be completed to the right to a short exact sequence in $\mathcal{C}$*

$$0 \to A \to B \to X \to 0.$$

An admissible monomorphism is denoted by $A \rightarrowtail B$.

- *A morphism $A \to B$ in $\mathcal{C}$ is called an admissible epimorphism if it can be completed to the left to a short exact sequence in $\mathcal{C}$*

$$0 \to X \to A \to B \to 0.$$

An admissible epimorphism is denoted by $A \twoheadrightarrow B$.

Given an exact category $\mathcal{C}$ let $Q\mathcal{C}$ be the category with the same objects as $\mathcal{C}$ and morphisms $\mathrm{Hom}_{Q\mathcal{C}}(A, B)$ given by the set of equivalence classes of diagrams

$$A \twoheadleftarrow X \rightarrowtail B.$$

The diagrams $A \twoheadleftarrow X \rightarrowtail B$ and $A \twoheadleftarrow X' \rightarrowtail B$ are said to be equivalent iff they fit in a commutative diagram

$$\begin{array}{ccccc} A & \twoheadleftarrow & X & \rightarrowtail & B \\ \| & & \downarrow{\cong} & & \| \\ A & \twoheadleftarrow & X' & \rightarrowtail & B. \end{array}$$

The composition of morphisms $A \twoheadleftarrow X \rightarrowtail B$ and $B \twoheadleftarrow X' \rightarrowtail C$ is defined via

$$A \twoheadleftarrow X \times_B X' \rightarrowtail C,$$

where $X \times_B X'$ denotes a pullback. If the resulting category $Q\mathcal{C}$ is not a small category we may replace it by an equivalent small subcategory. Recall that for a small category the classifying space is a geometric realization of the nerve of this category. Hence after passing to a small subcategory of $Q\mathcal{C}$ we obtain a well-defined (up to a homotopy equivalence) classifying space, which we denote by $BQ\mathcal{C}$. Note that there is a natural choice of a basepoint for $BQ\mathcal{C}$ given by the 0-object. Moreover, since for every object A in $Q\mathcal{C}$ there is a morphism $0 \twoheadleftarrow 0 \rightarrowtail A$ the space $BQ\mathcal{C}$ is path-connected.

Let $\mathcal{C}$ be a skeletally small exact category then Quillen [Q] showed that there is a natural isomorphism

$$\pi_1(BQ\mathcal{C}, 0) \cong K_0(\mathcal{C}),$$

$$\pi_2(BQ\mathcal{C}, 0) \cong K_1(\mathcal{C}).$$

This motivates the following definition of the higher K-groups.

Definition 50. *Let $\mathcal{C}$ be an exact skeletally small category, then the K-groups are defined to be the homotopy groups*

$$K_n(\mathcal{C}) := \pi_{n+1}(BQ\mathcal{C}),\ n \geq 0.$$

In his fundamental work Quillen along with the Q-construction gave another less technical one suited to define the higher algebraic K-groups of a ring, which he called a 'plus-construction'. There Quillen defined K-groups as homotopy groups of a modified version of a space $B\mathrm{GL}(R)$, which he called $B\mathrm{GL}(R)^+$. Even though the two constructions look very different they produce the same K-groups, which is quite complicated result(for the proof see e.g. [Sr], Chapter 7). Depending on the instances it might be more beneficial to use one or the other construction.

Later some alternative constructions of the higher K-groups were found. Waldhausen gave the so-called called $S_\bullet$-construction for Waldhausen's categories [Wa]. For exact categories there is an alternative construction by Gillet and Grayson [GG]. All of these constructions agree and give the same K-groups, but each of them has some advantages in certain situations. For the extensive treatment of this subject see e.g. [Wei], Chapter IV.

2.3.2 Fundamental theorems in K-theory

We list without proof fundamental theorems that are the basic tools for computing K-groups. We mainly follow [R] and [Wei]. Other useful sources for this subject include [Ber], [Mil], [Q], [Sr].

Morita invariance. Two rings R, S are called *Morita equivalent* if the categories of left R-modules and left S-modules are equivalent. Here we consider the category of all modules, not only finitely generated. If $F\colon \mathrm{Mod}(R) \to \mathrm{Mod}(S)$ is a Morita equivalence, then one may show that it preserves projectivity and takes finitely generated R-modules to finitely generated S-modules. Hence there is an induced equivalence between categories $\mathcal{P}_R$ and $\mathcal{P}_S$, as well as between $\mathrm{Mod}_{fg}(R)$ and $\mathrm{Mod}_{fg}(S)$. Any ring R is Morita equivalent to the matrix ring $M_n(R)$ for any $n \in \mathbb{N}$ (see [Re], Chapter 4). From this it is straightforward to deduce the Morita invariance for K- and G-groups (for detailed treatment see e.g. [La2]).

Theorem 51 (Morita invariance)**.** *Let R be a ring and let $n \in \mathbb{N}$. Then for any $j \geq 0$ there are natural isomorphisms*

$$K_j(M_n(R)) \cong K_j(R),$$

$$G_j(M_n(R)) \cong G_j(R).$$

Compatibility with products and colimits. For the proof see e.g. [Q], p.103 (8) and p.20 (12).

Theorem 52. *1. If $\mathcal{A}$ and $\mathcal{B}$ are exact categories then*

$$K_i(\mathcal{A} \times \mathcal{B}) \cong K_i(\mathcal{A}) \oplus K_i(\mathcal{B}).$$

2. Let $\{R_i, i \in I\}$ be a directed system of rings. Then the canonical map

$$\operatorname{colim}_{i\in I} K_j(R_i) \xrightarrow{\cong} K_j(\operatorname{colim}_{i\in I} R_i)$$

is an isomorphism for all $j \geq 0$.

Resolution. The following theorem allows to replace the initial category by a subcategory in the computation of K-groups, if every object of the category admits a finite resolution by objects from the subcategory.

Theorem 53 (Resolution)**.** *Let $\mathcal{B}$ be a full exact subcategory of an exact category $\mathcal{A}$. Assume $\mathcal{B}$ is closed under extensions and under kernels of admissible surjections in $\mathcal{A}$. Suppose every object $A \in \mathcal{A}$ has a finite resolution by objects from $\mathcal{B}$*

$$0 \to B_n \to \ldots \to B_1 \to B_0 \to A \to 0.$$

Then $K_j(\mathcal{A}) \cong K_j(\mathcal{B})$.

Localization. An abelian subcategory $\mathcal{B}$ of an abelian category $\mathcal{A}$ is called *Serre subcategory* if $\mathcal{B}$ is closed under subobjects, quotients, and extensions. We define a quotient category $\mathcal{A}/\mathcal{B}$ by the following "calculus of left fractions". A morphism f in $\mathcal{A}$ is called $\mathcal{B}$-iso if $\ker(f)$ and $\operatorname{coker}(f)$ are in $\mathcal{B}$. Objects of $\mathcal{A}/\mathcal{B}$ are the same as objects of $\mathcal{A}$. The morphisms between A_1, A_2 are given by the equivalence classes of diagrams in $\mathcal{A}$:

$$A_1 \xleftarrow{s'} A' \xrightarrow{f'} A_2, \ \ s' \text{ is a } \mathcal{B}\text{-iso}.$$

Two such diagrams $A_1 \xleftarrow{s'} A' \xrightarrow{f'} A_2$ and $A_1 \xleftarrow{s''} A'' \xrightarrow{f''} A_2$ are equivalent if there is a chain $A_1 \leftarrow A \to A_2$ that fit into a commutative diagram

$$\begin{array}{ccccc} & & A' & & \\ & {\scriptstyle s'}\swarrow & \uparrow{\scriptstyle \cong_{\mathcal{B}}} & \searrow{\scriptstyle f'} & \\ A_1 & \longleftarrow & A & \longrightarrow & A_2 \\ & {\scriptstyle s''}\nwarrow & \downarrow{\scriptstyle \cong_{\mathcal{B}}} & \nearrow{\scriptstyle f''} & \\ & & A'' & & \end{array}$$

where $A \to A'$ and $A \to A''$ are $\mathcal{B}$-isos. The composition of morphisms $A_1 \xleftarrow{s} A' \xrightarrow{f} A_2$ and $A_2 \xleftarrow{\beta} A''' \xrightarrow{g} A_3$ is defined as $A_1 \xleftarrow{s} A' \leftarrow A \to A''' \xrightarrow{g} A_3$, where A is a pullback of $A' \xrightarrow{f} A_2 \xleftarrow{\beta} A'''$. One might think of morphisms in $\mathcal{A}/\mathcal{B}$ as of left fractions $s^{-1}f$, where the set of denominators s coincide with $\mathcal{B}$-isos. The resulting category $\mathcal{A}/\mathcal{B}$ is abelian and the quotient functor $\operatorname{loc}\colon \mathcal{A} \to \mathcal{A}/\mathcal{B}$ is exact (see e.g. [Sw] or [Wei], p. 189)

Theorem 54 (Localization, [Q])**.** *If $\mathcal{B} \subseteq \mathcal{A}$ is a Serre subcategory of an abelian category, then there is a long exact sequence*

$$\ldots \to K_i(\mathcal{B}) \to K_i(\mathcal{A}) \xrightarrow{\operatorname{loc}} K_i(\mathcal{A}/\mathcal{B}) \to K_{i-1}(\mathcal{B}) \to \ldots \ .$$

The following application will be of a great importance for us in the computation of G-theory of group rings. Let R be a ring and let S be a central multiplicative set in R. Let $\mathcal{M}_S(R)$ be the category of all finitely generated S-torsion R-modules. Recall that a module M is called S-torsion if for every element $m \in M$ there exists $s \in S$ such that $sm = 0$. Clearly, $\mathcal{M}_S(R)$ is a Serre subcategory of $\mathcal{M}(R)$. The quotient category $\mathcal{M}(R)/\mathcal{M}_S(R)$ is naturally equivalent to $\mathcal{M}(S^{-1}R)$ and the localization sequence in this case looks as follows

$$\ldots \to K_i(\mathcal{M}_S(R)) \to G_i(R) \xrightarrow{\text{loc}} G_i(S^{-1}R) \to K_{i-1}(\mathcal{M}_S(R)) \to \ldots .$$

Devissage. This tool will allow us to reduce the computation of K-theory to a smaller category in the situation when it is possible to break up objects from the initial category into pieces from the smaller category.

Theorem 55 (Devissage)**.** *Let $\mathcal{A}$ be an abelian category, and let $\mathcal{B}$ be an exact abelian subcategory of $\mathcal{A}$ that is closed under subobjects and quotients. Assume that every object $A \in \mathcal{A}$ has a finite filtration*

$$0 = A_n \subseteq \ldots \subseteq A_1 \subseteq A_0 = A,$$

where $A_i \in \mathrm{Obj}(\mathcal{A})$ and each quotient A_{i-1}/A_i lies in $\mathcal{B}$. Then $K_j(\mathcal{A}) \cong K_j(\mathcal{B})$.

The following two applications of the Devissage Theorem will be used later.
Application 1. Let R be an Artinian ring, and let $\mathrm{Mod}^{ss}(R)$ be the subcategory of $\mathrm{Mod}_{fg}(R)$ consisting of semisimple R-modules. Since every finitely generated R-module has a finite composition series, the Devissage implies

$$K_j(\mathrm{Mod}_{fg}(R)) \cong K_j(\mathrm{Mod}^{ss}(R)).$$

Schur's lemma gives that $\mathrm{Mod}^{ss}(R)$ is equivalent to $\prod_i \mathrm{Mod}_{fg}(D_i)$, where the product runs over the set of non-isomorphic simple R-modules V_i and $D_i = \mathrm{End}_R(V_i)$. Therefore we conclude that

$$G_j(R) \cong \oplus_i K_j(D_i).$$

Application 2. Let R be a noetherian ring. Fix $x \in Z(R)$ and denote by $\mathrm{Mod}_{\langle x \rangle}(R)$ the abelian category of all modules M in $\mathrm{Mod}_{fg}(R)$ annihilated by some power of x, i.e., $x^n M = 0$ for some n. Clearly, all the quotients of the following filtration

$$0 = x^n M \subseteq \ldots \subseteq xM \subseteq M$$

lie in R/xR. Therefore, by the Devissage

$$K_j(\mathrm{Mod}_{\langle x \rangle}(R)) = G_j(R/xR).$$

2.4 Keating's computation of $G_1(\mathbb{Z}G)$

Let G be a finite group of order n. Let R be the ring of integers of an algebraic number field, e.g. $R = \mathbb{Z}$. In this subsection we overview the result of Keating [Ke], in which he completely determined the abelian group $G_1(RG)$.

For any ring T of characteristic 0 we put $T' = T[n^{-1}]$. Let $\mathcal{A} = \mathrm{Mod}_{fg}(R)$ and let $\mathcal{B} = \mathrm{Mod}_{\langle n\rangle}(R)$. The corresponding localization sequence

$$\ldots \to G_1(RG) \xrightarrow{\text{loc}} G_1(R'G) \xrightarrow{\delta} K_0(\mathrm{Mod}_{\langle n\rangle}(RG)) \to G_0(RG) \xrightarrow{\text{loc}} G_0(R'G)$$

after applying the Devissage becomes

$$\ldots \to G_1(RG) \xrightarrow{\text{loc}} G_1(R'G) \xrightarrow{\delta} \bigoplus_{i\in\mathcal{E}} K_0(\mathrm{End}_{RG}(V_i)) \to G_0(RG) \xrightarrow{\text{loc}} G_0(R'G),$$

where $\mathcal{E}$ is the set of isomorphism classes of simple RG-modules V_i with $nV_i = 0$.

Let k be the field of fractions of R. One of the main results in [Ke, Theorem 1] is that the base change homomorphism

$$G_1(RG) \to G_1(kG) = K_1(kG),\ [M] \mapsto [k \otimes_R M]$$

is injective. This immediately implies that $\mathrm{loc}\colon G_1(RG) \to G_1(R'G)$ is injective. Since given V_i a simple RG-module $\mathrm{End}(V_i)$ is a division ring, it is clear that $\bigoplus_{i\in\mathcal{E}} K_0(\mathrm{End}(V_i))$ is a free abelian group of rank $\varepsilon = |\mathcal{E}|$. From this we obtain

$$\mathrm{tors}\ G_1(RG) = \mathrm{tors}\ G_1(R'G).$$

Moreover, since the order of the group G is invertible in R' the group ring $R'G$ is semisimple and hence every finitely generated $R'G$-module is projective. Therefore,

$$G_1(R'G) = K_1(R'G).$$

It was proved by Swan that $\ker(\mathrm{loc}\colon G_0(RG) \to G_0(R'G))$ is a finite group, which means that the image of $G_1(R'G)$ under δ has rank ε. Consequently

$$\mathrm{rank}\ G_1(RG) = \mathrm{rank}\ K_1(R'G) - \varepsilon$$

and

$$\mathrm{tors}\ G_1(RG) = \mathrm{tors}\ K_1(R'G).$$

To get an explicit description of rank and torsion of $K_1(R'G)$ we need the following notation. Let

$$kG \cong \sum_{i=1}^{m} M_{n_i}(D_i)$$

be the Wedderburn's decomposition of an algebra kG into simple components. Denote by F_i the center of D_i. Let $\mathcal{O}_i$ be a maximal R-order in $Z(M_{n_i}(D_i))$. Hence $\mathcal{O} = \oplus_{i=1}^{m}\mathcal{O}_i$ is a maximal R-order in $Z(kG)$ and $\mathcal{O}'$ is a maximal R'-order in $Z(kG)$ by the properties of maximal orders stated in the Subsection 2.2.3. The order $R'G$ is the maximal R'-order in kG. In [Ke2, Theorem 2] Keating showed that $SK_1(R'G) = 0$, i.e., the reduced norm

$$N_{\mathrm{red}}\colon K_1(R'G) \hookrightarrow K_1(kG) \cong \bigoplus_{i=1}^{m} K_1(D_i) \xrightarrow{\cong} \bigoplus_{i=1}^{m} (F_i^{\times})_+$$

is injective. Therefore, it is enough to determine the image of the base change map $K_1(R'G) \to K_1(kG)$. This can be done by the following result of Wilson ([Wi], Lemma 3) which we present in our notation.

Lemma 56 (Wilson)**.** *If Λ is a maximal R'-order in kG then the image of $K_1(\Lambda)$ in $K_1(kG)$ consists of those elements in $K_1(kG)$ whose reduced norms are in $\mathcal{O}'$.*

From this it immediately follows that

$$K_1(R'G) \cong \mathcal{O}' \cap \bigoplus_{i=1}^{m} (F_i^{\times})_+ = \bigoplus_{i=1}^{m} U_+(\mathcal{O}'_i),$$

where $U_+(\mathcal{O}'_i)$ is the group of units of $\mathcal{O}'_i$ that are positive at every real place where D_i ramifies. Put $r_i = \operatorname{rank} U(\mathcal{O}_i)$ and let v_i be the number of distinct prime ideals in $\mathcal{O}_i$ that divide n. The following theorem of Keating summarizes everything written above about $G_1(RG)$.

Theorem 57. *Let G be a finite group of order n and let R be the ring of integers of a number field k. Then using the above notation we have*

$$\operatorname{rank} G_1(RG) = r_1 + \ldots + r_m + v_1 + \ldots + v_m - \varepsilon,$$

$$\operatorname{tors} G_1(RG) = \bigoplus_{i=1}^{m} \operatorname{tors} U_+(\mathcal{O}'_i) = \bigoplus_{i=1}^{m} \operatorname{tors} U_+(\mathcal{O}_i).$$

Chapter 3

The decomposition conjecture for G-theory of group rings

In [HTW] I. Hambleton, L. Taylor and B. Williams conjectured a general formula in the spirit of H. Lenstra for the decomposition of $G_n(RG)$ for any finite group G and noetherian ring R. The conjectured decomposition was shown to hold for some large classes of finite groups. D. Webb and D. Yao discovered that the conjecture failed for the symmetric group S_5, but remarked that it still might be reasonable to expect the HTW-decomposition for solvable groups. In this Chapter we revisit the conjecture. We present the current state of the conjecture and provide the new results, which are the main achievement of this work. On the side of negative results we show that the solvable group $\mathrm{SL}(2, \mathbb{F}_3)$ is a counterexample to the conjectured HTW-decomposition in degree 1. The contradiction to the conjecture will be obtained by examining the ranks of G_1. Nevertheless, we prove that for any finite group G the rank of $G_1(\mathbb{Z}G)$ does not exceed the rank of the expression in the HTW-decomposition. We also show that the torsion part of $G_1(\mathbb{Z}G)$ is predicted correctly by the HTW-decomposition for all finite groups G. We compare the ranks predicted by the conjecture in degrees $n = 0$ and $n \geq 2$ and see that the prediction given by the HTW-decomposition is correct. This provides evidence that the weaker version of the Hambleton-Taylor-Williams Conjecture might still hold true for all finite groups.

3.1 Hambleton-Taylor-Williams Conjecture

3.1.1 The statement and the state of the Conjecture

In [Le] Lenstra obtained a beautiful explicit formula for the decomposition of the Grothendieck group $G_0(RG)$ of the group ring RG for an abelian group G and noetherian ring R. Namely, if $C(G)$ denotes the set of all cyclic quotients of G (isomorphic quotients coming from different subgroups of G are considered to be different), then

$$G_0(RG) \cong \bigoplus_{C \in C(G)} G_0\Big(R \otimes_{\mathbb{Z}} \mathbb{Z}[\xi_{|C|}, \frac{1}{|C|}]\Big),$$

where $|C|$ is the order of a cyclic group C, and $\xi_{|C|}$ is a primitive $|C|$-th root of unity. In [We2], [We3] Webb proved the same decomposition formula for $G_n(RG)$, $n > 0$

for all abelian groups G, and obtained decomposition formulas for $G_n(\mathbb{Z}G)$ for certain nonabelian groups G, in particular for dihedral and generalized quaternion 2-groups. In [HTW] Hambleton, Taylor and Williams conjectured the general formula in the spirit of Lenstra for the decomposition of $G_n(RG)$ for any finite group G and noetherian ring R. Their conjecture is consistent with all previous results of Lenstra and Webb. Moreover it was shown to hold for finite nilpotent groups [HTW], [We5] and groups of square-free order [We4]. The conjecture was also proved for $G_0(\mathbb{Z}G)$, where G is a group of odd order having cyclic Sylow subgroups [LaWe].

In order to state the conjecture let G be a finite group, and let $\rho\colon G \to \mathrm{Aut}(V_\rho)$ be a rational irreducible representation of G. Then there is an associated division algebra $D_\rho = \mathrm{End}_{\mathbb{Q}G}(V_\rho)$ and we have the following Wedderburn decomposition of the rational group algebra [Se, p. 92]

$$\mathbb{Q}G \cong \prod_{\rho \in X(G)} M_{n_\rho}(D_\rho^{op}), \tag{3.1}$$

where ρ ranges over the set $X(G)$ of isomorphism classes of rational irreducible representations of G.

For such a representation $\rho\colon G \to \mathrm{Aut}(V_\rho)$, let k_ρ be the order of the kernel of the representation ρ and let d_ρ be the dimension of any of the irreducible complex constituents of $\mathbb{C} \otimes_{\mathbb{Q}} V_\rho$. Let $\omega_\rho = \frac{|G|}{k_\rho d_\rho}$. We remark that ω_ρ is an integer. Indeed, the kernel of the irreducible rational representation ρ coincides with the kernel of any of the irreducible complex constituents of $\mathbb{C} \otimes_{\mathbb{Q}} V_\rho$. Hence such a constituent is a complex irreducible representation of the quotient group $G/\ker\rho$. Therefore, integrality of ω_ρ follows from the fact that the dimension of a complex irreducible representation of a group divides the order of that group [Se, p. 52].

Let Λ_ρ be a maximal $\mathbb{Z}[1/\omega_\rho]$-order in D_ρ. Hambleton, Taylor and Williams conjectured the following decomposition formula, which we call the HTW-decomposition.

Conjecture (Hambleton-Taylor-Williams)**.** *Let G be a finite group and R a noetherian ring. Then*

$$G_n(RG) \cong \bigoplus_{\rho \in X(G)} G_n(R \otimes \Lambda_\rho), \quad \forall n \geq 0. \tag{3.2}$$

It turned out that in general this conjecture does not hold. Webb and Yao [WeY] showed that the formula failed for the symmetric group S_5, but remarked that it still might be reasonable to expect that the HTW-decomposition holds for solvable groups. In Section 3.4 we provide a solvable counterexample.

3.1.2 The map in the Conjecture

Let G be a finite group. Assume for a moment that $R = \mathbb{Z}$. Let Γ be a maximal $\mathbb{Z}$-order in $\mathbb{Q}G$ containing $\mathbb{Z}G$. Then

$$\Gamma \cong \prod_{\rho \in X(G)} \Gamma_\rho,$$

where Γ_ρ is a maximal $\mathbb{Z}$-order in the simple component $M_{n_\rho}(D_\rho^{op})$ corresponding to $\rho \in X(G)$ in the Wedderburn decomposition (3.1). Then by Proposition 47 $\Gamma_\rho[1/\omega_\rho]$ is Morita equivalent to Λ_ρ and

$$G_n(\Lambda_\rho) \cong G_n(\Gamma_\rho[1/\omega_\rho]).$$

Since G-theory is lacking functoriality, it is not obvious that there is a map between $G_n(\mathbb{Z}G)$ and $\bigoplus_{\rho\in X(G)} G_n(\Gamma_\rho[1/\omega_\rho])$. In the original paper [HTW] the HTW-conjecture was stated in terms of the existence of an abstract isomorphism, and so far no general construction of a candidate map is known. A straightforward approach to obtain a map $G_n(\mathbb{Z}G) \to \oplus_{\rho\in X(G)} G_n(\Gamma_\rho[1/\omega_\rho])$ by the extension of scalars does not work since in general $\Gamma_\rho[1/\omega_\rho]$ is not a flat $\mathbb{Z}G$-module. For instance, the summand corresponding to the trivial representation is $G_n(\mathbb{Z})$, since in this case the number ω_ρ equals 1. If $\mathbb{Z}$ was a flat $\mathbb{Z}G$-module, then it would also be projective as a $\mathbb{Z}G$-module due to result of Benson and Goodearl [BG, Theorem 3.4]. But this would imply that the cohomology groups $H^j(G, \mathbb{Z})$ are all trivial for $j > 0$, which is the case only if G is a trivial group. Therefore, if G is a non-trivial group, then $\mathbb{Z}$ viewed as a $\mathbb{Z}G$-module with a trivial G-action is never flat.

In the approach of Webb [We2] in those cases for which the conjecture was established the desired isomorphism was constructed in the following way. Let $\mathcal{U} = \bigoplus_{\rho\in X(G)} \Gamma_\rho[1/\omega_\rho]$. Then we have $\mathbb{Z}G \subseteq \Gamma \subseteq \mathcal{U} \subseteq \mathbb{Q}G$. Since the order Γ is finitely generated over $\mathbb{Z}G$ the restriction of scalars $\mathrm{Mod}_{fg}(\Gamma) \to \mathrm{Mod}_{fg}(\mathbb{Z}G)$ induces a map on G-groups

$$\mathrm{res}_n\colon G_n(\Gamma) \to G_n(\mathbb{Z}G).$$

On the other hand we may consider the localization map $\mathrm{Mod}_{fg}(\oplus_{\rho\in X(G)}\Gamma_\rho) \to \mathrm{Mod}_{fg}(\oplus_{\rho\in X(G)}\Gamma_\rho[1/\omega_\rho])$. It induces an extension of scalars homomorphism on G-groups

$$\mathrm{ext}_n\colon G_n(\Gamma) \to G_n(\mathcal{U}).$$

Then the idea is to find a topological analogue of the strategy of Lenstra, who considered a functor on the category of finitely generated Γ-module that carries the relations R_1 in the Heller-Reiner presentation $G_0^t(\Gamma)/R_1$ of $G_0(\mathbb{Z}G)$ isomorphically into the relations R_2 in the presentation $G_0^t(\Gamma)/R_2$ of $G_0(\mathcal{U})$ coming from the localization sequence, hence inducing the isomorphism of the quotient groups $G_0^t(\Gamma)/R_1 \xrightarrow{\cong} G_0^t(\Gamma)/R_2$. Following this strategy for some classes of groups it is possible to define the so-called Lenstra functor

$$L\colon \mathrm{Mod}^{\mathrm{tor}}(\Gamma) \to \mathrm{Mod}^{\mathrm{tor}}(\Gamma),$$

which carries the homotopy fiber of $\mathrm{res}\colon \mathrm{Mod}^{\mathrm{tor}}(\Gamma) \to \mathrm{Mod}^{\mathrm{tor}}(\mathbb{Z}G)$ to the homotopy fiber of $\mathrm{ext}\colon \mathrm{Mod}^{\mathrm{tor}}(\Gamma) \to \mathrm{Mod}^{\mathrm{tor}}(\mathcal{U})$ and hence induces a homotopy equivalence $\lambda\colon BQ\mathrm{Mod}^{\mathrm{tor}}(\mathbb{Z}G) \to BQ\mathrm{Mod}^{\mathrm{tor}}(\mathcal{U})$. "Reducing" the map given by L on the homotopy fiber sequence

$$\Omega BQ\mathrm{Mod}(\Gamma) \to \Omega BQ\mathrm{Mod}(\mathbb{Q}G) \to \Omega BQ\mathrm{Mod}^{\mathrm{tor}}(\Gamma)$$

Webb constructed a map between the following homotopy fiber sequences

$$\begin{array}{ccccc} \Omega BQ\mathrm{Mod}(\mathbb{Z}G) & \longrightarrow & \Omega BQ\mathrm{Mod}(\mathbb{Q}G) & \longrightarrow & \Omega BQ\mathrm{Mod}^{\mathrm{tor}}(\mathbb{Z}G) \\ \Big\downarrow W & & \Big\downarrow \Omega L & & \Big\downarrow \lambda \\ \Omega BQ\mathrm{Mod}(\mathcal{U}) & \longrightarrow & \Omega BQ\mathrm{Mod}(\mathbb{Q}G) & \longrightarrow & \Omega BQ\mathrm{Mod}^{\mathrm{tor}}(\mathcal{U}), \end{array}$$

such that $W\colon \Omega BQ\mathrm{Mod}(\mathbb{Z}G) \to \Omega BQ\mathrm{Mod}(\mathcal{U})$ is a weak equivalence. Therefore, the constructed map W induces the conjectured isomorphism of G-groups $W_*\colon G_*(\mathbb{Z}G) \xrightarrow{\cong} G_*(\mathcal{U})$.

3.1.3 A motivation

The initial interest in computing/decomposing the Grothendieck group $G_0(\mathbb{Z}G)$ for finite abelian groups G arose from the question of determining the so called SSF-group which hosts an obstruction for a diffeomorphism to be Morse-Smale. In this subsection we follow the survey of Bass [Ba], the paper by Grayson [Gr], and the work of Franks and Shub [FS].

Let M be a smooth compact manifold and $f\colon M \to M$ be a diffeomorphism. A point $x \in M$ is called *wandering* if there is a neighbourhood U of x such that $U \cap f^n(U) = \emptyset$ for all $n \neq 0$. Let $\mathcal{D}$ be the set of all self-diffeomorphisms of M equipped with the C^1 topology. Then f is called *structurally stable* if for each g from some sufficiently small neighborhood of f in $\mathcal{D}$ it holds that g is topologically conjugated to f, i.e., there exists a homeomorphism $h\colon M \to M$ such that $f \circ h = h \circ g$.

Definition 58. *A diffeomorphism $f\colon M \to M$ is called Morse-Smale if there is a finite number of non-wandering points and f is structurally stable.*

An example of a Morse-Smale diffeomorphism can be obtained from the gradient flow of the height function on the sphere. Morse-Smale diffeomorphisms provide particularly simple dynamical systems. Namely, for such a dynamical system (M, f) all chain recursions are just periodic orbits, there are only finitely many periodic points all of which are hyperbolic, and the invariant manifolds of periodic orbits meet transversely. These systems have been extensively studied. For all the details we refer the reader to [FS].

It is a natural question to ask if a given homotopy class contains a Morse-Smale diffeomorphism. The group SSF in which the obstruction lies is constructed as follows. Let $\mathcal{A}$ be the category of pairs (H, u), where H is a finitely generated abelian group and $u \in \mathrm{Aut}(H)$ such that there exists $n \in \mathbb{Z}_{>0}$ with $u^n - \mathrm{id}_H$ nilpotent. The morphisms in $\mathcal{A}$ from (H, u) to (H', u') are group homomorphisms $f\colon H \to H'$ satisfying $f \circ u = u' \circ f$. An object (H, u) is called a *permutation module* if H admits a $\mathbb{Z}$-basis permuted by u. Let P be a subgroup of $K_0(\mathcal{A})$ generated by the classes of permutation modules. Then we define the group SSF to be the quotient

$$\mathrm{SSF} = K_0(\mathcal{A})/P.$$

Assume additionally that $\dim M > 5$ and $\pi_1(M) = 0$. Let $f\colon M \to M$ be a diffeomorphism such that the eigenvalues of f_* on $H_*(M, \mathbb{Q})$ are roots of unity. Franks and Shub showed that the Lefschetz invariant

$$L(f) = \sum_{i\geq 0}(-1)^i[H_i(M, \mathbb{Z}), f_i] \in \mathsf{SSF}$$

vanishes if and only if f is isotopic to a Morse-Smale diffeomorphism (see [FS]).

Later Bass studied the group SSF and gave a presentation of it in terms of ideal class groups of cyclotomic fields, which was then improved by Lenstra [Le]. Denote by $\mathcal{A}_n$ the full subcategory of $\mathcal{A}$ that contains the objects (H, u) with $u^n = \mathrm{id}_H$, and let P_n be the subgroup of $K_0(\mathcal{A}_n)$ generated by the classes of permutation modules in $\mathcal{A}_n$. Then

$$\mathsf{SSF} \cong \varinjlim_n K_0(\mathcal{A}_n)/P_n,$$

where the limit is taken over the positive integers ordered by divisibility. For $(H, u) \in \mathcal{A}_n$ we may view H as a $\mathbb{Z}C_n$-module, where C_n is a cyclic group of order n with the generator of C_n acting by $u \in \mathrm{Aut}(H)$. It is clear that

$$K_0(\mathcal{A}_n) \cong G_0(\mathbb{Z}C_n).$$

From the isomorphism constructed in [Le]

$$\varphi\colon G_0(\mathbb{Z}C_n) \xrightarrow{\cong} \bigoplus_{d|n} G_0(\mathbb{Z}[\xi_d, 1/d]) \cong \bigoplus_{d|n}(\mathbb{Z} \oplus \mathrm{Cl}(\mathbb{Z}[\xi_d, 1/d])) \qquad (3.3)$$

Lenstra determined the image $\varphi(P_n)$, which turned out to be the free part $\mathbb{Z}^{\tau(n)}$ of the right hand side of (3.3), where $\tau(n)$ denotes the number of positive divisors of n. Hence

$$\mathsf{SSF} \cong \varinjlim_{d|n} \mathrm{Cl}(\mathbb{Z}[\xi_d, 1/d]) \cong \bigoplus_{d\geq 1} \mathrm{Cl}(\mathbb{Z}[\xi_d, 1/d]).$$

After the success of Lenstra's approach in understanding $G_0(\mathbb{Z}G)$ for finite abelian groups it was a natural question to ask how $G_n(\mathbb{Z}G)$ decomposes for an arbitrary finite group and $n \geq 0$.

3.2 The comparison of ranks of G_0-groups

We start by finding some evidence for the HTW-decomposition (3.2) that holds for all groups. In this section we compare the ranks of G_0 of both sides of the Hambleton-Taylor-Williams Conjecture. As a coefficient ring we take $R = \mathbb{Z}$. We denote by $R_0(G)$ the rank of $G_0(\mathbb{Z}G)$, and by $P_0(G)$ the rank of $\oplus_{\rho\in X(G)} G_0(\Lambda_\rho)$, where $X(G)$ as before is the number of isomorphism classes of irreducible representations of G over $\mathbb{Q}$. As an outcome of the computations we will see that both numbers coincide, which means that no counterexample to the HTW-decomposition in degree 0 can be obtained by this strategy. We emphasize that there are no known counterexamples to the conjecture for G_0.

As we already remarked a maximal order in a central simple algebra over a field is not necessarily unique. Nevertheless, given two maximal orders Λ and Γ the categories of left Λ- and Γ-modules are equivalent (see e.g. [SwEv, Theorem 5.15]). This equivalence restricts to the subcategories of finitely generated modules. Thus, when talking about G-groups of some maximal order in a central simple algebra we do not have to specify the choice of such an order.

The following result allows us to compute the rank of $G_0(\mathbb{Z}G)$ (for the proof see [SwEv, Theorem 4.1]).

Theorem 59. *Let R be a Dedekind ring for which the Jordan-Zassenhaus theorem holds. Let k be the quotient field of R of characteristic 0. Then the kernel of the extension of scalars map $l_*\colon G_0(RG) \to G_0(kG)$ is finite.*

Since the Jordan-Zassenhaus theorem holds for $\mathbb{Z}$ it is a straightforward corollary from Theorem 59 that

$$\operatorname{rank} G_0(\mathbb{Z}G) \leq \operatorname{rank} G_0(\mathbb{Q}G).$$

On the other hand $G_0(\mathbb{Q}G)$ is a free abelian group with generators given by the classes of simple $\mathbb{Q}G$-modules. By Corollary 2 we know that every simple $\mathbb{Q}G$-module M contains a full $\mathbb{Z}G$-lattice M', which implies that $l_*([M']) = [\mathbb{Q}\otimes_{\mathbb{Z}} M'] = [M]$ and l_* is surjective. From this we immediately conclude that

$$R_0(G) = \operatorname{rank} G_0(\mathbb{Z}G) = \operatorname{rank} G_0(\mathbb{Q}G) = \#X(G).$$

To determine $G_0(\Lambda_\rho)$, where Λ_ρ is a maximal $\mathbb{Z}[1/\omega_\rho]$-order in D_ρ we first recall some terminology. Let R be a Dedekind ring with a quotient field k. Suppose k is a global field. Let A be a central simple k-algebra. Denote by $I(R)$ the group of fractional ideals of R. Let $P_A(R)$ be a subgroup of $I(R)$ generated by the following principal ideals

$$P_A(R) = \langle xR \mid x \in k,\ x > 0 \text{ at every real place where } A \text{ ramifies}\rangle.$$

The group $P_A(R)$ is an analogue of the group of principal ideals. The quotient

$$\mathrm{Cl}_A(R) = I(R)/P_A(R)$$

is callled a *ray class group*. In the situation when A is a field $\mathrm{Cl}_A(R)$ becomes the usual class group of R.

The following result describes $G_0(\Lambda_\rho)$ [SwEv, Theorem 7.8].

Theorem 60. *Let R be a Dedekind ring with a quotient field k and let Λ be a maximal R-order in a central simple k-algebra A. Suppose k is a global field. Then the following sequence is exact*

$$0 \to \mathrm{Cl}_A(R) \to K_0(\Lambda) \to K_0(A) \to 0$$

and hence

$$K_0(\Lambda) \cong \mathbb{Z} \oplus \mathrm{Cl}_A(R).$$

Moreover, the group $\mathrm{Cl}_A(R)$ *is finite and therefore* $\operatorname{rank} K_0(\Lambda) = 1$.

Recall that we denoted by D_ρ the division algebra corresponding to the irreducible representation $\rho \in X(G)$. Let E_ρ be the center of D_ρ and $\mathcal{O}_\rho$ the ring of integers in E_ρ. Let now Γ_ρ be a maximal $\mathcal{O}_\rho$-order in D_ρ. By Lemma 46 the ring Γ_ρ is at the same time a maximal $\mathbb{Z}$-order in D_ρ. Then by the localization property of maximal orders $\Gamma_\rho[1/\omega_\rho]$ is a maximal $\mathbb{Z}[1/\omega_\rho]$-order as well a maximal $\mathcal{O}_\rho[1/\omega_\rho]$-order in D_ρ. By Theorem 60 we have

$$\operatorname{rank}(\Lambda_\rho) = \operatorname{rank} G_0(\Gamma_\rho[1/\omega_\rho]) = 1.$$

Hence the rank predicted by the HTW-decomposition is

$$P_0(G) = \sum_{\rho \in X(G)} \operatorname{rank} G_0(\Lambda_\rho) = \# X(G),$$

and finally $P_0(G) = R_0(G)$. Consequently, we have shown that rationally the HTW-Conjecture holds in degree zero for all finite groups G.

3.3 The computation of torsions for G_0-groups

In this section we present the computation of the torsion part of both sides of the HTW-decomposition. Even though the expressions obtained are quite explicit, it is completely not clear whether or not they are isomorphic for all finite groups. Hence in general the HTW-Conjecture remains open in degree 0.

3.3.1 The computation of $\operatorname{tors} G_0(\mathbb{Z}G)$

To describe the group $G_0(\mathbb{Z}G)$ in terms of the ideal structure in the rings $\mathcal{O}_i$ we follow the paper by Heller and Reiner [HeRe1]. As before for $i \in X(G)$ we denote by $\mathcal{O}_i$ the ring of integers in $E_i = Z(D_i)$. Let Γ be a maximal $\mathbb{Z}$-order in $A = \mathbb{Q}G$ which contains $\mathbb{Z}G$. Given an algebraic number field F with the ring of integers R we denote by $I(R)$ the group of fractional ideals of R. We denote by $G_0^t(R)$ the Grothendieck group of the category of all finitely generated $\mathbb{Z}$-torsion R-modules. There exists a commutative diagram with exact rows

$$\begin{array}{lccccccccc}
\boxed{\text{loc. seq. for } \Gamma} & K_1(\mathbb{Q}G) & \xrightarrow{\delta'} & G_0^t(\Gamma) & \xrightarrow{\eta'} & G_0(\Gamma) & \xrightarrow{\theta'} & G_0(\mathbb{Q}G) & \longrightarrow & 0 \\
 & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \beta} & & {\scriptstyle Swan}\downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \mathrm{id}} & & \\
\boxed{\text{loc. seq. for } \mathbb{Z}G} & K_1(\mathbb{Q}G) & \xrightarrow{\delta} & G_0^t(\mathbb{Z}G) & \xrightarrow{\eta} & G_0(\mathbb{Z}G) & \xrightarrow{\theta} & G_0(\mathbb{Q}G) & \longrightarrow & 0.
\end{array}$$

The maps α and β are induced by the restriction of scalars. Swan [Sw3] showed that the homomorphism α is surjective, which by the Five Lemma implies that the restriction homomorphism β is also surjective. Since $G_0(\mathbb{Q}G)$ is a free abelian group we have

$$G_0(\mathbb{Z}G) \cong G_0(\mathbb{Q}G) \oplus \operatorname{im}(\eta \circ \beta) \cong G_0(\mathbb{Q}G) \oplus \frac{G_0^t(\Gamma)}{\operatorname{im} \delta' + \ker \beta}. \tag{3.4}$$

For every $i \in X(G)$ there exists Λ_i a maximal $\mathcal{O}_i$-order in D_i, such that Γ_i is Morita equivalent to $M_{m_i}(\Lambda_i)$. Thus

$$G_0^t(\Gamma) \cong \bigoplus_{i \in X(G)} G_0^t(\Gamma_i) \cong \bigoplus_{i \in X(G)} G_0^t(\Lambda_i).$$

To determine the group appearing on the right hand side of the equation (3.4) we examine the components of appearing terms $G_0^t(\Gamma)$, $\ker \beta$, $\operatorname{im} \delta'$ separately.

The description of $G_0^t(\Lambda_i)$. By the result of Heller and Reiner

$$G_0^t(\Lambda_i) \cong I(\mathcal{O}_i) \cong \bigoplus_P \mathbb{Z},$$

where P ranges over the set of maximal ideals in $\mathcal{O}_i$. The isomorphism $\tau\colon G_0^t(\Lambda_i) \to I(\mathcal{O}_i)$ can be described as follows. Given a Λ_i-module M define

$$\operatorname{ann}(M) = \{x \in \mathcal{O}_i \mid xM = 0\} \in I(\mathcal{O}_i).$$

For any $\mathcal{O}_i$-torsion Λ_i-module M consider its composition series

$$0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_l = M$$

and define *the order ideal of* M as

$$\operatorname{ord}(M) = \prod_{j=1}^{l} \operatorname{ann}(M_j/M_{j-1}) \in I(\mathcal{O}_i).$$

The map sending $[M]$ to $\operatorname{ord}(M)$ clearly induces a well-defined homomorphism

$$\tau\colon G_0^t(\Lambda_i) \to I(\mathcal{O}_i).$$

Since the group $G_0^t(\Lambda_i)$ is generated by the modules of the form $\Lambda_i/\mathfrak{m}$, where $\mathfrak{m}$ is a maximal left ideal in Λ_i, we need to understand what is the order ideal of such a module $\Lambda_i/\mathfrak{m}$. Using the ideal theory in maximal orders (see [Re], §22) we know that there is the unique maximal two-sided ideal $\mathfrak{P}$ of Λ_i contained in $\mathfrak{m}$ and its intersection with $\mathcal{O}_i$ gives a prime ideal $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_i$ in $\mathcal{O}_i$. Using this description it is not difficult to check that the defined map is indeed an isomorphism (see [HeRe1]). Another useful observation about this map is that

$$\operatorname{ord}(\Lambda_i/\mathfrak{m}) = N\mathfrak{m} \in I(\mathcal{O}_i),$$

where N denotes the norm.

The description of $\operatorname{im} \delta'$. Consider the decomposition of $\mathbb{Q}G$ into the product of simple algebras

$$\mathbb{Q}G \cong \prod_{i=1}^{s} A_i.$$

The map $\delta'\colon K_1(\mathbb{Q}G) \to G_0^t(\Gamma)$ composed with τ decomposes into a direct sum of componentwise maps $\delta_i'\colon K_1(A_i) \to I(\mathcal{O}_i)$. The image of δ_i' is given by the group

$$P_{A_i}(\mathcal{O}_i) = \langle x\mathcal{O}_i \mid x \in E_i,\ x > 0 \text{ at every real place where } D_i \text{ ramifies}\rangle.$$

The description of $\ker\beta$**.** To determine the kernel of the homomorphism $\beta\colon G_0^t(\Gamma) \to G_0^t(\mathbb{Z}G)$ as a subgroup of $\prod_{i=1}^s I(\mathcal{O}_i)$ we note that β may be written as a direct sum

$$\beta = \bigoplus_p \beta_p\colon \bigoplus_p G_0(\Gamma/p\Gamma) \to \bigoplus_p G_0(\mathbb{Z}G/p\mathbb{Z}G),$$

where the sum ranges over the prime numbers p and

$$\beta_p\colon G_0(\Gamma/p\Gamma) \to G_0(\mathbb{Z}G/p\mathbb{Z}G)$$

denotes the restriction of scalars. Since β is an epimorphism thus each β_p is also surjective. Additionally if p does not divide $|G|$, we have that $\Gamma/p\Gamma \cong \mathbb{Z}G/p\mathbb{Z}G$ and hence in this situation β_p is an isomorphism. Consequently,

$$\tau(\ker\beta) = \prod_{p \mid |G|} W_p,\ W_p = \tau(\ker\beta_p).$$

To describe W_p for a prime $p \mid |G|$ let us unravel the definitions of the homomorphisms involved. Consider the factorization of p into the product of prime ideals in $\mathcal{O}_i$

$$p\mathcal{O}_i = \prod_{j=1}^{t_i} P_{ij}^{e_{ij}}.$$

By Devissage $G_0(\Lambda_i/P_{ij}^{e_{ij}}\Lambda_i) \cong G_0(\Lambda_i/P_{ij}\Lambda_i)$. The ring $\Lambda_i/P_{ij}\Lambda_i$ has up to an isomorphism the unique simple module which we denote by S_{ij}. Therefore it holds

$$\begin{aligned} G_0(\Gamma/p\Gamma) \cong \bigoplus_{i=1}^{s} G_0(\Lambda_i/p\Lambda_i) &\cong \bigoplus_{i=1}^{s}\bigoplus_{j=1}^{t_i} G_0(\Lambda_i/P_{ij}^{e_{ij}}\Lambda_i) \\ &\cong \bigoplus_{i,j} G_0(\Lambda_i/P_{ij}\Lambda_i) \cong \bigoplus_{i,j} \mathbb{Z}. \end{aligned} \tag{3.5}$$

Under the isomorphism $\tau\colon G_0^t(\Lambda_i) \to I(\mathcal{O}_i)$ the element $[S_{ij}]$ corresponds to the ideal $P_{ij} \in I(\mathcal{O}_i)$. By the restriction of scalars from Γ to $\mathbb{Z}G$ we may view every module S_{ij} as a $\mathbb{Z}G/p\mathbb{Z}G$-module. Note that the only elements of $\mathbb{Z}G/p\mathbb{Z}G$ that may act non-trivially on S_{ij} are those elements whose projection on $\Gamma_i/P_{ij}\Gamma_i$ is non-zero. Thus

$$W_p = \tau(\ker\beta_p) = \{\prod_{i=1}^{s}\prod_{j=1}^{t_i} P_{ij}^{a_{ij}} \mid \sum_{i,j} a_{ij}[S_{ij}] = 0 \in G_0(\mathbb{Z}G/p\mathbb{Z}G)\}. \tag{3.6}$$

It is useful to note that the class of S_{ij} in $G_0(\Lambda_i/P_{ij}\Lambda_i)$ can be expressed in terms of the simple $\mathbb{Q}G$-module V_i that corresponds to the i-th simple component A_i in the Wedderburn decomposition of $\mathbb{Q}G$ in the following way. First recall that for V_i

it holds

$$D_i = \mathrm{Hom}_{A_i}(V_i, V_i),\ V_i \cong D_i^{m_i},\ A_i \cong \mathrm{Hom}_{D_i}(V_i, V_i) \cong M_{m_i}(D_i). \tag{3.7}$$

There exists a finitely generated projective Λ_i-module U_i such that

$$\mathbb{Q}U_i \cong E_i U_i \cong V_i$$

and analogously to (3.7) for U_i it holds

$$\Lambda_i \cong \mathrm{Hom}_{\Gamma_i}(U_i, U_i),\ \Gamma_i \cong M_{m_i}(\Lambda_i) \cong \mathrm{Hom}_{\Lambda_i}(U_i, U_i).$$

One can check that

$$[U_i/P_{ij}U_i] = l_i[S_{ij}],$$

where $l_i^2 = [D_i : E_i]$. Furthermore, if for a fixed prime p we denote by $\{X_1, \ldots, X_r\}$ a full set of non-isomorphic simple $\mathbb{F}_pG$-modules, then for each prime ideal $P_{ij} \subseteq \mathcal{O}_i$ dividing p the composition series of an $\mathbb{F}_pG$-module $U_i/P_{ij}U_i$ gives

$$[U_i/P_{ij}U_i] = \sum_{k=1}^{t} d_{ij}^{(k)}[X_k] \in G_0(\mathbb{F}_pG), \tag{3.8}$$

where the non-negative integers $d_{ij}^{(k)}$ may be thought of as a generalization of the decomposition numbers in the situation of a non-splitting field. Recall, that we defined the decomposition numbers for a splitting modular system exactly to avoid the confusion of having many decomposition numbers. In terms of the generalized decomposition numbers the map $\beta_p\colon \prod_{i=1}^{s} I^{(p)}(\mathcal{O}_i) \cong G_0(\Gamma/p\Gamma) \to G_0(\mathbb{F}_pG)$ becomes

$$\beta_p(\prod_{i,j} P_{ij}^{a_{ij}}) = \sum_{i,j,k} a_{ij}\frac{d_{ij}^{(k)}}{n_i}[X_k]. \tag{3.9}$$

If $\mathbb{Q}$ appears to be a splitting filed for G, then each D_i coincides with $\mathbb{Q}$ and we just obtain the ordinary decomposition numbers in the expression (3.9). As a summary we have the *Heller-Reiner decomposition*

$$G_0(\mathbb{Z}G) \cong G_0(\mathbb{Q}G) \oplus \frac{\prod_{i=1}^{s} I(\mathcal{O}_i)}{\prod_{i=1}^{s} P_{A_i}(\mathcal{O}_i) \times \prod_{p \supset |G|} W_p}, \tag{3.10}$$

with W_p given by (3.6) and known as *Heller-Reiner relations.*

3.3.2 The computation of the predicted torsion

Note that in this Section we denoted by Λ_i a maximal $\mathbb{Z}$-order in D_i. From Theorem 60 we obtain that

$$G_0(\Lambda_i[1/\omega_i]) \cong \mathbb{Z} \oplus \frac{I(\mathcal{O}_i)}{P_{A_i}(\mathcal{O}_i) \times \prod_{p|\omega_i} I^{(p)}(\mathcal{O}_i)}, \tag{3.11}$$

where $I^{(p)}(\mathcal{O}_i)$ denotes the subgroup of $I(\mathcal{O}_i)$ generated by the prime ideals in $\mathcal{O}_i$ that divide p. Hence to test the HTW-Conjecture for the torsion part of G_0 we need to compare the following two groups

$$T_0(G) = \frac{\prod_{i=1}^{s} I(\mathcal{O}_i)}{\prod_{i=1}^{s} P_{A_i}(\mathcal{O}_i) \times \prod_{p \supset |G|} W_p}$$

and

$$PT_0(G) = \frac{\prod_{i=1}^{s} I(\mathcal{O}_i)}{\prod_{i=1}^{s} P_{A_i}(\mathcal{O}_i) \times \prod_{p|\omega_i} I^{(p)}(\mathcal{O}_i)}.$$

Examples.

- If $G = S_n$ is a symmetric group for some n, then $\mathbb{Q}$ is a splitting field for G and every $I(\mathcal{O}_i)/P_{A_i}(\mathcal{O}_i)$ is just $\mathrm{Cl}(\mathbb{Z}) = 1$. Hence the additional relations are not having any impact on the group, and in this case $T_0(G) = PT_0(G)$. Note, that S_5 is a counterexample to the HTW-Conjecture in degree 1 (see [WeY]), but in degree zero the HTW-decomposition holds for all symmetric groups.

- If G is a group such that all the number fields E_i's which are the centers of the division algebras D_i's appearing in the Wedderburn decomposition of $\mathbb{Q}G$ are totally imaginary, then again all the groups $I(\mathcal{O}_i)/P_{A_i}(\mathcal{O}_i)$ are trivial. In such case the HTW-Conjecture holds in degree zero. The group $\mathrm{SL}(2, \mathbb{F}_3)$ is an example of a group with this property and hence the HTW-Conjecture holds in degree zero for $\mathbb{Z}[\mathrm{SL}(2, \mathbb{F}_3)]$ despite the fact that it fails in degree 1.

3.4 The comparison of ranks for G_1-groups

3.4.1 The description of $R(G)$

Let G be a finite group. As we have seen in Section 2.4 the abelian group $G_1(\mathbb{Z}G)$ was completely determined by Keating [Ke]. Recall Keating's formula for the rank of $G_1(\mathbb{Z}G)$. We use the same notation as in the beginning of Chapter, namely, $\rho\colon G \to \mathrm{Aut}(V_\rho)$ denotes a rational irreducible representation of G, $D_\rho = \mathrm{End}_{\mathbb{Q}G}(V_\rho)$ is the corresponding division algebra, and the rational group algebra decomposes as $\mathbb{Q}G \cong \prod_{\rho \in X(G)} M_{n_\rho}(D_\rho^{op})$.

Theorem 61 (Keating's rank formula)**.** *Let Γ_ρ be the maximal $\mathbb{Z}$-order in the center of D_ρ. Let r_ρ be the rank of group of units in Γ_ρ, and let v_ρ be the number of primes of Γ_ρ that divide $|G|$. Let ε be the number of isomorphism classes of simple $\mathbb{Z}G$-modules annihilated by $|G|$. Then*

$$\text{rank } G_1(\mathbb{Z}G) = \sum_{\rho \in X(G)} (r_\rho + v_\rho) - \varepsilon.$$

Denote by E_ρ the center of D_ρ. Obviously it is an algebraic number field and moreover $E_\rho/\mathbb{Q}$ is an abelian extension (see [BaRo, Lemma 2.8]). Denote by $\mathcal{O}_\rho$ the ring of algebraic integers in E_ρ (it is the maximal $\mathbb{Z}$-order in E_ρ). Since E_ρ is an abelian number field it is either totally real or totally imaginary. Let $m_\rho = [E_\rho : \mathbb{Q}]$. Then by Dirichlet's unit theorem the rank r_ρ of the group of units in $\mathcal{O}_\rho$ is equal to $\#\{\text{real embeddings of } E_\rho\} + \#\{\text{conjugate pairs of complex embeddings of } E_\rho\} - 1$.

Therefore

$$r_\rho = \begin{cases} m_\rho - 1, & \text{if } E_\rho \text{ is totally real,} \\ m_\rho/2 - 1, & \text{if } E_\rho \text{ is totally complex.} \end{cases}$$

It is clear that

$$\varepsilon = \sum_{p|n} \#\{\text{isomorphism classes of simple } \mathbb{F}_p G\text{-modules}\},$$

where the sum ranges over all prime numbers that divide the order n of the group G. To compute the number of irreducible $\mathbb{F}_p$-representations of G explicitly we first establish some notation. Denote by d the L.C.M. of orders of all p-regular elements in G. Let k be the smallest positive integer such that $p^k = 1 \pmod d$. Denote by T the multiplicative group of exponents $\{p^i \mid i = 1, 2, \ldots, k\}$ modulo d.

Definition 62. *Two p-regular elements $g_1, g_2 \in G$ are called $\mathbb{F}_p$-conjugate if $g_1^t = hg_2h^{-1}$ for some $t \in T$ and $h \in G$.*

Theorem 63 (Berman [B])**.** *The number of irreducible representations of G over $\mathbb{F}_p$ equals the number of p-regular $\mathbb{F}_p$-conjugacy classes.*

Hence

$$\varepsilon = \sum_{p|n} \#\{p\text{-regular } \mathbb{F}_p\text{-conjugacy classes}\}.$$

Now we have a very computable description of the summands appearing in Theorem 61 and we denote by $R(G)$ the rank of $G_1(\mathbb{Z}G)$. More precisely we have

$$R(G) = \sum_{\rho \in X(G)} (r_\rho + v_\rho) - \varepsilon.$$

3.4.2 The description of $P(G)$

In this subsection we are going to compute the rank of $G_1(\mathbb{Z}G)$ as predicted by the Hambleton-Taylor-Williams Conjecture. If the HTW-decomposition holds for a group G and any noetherian coefficient ring R, then taking $R = \mathbb{Z}$ gives

$$G_1(\mathbb{Z}G) \cong \bigoplus_{\rho \in X(G)} G_1(\Lambda_\rho)$$

and

$$\text{rank } G_1(\mathbb{Z}G) = \sum_{\rho \in X(G)} \text{rank } G_1(\Lambda_\rho).$$

Denote by $P(G)$ the rank of $G_1(\mathbb{Z}G)$ that is predicted by the HTW-decomposition, i.e., $P(G) := \sum_{\rho \in X(G)} \text{rank } G_1(\Lambda_\rho)$. We are going to give an explicit description of $P(G)$ and compare it with the real rank $R(G)$ computed in the previous subsection. Obviously, if $P(G) \neq R(G)$, then the group G does not satisfy the HTW-decomposition.

For a rational irreducible representation ρ we determine the rank of $G_1(\Lambda_\rho)$ by applying the following theorem ([La3], [SwEv]).

Theorem 64 (Lam)**.** *Let R be a Dedekind ring with quotient field K and let A be a separable semisimple K-algebra such that*

(i) $R/\mathfrak{p}$ is finite for every non-zero prime ideal $\mathfrak{p} \subseteq R$, and

(ii) if L is a finite separable field extension of K and S is the integral closure of R in L, then the class group $\mathrm{Cl}(S)$ is a torsion group.

Let $Z(A)$ be the center of A, $\tilde{R}$ the integral closure of R in $Z(A)$, and Λ an R-order in A. Then

$$G_1(\Lambda) \underset{\textit{mod torsion}}{\cong} \tilde{R}^\times.$$

Let $R = \mathbb{Z}[1/\omega_\rho]$, $K = \mathbb{Q}$ and $A = D_\rho$. The prime ideals in the localization $\mathbb{Z}[1/\omega_\rho]$ are of the form $q\mathbb{Z}[1/\omega_\rho]$, where q is a prime integer that does not divide ω_ρ. Hence the first condition of Theorem 64 is satisfied, because

$$\mathbb{Z}[1/\omega_\rho]/q\mathbb{Z}[1/\omega_\rho] \cong (\mathbb{Z}/q\mathbb{Z})[1/\omega_\rho] \cong \mathbb{Z}/q\mathbb{Z}.$$

If L is an algebraic number field and $\mathcal{O}_L$ is the ring of algebraic integers in L, then the integral closure of $\mathbb{Z}[1/\omega_\rho]$ in L is $\mathcal{O}_L[1/\omega_\rho]$. To check that the second condition of Theorem 64 holds it is enough to show that $\mathrm{Cl}(\mathcal{O}_L[1/\omega_\rho])$ is finite. Recall that for a Dedekind ring $\mathcal{R}$ the ideal class group of $\mathcal{R}$ is given by the quotient $\mathrm{Cl}(\mathcal{R}) = \mathcal{I}_\mathcal{R}/\mathcal{P}_\mathcal{R}$, where $\mathcal{I}_\mathcal{R}$ is the group of fractional ideals of $\mathcal{R}$ and $\mathcal{P}_\mathcal{R}$ is the subgroup of principal fractional ideals of $\mathcal{R}$. Let $\phi\colon \mathcal{I}_{\mathcal{O}_L} \to \mathcal{I}_{\mathcal{O}_L[1/\omega_\rho]}$ be a map sending a fractional ideal I of $\mathcal{O}_L$ to the fractional ideal $\mathcal{O}_L[1/\omega_\rho] \otimes_{\mathcal{O}_L} I$ of $\mathcal{O}_L[1/\omega_\rho]$. This map is obviously a group homomorphism. Moreover ϕ takes principal fractional ideals of $\mathcal{O}_L$ to principal fractional ideals of $\mathcal{O}_L[1/\omega_\rho]$ and is surjective, since $\mathcal{O}_L$ and $\mathcal{O}_L[1/\omega_\rho]$ have the same field of fractions. Therefore ϕ induces a surjective group homomorphism

$$\bar{\phi}\colon Cl(\mathcal{O}_L) \twoheadrightarrow Cl\big(\mathcal{O}_L\Big[\frac{1}{\omega_\rho}\Big]\big).$$

Now finiteness of the group $Cl(\mathcal{O}_L[1/\omega_\rho])$ follows from the surjectivity of $\bar{\phi}$ and the classical result that the ideal class group of the ring of integers in an algebraic number field is finite.

The integral closure of $\mathbb{Z}[1/\omega_\rho]$ in $Z(D_\rho) = E_\rho$ is $\mathcal{O}_\rho[1/\omega_\rho]$. Therefore, Theorem 64 implies

$$G_1(\Lambda_\rho) \underset{\text{mod torsion}}{\cong} \big(\mathcal{O}_\rho\Big[\frac{1}{\omega_\rho}\Big]\big)^\times.$$

To determine the rank of units in $\mathcal{O}_\rho[1/\omega_\rho]$ we use the S-unit theorem (see, for example, [Ne, p. 88]). Let us briefly recall its statement. Let L be an algebraic number field and let S be a finite set of prime ideals in $\mathcal{O}_L$. Define

$$\mathcal{O}_L(S) := \{x \in L \mid ord_{\mathfrak{p}}(x) \geq 0, \text{ for all prime ideals } \mathfrak{p} \notin S\}.$$

Define the group $U(S)$ of S-units to be

$$U(S) := \big(\mathcal{O}_L(S)\big)^{\times} = \{x \in L \mid ord_{\mathfrak{p}}(x) = 0, \text{ for all } \mathfrak{p} \notin S\}.$$

Theorem 65 (S-unit theorem)**.** *The group of S-units is finitely generated and*

$$\text{rank } U(S) = \text{rank } \mathcal{O}_L^{\times} + \#S.$$

Let S be the set of all prime ideals in $\mathcal{O}_\rho$ that divide ω_ρ. Then $\mathcal{O}_{E_\rho}(S) = \mathcal{O}_\rho[1/\omega_\rho]$ and $U(S) = \big(\mathcal{O}_\rho[1/\omega_\rho]\big)^{\times}$. Hence by Theorem 65

$$\text{rank } \big(\mathcal{O}_\rho[1/\omega_\rho]\big)^{\times} = \text{rank } \mathcal{O}_\rho^{\times} + \#\{\text{prime ideals in } \mathcal{O}_\rho \text{ that divide } \omega_\rho\}$$

and finally

$$\text{rank } G_1(\Lambda_\rho) = r_\rho + \#\{\text{prime ideals in } \mathcal{O}_\rho \text{ that divide } \omega_\rho\}.$$

Let us denote by w_ρ the number of prime ideals in $\mathcal{O}_\rho$ that divide ω_ρ. Then

$$P(G) = \sum_{\rho \in X(G)} \text{rank } G_1(\Lambda_\rho) = \sum_{\rho \in X(G)} \big(r_\rho + w_\rho\big).$$

3.4.3 A solvable counterexample

In this subsection we show that $G = \mathrm{SL}(2, \mathbb{F}_3)$, the group of 2×2 matrices with determinant 1 over the finite field $\mathbb{F}_3$, is a counterexample to the Hambleton-Taylor-Williams Conjecture by comparing $R(G)$ and $P(G)$ that were described in the previous section. Note that the order of the group G is 24.

For the computation of $R(G)$ and $P(G)$ we need to know the table of complex irreducible characters of G. If ρ is an irreducible rational representation of G, then the center E_ρ of the corresponding division algebra D_ρ appearing in the Wedderburn decomposition is isomorphic to the field of character values $\mathbb{Q}(\chi_\rho^{\mathbb{C}}) := \mathbb{Q}(\chi_\rho^{\mathbb{C}}(g) \mid g \in G)$, where $\chi_\rho^{\mathbb{C}}$ is the character of any irreducible complex constituent of the complexification of the representation ρ (see [Je, Theorem 3.3.1]).

Denote by ξ a primitive cubic root of unity. The complex irreducible characters of $\mathrm{SL}(2, \mathbb{F}_3)$ are well-known (see [Bo, p. 132]) and are presented in Table 3.1.

The field $\mathbb{Q}(\xi)$ is the splitting field for the group G. The Galois group $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ acts on the set of complex representations of G, in particular it permutes irreducible complex representations. Let χ be the character of an irreducible rational representation of G. It is well known (see [CuRe2, (74.5)]) that χ can be realized as a sum of all distinct Galois conjugates of some complex irreducible character φ taken with multiplicity $m(\varphi)$, which is the Schur index of φ,

Table 3.1: Character table of $\mathrm{SL}(2, \mathbb{F}_3)$

repr.:	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\mathbb{Q}(\chi)$
size:	1	1	6	4	4	4	4	
order:	1	2	4	6	3	6	3	
χ_1	1	1	1	1	1	1	1	$\mathbb{Q}$
χ_2	3	3	-1	0	0	0	0	$\mathbb{Q}$
χ_3	2	-2	0	1	-1	1	-1	$\mathbb{Q}$
χ_4	1	1	1	ξ	ξ	ξ^2	ξ^2	$\mathbb{Q}(\xi)$
χ_5	1	1	1	ξ^2	ξ^2	ξ	ξ	$\mathbb{Q}(\xi)$
χ_6	2	-2	0	ξ	-ξ	ξ^2	-ξ^2	$\mathbb{Q}(\xi)$
χ_7	2	-2	0	ξ^2	-ξ^2	ξ	-ξ	$\mathbb{Q}(\xi)$

i.e., $\chi = m(\varphi) \sum_\sigma \varphi^\sigma$. And vice versa any complex irreducible representation gives rise to a unique rational irreducible representation in the way described above.

The Galois group $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ permutes characters χ_4 with χ_5, and χ_6 with χ_7. The character χ_3 is fixed by $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$, but the corresponding representation is not defined over $\mathbb{Q}$ and has Schur index 2. We have 2 absolutely irreducible rational representations ρ_1, ρ_2 with characters χ_1, χ_2, respectively; and 3 irreducible rational representations ρ_3, ρ_4, ρ_5, s.t. χ_3 is the character of one of the irreducible complex constituents of $\rho_3^{\mathbb{C}}$, χ_4 is the character of one of the irreducible complex constituents of $\rho_4^{\mathbb{C}}$, and χ_6 is the character of one of the irreducible complex constituents of $\rho_5^{\mathbb{C}}$ (here $\rho^{\mathbb{C}}$ denotes the complexification $\mathbb{C} \otimes_{\mathbb{Q}} \rho$ of a representation ρ).

The kernel of a representation ρ coincides with the kernel of the induced character $\ker \chi_\rho = \{g \in G \mid \chi_\rho(g) = \chi_\rho(e)\}$. Moreover, since the rational irreducible representation is expressible in terms of complex irreducible representations, the kernel of ρ coincides with the kernel of $\chi_\rho^{\mathbb{C}}$. Therefore we have the following list of centers E_ρ's and values of ω_ρ's given in Table 3.2.

Table 3.2

	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
E_ρ	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}(\xi)$	$\mathbb{Q}(\xi)$
$\mathcal{O}_\rho$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}[\xi]$	$\mathbb{Z}[\xi]$
$\omega_\rho = \frac{24}{\ker \chi_\rho^{\mathbb{C}} \ \dim \chi_\rho^{\mathbb{C}}}$	1	4	12	3	12
$v_\rho = \#\{\text{prime ideals in } \mathcal{O}_\rho \text{ that divide } 24\}$	2	2	2	2	2
$w_\rho = \#\{\text{prime ideals in } \mathcal{O}_\rho \text{ that divide } \omega_\rho\}$	0	1	2	1	2

For the computation of numbers v_ρ and w_ρ in Table 2 we used the following theorem (for a more general statement see [Ne, p. 47]) to determine the number of prime ideals in $\mathbb{Z}[\xi]$ that divide 2 and 3.

Theorem 66. *Let α be an algebraic integer such that $\mathbb{Z}[\alpha]$ is integrally closed, and let f be the minimal polynomial of α. Let p be a prime number and let*

$$f(x) = \prod_i f_i(x)^{e_i}$$

in $\mathbb{F}_p[x]$. Then the prime ideals that lie above p in $\mathbb{Z}[\alpha]$ are precisely the ideals $(p, f_i(\alpha))$.

For $p = 3$ the minimal polynomial of ξ factors as $x^2 + x + 1 = (x - 1)^2$ in $\mathbb{F}_3[x]$ and hence by Theorem 66 there is only one prime ideal above 3 in $\mathbb{Z}[\xi]$. For $p = 2$ the polynomial $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$ and hence there is exactly one prime ideal above 2 in $\mathbb{Z}[\xi]$.

The last step is to determine ε appearing in the description of $R(G)$. For this we need to compute the number of p-regular $\mathbb{F}_p$-conjugacy classes for $p = 2, 3$.

For $p = 3$ there are 3 conjugacy classes of 3-regular elements, namely the classes with representatives $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Since the first two elements belong to the center of G and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, these elements belong to 3 different $\mathbb{F}_3$-conjugacy classes.

For $p = 2$ there are 3 conjugacy classes of 2-regular elements, namely the classes with representatives $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$. Since $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^2 = \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$ the elements $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$ are $\mathbb{F}_2$-conjugated. Therefore there are two 2-regular $\mathbb{F}_2$-conjugacy classes. Finally

$$P(G)-R(G) = \sum_\rho (r_\rho+w_\rho)-\sum_\rho (r_\rho+v_\rho)+\varepsilon = \sum_\rho w_\rho-\sum_\rho v_\rho+\varepsilon = 6-10+5 = 1.$$

This shows that the actual rank of $G_1(\mathbb{Z}G)$ and the rank predicted by the HTW-Conjecture do not coincide and $G = \mathrm{SL}(2, \mathbb{F}_3)$ is a solvable counterexample to the conjectured formula. Thus Theorem A is proved.

3.4.4 Counting modular representations in terms of rational

In this subsection we prove an inequality estimating the number of modular irreducible representations of a finite group G in terms of rational irreducible representations of G. The result we obtain implies that $P(G) \geq R(G)$ for any finite group G. The proof of the inequality provides an explanation why in general the HTW-Conjecture does not hold for $G_1(\mathbb{Z}G)$. We are using the same notation as before.

Let p be a prime number that divides the order of G. Recall that for any rational irreducible representation ρ of G there is an associated algebraic number field E_ρ: the field of character values $\mathbb{Q}(\chi_\rho^{\mathbb{C}})$, where $\chi_\rho^{\mathbb{C}}$ is the character of any of the irreducible complex constituents of $\mathbb{C} \otimes_{\mathbb{Q}} \rho$. Let t_ρ be the number of different prime ideals in $\mathcal{O}_\rho$ that divide the principal ideal (p). Then the following inequality holds.

Theorem B. *Let G be any finite group and let p be a prime integer that divides the order of G. Then*

$$\#\{\textit{irreducible } \mathbb{F}_p\textit{-representations of } G\} \geq \sum_{\rho \in I_p} t_\rho,$$

where I_p is the set of rational irreducible representations ρ of G for which the corresponding number ω_ρ is not divisible by p.

The main ingredient in the proof of Theorem B is the following classical theorem due to Brauer and Nesbitt (see [BrNe], [CuRe]).

Theorem 67 (Brauer-Nesbitt)**.** *Let G be a finite group of order $|G| = p^a m$, where $(p, m) = 1$. If a complex irreducible representation ϕ has dimension divisible by p^a, then it remains irreducible after reduction mod p. Moreover, the character of ϕ vanishes on all elements of G whose order is divisible by p, and coincides with the Brauer character of $\bar{\phi}$ (reduction mod p of ϕ) on p-regular elements of G.*

We start with some preparatory statements and definitions before giving the proof of Theorem B. Recall Lemma 6 that any element $g \in G$ is expressible as $g = g_{p'} g_p$, where $g_{p'}$ and g_p commute, $g_{p'}$ has order coprime with p, and g_p has order a power of p.

Lemma 68. *Let H be a normal subgroup in G, and let $g = g_{p'} g_p \in G$. If $g_p \notin H$, then $\mathrm{ord}_{G/H}(\bar{g})$ is divisible by p, where $\mathrm{ord}_{G/H}(\bar{g})$ is the order of g considered as an element in the quotient group G/H.*

Proof. For an element $x \in G$ we denote by $\bar{x}$ the image of x in the quotient group G/H. Let $a = \mathrm{ord}_{G/H}(\bar{g})$. Since elements $g_{p'}$ and g_p commute in G we have $\bar{g}^a = \overline{g_{p'}}^a \overline{g_p}^a = e$. Hence $(\overline{g_{p'}}^{-1})^a = \overline{g_p}^a$. The order of the element $\overline{g_p}^a$ in G/H divides the order of g_p^a in G, and therefore $\mathrm{ord}_{G/H}(\overline{g_p}^a)$ is a power of p. The same way the order of $(\overline{g_{p'}}^{-1})^a$ in G/H is coprime with p. This implies that $(\overline{g_{p'}}^{-1})^a = \overline{g_p}^a = e$ and hence a is divisible by $\mathrm{ord}_{G/H}(\overline{g_p})$. At the same time $\overline{g_p} \neq e$ and hence $\mathrm{ord}_{G/H}(\overline{g_p})$ is divisible by p. Therefore a is divisible by p. □

Lemma 69. *Let φ_1, φ_2 be complex irreducible characters of G. Let $H_1 = \ker(\varphi_1)$ and $H_2 = \ker(\varphi_2)$. Suppose the following conditions are satisfied.*

1. *$\varphi_i(g) = 0$ for all $g \in G$, s.t. $\mathrm{ord}_{G/H_i}(\bar{g})$ is divisible by p, $i \in \{1, 2\}$;*
2. *$\varphi_1(g) = \varphi_2(g)$ for all $g \in G$, s.t. $\mathrm{ord}_G(g)$ is not divisible by p.*

Then φ_1 and φ_2 are equal.

Proof. Any element $g \in G$ is expressible in the form $g = g_{p'} g_p$, where $g_{p'}$ is p-regular and g_p is p-singular. If $g_p \notin H_1$, then by Lemma 68 we have that $\mathrm{ord}_{G/H_1}(\bar{g})$ is divisible by p, and therefore by the first condition $\varphi_1(g) = 0$. Analogously, if $g_p \notin H_2$, then $\varphi_2(g) = 0$. Hence we have the following equalities

$$\varphi_1(g) = \varphi_1(g_{p'} g_p) = \begin{cases} 0, & \text{if } g_p \notin H_1 \\ \varphi_1(g_{p'}) = \varphi_2(g_{p'}), & \text{if } g_p \in H_1 \end{cases} \tag{3.12}$$

and

$$\varphi_2(g) = \varphi_2(g_{p'}g_p) = \begin{cases} 0, & \text{if } g_p \notin H_2 \\ \varphi_2(g_{p'}) = \varphi_1(g_{p'}), & \text{if } g_p \in H_2. \end{cases} \tag{3.13}$$

Let us consider the inner product of the characters φ_1, φ_2

$$\langle \varphi_1, \varphi_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi_1(g)\overline{\varphi_2(g)} = \frac{1}{|G|} \sum_{\substack{g = g_{p'}g_p \in G, \\ g_p \in H_1 \cap H_2}} \varphi_1(g_{p'})\overline{\varphi_1(g_{p'})}, \tag{3.14}$$

where the last equality holds since all terms with $g_p \notin H_1 \cap H_2$ vanish. The value of the sum is a positive real number, because each term is a non-negative real number and taking g to be the identity element e gives a non-zero summand $|\varphi_1(e)|^2$. This implies that the inner product of irreducible characters φ_1, φ_2 is non-zero, and therefore $\varphi_1 = \varphi_2$. □

Let K be an algebraic number field that is a splitting field for G and a Galois extension of $\mathbb{Q}$. This means that any complex representation of G is realized over K. Let $\mathcal{O}_K$ denote the ring of algebraic integers of K and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ containing p. Denote the field $\mathcal{O}_K/\mathfrak{p}$ by $\bar{K}$. It is clearly a finite Galois extension of $\mathbb{F}_p$. Recall that to any representation ϕ over K we can associate a representation $\bar{\phi}$ over $\bar{K}$, whose composition factors are uniquely determined (see e.g. [CuRe, §82]). We call this process reduction mod p. Let $d\colon G_0(KG) \to G_0(\bar{K}G)$ be the map induced by reduction mod p.

Definition 70. *Let ϕ be an irreducible complex representation of G. We call ϕ p-special if the corresponding number $\omega_\phi = \frac{|G/\ker\phi|}{\dim\phi}$ is not divisible by p.*

Thus ϕ is p-special if and only if ϕ is a p-block of defect zero for the quotient group of G that it faithfully represents. The next lemma shows that the reduction mod p is injective on the set of p-special representations. Whenever we mention the set of representations, we mean the set of isomorphism classes of representations.

Proposition 71. *Let G be a finite group, p a prime number that divides $|G|$, and $K, \bar{K}$ defined as above. Then the following holds.*

(i) Reduction mod p of a p-special representation of G is an irreducible $\bar{K}$-representation of G.

(ii) The restriction of the map $d\colon G_0(KG) \to G_0(\bar{K}G)$ to the set of p-special representations of G is injective.

Proof. (i) Let ϕ be a p-special representation of G. Denote by H the kernel of ϕ. Then ϕ induces a representation of G/H, which we denote by $\phi_{G/H}$. Since ϕ is irreducible, the representation $\phi_{G/H}$ is irreducible as well. Now the Brauer-Nesbitt Theorem can be applied to $\phi_{G/H}$, because $\frac{|G/H|}{\dim\phi_{G/H}}$ is not divisible by p by the definition of a p-special representation. Therefore $\bar{\phi}_{G/H}$ is an irreducible $\bar{K}$-representation of G/H, which implies that $\bar{\phi}$ is an irreducible $\bar{K}$-representation of G.

(ii) The Brauer-Nesbitt Theorem guarantees that the character of $\phi_{G/H}$ vanishes on all elements of G/H having order divisible by p, and coincides with Brauer character of $\bar{\phi}_{G/H}$ on p-regular elements of G/H. Note that p-regular elements of G remain p-regular when passing to the quotient group G/H.

Suppose that the reduction mod p of two p-special representations ϕ_1 and ϕ_2 gives $\bar{K}$-equivalent representations $\bar{\phi}_1, \bar{\phi}_2$. Then the Brauer characters of $\bar{\phi}_1$ and $\bar{\phi}_2$ are the same, which by the Brauer-Nesbitt Theorem implies that the ordinary characters of ϕ_1 and ϕ_2 coincide on p-regular elements of G. This means that conditions of Lemma 69 are satisfied for the characters of ϕ_1 and ϕ_2, hence the representations ϕ_1 and ϕ_2 are K-equivalent. Therefore the restriction of the map d to the set of p-special representations of G is injective. □

To prove Theorem B we will also use the following theorem that describes the behavior of irreducible representations under extension of the base field (see [CuRe2, (74.5)]).

Theorem 72. *Let G be a finite group, k an arbitrary field, and E a splitting field for G, s.t. E is a finite Galois extension of k. Then we have*

(i) For a simple kG-module U there is an isomorphism of EG-modules

$$E \otimes_k U \cong (V_1 \oplus \ldots \oplus V_t)^{\oplus m},$$

where $\{V_1, \ldots, V_t\}$ is a set of non-isomorphic simple left EG-modules permuted transitively by the Galois group $\mathrm{Gal}(E/k)$, and $m = m_k(V_i)$ is the Schur index.

(ii) Let φ be an absolutely irreducible character of G afforded by some simple left EG-module V. Then there is a simple kG-module U, unique up to isomorphism, s.t. φ occurs in the character χ afforded by U. Then V occurs as a summand in the decomposition of $E \otimes_k U$, say $V = V_1$, and

$$\chi = m \sum_{i=1}^{t} \varphi_i, \quad k(\varphi_1) \cong \ldots \cong k(\varphi_t),$$

where φ_i is the character of G afforded by V_i, and $k(\varphi_i)$ is the field of character values.

Now we are ready to prove Theorem B.

Proof of Theorem B. The assumption of Theorem 72 is satisfied for $k = \mathbb{Q}$ and $E = K$, therefore it gives a one to one correspondence between rational irreducible representations of G and orbits of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ action on the set of irreducible K-representations of G. In particular, it gives a one to one correspondence between the set I_p and orbits of the $\mathrm{Gal}(K/\mathbb{Q})$-action on the set of p-special representations of G.

Given a p-special representation ϕ of G let φ be its character. Denote by E_ϕ the field of character values $\mathbb{Q}(\varphi)$. Then by [CuRe, Theorem 70.15] the size of the orbit of ϕ under the action of $\mathrm{Gal}(K/\mathbb{Q})$ is given by

$$|Orb(\phi)| = |E_\phi : \mathbb{Q}| = |\mathrm{Gal}(E_\phi/\mathbb{Q})|.$$

Next we examine the orbit $Orb(\phi)$ after reduction mod p. Since the irreducible representation ϕ is p-special, Proposition 71 implies that all Galois conjugates of ϕ remain irreducible when reduced mod p. Denote by $\bar{\phi}$ the reduction mod p of ϕ, and by $\overline{Orb(\phi)}$ the set $Orb(\phi)$ after reduction mod p. By Proposition 71 the set $\overline{Orb(\phi)}$ consists of pairwise non-isomorphic irreducible $\bar{K}$-representations. This implies that the set $\overline{Orb(\phi)}$ has the same number of elements as $Orb(\phi)$.

It is well known that the decomposition group $\mathfrak{D}(\mathfrak{p}/p) = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$ naturally surjects onto the Galois group $\mathrm{Gal}(\bar{K}/\mathbb{F}_p)$ with kernel the inertia group $\mathfrak{I}(\mathfrak{p}/p)$ (see e.g. [Se2, §7]). Therefore the Galois group $\mathrm{Gal}(\bar{K}/\mathbb{F}_p)$ preserves the set $\overline{Orb(\phi)}$.

Let us see how many orbits this action has. Let $\bar{\phi}^\sigma \in \overline{Orb(\phi)}$, $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Again by [CuRe, Theorem 70.15] the size of the orbit of $\bar{\phi}^\sigma$ under the action of $\mathrm{Gal}(\bar{K}/\mathbb{F}_p)$ is given by

$$|Orb(\bar{\phi}^\sigma)| = |\mathbb{F}_p(\bar{\varphi}^\sigma) : \mathbb{F}_p|,$$

where $\bar{\varphi}^\sigma$ is the character of $\bar{\phi}^\sigma$, and $\mathbb{F}_p(\bar{\varphi}^\sigma)$ is the field of character values. The way the process of reduction mod p is defined implies that $\mathbb{F}_p(\bar{\varphi}^\sigma) \subseteq \mathcal{O}_{\phi^\sigma}/(\mathfrak{p} \cap \mathcal{O}_{\phi^\sigma}) \cong \mathcal{O}_\phi/(\sigma^{-1}\mathfrak{p} \cap \mathcal{O}_\phi)$, where $\mathcal{O}_\phi$ is the ring of integers of the number field E_ϕ. For short denote the prime ideal $\sigma^{-1}\mathfrak{p} \cap \mathcal{O}_\phi$ by $\mathfrak{q}$. Hence for each $\bar{\phi}^\sigma \in \overline{Orb(\phi)}$ we have

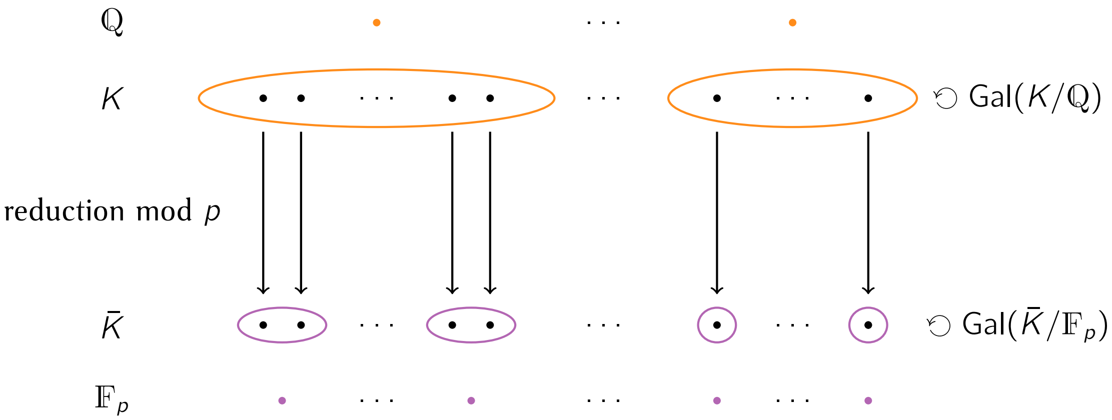
$$|Orb(\bar{\phi}^\sigma)| \leq |(\mathcal{O}_\phi/\mathfrak{q}) : \mathbb{F}_p|,$$

where $|Orb(\bar{\phi}^\sigma)|$ means the same as before. Therefore the number of orbits of the action of $\mathrm{Gal}(\bar{K}/\mathbb{F}_p)$ on the set $\overline{Orb(\phi)}$ is at least

$$\frac{|\overline{Orb(\phi)}|}{|(\mathcal{O}_\phi/\mathfrak{q}) : \mathbb{F}_p|} = \frac{|\mathrm{Gal}(E_\phi/\mathbb{Q})|}{|\mathrm{Gal}((\mathcal{O}_\phi/\mathfrak{q})/\mathbb{F}_p)|} = \frac{|\mathrm{Gal}(E_\phi/\mathbb{Q})|}{|\mathfrak{D}(\mathfrak{q}/p)|}|\mathfrak{I}(\mathfrak{q}/p)| = t_\rho|\mathfrak{I}(\mathfrak{q}/p)|.$$

The last equality holds since $E_\phi = E_\rho$ and the Galois group $\mathrm{Gal}(E_\phi/\mathbb{Q})$ acts transitively on prime ideals in $\mathcal{O}_\phi$ dividing p, and $\mathfrak{D}(\mathfrak{q}/p)$ is exactly the stabilizer of a prime ideal $\mathfrak{q}$ by $\mathrm{Gal}(E_\phi/\mathbb{Q})$.

Since $\bar{K}$ is a splitting field for G (see [CuRe, (83.7)]) and $\bar{K}$ is a finite Galois extension of $\mathbb{F}_p$, we may apply Theorem 72 to $k = \mathbb{F}_p$ and $E = \bar{K}$. As before it gives a one to one correspondence between irreducible $\mathbb{F}_p$-representations of G and orbits of the $\mathrm{Gal}(\bar{K}/\mathbb{F}_p)$-action on the set of irreducible $\bar{K}$-representations of G.



From what is computed above it follows that an irreducible rational representation $\rho \in I_p$ gives rise to at least $t_\rho|\mathfrak{I}(\mathfrak{q}/p)|$ different irreducible $\mathbb{F}_p$-representations of G, that correspond to orbits of the $\mathrm{Gal}(\bar{K}/\mathbb{F}_p)$-action on $\overline{Orb(\phi)}$, where ϕ is an irreducible K-representation occurring in decomposition of $K \otimes_{\mathbb{Q}} \rho$. Moreover, Proposition 71 and Theorem 72 guarantee that the sets of corresponding $\mathbb{F}_p$-representations coming from the two non-isomorphic representations $\rho_1, \rho_2 \in I_p$ do not have common elements, because the corresponding sets $\overline{Orb(\phi_1)}$ and $\overline{Orb(\phi_2)}$ have empty intersection, where ϕ_1, ϕ_2 are irreducible K-representations occurring in the decompositions of $K \otimes_{\mathbb{Q}} \rho_1, K \otimes_{\mathbb{Q}} \rho_2$, respectively. Therefore we get

$$\#\{\text{irreducible } \mathbb{F}_p\text{-representations of } G\} \geq \sum_{\rho \in I_p} t_\rho |\mathfrak{I}(\mathfrak{q}/p)| \geq \sum_{\rho \in I_p} t_\rho.$$

□

We have the following corollary from Theorem B.

Corollary 73. *For any finite group G the following inequality holds*

$$P(G) \geq R(G).$$

Proof. Note that

$$w_\rho = \sum_{p \mid \omega_\rho} \#\{\text{prime ideals in } \mathcal{O}_\rho \text{ that divide } p\} = \sum_{p \mid \omega_\rho} t_\rho,$$

$$v_\rho = \sum_{p \mid \, |G|} \#\{\text{prime ideals in } \mathcal{O}_\rho \text{ that divide } p\} = \sum_{p \mid \, |G|} t_\rho,$$

$$P(G) - R(G) = \varepsilon + \sum_{\rho \in X(G)} (w_\rho - v_\rho) = \sum_{p \mid \, |G|} (\#\{\text{irr. } \mathbb{F}_p\text{-rep. of } G\} - \sum_{\substack{\rho \in X(G) \\ p \nmid \omega_\rho}} t_\rho)$$

$$= \sum_{p \mid \, |G|} (\#\{\text{irreducible } \mathbb{F}_p\text{-representations of } G\} - \sum_{\rho \in I_p} t_\rho) \geq 0,$$

where the last inequality holds by Theorem B applied to each summand. □

3.5 The comparison of torsions for G_1-groups

Analogously as to what we have done for the ranks of G_1 we can do the comparison test for the torsion of $G_1(\mathbb{Z}G)$ as computed by Keating and the torsion of $G_1(\mathbb{Z}G)$ as predicted by the HTW-decomposition. We will see that in contrast to the rank the HTW-Conjecture predicts the correct torsion for G_1. Keating's result gives

$$\text{tors}\, G_1(\mathbb{Z}G) = \bigoplus_{\rho \in X(G)} \text{tors}\, U_+(\mathcal{O}_\rho). \tag{3.15}$$

To compute the torsion predicted by the HTW-decomposition we need to determine the tors $G_1(\Lambda_\rho)$ for Λ_ρ a maximal $\mathbb{Z}[1/\omega_\rho]$-order in D_ρ. Our goal will be achieved by combining another result of Keating which allows to determine K_1 of a maximal order in a division algebra with some analysis of local Schur indices.

3.5.1 Schur indices

Let A be a central simple k-algebra. Thus $A \cong M_l(D)$ for some uniquely determined division k-algebra D. The *Schur index of A* denoted by $\text{ind}(A)$ is the index of D, i.e., a square root of $\dim_k(D)$. Let χ be a complex irreducible character of a group G and let K be a field of characteristic 0. The *Schur index of* χ *over* K, which we denote by $m_K(\chi)$, is defined as the Schur index of the simple component $A(\chi, K)$ in the decomposition of KG that corresponds to the character χ.

Another way of thinking about the Schur index of χ over K is the following. Let $K \leq L$, L be a splitting field for G and L/K is a Galois extension. Then the Schur index $m_K(\chi)$ measures to which extend χ fails to be realized over K. Namely, let ϕ be an L-representation that affords the character χ, and let φ be an irreducible K-representation, such that ϕ appears as a constituent in $L \otimes_K \varphi$. Then the Schur index of χ over K is a multiplicity of ϕ in $L \otimes_K \varphi$ (see also Theorem 72). The proof of the next characterizations of the Schur index can be found for instance in [CuRe], Theorem (70.12).

Lemma 74 (Characterizations of Schur index)**.** *Let K be a field of characteristic 0 and let χ be a complex irreducible character of G.*

1. *The Schur index $m_K(\chi)$ is the smallest positive integer such that there exists degree $m_K(\chi)$ extension L of a field of character values $K(\chi)$, such that χ is afforded by some L-representation of G.*

2. *The Schur index $m_K(\chi)$ is the smallest positive integer such that $m_K(\chi)\chi$ is afforded by a $K(\chi)$-representation of G.*

The following references [Hu] Chapter 38 and [CuRe] Section 70 contain a detailed treatment of Schur indices, in particular the equivalence of the definition of $m_K(\chi)$ in terms of the index of the simple component A and the definition in terms of the realization of χ over K can be found there. The first description of a Schur index in Lemma 74 implies that

$$m_K(\chi) = m_{K(\chi)}(\chi). \tag{3.16}$$

Next we will define local indices of a central simple algebra. Let E be a number field with ring of integers R. Each prime ideal P in R gives rise to a P-adic valuation on E. Let A be a central simple E-algebra. Denote by $A_P = E_P \otimes_E A$ the P-adic completion of A. Then A_P is a central simple E_P-algebra.

Definition 75. *The index $m_P(A) = \mathrm{ind}(A_P)$ is called the local Schur index of A at P.*

Let χ be an irreducible complex character of G, $E = \mathbb{Q}(\chi)$ and $A = A(\chi, E)$ be the simple component in EG corresponding to χ. Then clearly A is a central simple E-algebra. In this situation the following result of Benard [Be] guarantees that the local indices $m_P(\chi) := m_{E_P}(\chi) = m_P(A)$ agree at primes of E that lie above the same rational prime p.

Theorem 76 (Benard)**.** *Let $A = A(\chi, E)$ be as above. Let p be a rational prime and P_1, P_2 be primes of E dividing p. Then the algebras A_{P_1} and A_{P_2} have the same index.*

For every prime ideal P in the ring of integers of $E = \mathbb{Q}(\chi)$ lying above p the localization E_P is the composite of $\mathbb{Q}_p$ with E (see e.g. [Se2] Chapter 2, §3)

$$E_P = \mathbb{Q}_p E = \mathbb{Q}_p(\chi).$$

Therefore, we have an immediate corollary from Theorem 76 and equality (3.16) that

$$m_P(\chi) = m_{\mathbb{Q}_p}(\chi) \tag{3.17}$$

for all prime ideals P lying above p. This corollary reduces the computation of local Schur indices over number fields to the determination of indices over the p-adic fields $\mathbb{Q}_p$. The following result due to Benard gives an explicit way to compute $m_{\mathbb{Q}_p}(\chi)$ in terms of the values of χ and the values of an irreducible Brauer character for those characters χ whose p-block has cyclic defect group (see [Be]).

Theorem 77 (Benard's formula)**.** *Let p be a rational prime and χ a complex irreducible character lying in a p-block with cyclic defect group. Let ϕ be an irreducible modular constituent of χ, then*

$$m_{\mathbb{Q}_p}(\chi) = [\mathbb{Q}_p(\chi, \phi) \colon \mathbb{Q}_p(\chi)].$$

Benard's formula implies the following theorem which shows that there are only finitely many rational primes for which local Schur index of A is non-trivial, in particular those primes should divide the order of the group G.

Theorem 78. *Let p be a finite rational prime and χ an irreducible complex character of G. If p does not divide $\omega_\chi = \frac{|G|}{|\ker(\chi)|\chi(1)}$, then $m_{\mathbb{Q}_p}(\chi) = 1$.*

Proof. Let H be the kernel of χ. Then χ may be viewed as an irreducible character of a group $\overline{G} = G/H$. Since p does not divide $|\overline{G}|/\chi(1)$ the character χ belongs to the block of defect 0. Let χ^* be the reduction modulo p of χ. The Brauer-Nesbitt theorem implies that χ^* is an irreducible Brauer character lying in the same p-block as χ. Moreover,

$$\chi(g) = \chi^*(g), \ \forall g \in \overline{G}_{p'}.$$

From this $\mathbb{Q}_p(\chi^*, \chi) = \mathbb{Q}_p(\chi)$ and hence the Benard's formula (Theorem 77) gives

$$m_{\mathbb{Q}_p}(\chi) = [\mathbb{Q}_p(\chi) \colon \mathbb{Q}_p(\chi)] = 1.$$

This finishes the proof, since for the Schur index it does not matter whether we view χ as a character of G or $\overline{G}$. □

3.5.2 SK_1 of maximal orders

The next result reduces the computation of SK_1 of a maximal order in a division algebra to the determination of local Schur indices. For the detailed treatment see §45C in [CuRe2].

Theorem 79. *Let R be a Dedekind ring with field of fractions k an algebraic number field. Let Δ be a maximal R-order in a central division k-algebra D. Then*

$$SK_1(\Delta) \cong \prod_P SK_1(\Delta_P),$$

where the sum ranges over the maximal ideals P of R. Let m_P be the local Schur index of D at P and $q_P = |R/P|$. The group $SK_1(\Delta_P)$ is a cyclic group of order $(q_P^{m_P} - 1)/(q_P - 1)$, which is non-trivial only for finite number of P's with $m_P > 1$. Furthermore, there is an exact sequence

$$1 \to SK_1(\Delta) \to K_1(\Delta) \to U_+(R) \to 1.$$

Now we may apply Theorem 79 to our situation. Let us fix an irreducible rational representation $\rho \in X(G)$. Let $D = D_\rho$, $E = E_\rho = Z(D)$, $\mathcal{O} = \mathcal{O}_\rho$, let Λ be a maximal $\mathbb{Z}[1/\omega_\rho]$-order in D (at the same time it is a maximal $\mathcal{O}[1/\omega_\rho]$-order in D), A a simple component of EG that corresponds to ρ, and χ a character of any of the irreducible complex constituents of ρ. The prime ideals in $\mathcal{O}[1/\omega_\rho]$ are in one-to-one correspondence with prime ideals of $\mathcal{O}$ not dividing ω_ρ. Let P be a prime ideal in $\mathcal{O}[1/\omega_\rho]$ and P' the corresponding prime ideal in $\mathcal{O}$. Let p be the unique rational prime that belongs to P'. Note that since P' does not divide ω_ρ it follows that $p \nmid \omega_\rho$. Since $E_P = E_{P'}$ to determine the structure of $SK_1(\Lambda_P)$ we may work with the local Schur index at P'. By (3.17) we have

$$m_{P'}(D) = m_{\mathbb{Q}_p(\chi)}(A) = m_{\mathbb{Q}_p}(\chi) = 1,$$

where the last equality holds by Theorem 78. Consequently, by Theorem 79 we obtain that $SK_1(\Lambda)$ is a trivial group and

$$K_1(\Lambda) \cong U_+(\mathcal{O}[1/\omega_\rho]).$$

Therefore,

$$\begin{aligned}\bigoplus_{\rho\in X(G)} \text{tors } G_1(\Lambda_\rho) &\cong \bigoplus_{\rho\in X(G)} \text{tors } U_+(\mathcal{O}_\rho[1/\omega_\rho]) \\ &= \bigoplus_{\rho\in X(G)} \text{tors } U_+(\mathcal{O}_\rho) \cong \text{tors } G_1(\mathbb{Z}G),\end{aligned}$$

where the last equation is the result by Keating (3.15). Hence, we have showed that the HTW-decomposition predicts the correct torsion for $G_1(\mathbb{Z}G)$ and hence Theorem D is proved.

3.6 The comparison of ranks for higher degrees

In this section we will present the result due to Kuku which allows us to perform the comparison test for ranks for the HTW-Conjecture in higher degrees. The outcome is that for $n \geq 2$ the HTW-decomposition predicts the correct rank for $G_n(\mathbb{Z}G)$ for all finite groups G. We start with the finiteness result for G_n and SG_n of orders (see [Ku], Theorem 7.1.13).

Theorem 80 (Kuku)**.** *Let R be the ring of integers in a number field K. Let Δ be any R-order in a semisimple K-algebra Σ. Let Γ be a maximal R-order in Σ that contains Δ. Then the following holds.*

1. *For all $n \geq 2$ the map $\text{res}_n \colon G_n(\Gamma) \to G_n(\Delta)$ induced by the restriction of scalars has finite kernel and cokernel. If n is even, then res_n is injective.*

2. *$G_n(\Delta)$ is finitely generated for all $n \geq 1$.*

3. *For all $n \geq 2$ the group $SG_n(\Delta)$ is finite. If n is even, then $SG_n(\Delta) = 0$.*

In particular Theorem 80 implies that if Γ is a maximal R-order in KG that contains RG, then

$$\text{rank } G_n(RG) = \text{rank } G_n(\Gamma) = \sum_i \text{rank } G_n(\Gamma_i), \ \forall n \geq 2,$$

where the sum runs over the simple components of Σ and $\Gamma_i \subseteq \Sigma_i$ denote a maximal order in a simple component Σ_i. Note that for degree $n = 1$ the situation is different and we don't have such an equality of ranks. Let Λ_i denotes a maximal R-order in D_i. Since

$$G_n(\Gamma_i) \cong G_n(\Lambda_i)$$

to conclude that for $n \geq 2$ the HTW-Conjecture predicts the correct rank for $G_n(\mathbb{Z}G)$ it is enough to check that inverting ω_i in Λ_i has no effect on the rank of G_n. This can be done by applying the following finiteness result of Kuku on G_n of a finite ring to the localization sequence (see [Ku], Theorem 7.1.12).

Theorem 81. *Let T be a finite ring with 1. Then for all $n \geq 1$ it holds*

1. *$K_n(T)$ is a finite group.*
2. *$G_n(T)$ is a finite group. If n is even then $G_n(T)$ is a trivial group.*

Let us consider the localization sequence

$$\ldots \to G_n(\Lambda_i/\omega_i\Lambda_i) \to G_n(\Lambda_i) \to G_n(\Lambda_i\Big[\frac{1}{\omega_i}\Big]) \to G_{n-1}(\Lambda_i/\omega_i\Lambda_i) \to \ldots.$$

The ring $\Lambda_i/\omega_i\Lambda_i$ is finite and therefore for $n \geq 2$ Theorem 81 gives that the groups $G_n(\Lambda_i/\omega_i\Lambda_i)$ and $G_{n-1}(\Lambda_i/\omega_i\Lambda_i)$ are finite. Hence,

$$\text{rank } G_n(\Lambda_i) = \text{rank } G_n(\Lambda_i\Big[\frac{1}{\omega_i}\Big]) \text{ for all } n \geq 2.$$

Therefore for $n \geq 2$ it holds

$$\text{rank } G_n(\mathbb{Z}G) = \text{rank } G_n(\Gamma) = \sum_{i\in X(G)} \text{rank } G_n(\Lambda_i) = \sum_{i\in X(G)} \text{rank } G_n(\Lambda_i\Big[\frac{1}{\omega_i}\Big]),$$

which confirms the HTW-Conjecture for ranks in degree $n \geq 2$, and together with the result of Section 3.2 implies Theorem C.

3.7 Jacobinski conductor formula

Let G be a finite group of order n. Let R be a Dedekind ring with field of fractions F and assume that $\text{char}F$ does not divide n. Let $A = FG$. The following result (see e.g. [Re], Theorem (41.1)) provides information about maximal orders in A containing RG.

Lemma 82. *Let Γ be any R-order in A containing RG. Then*

$$RG \subseteq \Gamma \subseteq n^{-1}RG.$$

Proof. Let us fix an F-basis of A consisting of the elements of G. For every element $a \in A$ consider its linear action a_l on A given by the multiplication with a on the left. Then for each $g \in G$ the trace of g_l is zero unless $g = e$, in which case the trace equals n. Since every $x = \sum_{g\in G} \lambda_g g \in \Gamma$ is integral over R its characteristic polynomial $\chi_{A/K}x$ has coefficients in R and hence $\text{Tr}(x) \in R$. For every $g \in G$ it holds

$$\text{Tr}(xg^{-1}) = n\lambda_g \in R,$$

because $G \subseteq \Gamma$. This implies that $n\Gamma \subseteq RG$, which finishes the proof. □

As a corollary of Lemma 82 we have that the order RG is a maximal R-order in A if and only if n is invertible in R. Suppose that RG is a maximal order and n is not invertible in R. Consider a subring Λ in A generated by RG and an idempotent $e = n^{-1}\sum_{g\in G} g$. It is easy to see that Λ is a $\mathbb{Z}$-order in A that properly contains RG, which contradicts the maximality of RG. The implication in the opposite direction is immediate from Lemma 82. In particular $\mathbb{Z}G$ is not a maximal order in $\mathbb{Q}G$ unless G is a trivial group. For the rest of this subsection let Γ be a maximal R-order in A containing RG. Define the *left* and *right conductors* of Γ into RG as follows

$$(\Gamma : RG)_l = \{x \in A \colon x\Gamma \subseteq RG\},$$

$$(\Gamma : RG)_r = \{x \in A \colon \Gamma x \subseteq RG\}.$$

Note that the right conductor is the largest left Γ-submodule in RG. From Lemma 82 we see that the element n belongs to both $(\Gamma : RG)_l$ and $(\Gamma : RG)_r$. The following result of Jacobinski [Ja] refines the lemma and gives an explicit description of the conductors. We present the proof here which follows [Re, Section 41]. Let $A = \bigoplus_{i=1}^k A_i$ be the decomposition of A into simple algebras. Then $\Gamma = \sum_{i=1}^k \Gamma_i$, where Γ_i is a maximal R-order in A_i. Let tr_i denote the reduced trace from A_i to F. The *inverse different* of Γ_i with respect to tr_i is given by

$$\mathcal{D}_i^{-1} := \{x \in A_i \colon \mathrm{tr}_i(x\Gamma_i) \subseteq R.\}$$

Theorem 83 (Jacobinski)**.**

$$(\Gamma : RG)_l = (\Gamma : RG)_r = \sum_{i=1}^k \frac{n}{n_i}\mathcal{D}_i^{-1}.$$

Proof. Consider the bilinear form $\tau \colon A \times A \to K$ given by the trace $\tau(x, y) = \mathrm{Tr}_{A/F}(xy)$ and fix an F-basis of A given by the elements of G. As we remarked in the proof of Lemma 82 for $g, h \in G$ it holds that

$$\tau(g, n^{-1}h) = \delta_{gh},$$

and hence $\{n^{-1}g, g \in G\}$ is a dual basis to the chosen one with respect to τ. With every full R-lattice Λ in A we may associate a dual R-lattice given by

$$\tilde{\Lambda} = \{a \in A \mid \tau(a, \Lambda) \subseteq R\}.$$

It is easy to check that the map $\Lambda \to \tilde{\Lambda}$ is an inclusion reversing bijection from the set of full left R-lattices to the set of full right R-lattices in A, which satisfies $\tilde{\tilde{\Lambda}} = \Lambda$ and takes any R-free lattice to the R-free lattice generated by the dual basis. From this we immediately conclude that

$$\tilde{RG} = \bigoplus_{g\in G} Rn^{-1}g = n^{-1}RG.$$

Since $\Lambda = (\Gamma : RG)_r$ is the maximal left Γ-module in RG we obtain that its dual $\tilde{\Lambda}$ is the smallest right Γ-module containing $\tilde{RG}$. Therefore,

$$\tilde{\Lambda} = \tilde{RG} \cdot \Gamma = n^{-1} RG \cdot \Gamma = n^{-1}\Gamma, \ \Lambda = n\tilde{\Gamma}.$$

To describe $\tilde{\Gamma}$ we write every $X \in A$ in the from $x = \sum_i x_i$, where $x_i \in A_i$, and use the fact that the trace can be expressed in terms of reduced traces as follows

$$\mathrm{Tr}(x) = \sum_{i=1}^{k} n_i \mathrm{tr}_i(x_i),$$

which implies that

$$\tilde{\Gamma} = \{x \in A \mid n_i \mathrm{tr}_i(x_i\Gamma) \subseteq R, \ 1 \le i \le k\} = \bigoplus_{i=1}^{k} n_i^{-1}\mathcal{D}_i^{-1},$$

$$(\Gamma : RG)_r = \bigoplus_{i=1}^{k} \frac{n}{n_i}\mathcal{D}_i^{-1}.$$

The same argument works for the left conductor. □

Now we focus on the situation $R = \mathbb{Z}$ and $A = \mathbb{Q}G$. Let $A = \bigoplus_{\rho \in X(G)} A_\rho$ be the decomposition of A into simple components, where $X(G)$ is the set of irreducible representations of G over $\mathbb{Q}$. For each $\rho \in X(G)$ the associated simple component A_ρ is determined by the corresponding central primitive idempotent in $\mathbb{Q}G$ given by

$$e_\rho = \frac{1}{n}\sum_{g \in G} \chi_\rho(g^{-1})g.$$

Then $A_\rho = A \cdot e_\rho$ and let pr_ρ denote the projection of A into the component A_ρ, which is given by the multiplication by e_ρ. Let $\omega_\rho = \frac{n}{k_\rho d_\rho}$, $\rho \in X(G)$ be the numbers appearing in the HTW-decomposition. Note that the number $n_\rho = [A_\rho : Z(A_\rho)]^{1/2}$ that appears in the Jacobinski formula coincides with the dimension d_ρ of any of the complex constituents of the representation ρ complexified. This is true due to the following observation. Denote by E_ρ the center of A_ρ and let $A_\rho \cong M_{m_\rho}(D_\rho)$. Then

$$\mathbb{C} \otimes_{\mathbb{Q}} A_\rho \cong \mathbb{C} \otimes_{\mathbb{Q}} M_{m_\rho}(D_\rho) \cong (\mathbb{C} \otimes_{\mathbb{Q}} E_\rho) \otimes_{E_\rho} M_{m_\rho}(D_\rho),$$

$$\mathbb{C} \otimes_{\mathbb{Q}} E_\rho \cong \bigoplus_{[E_\rho:\mathbb{Q}]} \mathbb{C},$$

$$\mathbb{C} \otimes_{E_\rho} M_{m_\rho}(D_\rho) \cong M_{m_\rho}(M_{[D_\rho:E_\rho]^{1/2}}(\mathbb{C})).$$

Hence the dimension of any complex constituent of $\mathbb{C} \otimes_{\mathbb{Q}} \rho$ equals $m_\rho [D_\rho : E_\rho]^{1/2}$ and consequently

$$n_\rho^2 = [M_{m_\rho}(D_\rho) : E_\rho] = m_\rho^2 [D_\rho : E_\rho] = d_\rho^2,$$

which proves the claim. The following lemma shows how the numbers ω_ρ and the Jacobinski conductor formula are related.

Lemma 84. *For every $\rho \in X(G)$ the images of $\mathbb{Z}[1/\omega_\rho]G$ and $\mathbb{Z}[1/\omega_\rho] \otimes_{\mathbb{Z}} \Gamma$ in the factor A_ρ under the projection pr_ρ coincide.*

Proof. Let $\rho \in X(G)$ be fixed and let $H < G$ be the kernel of the representation ρ. Denote by $q\colon \mathbb{Q}G \to \mathbb{Q}[G/H]$ the homomorphism of group algebras induced by the quotient map $G \to G/H$. We denote the restriction $q_{|_{\mathbb{Z}G}}\colon \mathbb{Z}G \to \mathbb{Z}[G/H]$ by the same letter q. Let

$$\mathbb{Q}[G/H] = \bigoplus_{\rho' \in X(G/H)} A'_{\rho'}$$

be the decomposition of $\mathbb{Q}[G/H]$ into simple algebras. The representation ρ may be viewed as a representation of G/H, since the elements of H act trivially, and it is clearly an irreducible rational representation. Denote the corresponding simple component of $\mathbb{Q}[G/H]$ by A'_ρ. We claim that $q(A_\rho) = A'_\rho$ and $q_{|_{A_\rho}}\colon A_\rho \to A'_\rho$ is an isomorphism of algebras. To see this recall that $A_\rho = \mathbb{Q}G \cdot e_\rho$ and $A'_\rho = \mathbb{Q}[G/H] \cdot e'_\rho$, where e'_ρ denotes the central primitive idempotent in $\mathbb{Q}[G/H]$ associated to $\rho \in X(G/H)$.

$$e_\rho = \frac{1}{n} \sum_{\bar{g} \in G/H} \sum_{h \in H} \chi_\rho(h^{-1}\bar{g}^{-1})\bar{g}h = \frac{1}{n} \sum_{\bar{g} \in G/H} \big(\chi_\rho(\bar{g}^{-1}) \sum_{h \in H} \bar{g}h\big),$$

$$q(e_\rho) = \frac{|H|}{n} \sum_{\bar{g} \in G/H} \chi_\rho(\bar{g}^{-1})\bar{g} = e'_\rho.$$

From this it is immediate that $q(A_\rho) = A'_\rho$ and since A_ρ is a simple algebra we obtain that $q_{|_{A_\rho}}\colon A_\rho \to A'_\rho$ is an isomorphism. Let $\Gamma' = q(\Gamma)$, then Γ' is a maximal $\mathbb{Z}$-order in $\mathbb{Q}[G/H]$ that contains $\mathbb{Z}[G/H]$, and $\Gamma' = \oplus_{\rho' \in X(G/H)} \Gamma'_{\rho'}$, where $\Gamma'_{\rho'}$ is a maximal $\mathbb{Z}$-order in $A'_{\rho'}$. Since the restriction of q induces an isomorphism from A_ρ to A'_ρ we have the following commutative diagram

$$\begin{array}{ccc}
\mathbb{Z}G & \xrightarrow{\;q\;} & \mathbb{Z}[G/H] \\
\downarrow{\scriptstyle \mathrm{pr}_\rho} & & \downarrow{\scriptstyle \mathrm{pr}'_\rho} \\
\mathbb{Z}G \cdot e_\rho & \xrightarrow[\cong]{\;q\;} & \mathbb{Z}[G/H] \cdot e'_\rho \\
\hookdownarrow & & \hookdownarrow \\
\Gamma_\rho & \xrightarrow[\cong]{\;q\;} & \Gamma'_\rho .
\end{array}$$

By the Jacobinski conductor formula and the remark made above that $n_\rho = d_\rho$ we obtain

$$\frac{|G/H|}{d_\rho} \Gamma'_\rho \subseteq \mathbb{Z}[G/H] \cdot e'_\rho,$$

and therefore,

$$\omega_\rho \Gamma_\rho = \frac{|G/H|}{d_\rho} \Gamma_\rho \subseteq \mathbb{Z}G \cdot e_\rho.$$

And finally, since $\mathbb{Z}G \cdot e_\rho \subseteq \Gamma_\rho$ we conclude that

$$\mathbb{Z}[1/\omega_\rho] \otimes_{\mathbb{Z}} \Gamma_\rho = \mathbb{Z}[1/\omega_\rho]G \cdot e_\rho,$$

which finishes the proof. □

3.8 The known results for higher G-groups

In the same paper [HTW] where the conjecture was stated for the first time Hambleton, Taylor and Williams gave a short proof of the HTW-decomposition in the case when G is a finite nilpotent group. Here we provide a more detailed treatment of their proof following the paper [HTW]. The proof goes in two steps. Firstly, the decomposition is established for p-groups. For such a group it is possible to define a map $G_n(\mathbb{Z}G) \to \bigoplus_{i\in X(G)} G_n(\Gamma_i[1/\omega_i])$ using the extension of scalars approach with some modifications for the summand corresponding to the trivial representation. Then the HTW-decomposition for nilpotent groups is derived from the HTW-decomposition for p-groups.

Let $j\colon R \to RG$ be the natural inclusion. Since G is a finite group j induces a restriction map from the category of finitely generated RG-modules to the category of finitely generated R-modules

$$j^*\colon \mathrm{Mod}_{fg}(RG) \to \mathrm{Mod}_{fg}(R)$$

and for every $n \geq 0$ we have the corresponding map

$$\mathrm{res}_n\colon G_n(RG) \to G_n(R).$$

On the other hand, every finitely generated R-module M may be turned into an RG-module, where the elements of G act trivially

$$e_*\colon \mathrm{Mod}_{fg}(R) \to \mathrm{Mod}_{fg}(RG).$$

This functor also induces a homomorphism on G_n which we denote by e_n

$$e_n\colon G_n(R) \to G_n(RG).$$

Clearly, the composition $j^*e_*\colon \mathrm{Mod}_{fg}(R) \to \mathrm{Mod}_{fg}(R)$ is the identity functor and thus $G_n(R)$ is a direct summand in $G_n(RG)$.

Lemma 85. *Let G be a p-group and let R be a noetherian ring. Then the following sequence is split exact*

$$0 \longrightarrow G_n(RG) \xrightarrow{\mathrm{loc}_n \oplus \mathrm{res}_n} G_n(R[1/p]G) \oplus G_n(R) \xrightarrow{\mathrm{res}'_n - \mathrm{loc}'_n} G_n(R[1/p]) \longrightarrow 0.$$

Proof. Consider the localization sequence associated to the localization $RG \to R[1/p]G$

$$\ldots \longrightarrow K_n(\mathcal{M}_p(RG)) \longrightarrow G_n(RG) \xrightarrow{\mathrm{loc}_n} G_n(R[1/p]G) \longrightarrow K_{n-1}(\mathcal{M}_p(RG)) \longrightarrow \ldots$$

where $\mathcal{M}_p(R)$ denotes the category of finitely generated p-torsion RG-modules, i.e., those finitely generated modules for which every element is annihilated by some power of p. If $M \in \mathcal{M}_p(R)$ then there is a finite filtration of M with the quotients annihilated by p. Thus without loss of generality we may assume $p \cdot M = 0$ and therefore M is an R/pR-module. The same way as we proved the Proposition 13 we can show that if M is non-zero then for a p-group G the set M^G of elements in M fixed by G is non-empty. Hence M has a finite filtration with quotients given by the RG-modules with the trivial G-action. The full subcategory of $\mathcal{M}_p(R)$ consisting of the modules with the trivial G-action is an abelian subcategory, therefore by the Devissage Theorem $e_{*|_{\mathcal{M}_p(R)}}$ induces an isomorphism of K-groups

$$h_n\colon K_n(\mathcal{M}_p(R)) \xrightarrow{\cong} K_n(\mathcal{M}_p(RG)),$$

where the inverse map is induced by $j^*_{|_{\mathcal{M}_p(RG)}}$. Combining the localization sequence for $R \to R[1/p]$ with the localization sequence for $RG \to R[1/p]G$ we get the following commutative diagram

$$\begin{array}{ccccccccccc}
\dots \longrightarrow & K_n(\mathcal{M}_p(R)) & \longrightarrow & G_n(R) & \xrightarrow{\mathrm{loc}'_n} & G_n(R[1/p]) & \longrightarrow & K_{n-1}(\mathcal{M}_p(R)) & \longrightarrow \dots \\
& {\scriptstyle h_n}\downarrow{\scriptstyle \cong} & & {\scriptstyle e_n}\downarrow\uparrow{\scriptstyle \mathrm{res}_n} & & {\scriptstyle e'_n}\downarrow\uparrow{\scriptstyle \mathrm{res}'_n} & & {\scriptstyle h_{n-1}}\downarrow{\scriptstyle \cong} & \\
\dots \longrightarrow & K_n(\mathcal{M}_p(RG)) & \xrightarrow{\alpha_n} & G_n(RG) & \xrightarrow{\mathrm{loc}_n} & G_n(R[1/p]G) & \longrightarrow & K_{n-1}(\mathcal{M}_p(RG)) & \longrightarrow \dots
\end{array} \tag{3.18}$$

Note that $G_n(RG) \cong G_n(R) \oplus X_n$ for some abelian group X_n with a projection $G_n(RG) \to G_n(R)$ given by res_n, and similarly $G_n(R[1/p]G) \cong G_n(R[1/p]) \oplus Y_n$ for some abelian group Y_n with a projection given by res'_n. Now it is easy to see that the homomorphism

$$\mathrm{loc}_n \oplus \mathrm{res}_n\colon G_n(RG) \to G_n(R[1/p]G) \oplus G_n(R)$$

is injective, since the kernel of loc_n coincides with the image of α_n, which is contained in the image of $G_n(R)$ under e_n. But then if the element in the image of e_n is mapped to zero under res_n it must be zero itself, which finishes the proof of injectivity. From the commutativity of the middle square in the diagram (3.18) it immediately follows that $\mathrm{im}\,(\mathrm{loc}_n \oplus \mathrm{res}_n) = \ker(\mathrm{res}'_n - \mathrm{loc}'_n)$. The surjectivity of $\mathrm{res}'_n - \mathrm{loc}'_n$ is obvious from the surjectivity of the res'_n. Hence we have showed that the sequence

$$0 \longrightarrow G_n(RG) \xrightarrow{\mathrm{loc}_n \oplus \mathrm{res}_n} G_n(R[1/p]G) \oplus G_n(R) \xrightarrow{\mathrm{res}'_n - \mathrm{loc}'_n} G_n(R[1/p]) \longrightarrow 0 \tag{3.19}$$

is exact. The homomorphism $e'_n \oplus 0\colon G_n(R[1/p]) \to G_n(R[1/p]G) \oplus G_n(R)$ gives the desired splitting of the sequence (3.19), which finishes the proof. □

As a corollary of the Lemma 85 we obtain the HTW-decomposition for p-groups. Given a finite p-group G and an irreducible rational representation ρ of G put

$$\Gamma_\rho = \begin{cases} \text{a maximal } \mathbb{Z}[1/p]\text{-order in } D_\rho, & \text{if } \rho \text{ is not trivial} \\ \mathbb{Z}, & \text{if } \rho \text{ is trivial.} \end{cases}$$

Theorem 86. *Let R be a noetherian ring and G a finite p-group for some prime p. Then*

$$G_n(RG) \cong \bigoplus_{\rho \in X(G)} G_n(R \otimes_{\mathbb{Z}} \Gamma_\rho),$$

where $X(G)$ denotes the set of irreducible rational representations of G.

Proof. Since for a p-group G its order is invertible in the ring $\mathbb{Z}[1/p]$ we know that $\mathbb{Z}[1/p]G$ is a maximal $\mathbb{Z}[1/p]$-order in $\mathbb{Q}G$. Therefore, it decomposes into the product

$$\mathbb{Z}[1/p]G \cong \prod_{\rho \in X(G)} \Lambda_\rho,$$

where Λ_ρ is a maximal $\mathbb{Z}[1/p]$-order in the corresponding factor $M_{n_\rho}(D_\rho)$. Since G_n preserves products we immediately have

$$G_n(R[1/p]G) \cong \bigoplus_{\rho \in X(G)} G_n(R \otimes_{\mathbb{Z}} \Lambda_\rho).$$

The image of the splitting map $e_n \colon G_n(R[1/p]) \to G_n(R[1/p]G)$ is a direct summand of $G_n(R[1/p]G)$ that corresponds to the trivial rational representation $G_n(R \otimes_{\mathbb{Z}} \mathbb{Z}[1/p])$. Hence by the Lemma 85 $G_n(\mathbb{Z}G)$ is isomorphic to a direct sum of G_n of maximal $\mathbb{Z}[1/p]$-orders Λ_ρ's corresponding to nontrivial irreducible rational representations and $G_n(\mathbb{Z})$, which corresponds to the trivial representation. Since Λ_ρ is Morita equivalent to a maximal $\mathbb{Z}[1/p]$-order in D_ρ by the Morita invariance property of G-theory we obtain

$$G_n(RG) \cong \bigoplus_{\rho \in X(G)} G_n(R \otimes_{\mathbb{Z}} \Gamma_\rho),$$

which finishes the proof. □

Definition 87. *We say that for a group G the HTW-decomposition holds if for every noetherian ring R and every $n \geq 0$ the groups $G_n(RG)$ and $\bigoplus_{\rho \in X(G)} G_n(R \otimes_{\mathbb{Z}} \Gamma_\rho)$ are isomorphic, where Γ_ρ is a maximal $\mathbb{Z}[1/\omega_\rho]$-order in D_ρ.*

The following observation ([HTW], Remark 11) allows us to extend the class for which the HTW-decomposition holds.

Proposition 88. *Let H and H' be finite groups of relatively prime order for which the HTW-decomposition holds. Then the HTW-decomposition holds for $H \times H'$. In particular, the HTW-decomposition holds for all finite nilpotent groups.*

Proof. Let R be a ring, then $R[H \times H'] \cong RH[H']$ and therefore by the HTW-decomposition for the group H' with a coefficient ring RH we obtain

$$\begin{aligned} G_n(R[H \times H']) &\cong \bigoplus_{\rho' \in X(H')} G_n(RH \otimes_{\mathbb{Z}} \Gamma_{\rho'}) \\ &\cong \bigoplus_{\rho' \in X(H')} G_n(R \otimes_{\mathbb{Z}} \Gamma_{\rho'}[H]) \\ &\cong \bigoplus_{\substack{\rho' \in X(H') \\ \rho \in X(H)}} G_n(R \otimes_{\mathbb{Z}} \Gamma_{\rho'} \otimes_{\mathbb{Z}} \Gamma_{\rho}). \end{aligned} \tag{3.20}$$

If α is an irreducible rational representation of $H \times H'$, then there exist unique up to isomorphism irreducible representations $\rho \in X(H)$ and $\rho' \in X(H')$ such that α is a direct summand of $\rho \otimes_{\mathbb{Q}} \rho'$. This is true due to the following observation. By Theorem 72 every irreducible rational representation $\rho \in X(H)$ is obtained from the Galois orbit of some irreducible complex representation φ of H

$$\rho \cong m_{\mathbb{Q}}(\varphi) \sum_{\phi \in \mathrm{Orb}(\varphi)} \phi,$$

where $m_{\mathbb{Q}}(\varphi)$ is the Schur index and $\mathrm{Orb}(\varphi)$ denotes the orbit of ϕ under the action of a Galois group $\mathrm{Gal}(\mathbb{Q}(\xi_{|H|})/\mathbb{Q})$. Furthermore, the set of isomorphisms classes of irreducible complex representations of $H \times H'$ is given by

$$\mathrm{Irr}_{\mathbb{C}}(H \times H') = \{\phi \otimes_{\mathbb{C}} \phi' \mid \phi \in \mathrm{Irr}_{\mathbb{C}}(H),\ \phi' \in \mathrm{Irr}_{\mathbb{C}}(H')\}.$$

Hence, for any $\rho \in X(H)$ and $\rho' \in X(H')$ it holds

$$\rho \otimes_{\mathbb{Q}} \rho' \cong m_{\mathbb{Q}}(\varphi) m_{\mathbb{Q}}(\varphi') \sum_{\substack{\phi \in \mathrm{Orb}(\varphi) \\ \phi' \in \mathrm{Orb}(\varphi')}} \phi \otimes_{\mathbb{C}} \phi'.$$

For each $\phi \otimes_{\mathbb{C}} \phi'$ appearing as a summand in $\rho \otimes_{\mathbb{Q}} \rho'$ every element from its orbit under the action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\xi_{|H \times H'|})/\mathbb{Q})$ also appears as a direct summand in $\rho \otimes_{\mathbb{Q}} \rho'$. Since $\rho \otimes_{\mathbb{Q}} \rho'$ is a rational representation and it contains as a direct summand the orbit of $\phi \otimes \phi'$, which is a representation with rational character values, we conclude that $\rho \otimes \rho'$ contains as a summand an irreducible rational representation that corresponds to $\phi \otimes \phi'$. From this we see that every irreducible rational representation of $H \times H'$ is contained as a constituent in the uniquely determined representation of the form $\rho \otimes_{\mathbb{Q}} \rho'$ with $\rho \in X(H),\ \rho' \in X(H')$.

Since $\mathbb{Q}(\xi_{|H|})$ and $\mathbb{Q}(\xi_{|H'|})$ are splitting fields for H and H', respectively, we obtain that in the situation when the orders of the groups H and H' are relatively prime the Galois group

$$\mathrm{Gal}(\mathbb{Q}(\xi_{|H \times H'|})/\mathbb{Q}) \cong \left(\mathbb{Z}/(|H| \cdot |H'|) \cdot \mathbb{Z}\right)^{\times}$$

decomposes into the product of the Galois groups

$$\mathrm{Gal}_H := \mathrm{Gal}(\mathbb{Q}(\xi_{|H|})/\mathbb{Q}) \cong \left(\mathbb{Z}/|H|\cdot\mathbb{Z}\right)^{\times}$$

$$\mathrm{Gal}_{H'} := \mathrm{Gal}(\mathbb{Q}(\xi_{|H'|})/\mathbb{Q}) \cong \left(\mathbb{Z}/|H'|\cdot\mathbb{Z}\right)^{\times}.$$

This yields that the orbit of any irreducible representation $\varphi\otimes_{\mathbb{C}}\varphi'$ of $H\times H'$ under the action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\xi_{|H\times H'|})/\mathbb{Q})$ equals

$$\mathrm{Orb}(\varphi\otimes_{\mathbb{C}}\varphi') = \{\phi\otimes_{\mathbb{C}}\phi' \mid \phi\in\mathrm{Orb}_{\mathrm{Gal}_H}(\varphi),\ \phi'\in\mathrm{Orb}_{\mathrm{Gal}_{H'}}(\varphi')\}.$$

Hence, if $(|H|,|H'|)=1$ then for every irreducible rational representation α of $H\times H'$ there exist a positive integer r and uniquely determined $\rho\in X(H)$, $\rho'\in X(H')$ such that

$$r\cdot\alpha\cong\rho\otimes_{\mathbb{Q}}\rho'.$$

Furthermore, Γ_α and $\Gamma_\rho\otimes_{\mathbb{Z}}\Gamma_{\rho'}$ are both $\mathbb{Z}[1/\omega_\alpha]$-maximal orders in Morita equivalent division algebras. □

Concluding remarks.

In addition to what was done in Section 3.4 it is easy to compute both values $P(G), R(G)$ using the provided description. For $G=\mathrm{SL}(2,\mathbb{F}_3)$ these are $P(G)=6, R(G)=5$. Using the computer algebra system GAP [GAP] we computed the difference $P(G)-R(G)$ for all finite groups of order less than 200.

If it is possible to correct the HTW-decomposition following the same pattern but choosing different numbers ω_ρ to be inverted, then these new numbers ω_ρ should satisfy the following relation

$$\sum_{\rho\in X(G)}\#\{\text{prime ideals in } \mathcal{O}_\rho \text{ that divide } \omega_\rho\} - \sum_{\rho\in X(G)} v_\rho + \varepsilon = 0.$$

The inequality $P(G)\geq R(G)$ obtained in Corollary 73 leads to the natural guess that the weaker version of the HTW-Conjecture might hold. Namely, instead of asking for the isomorphism in the HTW-decomposition, one might conjecture that there exists either an injective homomorphism $G_n(\mathbb{Z}G)\hookrightarrow\bigoplus_{\rho\in X(G)}G_n(\Lambda_\rho)$ or a surjective homomorphism $\bigoplus_{\rho\in X(G)}G_n(\Lambda_\rho)\twoheadrightarrow G_n(\mathbb{Z}G)$. Since there is no map known between $G_n(\mathbb{Z}G)$ and $\bigoplus_{\rho\in X(G)}G_n(\Lambda_\rho)$ that would work for all finite groups G we have to consider both of these options.

Bibliography

[AG] M. Auslander, O. Goldman, Maximal orders, Transactions of the American Mathematical Society, Vol. 97 (1), pp. 1-24, 1960.

[Ba] H. Bass, Lenstra's calculation of $G_0(R\pi)$, and applications to Morse-Smale diffeomorphisms, Springer Lecture Notes 88, pp. 287-318, 1981.

[BaRo] L. Babai, L. Ronyai, Computing irreducible representationns of finite groups, Mathematics of computation, vol. 55, 192, pp. 705-722, 1990.

[Be] M. Benard, Schur indices and cyclic defect groups, Ann. of Math., pp. 283-304, 1976.

[Be1] M. Benard, The Schur subgroup I, Journal of Algebra 22, pp. 374-377, 1972.

[B] S. D. Berman, The number of irreducible representations of a finite group over an arbitrary field, Dokl. Akad. Nauk SSSR 106, pp. 67-76, 1956.

[Ber] A. J. Berrick, An approach to Algebraic K-theory, Research Notes in Math., vol. 56, Pitman, 1986.

[BG] D. J. Benson, K. L. Goodearl, Periodic flat modules, and flat modules for finite groups, Pacific Journal of Mathematics, vol. 196 (1), pp. 45-67, 2000.

[BMS] H. Bass, J. W. Milnor, J.-P. Serre, Solution of the congruence subgroup problem for $\mathrm{SL}_n(n \geq 3)$ and $Sp_{2n}(n \geq 2)$, Publications mathématiques de l'I.H.É.S., tome 33, pp. 59-137, 1967.

[Bo] C. Bonnafé, Representations of the group $\mathrm{SL}(2, \mathbb{F}_q)$, Algebra and Applications 13, Springer, London, 2011.

[BrNe] R. Brauer, C. Nesbitt, On the modular characters of groups, Ann. of Math. 42, no. 2, pp. 556-590, 1941.

[CuRe] C.W. Curtis, I. Reiner, Representation theory of finite groups and associative algebras, Wiley, 1962.

[CuRe1] C.W. Curtis, I. Reiner, Methods of Representation Theory: With Applications to Finite Groups and Orders, vol. 1, Wiley, 1990.

[CuRe2] C.W. Curtis, I. Reiner, Methods of Representation Theory: With Applications to Finite Groups and Orders, vol. 2, Wiley, 1987.

[FS] J. Franks, M. Shub, The existence of Morse-Smale diffeomorphisms, Topology, Vol. 20, pp. 273-290, 1981.

[FeTh] W. Feit, J. G. Thompson, Solvability of groups of odd order, Pacific Journal of Mathematics 13, pp. 775-1029, 1963.

[Ge] S. Gersten, K-theory of free rings, Comm. Alg. 1, pp. 39-64, 1974.

[GG] H. Gillet, D. Grayson, The loop space of the Q-construction, Ill. J. of Math. 11, pp. 574-597, 1987.

[Gr] D. Grayson, SK_1 of an interesting principal ideal domain, Journal of Pure and Applied Algebra 20, pp. 157-163, 1981.

[HaSc] H. Hasse, O. Schilling, Die Normen aus einer normalen Divisionsalgebra, J. reine angew. Math. 174, pp. 248-252, 1936.

[HeRe] A. Heller, I. Reiner, Grothendieck groups of orders in semisimple algebras, Trans. Amer. Math. Soc. 112, pp. 344-355, 1964.

[HeRe1] A. Heller, I. Reiner, Grothendieck groups of integral group rings, Illinois J. Math. 9 (2), pp. 349-360, 1965.

[HTW] I. Hambleton, L. R. Taylor, E. B. Williams, On $G_n(RG)$ for G a finite nilpotent group, J. of Alg. 116, pp. 466-470, 1988.

[Hu] B. Huppert, Character theory of finite groups, de Gruyter, 1998.

[Ja] H. Jacobinski, On extensions of lattices, Michigam Math. J., 13, pp. 471-475, 1966.

[Je] E. Jespers, Orders and generic constructions of units, De Gruyter Textbook, 2016.

[Ke] M. E. Keating, G_1 of an integral group ring, J. London Math. Soc. (2), 14, pp. 148-152, 1976.

[Ke2] M. E. Keating, Values of tame symbols on division algebras, J. London Math. Soc. (2), 14, pp. 25-30, 1976.

[Ku] A. Kuku, Representation Theory and Higher Algebraic K-Theory, Chapman and Hall, London, 2007.

[La] T. Y. Lamm, A first course in noncommutative rings, Springer, 2001.

[La2] T. Y. Lam, Lectures on modules and rings, Springer, 1999.

[La3] T. Y. Lam, Induction theorems for Grothendieck groups and Whitehead groups of finite groups, Ann. Ec. Norm. Sup. 1, pp. 91-148, 1968.

[LaWe] R. Laubenbacher, D. L. Webb, G_0 of integral group rings for groups with cyclic Sylow subgroups, Contemporary Math 126, pp. 97-111, 1992.

[Le] H. W. Lenstra, Grothendieck groups of abelian group rings, J. Pure Appl. Algebra 20, pp. 173-193, 1981.

[Lü] W. Lück, L^2-Invariants: Theory and Applications to Geometry and K-Theory, Springer-Verlag, 2002.

[Mil] J. W. Milnor, Introduction to algebraic K-theory, Annals of Mathematics Studies, vol. 72, Princeton University Press, 1971.

[Na] G. Navarro, Characters and blocks of finite groups, London Math. Soc. Lecture Notes Series, Vol. 250, Cambridge, 1998.

[Ne] J. Neukirch, Algebraic number theory, Springer, Berlin, 1999.

[Q] D. Quillen, Higher algebraic K-theory I, Algebraic K-theory, I: Higher K-theories (Proc. Conf., Battelle Memorial Inst., Seattle, Wash., 1972), Lecture Notes in Math. 341, Springer, Berlin, pp. 85-147, 1973.

[R] J. Rosenberg, Algebraic K-theory and its applications, Springer, 1994.

[Re] I. Reiner, Maximal orders, Academic Press, 1975.

[S] J. Semikina, A solvable counterexample to the Hambleton-Taylor-Williams Conjecture, arXiv:1610.01510v2.

[Se] J.-P. Serre, Linear representations of finite groups, Graduate Texts in Mathematics 42, Springer, 1977.

[Se2] J.-P. Serre, Local fields, Springer-Verlag, 1979.

[Se3] J.-P. Serre, Local algebra, Springer-Verlag, 2000.

[Sr] V. Srinivas, Algebraic K-theory, Progress in Math., vol. 90, Birkhäuser Basel, 1991.

[SwEv] R. G. Swan, E. G. Evans, K-theory of Finite Groups and Orders, Lecture Notes in Math. 149, Springer, Berlin, 1970.

[Sw] R. G. Swan, Algebraic K-theory, Lecture Notes in Math. 76, Springer, 1968.

[Sw2] R. G. Swan. Induced representations and projective modules. Ann. of Math. (2), 71, pp. 552-578, 1960.

[Sw3] R. G. Swan, The Grothendieck ring of a finite group, Topology, vol. 2, pp. 85-110, 1963.

[W] P. Webb, A course in finite group representation theory, Cambridge University Press, 2016.

[Wa] F. Waldhausen, Algebraic K-theory of spaces, Springer, Lecture Notes in Math. 1126, pp. 318-419, 1985.

[We1] D. Webb, Grothedieck groups of dihedral and quaternion group rings, J. Pure Appl. Algebra 35, pp. 197-223, 1985.

[We2] D. Webb, The Lenstra map on classifying spaces and G-theory of group rings, Invent. Math. 84, pp. 73-89, 1986.

[We3] D. Webb, Quillen G-theory of abelian group rings, J. Pure Appl. Algebra 39, no. 1-2, pp. 177-195, 1986.

[We4] D. Webb, G-theory of Group Rings for Groups of Square-Free Order, K-Theory 1, pp. 417-422, 1987.

[We5] D. Webb, Higher G-theory of nilpotent group rings, J. Algebra 116, no. 2, pp. 457-465, 1988.

[WeY] D. Webb, D. Yao, A simple counterexample to the Hambleton-Taylor-Williams Conjecture, K-theory 7(6), pp. 575-578, 1993.

[Wei] C. Weibel, The K-book : An Introduction to Algebraic K-theory, Graduate Studies in Mathematics, American Math. Soc., Vol. 145, 2013.

[Wei2] C. Weibel, The development of algebraic K-theory before 1980, AMS Contemp. Math. 243, pp. 211-238, 1999.

[Wi] S. M. J. Wilson, Reduced norms in the K-theory of orders, J. Algebra, Vol. 46 (1), 1977.

[GAP] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.8.5*; 2016, `http://www.gap-system.org`.

Zusammenfassung

In this thesis we investigate Quillen's G-theory of group rings mostly focusing on the case of finite groups. We study the Hambleton-Taylor-Williams decomposition conjecture for G-theory of the integral group rings. The conjecture expresses $G_n(\mathbb{Z}G)$ as a direct sum of the groups G_n of maximal orders in the simple components of $\mathbb{Q}G$ with certain integers inverted. The HTW-conjecture generalizes the results of Lenstra and Webb on abelian groups. Since G-theory lacks functoriality (as opposed to K-theory) it is a highly nontrivial task to construct a map between G-groups of different rings. The construction of the map between two sides of the HTW-decomposition is a part of the conjecture.

Even though Webb and Yao found a counterexample to the HTW-decomposition in degree 1 they still expected the conjecture to hold for solvable groups. Using the results of Keating we explicitly compute the ranks of both sides of the conjecture for G_1 and show that the solvable group $\mathrm{SL}(2, \mathbb{F}_3)$ is a counterexample to the conjectured decomposition. Nevertheless, we prove that for any finite group G the rank of $G_1(\mathbb{Z}G)$ does not exceed the rank of the expression in HTW-decomposition. To show this we use the methods from modular representation theory, in particular the results of Brauer and Nesbitt on blocks of defect zero. Since the results of Brauer and Nesbitt are only valid for a splitting field of G to get the desired inequality for ranks we first look at representations over a splitting field and then "glue" the representations over $\mathbb{Q}$ and $\mathbb{F}_p$ out of them using the action of the corresponding Galois group. The inequality for ranks of G_1 leads us to the natural guess that a weaker version of the conjecture might hold for all finite groups.

On the side of positive results using some analysis of local Schur indices we proved that the HTW-decomposition gives a correct prediction for the torsion subgroup of $G_1(\mathbb{Z}G)$ for all finite groups G. Furthermore, we show that the ranks of $G_n(\mathbb{Z}G)$ agree with the prediction of the conjecture in all degrees apart from the degree $n = 1$.