Vrije Universiteit Brussel

Faculty of Science and Bio-Engineering science
Departement Mathematics

The Isomorphism problem for Integral Group Rings of Finite Groups

Graduation thesis submitted for the degree
Master in Mathematics,

Promotor
Prof.Dr.Eric JESPERS

Geoffrey JANSSENS

Contents

Dankwoord

Mijn dank moet aan zeer veel mensen. Maar al dit zal ik pas vrijgeven bij het einde van de 2de semester. Tenslotte in paar maanden tijd kan veel gebeuren.

Introduction

We start this thesis with some history. This is strongly based on [15, p.125-129].

In 1837 Sir William Rowan Hamilton gave the first formal theory of complex numbers, defining them as ordered pairs of real numbers, just as is done nowadays, thus ending almost three hundred years of discussions regarding their legitimacy. Since he was well aware of their interpretation as vectors in a two-dimensional plane he realized that he had in fact constructed an algebra which allowed him to work with vectors in a plane. He was also aware that the greatest problem of his time, coming from physics, was to contruct a language which would be appropriate to develop dynamics; something similar to what was done by Newton when he invented calculus. To that end, it was necessary to create an algebra to operate with vectors in space. But he was stumped over the multiplication of these three-dimensional elements. Nowadays, it is proved that it is impossible. Thus after considerable effort, he realized that it would not be possible to construct such a structure and, based on geometrical considerations, perceived that he would be able to describe an algebra, not of vectors, but of the operators that act on vectors in space, working with four-dimensional algebras. In that way he invented in October 1843 the so-called quaternions. These are elements of the form $\alpha = a+bi+cj+dk$. The letters i, j, k are formal symbols and the coefficients a, b, c, d represent real numbers. They have to be added componentwise and the multiplication is the distributive expansion of the following rule on the basic elements:

$$i^2 = j^2 = k^2 = ijk = -1.$$

A funny anecdote tells that he was a drunk when he invented this multiplication. Because he was affraid to forget his illumination, he carved the multiplication rules on a bridge. More precisely, the Broughambridge in Dublin which can be visited for these interesting carvings. Another version of the anecdote says that he was walking with his wife. While his wife was talking with him, he was in fact thinking about the problem and suddenly invented the rules. With this invention Hamilton found the first noncommutative algebra.

In December of the same year, the English mathematician John T.Graves introduced a new set of numbers, the octonions, which can be defined as the set

of elements of the form $a_0 + a_1e_1 + \ldots + a_7e_7$. The elements $e_1, \ldots, e_7$ are, again, formal symbols and are added componentswise and the multiplication has some specific rules. A striking fact about octonions is that the product so defined is not even associative. Grave did not publish his contruction and these numbers will be rediscovered bi Sir Arthur Cayley in 1845. Hamilton realized that it was possible to extend this construction even further which allowed him to define biquaternions. Soon afterwards he introduced the hypercomplex systems.

This part of the history can be regarded as the first steps in ring theory. The interest in algebras grew larger and larger and in 1871 Benjamin Pierce gave a classification of the algebras known at the time and determined 162 algebras of dimension less than or equal to 6. As tools for his method of classification, B.Pierce introduced some very important elements and the use of idempontents to obtain a decomposition of a given algebra. During that same century, important developments were taking place in the theory of non-associative algebras. Following the work of S.Lie and W.Killing in the study of Lie groups and Lie algebras. A.Study and G.Scheffers introduced between 1889 and 1898 some basic notions for the development of structure theory such as the concepts of simple and semisimple algebras (although using different terminology). Their results inspired both T. Molien and E. Cartan. They independently obtained important results regarding the structure theory of finite-dimensional real or complex algebras, introducing in this context the notions of simple and semisimple algebras and characterizing simple algebras as complete matrix algebras. All this work culminated in the beautiful theorems of J.H.M Wedderburn describing the structure of finite-dimensional algebras over an arbitrary field, using techniques related to the existence of idempotent elements, as suggested by the earlier work of B. Pierce.

The first definition of an abstract group was given by A. Cayley. In this same paper the notion of a group ring appears for the first time. Explicitly, given a finite group $G = \{g_1, \ldots, g_n\}$ consider all elements of the form $x_1g_1 + x_2g_2 + \ldots + x_ng_n$ where $x_1, x_2, \ldots, x_n$ are either real or complex numbers. The the product of two such elements $\alpha = \sum_{i=1}^{n} x_ig_i$ and $\beta = \sum_{i=1}^{n} y_ig_i$ is given by $\alpha\beta = \sum_{i,j}(x_iy_i)(g_ig_j)$.

This is precisely the definition used nowadays. The only difference laying in the fact that we not only look at real or complex numbers but at a general ring R. We note such a group ring by RG. Despite of this, his paper had no immediate influence on contemporary mathematicians and group rings remained unknown for quite some time. They were introduced again by Theodor Molien when he realized that this was a natural setting in which to apply some of his earlier criteria for semisimplicity. Moreover, he discovered some of the basic results in the theory of complex representations of finite groups, including the orthogonality relations for group characters.

The connection between group represention theory and the structure theory

of algebra - which is obtained through group rings - was widely recognized after a most influential paper by Emmy Noether [40], some joint work of hers with Richard Brauer [41] and Brauer's paper [42], giving the subject a new impulse. Later, the subject gained importance of its own after the inclusion of questions on group rings in I.Kaplansky's famous list of problems [44], [45]. The first book which was entirely devoted to the subject was written by D.S. Passman [46]. Since then, many articles and books were written about group rings.

One of the most important and challenging problems in group rings is the Isomorphism problem. This postulates that integral group rings completely determine the corresponding group or more precisely: does $\mathbb{Z}G \cong \mathbb{Z}H$ for two finite groups G and H imply that the groups are isomorphic $G \cong H$?

The isomorphism problem of group rings appears for the first time in G. Higman's Ph.D Thesis, [43]. In it, he says:

" Whether it is possible for two non-isomorphic groups to have isomorphic integral group rings, I do not know: but the results of section 5 suggest it is unlikely."

It was first posed as a problem in the Algebra Conference at Michigan in 1947 by T.M. Thrall, who formulated it in the following terms:

"Given a group G and a field K, determine all groups H such that $KG \cong KH$."

In 1950, S. Perlis and G. Walker proved that finite abelian groups are determined by their group rings over the field of rational numbers. Passman, Coleman and Deskins found positive results for fields of characteristic p. These results seem to suggest that, for a given family of groups, it might be possible to obtain an adequate field for which the isomorphism problem has a positive answer. However, in 1972, E. Dade [47] gave an example of two groups (which are metabelian groups) which are not isomorphic, but are such that their respective group algebras over any field are isomorphic. The integral group rings of the groups of Dade are however not isomorphic. Thus the natural setting in which to consider the isomorphism problem is precisely that where the coefficient ring is the ring of integers. This leads to

$$\text{(ISO)} \quad \text{If } \mathbb{Z}G \text{ then } \mathbb{Z}H \Rightarrow G \cong H.$$

Under this form the conjecture has been cited in a list of important open problems by Richard Brauer himself. In contrast to Higman. In the second part of the last century several important results were obtained. For example Higman proved it for finite abelian groups, Whitcomb for metabelian finite groups. Up until the 80's there was no other great break through and interest in (ISO) faded. In 1974 Zassenhaus made several conjectures which are stronger then (ISO).

These conjectures could be seen as childs dream, but it gave a new light to the story. Through this conjectures Roggenkamp and Scott proved in the 1980's the Isomorphism problem for nilpotent groups. This is still the latest very important positive result together with the one of Weiss.Thus, evolution on the conjecture has always been slow and hard work, nevertheless (ISO) was almost consider as true. But in 1998 Martin Hertweck found in his Ph.D thesis the first counterexample to (ISO). Still no other is known. In 2001 his result was published in [5]. The goal of this thesis is to explain clearly and completely his counterexample. For this we shall first begin with a survey on all the other conjectures that influenced the research in (ISO) and explain some general theory to find counterexamples.

Summary

The goal of this thesis is to work-out completely the counterexample of Hertweck to the Isomorphism problem. This will be done in the second last Chapter. Theoreticly the reader could begin almost immediatly with the Chapter about the counterexamples because it doesn't use much advanced knoweldge. In this case the reader would see a lot of grouptechnical proofs and an impressive group, but would not know really what is happening (of course, except if the reader already has the knoweledge of the other Chapters).

For a group G and a ring R the group ring RG is defined as the set of formal sums $\sum_{g\in G} r_g g$, where addition is componentswise and multiplication is defined by $(r_g g)(r_h h) = r_g r_h gh$ and expanded distributivly to the whole ring. The thesis will start with a pre-requisites Chapter in which we will remaind some basic definitions and theorems. In Section 1.1 we remaind the definition of a group ring, the augmentation ideal and mention how this can be used to obtain a decomposition of RG. We also give the definition of a semisimple ring and some of its decompositions (for instance, the Pierce decomposition, the Wedderburn-Artin decomposition and the theorem of Perlis-Walker in the case G is abelian). The group ring $\mathbb{Z}G$ is generated by G over $\mathbb{Z}$ and $\mathbb{Q}\mathbb{Z}G = \mathbb{Q}G$. Such a ring is called a $\mathbb{Z}$-order in the cas G is finite. This fact is very useful, and therefore we give the general definition of a $\mathbb{Z}$-order in Section 1.2. Some properties of orders and the unit theorem of Dirichlet can also be found in Section 1.2. In Chapter 3 and 6, we will talk a lot about units because the main point of the counterexample to the Isomorphism Problem is to create a unit with some properties. For this reason, we devote Section 1.3 to a survey of basic unit constructions. More precisely, we will discuss about Bass cyclic, bicyclic and unipotent units.

The Isomorphism problem is a question concerning the properties and thus structure of a group ring. One of the best structure results of rings is the theorem of Wedderburn-Artin. This says that a ring R is semisimple if and only if it is the direct sum of matrix rings over division rings. Moreover, this decomposition in so called simple components is unique up to isomorphism. The theorem of Maschke answers the question when a group ring RG is semisimple. More precisely, a group ring RG is semisimple if and only if R is semisimple, G a

finite group and $|G| \in \mathcal{U}(R)$. So the group algebras $\mathbb{Q}G$ and $\mathbb{C}G$ of a finite group G are semisimple. The Wedderburn-Artin decomposition of the latter giving rise to the irreducible characters of the group G. The fact that $\mathbb{Q}G$ is semisimple is especially of interest for the study of integral group rings $\mathbb{Z}G$ since it is a $\mathbb{Z}$-order in $\mathbb{Q}G$. Thus in some sense it is logical to investigate at the Wedderburn components of the group ring $\mathbb{Q}G$. The simple components are generated (as an ideal) by one central idempotent. The set of these generators are called the primitive central idempotents. Using character theory several expressions for these are known. Character-free expressions are much harder to find and are known, e.g, for supersolvable-by-abelian finite groups. Chapter 2 is concerned with such expressions. More precisely, in Section 2.1 we give a survey of the knowledge on primitive central idempotents. Section 2.2 contains a new expression for the primitive central idempotents of $\mathbb{Q}G$ for an arbitrary finite group G discovered by the author of this thesis at the beginning of the academical year 2011-2012. The Section is in fact almost an identical copy of my paper, [28], accepted for publication in february 2012. More precisely, it gives a new almost character-free expression for the primitive central idempotents of $\mathbb{Q}G$ (with a complete character-free upperbound) that may be implemented in GAP.

In the following Chapters other approaches to (ISO) are given. As mentioned in the introduction, fundamental contributions to the Isomorphism problem were made through a whole family of conjectures. Due to their importance, a complete Chapter is devoted to them (i.e. Chapter 3). The first section of this Chapter will, of course, concern (ISO) itself. After a brief but complete summary of all known results, a short overview of Herweck's counterexample given.

In Section 3.2, the Zassenhaus conjectures are honored. A finite subgroup H of the group of augmented units, $V(\mathbb{Z}G)$, that also generates the group ring, $\mathbb{Z}H = \mathbb{Z}G$, is called a group basis. The second Zassenhaus conjecture states that each two group basises are rationally conjugated. This conjecture clearly implie the Isomorphism problem for integral group rings. Zassenhaus made also three other conjectures, that have a direct link with (ISO). The relations between all these conjectures and with the Isomorphism problem are explained in Subsection 3.2.1 This subsection giving the importance of the Zassenhaus conjecture, we will devote Subsection 3.2.2 to a pretty complete survey of the contemporary state of research on all the Zassenhaus conjectures.

As said, the Zassenhaus conjectures explain how units and group basis are conjugated to each other. In particular the first Zassenhaus conjecture asserts that all the augmented units are conjugated to trivial units (these are the elements of the groupbasis G). Since that these conjectures are of importance, the reader will not be astonished that the embedding of the trivial units in the group of augmented units could also play a role to (ISO). This is the content of Section 3.3. It says that G has always a normal complement in $\mathcal{U}(\mathbb{Z}G)$ and moreover this

complement is free. The exact link with (ISO) is proved in the first subsection and a complete survey of this conjecture is given in the following subsection. The reader will remark that not so much is known. A recent result linking the Yang-Baxter equation with complements of G in $\mathcal{U}(\mathbb{Z}G)$ could maybe help in the future, but we will come back on this in Chapter 7.

In Section 2.4 the inbedding of G in $\mathcal{U}(\mathbb{Z}G)$ is still the main stream. However, this time the units normalizing the group basis G have a glory period. The normalizer problem asserts that the normalizer $\mathcal{N}_{\mathcal{U}(\mathbb{Z}G)}(G)$ consists only of the obvious normalizers. These are $G\mathcal{Z}(\mathbb{Z}G)$. One of the main insight of Mazur and Hetweck, was to remark that the Normalizer problem was very usefull for constructing counterexamples to (ISO). Despite the lack of results about this conjecture, we give a pretty long survey on it devided over several subsections. A first one, that gives a classical suvery on the normalizer problem. Then followed by 3 subsections representing each an other method of attack of the conjecture. As always, known results about them are outlined and the origin of these methodes are explained. To be more concrete:

In Subsection 3.4.1 we note that the normalizer problem can also be interpreted as a problem concerning outer automorphisms. In fact, we define a set $Aut_{\mathbb{Z}}(G)$ of automorphisms of G that becomes inner over $\mathbb{Z}G$. This means that they are of the form $\mathrm{conj}(u)$ with $u \in \mathcal{U}(\mathbb{Z}G)$. If we take out all the automorphisms that were already inner over G then we get the set $\mathrm{Out}_{\mathbb{Z}}(G)$ of $\mathbb{Z}$-outerautomorphisms of G. One can easily check that the normalizer problem is equivalent with saying that $\mathrm{Out}_{\mathbb{Z}}(G) = 1$.

In Subsection 3.4.2 we go a bit larger and look at the group $\mathrm{Aut}_{Col}(G)$ of Coleman automorphisms. These are automorphisms whose restriction to a Sylow subgroup of G equals the restriction of some inner automorphism of G. Due to a theorem of Coleman, this group contains the group $\mathrm{Aut}_{\mathbb{Z}}(G)$. And thus may indeed be of interest in our story.

In Subsection 3.4.3 we go a bit further in a construction of Hertweck made in his Ph.D thesis. He created from a normalizer $t \in N_{\mathcal{U}(\mathbb{Z}G)}(G)$ the semi-direct product $G_\tau = G \rtimes_\tau \langle x \rangle$, where x is an element of the same order as $\tau = \mathrm{conj}(t)$. Through this he made central units in $\mathbb{Z}G_\tau$. We did the remark that these central units are only of interest if the normalizer element t was not an obvious normalizer, thus need that the normalizer problem is false. That's why we devote a short subsection to central units. Only a few constructions of central units are known and very recently the construction of a subgroup of finite index in the set of central units of a nilpotent group has been generalized. This generalization is due to Jespers, Van Gelder, Olteanu and Del Rio and we very shortly mentionned their results (that are, yet, not published).

Subsection 3.4.4 is based on a seminar hold by Andreas Bächle that I followed during this year. In this subsection we look at two generalizations of the

normalizer problem. Instead of examing groups satisfying the normalizer problem, we look at groups such that all its subgroups fulfill the normalizer property. Several nice results are known and are all mentioned in this subsection.

At this part of the thesis, the reader will have a good knoweledge of the contemporary state of research and will be convinced that in fact all these problems (who are studied all in their own right) have in fact their origin in the Isomorphism problem. Unfortunately, this do not suffice to produce counterexamples. Therefore, we need technics to make units and a general obstruction theory. The first is obtained with Chapter 4, by using pullback diagrams in the categories of rings and groups. Several usefull ring and group pullback diagrams are showed and we explain why actuelly they are useful. This, inter alia, through an example.

Chapter 5, have their origin in papers by Scott and Roggenkamp, and Roggenkamp and Kimmerle. This chapter is of primordial importance for the later chapters because the mentioned papers outlined a first general theory how counterexamples to the several Conjectures (especially (ISO)) could be found. The idea behind the obstruction theory, is to split the group up in several smaller groups which satisfie the concerned conjecture and finally pullback the results to the initial group. This will be possible if and only if some automorphisms in the smaller groups are of a certain form. More precisely if a certain family of automorphisms is a conboundery of a certain cohomology set. All this is the content of Section 5.2 . In Section 5.1 we first enlarge a bit the idea of splitting up the group through so called subdirect products. A subdirect product is a subgroup of some direct product of groups. Section 5.1 is concerned with the natural questions: what are the possibilities to represnt G as a subdirect product? Can we describe the structure of subdirect products in terms of the subgroups of the direct factors? For the direct product of two factors, the answers are known and seems to be the theory of pullback diagrams. If one look at a direct product of three factors, the situation is already much harder. We cite all the known results to this questioins in Section 5.1.

In Chapter 6 we finally arrive at the goal of this thesis. Remember that the goal was to explain, for the first time, in a complete and convincing way the marvelous ideas behind the counterexample of Hertweck to the Isomorphism problem. Therefore, we first have to work out his counterexample to the Normalizer problem. This is done in Section 5.1 and go through 4 steps. A subsection is devoted to each of these steps. The counterexample to the normalizer problem is above all a magnificant application of the pullbacks technics from Chapter 4 and a perfect use of counterexamples to other problems found in the second part of last century. In Section 5.2 the main counterexample (the one to (ISO)) is explained. After a short ouline of the philosphy, four subsections are devoted to the several main steps. This proof is mainly a great application of the obstruction

theory of Chapter 5 and a compilation of ideas from a whole family of articles. In section 5.3, we show that the technics of Hertweck are very useful for constructing counterexamples to other conjectures. We do this by explaining his counterexample, [6], to the second Zassenhaus conjecture and pointing out the similarities with his counterexample to (ISO). In fact, he gives even a counterexample to the automorphism version of the Zassenhaus conjecture.

In the 7-th and last Chapter, we pave the way to possible further research.

1 Preliminaries

1.1 General

Let G be a group and R a ring. By RG we denote the set of all formal linear combinations of the form $\alpha = \sum_{g\in G} a_g g$ where $a_g \in R$ and only a finite number terms is non-zero. The sum of two elements in RG is componentswise:

$$(\sum_{g\in G} a_g g) + (\sum_{g\in G} b_g g) = \sum_{g\in G} (a_g + b_g)g.$$

And the product is defined as

$$(\sum_{g\in G} a_g g).(\sum_{g\in G} b_g g) = \sum_{g,h\in G} a_g b_h gh.$$

This operations make of RG a ring and is called the group ring of G over R. If R is commutative then we see easily that RG is even a R-algebra. We could also define group rings through a universal property. This implies that each group homomorphism $f : G \to H$ can be uniquely extended to a ring homomorphism $f : RG \to RH$. In particular if we take $H = \{1\}$ we obtain the map $\epsilon : RG \to R : \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g$. This is called the augmentation mapping of RG and its kernel, is denoted by $\Delta(G)$ and is called the augmentation ideal of RG. If $\alpha = \sum_{g\in G} a_g g \in \Delta(G)$ then $\sum_{g\in G} a_g = 0$. Thus $\alpha = \sum_{g\in G} a_g(g-1)$. Furthermore, all the elements of the form $g - 1$ belong to $\Delta(G)$. Alltogether we showed that the set $\{g - 1 : g \in G, g \neq 1\}$ is a R-basis of $\Delta(G)$.

An isomorphism $\phi : \mathbb{Z}G \to \mathbb{Z}H$ is called a normalized isomorphism if for every element $\alpha \in \mathbb{Z}G$ we have that $\epsilon(\alpha) = \epsilon(\phi(\alpha))$ or equivalently, if for every every element $g \in G$ we have that $\epsilon(\phi(g)) = 1$. Remark that if there exists an isomorphism $\phi : \mathbb{Z}G \to \mathbb{Z}H$, then there also exists a normalized isomorphism between these rings. Therefore define the map $\psi : \mathbb{Z}G \to \mathbb{Z}H$ that sends a $\alpha = \sum_{g\in G} r_g g \in \mathbb{Z}G$ to $\psi(\alpha) = \sum_{g\in G} \epsilon(\phi(g))^{-1} r_g \phi(g)$. It is easy to verify that ψ is a normalized isomorphism. Another advantage of working with normalized isomorphism is the following theorem, called the Normal Subgroup Correspondence (for a proof see [15, p. 291]). First, recall that $\hat{N} = \sum_{x\in N} x$.

Theorem 1.1.1 (Normal Subgroup Correspondence) *Let G and H be finite groups such that $\mathbb{Z}G \cong \mathbb{Z}H$ and let N be a normal subgroup of G. Let*

$\theta : \mathbb{Z}G \to \mathbb{Z}H$ be a normalized isomorphism. Then, there exists $M \lhd H$ such that $\theta(\hat{N}) = \hat{M}$ and $|N| = |M|$.

A general idea in ringtheory and also in this thesis is to decompose RG as a direct sum of certain subrings. For this we recall the relationship between subgroups of G and ideals of RG. Denote the set of all subgroups of G by $\mathcal{S}(G)$ and the set of all left ideals of RG by $\mathcal{I}(RG)$.

Definition 1.1.2 *For a subgroup $H \in \mathcal{S}(G)$, we denote by $\Delta_R(G, H)$ the left ideal of RG generated by the set $\{h - 1 : h \in H\}$.*

The most of the time we will omit the subscript R and simply write $\Delta(G, H)$. Let $\mathcal{T} = \{q_i\}_{i \in I}$ be a transversal of H in G. One can show that $\{q(h-1) : q \in \mathcal{T}, h \in H, h \neq 1\}$ is a R-basis of $\Delta(G, H)$. A conceptual nicer description can be given if H is a normal subgroup of G. For this look at the canonical map $\omega : G \to G/H$ and extend it to the group rings $RG \to R(G/H)$. We still note this map with ω. Then we have following description of $\Delta(G, H)$.

Proposition 1.1.3 *Let $H \lhd G$. Then $\Delta(G, H) = Ker(\omega)$.*

With this, we have constructed a mapping from $\mathcal{S}(G)$ to $\mathcal{I}(RG)$., such that norma subgroups of G are mapped to two-sided ideals of RG. One can also construct a map in the other direction, but it is not of interest for this thesis. With this theory we can already state first decomposition theorems. But first we have to associate with a subgroup H two elements. A first one is $\hat{H} = \sum_{h \in H} h$ and an other is $\widetilde{H} = \frac{1}{|H|}\hat{H}$. It is easily shown that $\widetilde{H}$ is an idempotent and if $H \lhd G$ then it is moreover central. Following decomposition will be used a lot of times in this thesis.

Proposition 1.1.4 *Let R be a ring and let H be a normal subgroup of a group G. If $|H|$ is invertible in R, then*

$$RG = RG(\widetilde{H}) \oplus RG(1 - \widetilde{H})$$

where

$$RG(\widetilde{H}) \cong R(G/H) \text{ and } RG(1 - \widetilde{H}) = \Delta(G, H).$$

Thus in particular if $|G|$ is invertible in R, then $RG \cong R \oplus \Delta(G)$. If one take $H = \acute{G}$ the commutator subgroup of G then we know more about the components of the decomposition. In this case $RG(\widetilde{\acute{G}})$ is the sum of all commutative simple components of RG and $\Delta(G, \acute{G})$ is the sum of all others.

In the following of the section we will mention the Pierce decomposition and the Wedderburn-Artin decomposition. But for this we first have to introduce the notion of semisimple rings.

Definition 1.1.5 *An R-module M is called semisimple if every submodule of M is a direct summand.*

Definition 1.1.6 *A ring R is called (left-)semisimple if it is semisimple as a left module over itself. similarly, one defines a right-semisimple ring. One can show that a ring is left-semisimple if and only if it is right-semisimple and therefore one simply speaks of semisimple rings.*

Recall that the submodules of ${}_RR$ are precisely the left ideals of the ring r. Therefore r is semisimple if and only if every left ideal is a direct summand. Following theorem is well-known.

Theorem 1.1.7 *Let R be a ring. Then, the following conditions are equivalent.*

(i) Every R-module is semisimple.

(ii) R is a semisimple ring.

(iii) R is a direct sum of a finite number of minimal left ideals.

We can also characterize semisimple rings as follow.

Theorem 1.1.8 *Let R be a ring. Then r is semisimple if and only if every left ideal L of R is of the form $L = Re$, where $e \in R$ is an idempotent.*

Therefore, we can use idempotents to decompose semisimple rings into a direct sum of minimal left ideals. This is the classical Perice decomposition.

Theorem 1.1.9 *Let $R = \oplus_{i=1}^{t} L_i$ be a decomposition of a semisimple ring as a direct sum of minimal left ideals. Then, there exists a family $\{e_1, \ldots, e_t\}$ of elements of R such that:*

(i) $e_i \neq 0$ is an idempotent element, $1 \leq i \leq t$.

(ii) If $i \neq j$, then $e_i e_j = 0$.

(iii) $1 = e_1 + \ldots + e_n$.

(iv) e_i cannot be written as $e_i = e_i^{'} + e_i^{''}$, where $e_i^{'}, e_i^{''}$ are idempotents such that $e_i^{'}, e_i^{''} \neq 0$ and $e_i^{'} e_i^{''} = 0, 1 \leq i \leq t$.

Conversely, if there exists a family of idempotents $\{e_1, \ldots, e_t\}$ satisfying the conditions above, then the left ideals $L_i = Re_i$ are minimal and $R = \oplus_{i=1}^{t} L_i$.

A family of idempotents satisfying the conditions of previous theorem is called a complete family of orthogonal idempotents. Now we try to construct a decomposition in two-sided ideals. For this we first need following proposition.

Proposition 1.1.10 *Let $R = \oplus_{i=1}^{t} L_i$ be a decomposition of a semisimple ring r as a direct sum of minimal left ideals. Then every simple R-module is isomorphic to one of the ideals L_i in the given decomposition.*

Giiven a decomposition of a semisimple ring R as a direct sum of minimal left ideals, re-ordering if necessary, we can group isomorphic left ideals together:

$$R = \underbrace{L_{11} \oplus \ldots \oplus L_{1r_1}}_{A_1} \oplus \underbrace{L_{21} \oplus \ldots \oplus L_{2r_2}}_{A_2} \oplus \ldots \oplus \underbrace{L_{s1} \oplus \ldots \oplus L_{sr_s}}_{A_s}.$$

With $L_{ij} \cong L_{ik}$ and $L_{ij}L_{kh} = (0)$ if $i \neq k$. And by the previous proposition all the minimal left ideals are isomorphic to one of the ideals in the decomposition of R given above.

Theorem 1.1.11 *With the notation above, let A_i denote the sum of all left ideals isomorphic to $L_{i1}, 1 \leq i \leq s$. Then:*

(i) Each A_i is a minimal two-sided ideal of R .

(ii) $A_iA_j = (0)$ if $i \neq j$.

(iii) $R = \oplus_{i=1}^{s} A_i$ as rings, where s is the number of isomorphic classes of minimal left ideals of R.

Moreover, all the ideals A_i are simple rings.

Also this decomposition is unique and determine completely all the two-sided ideals of R.

Definition 1.1.12 *The unique minimal two-sided ideals of a semisimple ring R are called the simple components of R.*

Since all the left ideals are generated by an idempotent in a semisimple ring, this is also the case for twosided ideals. This leads to a new family of idempotents.

Theorem 1.1.13 *Let $R = \oplus_{i=1}^{s} A_i$ be a decomposition of a semisimple ring as a direct sum of minimal two-sided ideals. Then, there exists a family $\{e_1, \ldots, e_s\}$ of elements of R such that:*

(i) $e_i \neq 0$ is a central idempotent, $1 \leq i \leq t$.

(ii) If $i \neq j$ then $e_ie_j = 0$.

(iii) $1 = e_1 + \ldots + e_t$.

(iv) e_i cannot be written as $e_i = e_i^{'} + e_i^{''}$ where $e_i^{'}, e_i^{''}$ are central idempotents such that $e_i^{'}, e_i^{''} \neq 0$ and $e_i^{'}e_i^{''} = 0, 1 \leq i \leq t$.

These elements are called the primitive central idempotents of R and in the next chapter we will give a description of the primitive central idempotents of a rational group algebra $\mathbb{Q}G$. For the moment we have a decomposition in twosided ideals. But there is more information known of these ideals.

Theorem 1.1.14 *(Wedderburn-Artin) A ring r is semisimple if and only if it is a direct sum of matrix algebras over division rings:*

$$R \cong M_{n_1}(D_1) \oplus \ldots \oplus M_{n_s}(D_s).$$

Moreover, the length and of the decomposition and the division rings are uniquely determined.

This decomposition will be called the Wedderburn decomposition.

The only remaining point is to known when a group ring is semisimple. Necessary and sufficient conditions were obtained by Mascke.

Theorem 1.1.15 *(Maschke's Theorem) Let G be a group. Then, the group ring RG is semisimple if and only if the following condtions hold.*

(i) R is a semisimple ring.

(ii) G is finite.

(iii) $|G|$ is invertible in R.

Thus a group algebra KG with K a field is semisimple if and only if $\mathrm{char}(K) \nmid |G|$. Typical of semisimple group algebras are $\mathbb{Q}G$ and $\mathbb{C}G$. The last one, give raise to typical representation theory and the first one, will be of great utility for the study of the integral group ring $\mathbb{Z}G$.

Perlis and Walker gave a description for group rings of finite abelian groups.

Theorem 1.1.16 *(Perlis-Walker) Let G be a finite abelian group, of order n, and let K be a field such that $\mathrm{char}(K) \nmid n$. Then*

$$KG \cong \oplus_{d|n} a_d K(\zeta_d)$$

where ζ_d denotes a primitive root of unity of order d and $a_d = \frac{n_d}{[K(\zeta_d):K]}$. In this formula, n_d denotes the number of elements of order d in G.

1.2 Orders

A finite extension field K of $\mathbb{Q}$ is called an algebraic number field. An element $\beta \in K$ is called an algeraic integer if it satisfies a monic equation in $\mathbb{Z}[X]$:

$$\beta^n + b_{n-1}\beta^{n-1} + \ldots + b_0 = 0,$$

with $b_i \in \mathbb{Z}$. It is well known that the algebraic integers of K form a ring, which is denoted $\mathcal{O}_K$ Moreover if α is an algebraic number, it follows from the definition that it satisfies an equation $c_n\alpha^n + c_{n-1}\alpha^{n-1} + \ldots + c_0 = 0$, with $c_i \in \mathbb{Z}$ and $c_n \neq 0$. Consequently $\gamma = c_n\alpha$ satisfies the monic equation $\gamma^n + c_{n-1}\gamma^{n-1} + \ldots + c_n^{n-1}c_0 = 0$ with $c_i \in \mathbb{Z}$. Thus $c_n\alpha \in \mathcal{O}_K$. Since $[K : \mathbb{Q}]$ is finite it follows that $\mathcal{O}_K$ is finitely generated as an abelian group. Resumed we have proved that $K = \mathbb{Q}\mathcal{O}_K$ and $\mathcal{K}$ is finitely generated. With this we arrived at the definition of an $\mathbb{Z}$-order.

Definition 1.2.1 *Let A be a $\mathbb{Q}$-algebra. A subring R of A containig its unity is called a $\mathbb{Z}$-order, in A if R is finitely generated as a $\mathbb{Z}$-module and $\mathbb{Q}R = A$.*

By the theorem of the primitive element K is necessarily of the form $\mathbb{Q}(a)$, for some $a \in K$.By the above remark we even can take $\alpha \in \mathcal{O}_K$. Then $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$ but equality does not always hold. For example, if we take $K = \mathbb{Q}(\sqrt{d})$, where we assume that $d \in \mathbb{Z}$ is square free, a quatratic field then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ if $d \equiv 2$ or 3 mod 4 and $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ otherwise.

With still the same notations, we also have that $M_n(\mathcal{O}_K)$ is a $\mathbb{Z}$-order in $M_n(K)$. If a is an algebraic integer, then the subring $\mathbb{Z}[a]$ of $\mathbb{Q}(a)$ generated by a is a $\mathbb{Z}$-order in $\mathbb{Q}(a)$. The integral group ring $\mathbb{Z}G$ of a finite group G is an order in the rational group algebra $\mathbb{Q}G$. More generally, $\mathcal{O}_K G$ is a $\mathbb{Z}$-order in KG. This last example is a very usefull one, because the rational group algebra behave way better and an other advantage lies in following proposition.

Proposition 1.2.2 *Let R_1 and R_2 be orders in a $\mathbb{Q}$-algebra A and say that $R_2 \subseteq R_1$. Then*

$$\mathcal{U}(R_2) = R_2 \cap \mathcal{U}(R_1).$$

Thus if $R_2 \subseteq R_1$ and $u \in R_2$ is invertible in R_1, then $u^{-1} \in R_2$, that is, u is invertible in R_2.

Now, let $n > 1$ and let ζ_n be a primitive n-th root of unity; Then $K = \mathbb{Q}(\zeta_n)$ is called the n-th cyclotomic field. The m-th cyclotomic polynomial over $\mathbb{C}$ is

$$\Phi_m(x) = \prod_{0<k<m,(k,m)=1} (x - \zeta_m^k).$$

This has clearly degree $\phi(m)$. Well known and usefull facts are the following

1. $\Phi_m(x) \in \mathbb{Z}[x]$,
2. $\Phi_m(x)$ is irreducible over $\mathbb{Q}$,
3. $x^n - 1 = \prod_{d|n,1\leq d\leq n} \Phi_d(x)$,
4. $\sum_{d|n,1\leq d\leq n} \phi(d) = n$,

5. the cyclotomic field $\mathbb{Q}[\zeta_n] = \mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$ in $\mathbb{C}$,

6. $\dim_{\mathbb{Q}}\mathbb{Q}[\zeta_n] = [\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \phi(n)$.

One can prove that the Wedderburn decomposition is the following.

Theorem 1.2.3 *The Wedderburn Decomposition of the rational group algebra of a finite cyclic group C_n is given by*

$$\mathbb{Q}C_n \cong \bigoplus_{m|n, 0<m\leq n} \mathbb{Q}(\zeta_m).$$

If one look at the prove, we would see that an explicit isomorphism is constructed and that under this isomorphism the generator x of C_n is send to the primitive root of unities:

$$\mathbb{Q}C_n \to \bigoplus_{m|n} \mathbb{Q}[\zeta_m] : x \mapsto (\zeta_1, \ldots, \zeta_m, \ldots, \zeta_n).$$

The ring $\mathbb{Z}[\zeta_m]$ is a $\mathbb{Z}$-order in $\mathbb{Q}[\zeta_m]$. The unit group of such a ring has been characterized.

Theorem 1.2.4 *(Dirichlet's unit theorem) Let $\mathbb{Q} \subset K$ be a finite extension of degree $n = n_1 + 2n_2$ where n_1 and $2n_2$ denote the number of real and complex embeddings of K respectively. Let $\mathcal{O}_K$ be the ring of algebraic integers of K and $\mathcal{U} = \mathcal{U}(\mathcal{O}_K)$ its unit group. then $\mathcal{U}$ is a finitly generated abelian group. Moreover, $\mathcal{U} = C \times F$ where C is a finite cyclic group and F is torsion free, of rank $\rho = n_1 + n_2 - 1$.*

According to Dirichlet's theorem, F can be written as a direct product of ρ infinite cyclic groups, $F = \langle u_1 \rangle \times \langle u_2 \rangle \times \ldots \times \langle u_\rho \rangle$. The units $\{u_1, u_2, \ldots, u_\rho\}$ are called a fundamental system of units. In general, it is extremly difficult to find these units. However, in the special case of cyclotomic fields $K = \mathbb{Q}(\zeta_n)$, we can construct units as follows.

Let $u = (1 - \zeta_n^i)/(1 - \zeta_n)$, where $(i, n) = 1$. Then there exists a $k \in \mathbb{Z}$ such that $ik \equiv 1 \bmod n$. We get

$$\frac{1 - \zeta_n}{1 - \zeta_n^i} = \frac{1 - \zeta_n^{ki}}{1 - \zeta_n^i} = 1 + \zeta_n + \ldots + \zeta_n^{i(k-1)} \in \mathbb{Z}[\zeta_n].$$

It follows that u is a unit in $\mathcal{O}_K$. These units are called cyclotomic units. One can show that they generate a subgroup of finite index in $\mathcal{U}(\mathcal{O}_K)$.

1.3 Units

All the conjectures that the reader will met in this thesis is a story about how the trivial units (thus the group G) is inbedded in the integral group ring

$\mathbb{Z}G$. In particular how it behaves in the group of units $\mathcal{U}(\mathbb{Z}G)$. Thus it's logic to have a general knoweldges of the different known construction of units. In this subsection we will remaind the construction of the cyclotomic, Bicylic and Bass cyclic units and some theorems about torsion units.

Let in this section R be a general ring and denote $\mathcal{U}(R)$ the group of invertibles elements of R and G an arbitrary group, except if written otherwise.

The augmentation map $\epsilon : RG \to R$ is a ring homomorphism, thus $\epsilon(u) \in R$ for all $u \in \mathcal{U}(RG)$. Denote by $\mathcal{U}_1(RG)$ the subgroup of units of augmentation 1 in $\mathcal{U}(RG)$. In mathematical form:

$$\mathcal{U}_1(RG) = \{u \in \mathcal{U}(RG) : \epsilon(u) = 1\}.$$

Some authors also use the notation $V(RG)$ and in this thesis we also opted for that. The only invertible elements of $\mathbb{Z}$ are ± 1. Therefore, for a unit u of the integral group ring $\mathbb{Z}G$ we have that $\epsilon(u) = \pm 1$, thus we see that

$$\mathcal{U}(\mathbb{Z}G) = \pm\mathcal{U}_1(\mathbb{Z}G).$$

For a general ring we clearly have that $\mathcal{U}(RG) = \mathcal{U}(R) \times V(RG)$. There are only a few constructions of units. Most of them are pretty old. We will describe these. The only group rings in which we are interested are $\mathbb{Z}G$ and the group algebras KG, where K is some field. Like the most of time, finitness and infinty give raise to two different situations where the first is, the most of the time, easier to handle. This is also the case with units. So we devote a first subsection to torsion units and thereafther continue with the others.

1.3.1 Torsion units

The elements of the form rg with $r \in \mathcal{U}(RG)$ are invertible with invers $r^{-1}g^{-1}$. These units are called the trivial units of RG. Thus for example $\pm G$ are the trivial units of the integral group ring $\mathbb{Z}G$. It may be of interest to know, when these units are the only on. But the reader will see that, generally speaking, group rings have also nontrivial units. In this thesis we are interested in finite groups. Fortunatly Higman classified all the finite groups such that $\mathbb{Z}G$ contains only trivial units. He went even a bit further, and did it for torsion groups.

Theorem 1.3.1 *(Higman) Let G be a torsion group. then, all units of $\mathbb{Z}G$ are trivial if and only if G is either an abelian group of exponent equal to $1, 2, 3, 4$ or 6 or a Hamiltonian group*

With an Hamiltonian group we mean a nonabelian torsion group such that all its subgroups are normal. Dedekind and Baer proved that these are of the form $K_8 \times E \times A$, where K_8 is quaternion group of order 8, A is an abelian group

with only elements of odd order and E is an elementary abelian 2-group. Thus for integral group rings, there are indeed the most of time nontrivial units.

In the case of group algebras KG where K is a field of arbitrary characteristic, the classification was made by Passman.

Theorem 1.3.2 *(Passman) Let G be a group which is not torsion-free and let K be a field of characteristic $p \geq 0$. Then KG has only trivial units if and only if one of the following conditions holds.*

1. *$K = \mathbb{F}_2$ and $G = C_2$ or C_3.*
2. *$K = \mathbb{F}_3$ and $G = C_2$.*

Again we remark that there should be nontrivial units. The proof of this theorem is quite interesting, because it make use of the so called unipotent units and the classification of group rings with no nilpotent elements: let η be a nilpotent element of a ring R, i.e. $\eta^k = 0$ for some positive integer k. This property yield following typical argument:

$$(1-\eta)(1+\eta+\eta^2+\ldots+\eta^{k-1}) = 1-\eta^k = 1,$$
$$(1+\eta)(1-\eta+\eta^2-\ldots\pm\eta^{k-1}) = 1\pm\eta^k = 1$$

Thus, $1 \pm \eta$ are units of R and are called unipotent units.

So, we already know that it is a vain hope, to work with only trivial units. Everyone have to begin somewhere, so lets begin by looking to units that behaves well towards the other elements. For example look at central torsion units. Higman showed as first that for integral group rings over finite abelian groups the torsion units (who are all central) are trivial. But in fact one can say even more.

Theorem 1.3.3 *Let G be an arbitrary group. Then all the torsion central units of $\mathbb{Z}G$ are trivial.*

The proof of this theorem follows immediatly from following proposition.

Proposition 1.3.4 *Let G be an arbitrary group. Suppose that $\gamma \in \mathbb{Z}G$ commutes with γ^* and that moreover it is a torsion unit. then $\gamma = \pm g_0$ for some $g_0 \in G$.*

In this proposition we introduced the standart involution of $\mathbb{Z}G$:

$$* : \mathbb{Z}G \to \mathbb{Z}G : \gamma = \sum \gamma(g)g \mapsto \gamma^* = \sum \gamma(g)g^{-1}.$$

And this proposition is in fact a trivial corollary of the following nice theorem of Passman and Bass:

Theorem 1.3.5 *(Passman-Bass) Let G be an arbitrary group and $\gamma = \sum \gamma(g)g \in \mathbb{Z}G$ a torsion element and $\gamma(1) \neq 0$. then $\gamma = \pm 1$.*

With this we ended the story about torsion units. Let's now look at constructions of non torsion units.

1.3.2 Nontorsion units

A first construction that we brievly discuss is the construction of the Bicyclic units. As the reader will see these units are only relevant for non-abelian groups. The Bicylic units are in fact a special case of unipotent units.

Bicyclic units

Admit that we have a ring R with zero devisors, say x and y. Thus $xy = 0$. For any other element $t \in R$ we calculate immediatly that $\eta^2 = (ytx)^2 = 0$. This leads to the unipotent unit $1 + \eta$. In the case that $R = \mathbb{Z}G$, a simple way of obtaining a zero divisor is to consider a element $a \in G$ of finite order $n > 1$, since then $a - 1$ is a zero divisor due to $(a - 1)(1 + a + \ldots + a^{n-1}) = 0$. Thus, taking any other element $b \in G$, we can construct a unit:

$$\mu_{a,b} = 1 + (a - 1)b\hat{a}$$

with $\hat{a} = \widehat{\langle a \rangle} = 1 + a + \ldots + a^{n-1}$. This leads to the following definition.

Definition 1.3.6 *Let a be an element of finite order n in a group G and let b be any elment of G. The unit $\mu_{a,b}$ constructed above is called a bicylic unit of the group ring $\mathbb{Z}G$.*

We denote by $\mathcal{B}_2$ the subgroup of $\mathcal{U}(\mathbb{Z}G)$ generated by all the bicyclic units of $\mathbb{Z}G$.

Clearly, if a an b commute then $\mu_{a,b} = 1$. The goal of this construction is to find units different of the trivial one. Following proposition says when this is the case.

Proposition 1.3.7 *Let g, h elements of a group G with $o(g) = n < \infty$. Then, the bicyclic unit $\mu_{g,h}$ is trivial if and only if h normalizes $\langle g \rangle$ and, in this case, $\mu_{g,h} = 1$.*

Thus if G is a finite group. Then the group $\mathcal{B}_2$ is trivial if and only if every subgroup of G is normal. This happens if and only if G is abelian or Hamiltonian. From the previous proposition we also proof easily that the bicyclic units are of infinite order.

Corollary 1.3.8 *Every bicyclic unit $\mu_{g,h} \neq 1$ of $\mathbb{Z}G$ is of infinite order.*

Proof. Given $\mu_{g,h} = 1 + (g - 1)h\hat{g}$ we have that $\mu_{g,h}^s = (1 + (g - 1)h\hat{g})^s = 1 + s(g - 1)h\hat{g}$. So $\mu_{g,h}^s = 1$ if and only if $(g - 1)h\hat{g} = 0$ and this happens if and only if $\mu_{g,h} = 1$. □

Bass cyclic units

Now we turn to finite commutative groups. First, remember the definition of Euler's totient function ϕ. If $n = p_1^{n_1} \cdots p_t^{n_t}$ is the prime decomposition of a natural number n then $\phi(n) = p_1^{n_1-1}(p_1 - 1) \cdots p_t^{n_t-1}(p_t - 1)$. An interesting property of this function is given by Euler's Theorem, that says that for relative prime integers i and n the congruence $i^{\phi(n)} \equiv 1 \bmod n$ holds. In the construction of the bicyclic units the idea of adding up the powers of some element a was primordial. We will again start with this idea. Thus take an element $g \in G$ and look at $(1 + g + \ldots + g^{i-1})$. This element belongs to the group ring $\mathbb{Z}(\langle g \rangle) \subset \mathbb{Q}(\langle g \rangle)$. By the theorem of Perlis and Walker we have the isomorphism $\mathbb{Q}(\langle g \rangle) \cong \sum_{d|n} \mathbb{Q}(\zeta_d)$ where ζ_d is a primitive d-th root of unity. Moreover, under this isomorphism g projects in each component to the corresponding root of unity. Now, notice that an element of the form $(1 + g + \ldots + g^{i-1})$ projects, in each component, to an element of the form:

$$\alpha_d = 1 + \zeta_d + \ldots + \zeta_d^{i-1}$$

in $\mathbb{Z}[\zeta_n]$. If $\zeta_d \neq 1$, then the element α_d is invertible in $\mathbb{Z}[\zeta_d]$, and is called a cyclotomic unit. Its invers is

$$\alpha_d^{-1} = \frac{\zeta_d - 1}{\zeta_d^i - 1} = \frac{\zeta_d^{ik}}{\zeta_d^i - 1} = 1 + \zeta_d^i + \ldots + \zeta_d^{i(k-1)},$$

where k is any integer such that $ik \equiv 1 \bmod n$. Clearly $\alpha_d^{-1} \in \mathbb{Z}[d] \subseteq \mathbb{Z}[\zeta_n]$. However, in the first component, $(1 + \ldots + g^{i-1})$ project precisely to the value i, which is not invertible. Therefore we add some term that will project to zero in all the components except the first one. There it will make the projection equal to 1. According to Euler's Theorem there exists some $t \in \mathbb{Z}$ such that $i^{\phi(n)} = 1 + tn$. Consider now the element

$$(1 + g + \ldots + g^{i-1})^{\phi(n)} - t\hat{g}.$$

We note this element by μ_i. Remark that $-t = \frac{(1-i^{\phi(n)})}{n}$. Because the projection of $\hat{g}$ in $\mathbb{Q}(\zeta_d)$, with $\zeta_d \neq 1$, is equal to 0, the projection of μ_i on these components is still a unit. Now, in the first component, the projection is $i^{\phi(n)} - tn = 1$. Thus, the projection of μ_i in all the components of $\sum_{d|n} \mathbb{Z}[\zeta_d]$ is a unit. If we denote by R the pre-image of this ring under the isomorphism, it follows that μ_i is a unit in R. From typical order theory results, the element μ_i is also a unit in $\mathbb{Z}\langle g \rangle$. Thus resumed we found the following family of units.

Definition 1.3.9 *Let g be an element of order n in a group G. A Bass cyclic unit is an element of the group ring $\mathbb{Z}G$ of the form:*

$$\mu_i = (1 + g + \ldots + g^{i-1})^{\phi(n)} + \frac{1 - i^{\phi(n)}}{n}\hat{g},$$

where i is an integer such that $1 < i < n-1$ and $(i,n) = 1$. And its invers is given by

$$\mu_i^{-1} = (1 + g^i + \ldots + g^{i(k-1)})^{\phi(n)} + \frac{1 - k^{\phi(n)}}{n}\hat{g},$$

where k is any integer such that $ik \equiv 1 mod\ n$.

One can prove that, with i as in the definition, the Bass cyclic unit μ_i of infinite order is and thus not trivial. If $i = n-1$ then we get

$$\mu_i = (1 + g + \ldots + g^{n-2})^{\phi(n)} + \frac{(1 - i^{\phi(n)})}{n}\hat{g}.$$

The projection of this element in any component agrees with that of $(-g^{-1})^{\phi(n)}$. Thus $\mu_i = (-g^{-1})^{\phi(n)}$ is trivial. Resumed we have that μ_i is torsion if and only if $i \equiv \pm 1 \mod n$.

2 Primitive central idempotents

2.1 Survey

Let G be a finite group. The complex group algebra $\mathbb{C}G$ is semisimple and a description of its primitive central idempotents is well known. These are the elements

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

where χ runs through the irreducible characters of G. Using Galois descent one obtains that the primitive central idempotents of the semisimple rational group algebra $\mathbb{Q}G$ are the elements

$$e_{\mathbb{Q}}(\chi) = \sum_{\sigma \in G_\chi} \sigma(e(\chi)),$$

with $G_\chi = Gal(\mathbb{Q}(\chi)/\mathbb{Q})$. The problem with this expresion is the difficulty for a computer to calculate the formula, because it first has to calculate the charactertable and the Galoisgroup. In the next section, 2.2, we give a new formula that reduces the calculations. Unfortunately the Galoisgroup still didn't disappeared completely, but a completely characterfree upperbound is given. The reader could now go immediately to the next section and begin to read the formula. But in fact the obtained formula is an answer to a remark of Jespers, Olteanu and del Rio ([1, Remark 3.4]). For arbitrary finite groups they obtained in [1] a description of $e_{\mathbb{Q}}(\chi)$ expressing it as a $\mathbb{Q}$-linear combination of the elements $e(G, H_i, K_i)$, with (H_i, K_i) Shoda pairs in some subgroups of G. Thus to understand completely from where the result comes, one should understand the result of Jespers et al. That's why we begin by a survey on primitive central idempotents of $\mathbb{Q}G$. This survey is based on the thesis of Inneke van Gelder, [48].

Recall that if H is a subgroup of G, $\widetilde{H} = \frac{1}{|H|}\sum_{h \in H} h$ is an idempotent of $\mathbb{Q}G$ which is central if and only if H is normal in G. If $g \in G$, we write $\tilde{g} = \widetilde{\langle g \rangle}$. If $G \neq \{1\}$, we denote by $\mathcal{M}(G)$ the set of all minimal normal non trivial subgroups of G and define

$$\epsilon(G) = \prod_{M \in \mathcal{M}(G)} (1 - \widetilde{M}).$$

and by convention $\epsilon(1) = 1$. If N is an normal subgroup of G, then we obtain an isomorphism $\mathbb{Q}G\widetilde{N} \cong \mathbb{Q}(G/N)$. Let $\epsilon(G, N)$ denote the preimage of $\epsilon(G/N)$ under this isomorphism. Clearly,

$$\epsilon(G,N) = \begin{cases} \widetilde{N} & \text{if} \quad N = G \\ \prod_{M/N\mathcal{M}(G/N)}(\widetilde{N} - \widetilde{M}) = \widetilde{N}\prod_{M/N\in\mathcal{M}(G/N)}(1-\widetilde{M}) & \text{if} \quad N \neq G. \end{cases}$$

Note that both $\epsilon(G)$ and $\epsilon(G, N)$ are central idempotents of $\mathbb{Q}G$. For an abelian group G, the primitive central idempotents of $\mathbb{Q}G$ have been described as elements of the form $\epsilon(G, N)$.

Proposition 2.1.1 *Let G be a finite abelian group. The primitive central idempotents of $\mathbb{Q}G$ are precisely all elments of the form $\epsilon(G, N)$, with N a subgroup of G so that G/N is cyclic. In particular, if e is a primitive central idempotent of $\mathbb{Q}G$, then supp(e) is a subgroup of G, and e is a $\mathbb{Z}$-linear combination of idempotents of the form $\widetilde{H}$, where H is a subgroup of G.*

For larger families of groups, we need other idempotents that are sums of the idempotents $\epsilon(G, H)$. At its turn it need the notion of Shoda pairs.

Definition 2.1.2 *A pair (H, K) of subgroups of G is called a Shoda pair if it satisfies the following conditions:*

(S1) $K \lhd H$,

(S2) H/K is cyclic,

(S3) if $g \in G$ and $[H, g] \cap H \subseteq K$, then $g \in H$.

For example if G is an abelian group, then for every subgroup H of G such that G/H is cyclic, (G, H) is a Shoda pair. The utility of shoda pairs follows from the next proposition that is a rephrasing of a theorem of Shoda

Proposition 2.1.3 *If χ is a linear character of a subgroup H of G with kernel K, then the induced character χ^G is irreducible if and only if (H, K) is a Shoda pair.*

We now define some central elements in the group ring, which will play an important role. Given two subgroups H and K of G such that $K \lhd H$, let $e(G, H, K)$ denote the sum of all G-conjugates of $\epsilon(H, K)$. Since the G-stabilizer of $\epsilon(H, K)$ is exactly $\mathrm{Cen}_G(\epsilon(H, K))$, we get the following formula for T a right transversal of $\mathrm{Cen}_G(\epsilon(H, K))$ in G:

$$e(G,H,K) = \sum_{t\in T} \epsilon(H,K)^t.$$

Clearly $e(G, H, K)$ is a central element of $\mathbb{Q}G$ and if the G-conjugates of $\epsilon(H, K)$ are orthogonal, then $e(G, H, K)$ is a central idempotent of $\mathbb{Q}G$.

The primitive central idempotents of $\mathbb{Q}G$ associated to a monomial irreducible complex character can be computed using the elements of the form $e(G, H, K)$.

Definition 2.1.4 *A character χ of G is called monomial if there exist a subgroup $H \leq G$ and a linear character ψ of H such that $\chi = \psi^G$, the induced character on G. The group G is called monomial if all its irreducible characters are monomial.*

Theorem 2.1.5 *Let G be a finite group, H a subgroup of G, χ a linear character of H and χ^G the induced character of χ on G. If χ^G is irreducible then the primitive central idempotent of $\mathbb{Q}G$ associated to χ^G is*

$$e_{\mathbb{Q}}(\chi^G) = \frac{[Cen_G(\epsilon(H,K)) : H]}{[\mathbb{Q}(\chi) : \mathbb{Q}(\chi^G)]} e(G, H, K),$$

where K is the kernel of χ.

The following two corollaries follow easily from this theorem

Corollary 2.1.6 *If (H, K) is Shoda pair of G, then there is an $\alpha \in \mathbb{Q}$, necessarily unique, such that $\alpha e(G, H, K)$ is a primitive cnetral idempotent of $\mathbb{Q}G$*

Corollary 2.1.7 *A finite group G is monomial if and only if every primitive central idempotent of $\mathbb{Q}G$ is of the form $\alpha e(G, H, K)$ for $\alpha \in \mathbb{Q}$ and (H, K) a Shoda pair of G.*

So far, we have seen that the primitive central idempotent of $\mathbb{Q}G$ associated to a monomial irreducible character χ^G is of the form $\alpha e(G, H, K)$ for $\alpha \in \mathbb{Q}$ and a Shoda pair (H, K) of G. Now we search sufficient conditions for α to be 1. Clearly, $\alpha = 1$ if and only if $e(G, H, K)$ is an idempotent. This happens, for example, if the G-conjugates of $\epsilon(H, K)$ are orthogonal. This leads to the notion of strong shoda pair.

Definition 2.1.8 *A strong Shoda pair of G is a pair (H, K) of subgroups of G satisfying the following conditions:*

(SS1) $K \leq H \lhd N_G(K)$,

(SS2) H/K *is cyclic and a maximal abelian subgroup of* $N_G(K)/K$,

(SS3) for every $g \in G$ $N_G(K), \epsilon(H, K)\epsilon(H, K)^g = 0$.

The link between Shoda pairs and Strong Shoda pairs is the following.

Proposition 2.1.9 *The following conditions are equivalent for a pair (H, K) of subgroups of G:*

1. (H, K) *is a strong Shoda pair of* G,
2. (H, K) *is a Shoda pair of* $G, H \triangleleft N_G(K)$ *and the* G*-conjugates of* $\epsilon(H, K)$ *are orthogonal.*

Moreover, under this conditions $e(G, H, K)$ *is a central primitive idempotent.*

These idempotents will be sufficient to describe the primitive central idempotents of an abelian-by-supersolvable group. Remember that a supersolvable group is a group with a series of a normal subgroup of G with cyclic factors and abelian-by-supersolvable means that G has an abelian normal subgroup A such that G/A is supersolvable. There has been proved.

Theorem 2.1.10 *Let* G *be a finite abelian-by-supersolvable group and* $e \in \mathbb{Q}G$. *Then the following conditions are equivalent.*

1. e *is a primitive central idempotent of* $\mathbb{Q}G$.
2. $e = e(G, H, K)$ *for a strong shoda pair* (H, K) *of* G.
3. $e = e(G, H, K)$ *for a pair* (H, K) *of subgroups of* G *satisfying the following conditions:*
   (a) $K \triangleleft H \triangleleft Cen_G(\epsilon(H, K))$;
   (b) H/K *is cyclic and a maximal abelian subgroup of* $Cen_G(\epsilon(H, K))/K$;
   (c) *the* G*-conjugates of* $\epsilon(H, K)$ *are orthogonal.*

These idempotents also suffise to describe the primitive central idempotents of metabelian groups.

Theorem 2.1.11 *Let* G *be a metabelian finite group and let* A *be a maximal abelian subgroup of* G *containing* G'. *The primitive central idempotents of* $\mathbb{Q}G$ *are the elements of the form* $e(G, H, K)$, *where* (H, K) *is a pair of subgroups of* G *satisfying the following conditions:*

1. H *is a maximal element in the set* $\{B \leq G | A \leq B$ *and* $B' \leq K \leq B\}$.
2. H/K *is cyclic.*

2.2 New result

This chapter is a work done by the Author during the summer of 2011, [28].

As mentioned earlier on, Jespers, Olteanu and del Rio obtained a description of $e_{\mathbb{Q}}(\chi)$ for arbitrary finite groups in [1]. More precisely they showed following theorem.

Theorem 2.2.1 *Let G be a finite gorup of order n and χ an irrducible character of G. Then the primitive central idempotent $e_{\mathbb{Q}}(\chi)$ of $\mathbb{Q}G$ associated to χ is of the form*

$$e_{\mathbb{Q}}(\chi) = \frac{\chi(1)}{[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\chi)]} \sum_i a_i \frac{[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\psi_i)]}{[G : Cen_G(\epsilon(H_i, K_i)]} e(G, H_i, K_i),$$

where $a_i \in \mathbb{Z}$, (H_i, K_i) are strong Shoda pairs of subgroups of G (equivalently K_i is a normal subgroup of H_i with H_i/K_i cyclic) and ψ_i are linear characters of H_i with kernel K_i.

They posed the question ([1, Remark 3.4]) whether one could determine the scalars and the Shoda pairs involved. In this section we answer both questions by giving a full description of the primitive central idempotents of $\mathbb{Q}G$, for G a finite group.

Throughout G is a finite group. For χ an arbitrary complex character of G (so not necessarily irreducible) we put:

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

and

$$e_{\mathbb{Q}}(\chi) = \sum_{\sigma \in G_\chi} \sigma(e(\chi)).$$

Note that in general these elements do not have to be idempotents. Recall that the Möbius μ-function, $\mu : \mathbb{N} \to \{-1, 0, 1\}$, is the map defined by $\mu(1) = 1$, $\mu(n) = 0$ if $a^2|n$ with $a > 1$ and $\mu(n) = (-1)^r$ if $n = p_1 p_2 \dots p_r$ for different primes $p_1, \dots, p_r$. The induction of a character ϕ of a subgroup H to G is defined as

$$\phi_H^G(g) = \frac{1}{|H|} \sum_{y \in G} \dot{\phi}(y^{-1}gy),$$

where $\dot{\phi}(g) = \phi(g)$ if $g \in H$ and $\dot{\phi}(g) = 0$ if $g \notin H$. By 1_G we note the trivial character of G.

To prove our result we make use of the Artin Induction Theorem. Although this is probably well known, we state and prove it in the following specific form. Recall that for a rational valued character χ of a group G, $\chi(g) = \chi(g^i)$ for $(i, o(g)) = 1$.

Proposition 2.2.2 *(Artin) If ψ is a rational valued character of G, then*

$$\psi = \sum_{i=1}^{r} d_{C_i} 1_{C_i}^G,$$

where the sum runs through a set $\{C_1, \dots, C_r\}$ of representatives of conjugacy classes of cyclic subgroups of G. Furthermore, if $C_i = \langle c_i \rangle$ then

$$d_{C_i} = \frac{[G : Cen_G(c_i)]}{[G : C_i]} \sum_{C_i^* \geq C_i} \mu([C_i^* : C_i])\psi(z^*),$$

where the sum runs through all the cyclic subgroups C_i^* of G containing C_i and $C_i^* = \langle z^* \rangle$.

Proof. For every cyclic subgroup $C = \langle c \rangle$ of G, there exists exactly one $i \in \{1, \ldots, r\}$ such that C is G-conjugated to C_i. Say, $C = C_i^{g^{-1}}$. Set $a_C = \frac{|Cen_G(c)|}{|G|} d_C$. First we prove that $a_C = a_{C_i}$ and $1_C^G = 1_{C_i}^G$. To prove the second equality, note that $1_C^G(g) = \frac{1}{|C|} \sum_{y \in G} \dot{1}_C(y^{-1}gy)$, where the function $\dot{1}_C(y^{-1}gy)$ is defined as 1 if $y^{-1}gy \in C$ and 0 otherwise. This combined with the facts that conjugation preserves the order of subgroups and that it is an automorphism of G we easily see that $1_C^G = 1_{C_i}^G$.

Now we prove that $a_C = a_{C_i}$. Define the sets $(C_i)\uparrow^{\geq} = \{K \mid C_i \leq K \leq G\}$ and $(C)\uparrow^{\geq} = \{K \mid C \leq K \leq G\}$. There is a bijective correspondance between these sets. A map from $(C_i)\uparrow^{\geq}$ to $(C)\uparrow^{\geq}$ is given by conjugation with g^{-1} and the invers map is conjugation by g. Along with the fact that $C^g = \langle c^g \rangle$ if $C = \langle c \rangle$ and $|C| = |C^g|$, we see immediatly that $a_C = a_{C_i}$.

All this yields, $\sum_C a_C 1_C^G = \sum_{i=1}^r k_i a_{C_i} 1_{C_i}^G = \sum_{i=1}^r d_{C_i} 1_{C_i}^G$, where $k_i = |\mathcal{C}_G(c_i)| = \frac{|G|}{|Cen_G(c_i)|}$ (with $\mathcal{C}_G(c_i)$ the conjugacy class of c_i in G). The result now follows from Artin's Induction Theorem,[**?**, page 489], which says that every rational valued character of G is of the form $\sum_C a_C 1_C^G$, with a_C as above and the sum runs over all cyclic sungroups C of G. □

Theorem 2.2.3 *Let G be a finite group and χ an irreducible complex character of G. Let $C_i = \langle c_i \rangle$, then we denote*

$$b_{C_i} = \frac{[G : Cen_G(c_i)]}{[G : C_i]} \sum_{C_i^* \geq C_i} \mu([C_i^* : C_i])\Big(\sum_{\sigma \in G_\chi} \sigma(\chi)\Big)(z^*)$$

where the sum runs through all the cyclic subgroups C_i^* of G which contain C_i and z^* is a generator of C_i^*. Then

$$e_{\mathbb{Q}}(\chi) = \sum_{i=1}^r \frac{b_{C_i}\chi(1)}{[G : Cen_G(\tilde{C}_i)]} e(G, C_i, C_i) = \sum_{i=1}^r \frac{b_{C_i}\chi(1)}{[G : C_i]} \Big(\sum_{k=1}^{m_i} \tilde{C}_i^{g_{ik}}\Big),$$

where the first sums runs through a set $\{C_1, \ldots, C_r\}$ of representatives of conjugacy classes of cyclic subgroups of G and $T_i = \{g_{i1}, \ldots, g_{im_i}\}$ a right transversal of C_i in G.

Proof. Let χ be an irreducible complex character of G. First we suppose that $\chi(G) \subseteq \mathbb{Q}$. Then $G_\chi = \{1\}$ and then by Proposition 2.2.2, $\chi = \sum_{i=1}^r b_{C_i} 1_{C_i}^G$.

We get

$$\begin{aligned} e_{\mathbb{Q}}(\chi) = e(\chi) &= \tfrac{\chi(1)}{|G|}\textstyle\sum_{g\in G}(\sum_{i=1}^{r} b_{C_i} 1_{C_i}^G(g^{-1}))g \\ &= \tfrac{\chi(1)}{|G|}\textstyle\sum_{i=1}^{r} \frac{b_{C_i}}{1_{C_i}^G(1)} \sum_{g\in G} 1_{C_i}^G(1)1_{C_i}^G(g^{-1})g \\ &= \tfrac{\chi(1)}{|G|}\textstyle\sum_{i=1}^{r} \frac{b_{C_i}}{1_{C_i}^G(1)} |G| e(1_{C_i}^G) \\ &= \textstyle\sum_{i=1}^{r} \frac{b_{C_i}\,\chi(1)}{[G:C_i]} e(1_{C_i}^G) \end{aligned}$$

Let $T_i = \{g_{i1}, \ldots, g_{im_i}\}$ be a right transversal of C_i in G. Then

$$\begin{aligned} e(1_{C_i}^G) &= \tfrac{1}{|G|}\textstyle\sum_{g\in G} 1_{C_i}^G(1)1_{C_i}^G(g^{-1})g \\ &= \tfrac{1}{|G|}\textstyle\sum_{g\in G} \frac{|G|}{|C_i|} 1_{C_i}(1)1_{C_i}^G(g^{-1})g \\ &= \textstyle\sum_{g\in G} \frac{1}{|C_i|}(\frac{1}{|C_i|}\sum_{y\in G} \dot{1}_{C_i}(yg^{-1}y^{-1}))g \\ &= \textstyle\sum_{g\in G} \frac{1}{|C_i|}(\sum_{j=1}^{m_i} \dot{1}_{C_i}(g_{ij}g^{-1}g_{ij}^{-1}))g \\ &= \tfrac{1}{|C_i|}\textstyle\sum_{j=1}^{m_i}\sum_{h\in C_i} 1_{C_i}(h^{-1})g_{ij}^{-1}hg_{ij} \\ &= \textstyle\sum_{j=1}^{m_i} \tilde{C}_i^{g_{ij}} \end{aligned}$$

With this expression for $e(1_{C_i}^G)$ we obtain one of the equalities in the statement of the result.

Obviously, the sum $\sum_{k=1}^{m_i} \tilde{C}_i^{g_{ik}}$ adds the elements of the G-orbit of $\tilde{C}_i = \epsilon(C_i, C_i)$ and each of them $[Cen_G(\tilde{C}_i) : C_i]$ times. So

$$\sum_{k=1}^{m_i} \tilde{C}_i^{g_{ik}} = [Cen_G(\tilde{C}_i) : C_i] e(G, C_i, C_i).$$

A simple substitution in the earlier found expression for $e_{\mathbb{Q}}(\chi)$ yields the theorem.

Assume now that χ is an arbitrary irreducible complex character of G. Then it is clear and well known that $\sum_{\sigma\in G_\chi} \sigma\circ\chi$ is a rational valued character of G. Hence, by the first part we get

$$\begin{aligned} e(\textstyle\sum_{\sigma\in G_\chi}\sigma(\chi)) &= \tfrac{1}{|G|}\textstyle\sum_{g\in G}(\sum_{\sigma\in G_\chi}\sigma(\chi(1)))(\sum_{\sigma\in G_\chi}\sigma(\chi(g^{-1})))g \\ &= \tfrac{|G_\chi|\cdot\chi(1)}{|G|}\textstyle\sum_{\sigma\in G_\chi}\sum_{g\in G}\sigma(\chi(g^{-1})))g \\ &= \tfrac{|G_\chi|\cdot\chi(1)}{|G|}\textstyle\sum_{\sigma\in G_\chi}\sigma(\sum_{g\in G}\chi(g^{-1})g) \\ &= |G_\chi| e_{\mathbb{Q}}(\chi) \end{aligned}$$

So $e(\sum_{\sigma\in G_\chi}\sigma(\chi)) = |G_\chi| e_{\mathbb{Q}}(\chi)$. Since $\sum_{\sigma\in G_\chi}\sigma(\chi(1)) = |G_\chi|\chi(1)$, the rational case yields the theorem. □

We finish with some remarks. First note that the elements $e(G, C_i, C_i)$ are not necessarily idempotens. Second, the definition of b_{C_i} is not character-free. However one easily obtains a character free upperbound:

$$b_{C_i} \leq \frac{1}{[G : C_i]} \sum_{C_i^* \geq C_i} \mu([C_i^* : C_i])\phi(n)\chi(1) \leq \frac{[G : Z(G)]}{[G : C_i]} \sum_{C_i^* \geq C_i} \mu([C_i^* : C_i])\phi(n),$$

where ϕ denotes the ϕ-Euler function. Hence, we obtain a finite algorithm, that easily can be implemented in for example GAP, to compute all primitive central idempotents of $\mathbb{Q}G$. This answers one of the questions posed in [1, Remark 3.4]. Also the description of the idempotents only makes use of pairs of subgroups (C_i, C_i), with C_i cyclic. This answers the second question posed in [1, Remark 3.4].

3 The conjectures

3.1 Isomorphism problem

3.1.1 Survey

The second book of Sehgal, [14], is a standard bibliography about group rings. Most results known about the Isomorphism problem till 1993 are discussed there. Other nice surveys about the Isomorphism problem are [17] and [21]. The first and only known counterexample to the Isomorphism problem was found by Hertweck. The only reference for this is [5]. But we will work out and explain al the subtilities of the counterexample in this masterproof. Technics analogous to the one from the latter, combined with ideas of Scott, gave rise to the least known counterexample to the second Zassenhaus conjecture. We will later on come back on this.

Most general results known about the integral Isomorphism problem up to 1993 are discussed in Sehgal's book [14]. Other ealier nice suverys about the Isomorphism problem can be found in [17] and [21]. Most of these general results are of the type that (ISO) has a positive answer for a certain class of finite groups, such as abelian groups (Higman, REF) and nilpotent groups (Roggenkamp and Scott, REF). Only in 2001, in [5], Hertweck gave a counterexample to (ISO). The main goal of this thesis is to fully explore this work. Some of the outlined techniques used, combined with ideas of Scott (REF) gave rise to the least known counterexample to the second Zassenhaus conjecture (REF). We will return to this later in the thesis (See chapter 6, section 6.3).

In order to study (abstract) groups one introduced in the beginning of last century the notion of a group representation. Representation theory of a group G over a ring R is nothing else than the study of the RG-modules. Thus a natural question posed, for example, by Richard Brauer is : " wich properties of the group are reflected by RG? Could it even be that a group is determinated by its group ring? ". He never mentionned his point of view. Dade showed that a group exists that is *not* determinated by its group algebra KG, for K an arbitrary field. Of course there are also rings that are not a field and that give rise to interesting representation theory. A great example of this is " integral

representation theory". So, we can still wonder if a group is determined by its integral group rings. Higman gave following conjecture:

Conjecture 1 *Integral Isomorphism Problem*

Let G be an arbitrary finite group. Then we have following implication:

$$\mathbb{Z}G \cong \mathbb{Z}H \Longrightarrow G \cong H.$$

The known results at the end of last century suggested a positive answer. We remind the reader some of the known results.

Theorem 3.1.1 *Let G be a finite group, A an abelian group and B a nilpotent group such that $(|A|, |B|) = 1$. (ISO) has a positive answer in the following cases:*

1. *G is abelian (Higman, REF).*
2. *G is a Hamiltionian 2-group (REF).*
3. *G is a metabelian group (Whitecomb, REF).*
4. *G is a Nilpotent group (Roggenkamp and Scott, REF).*
5. *$G = A \rtimes B$ is a semidirect product of A and B, thus abelian-by-nilpotent (Weiss, REF).*
6. *G is a nilpotent-by-abelian group (Kimmerle, REF).*
7. *G is a simple group (Kimmerle and Sandling, REF).*
8. *G is a circle group (REF).*
9. *G is the adjoint group or the group of units of a finite ring (REF).*

Furthermore every finite group can be embedded in a finite group for which (ISO) has a positive solutation (REF). So it came as a big suprise when Martin Hertweck gave a counterexample to (ISO) in 2001, [5]. His counterexample is a nilpotent-by-nilpotent group of even order and derived length 4. So whether (ISO) has a positive answer for soluble groups of length 3 or for groups of odd order are still open questions. L.L. Scott pointed on an other relevant question, [32]:

...It remains quite plausible that the isomorphism problem or even the original Zassenhaus conjecture might have a positive answer for all finite groups G without two nontrivial normal p-subgroups for distinct primes p. These groups deserve special attention, since every finite group is a subdirect product of groups of this form.

In order to state the counterexample we fix some notation and reformulate (ISO) a bit differently. For a finite group G and a commutative ring R with 1, we write $\mathcal{U}(RG)$ for the unit group of the group ring RG and $V(RG)$ for the group of normalized units (i.e. units of augmentation 1). A group basis of RG is a subgroup H of $V(RG)$ with $RG = RH$ and $|G| = |H|$. Thus we can say that the isomorphism problem questions whether there is only one isomorphism class of group bases of $\mathbb{Z}G$. We state the counterexample.

Theorem 3.1.2 *There is a finite solvable group $X = G \rtimes \langle c \rangle$, a semidirect product of a normal subgroup G of X and a cyclic subgroup $\langle c \rangle$, such that the following proposition hold.*

1. *There is a non-inner group automorphism τ of G and $t \in V(\mathbb{Z}G)$ such that $g\tau = g^t$ for all $g \in G$.*
2. *In $\mathbb{Z}X$ we have that $t^c = t^{-1}$.*
3. *The group $Y = \langle G, tc \rangle$ is a group basis of $\mathbb{Z}X$ which is not isomorphic to X.*
4. *The group X has order $2^{21}.97^{28}$, it has a normal Sylow 97-subgroup and it has derived length 4.*

A natural question arises: " How do you find such a counterexample? ". The answer is long and not trivial, but we can already mention that this goes through the Normaliser Problem (see section 3.4). Also the proofs of Roggenkamp-Scott and Weiss (Theorem 3.1.1) are in some sense indirect, they prove the so called Zassenhaus conjecture (see section 3.2). As an immediate consequence one obtains a positive answer to (ISO) for some classes of groups.

Of course (ISO) also make sense for infinite groups. In this case, a counterexample was found by Mazur and this was an inspiration for M.Hertweck. We will completely work out the counterexample in section 6.2. Before doing this the reader need more intuition in (ISO).This will be done in section 3.2, 3.3 and 3.4 by giving background on thse important conjectures (Zassenhaus, normal complements and the Normalizer Problem) that made (ISO) develop through decennia. First we give more detail on the construction of the counterexample.

3.1.2 Hertweck's counterexample to ISO

In this section we give more detail on the construction of the counterexample. Explanations and proofs will be given in later chapters (Chapter 6, sectioin 6.2).

The group X is a semidriect product $Q \rtimes P$, with Q a normal Sylow 97-Sylow subgroup and$P$ a Sylow 2-subgroup.

Construction of P and Q

Construction of P

By $\langle x : x^n \rangle$ we denote a cyclic group generated by an element x of order n.

$P = \left(\langle u : u^{32} \rangle \times \langle v : v^4 \rangle \times \langle w : w^8 \rangle\right) \rtimes \left(\langle a : a^{128} \rangle \times \langle b : b^2 \rangle \times \langle c : c^8 \rangle\right)$,

the operation of a, b and c are give by:

- $u^a = u,\ v^a = u^{16}v$ and $w^a = u^4 w$;
- $x^b = x^{-1}$ and $x^c = x^5$ for alle $x \in \langle u, v, w \rangle$.

Construction of Q

The normal Sylow 97-Subgroup Q of X is the direct product of normal subgroups N and M of X, defined as follows. Let $D = (\langle d_3 \rangle \times \langle d_2 \rangle) \rtimes \langle d_1 \rangle \cong C_{97}^{(2)} \rtimes C_{97}$ with $d_2^{d_1} = d_3 d_2$ and $[d_3, d_1] = 1$ and let $R = D \times D = D^{(2)}$. Also define $N = R^{(4)}$. The group M be an elementary abelian group of order 97^4.

Action of P on Q

The elements u, v, w, b, c centralize M and a operates faithfully on M. The group M can be thought of as the additive group of the finite field $\mathbb{F}_{97^4}$ with a acting as multiplication by a fixed root of unity of order 128 in the field $\mathbb{F}_{97^4}$.

The largest normal 2-subgroup of X is $O_2(X) = C_P(Q) = \langle u, v, c^2 \rangle$. Let $\overline{X} = X/O_2(X)$. Then $\overline{P} = \langle \overline{a} \rangle \times \overline{H}$ with $H = \langle w, b, c \rangle$ and $\overline{H} = C_8 \rtimes Aut(C_8)$ (this will follow from the proof of lemma 6.2.7, section 6.2).

An automorphism $\delta \in Aut(D)$ of order 64 is given by

$$\delta : \begin{cases} d_1 & \mapsto & d_2^{19} \\ d_2 & \mapsto & d_1 \\ d_3 & \mapsto & d_3^{-19} \end{cases}$$

since the relation $(d_2\delta)^{d_1\delta} = d_1^{d_2^{19}} = d_3^{-19} d_1 = d_3\delta \cdot d_2\delta$ is satisfiedn so δ respects the relation $d_2 = d_3 d_2$ and $[d_3, d_1] = 1$. From $19^{16} \equiv -1 \mathrm{mod}\ 97$ it follow that

$$\delta^{16} : \begin{cases} d_1 & \mapsto & d_1^{19^8} \\ d_2 & \mapsto & d_2^{19^8} \\ d_3 & \mapsto & d_3^{-1} \end{cases} \quad \text{and} \quad \delta^{32} : \begin{cases} d_1 & \mapsto & d_1^{-1} \\ d_2 & \mapsto & d_2^{-2} \\ d_3 & \mapsto & d_3 \end{cases}$$

so δ has order 64 and an automorphism $\rho \in \mathrm{Aut}(R)$ of order 128 is defined by $(x, y)\rho = (y, x\delta)$ for all $x, y \in D$. The operation of P on N is defined by

$$\begin{aligned} (r_1, r_2, r_3, r_4)^a &= (r_{1\rho}, r_{2\rho}, r_{3\rho}, r_{4\rho}), \\ (r_1, r_2, r_3, r_4)^w &= (r_4\rho^{64}, r_1, r_2, r_3), \\ (r_1, r_2, r_3, r_4)^b &= (r_1, r_4\rho^{64}, r_3\rho^{64}, r_2\rho^{64}), \\ (r_1, r_2, r_3, r_4)^c &= (r_1, r_2\rho^{64}, r_3, r_4\rho^{64}), \end{aligned}$$

for all $(r_1, r_2, r_3, r_4) \in N$ and u, v centralize $R^{(4)}$.

Write $G = Q \rtimes (\langle u \rangle \times \langle v \rangle \times \langle w \rangle) \rtimes (\langle a \rangle \times \langle b \rangle)$. Then $X = G \rtimes \langle c \rangle$. This yields the constructiioin of the group X.

Finally we remark that $X' = Q\langle u^2, v^2, w^2 \rangle$ and $X'' = N$ so the derived length of X is 4.

At this point we know how the group X is constructed. However, several questions remain: why the numbers 2 and 97, which unit t is used in Theorem 3.1.2 is used and the path that Herweck followed to discover the counterexample

The numbers 2 and 97

Every group and ring theorist knows that the number 2 is a special number. So in some sense it is natural to look at even groups. But besides this general idea, there also is a mathematical reason. Hertweck used a counterexample to the Normalizer Problem for constructing the counterexample to (ISO) (see subsection 6.2.4). Since the Normalizer problem has a positive answer for odd groups, one looks at groups of even order. The question, "'why the number 97?" remains. In the proof of the counterexample the normalized units of $\mathbb{Z}\langle w : w^8 \rangle$ play an important role. These units are wellknown and a proof can be found in [15, p. 251]. The group of units of $\mathbb{Z}\langle w \rangle$ is generated by w and by the unit $\nu = 2 - w^4 + (1 - w^4)(w + w^{-1})$. One can rewrite this as

$$\nu = \widetilde{w^4} + (1 - \widetilde{w^4})(x + y(w + w^{-1}))$$

where $\widetilde{w}$ denots $\widetilde{\langle w \rangle}$. If we see $\langle w \rangle$ as a part of $\mathbb{Q}(\zeta 8)$, then the unit ν corresponds with the unit $3 + 2\sqrt{2}$ of $\mathbb{Z}[\sqrt{2}]$. One can check that $p = 97$ is the smallest prime for which there is a $k \in \mathbb{N}$ such that $(3 + 2\sqrt{2})^k = pr + 8s\sqrt{2}$ for some $r, s \in \mathbb{Z}$ (take $k = 12$). Following proposition will be proven in subsection 6.1.2, proposition 6.1.3.

Proposition 3.1.3 *Let q be some natural power of the prime 97 and let $\theta = \nu^{12q}$. Then*

$$\theta = \widetilde{w^4} + (1 - \widetilde{w^4})(qr_0 + 8s_0(w + w^{-1}))$$

for some $r_0, s_0 \in \mathbb{Z}$. Moreover,

1. $qr_0 \equiv 1 \ mod\ 8$,
2. $(qr_0)^2 - 2(8s_0)^2 = 1$,
3. $\theta^2 \equiv w^4 \ mod\ q$,
4. $\theta^2 \equiv 1 \ mod\ 8$.

The element θ described above will play an important role and this explains from where the relevance of the number 97. As wil bel explained later, all the families satisfiying the above aritmethic equation would fit into a counterexample.

The unit

Let G be the subgroup $\langle Q, u, v, w, a, b\rangle$ of X and let $S = \langle u, v, w, a, b\rangle$ a Sylow 2-subgroup of G. The automorphism $\tau \in \mathrm{Aut}(G)$ of part 1 in Theorem 3.1.2 is defined by $x\tau = x$ for all $x \in \langle Q, u, v, w, b\rangle$ and $a\tau = u^{16}a$. Note that

$$\tau|_S = conj(w^4)|_S.$$

It follows that τ is a non-inner group automorphism since

$$w^4 Z(S) \cap C_S(Q) = w^4\langle u^{16}, v^2, a^8\rangle \cap \langle u, v\rangle = \emptyset.$$

(a longer explenation will follow in section 6.2). A unit $t \in V(\mathbb{Z}G)$ will be constructed with $g\tau = g^t$ for all $g \in G$ and $t^c = t^{-1}$.

Claim 5 of Herweck's paper says:

Lemma 3.1.4 *Let $\mathcal{I}$ be the set of the primitive central idempotents of $\mathbb{Q}Q$ except $\widetilde{Q}$. No idempotent of $\mathcal{I}$ is fixed (via conjugation) by an element of $\overline{a}\overline{H}$. It follows that, $\mathcal{I}$ is the disjoint union of sets E and F with $E^{\overline{a}} = F$, and $E^{\overline{x}} = E$ for all $x \in \langle H, a^2\rangle$.*

Choose sets E and F with these properties and denote by E^+ and F^+ the sum of all the idempotents of respectively E and F. Let $q = 97^{28}$ be the order of the normal Sylow 97-subgroup Q of G and define the following element:

$$\kappa_q = q(E^+ + u^{16}F^+) \in \mathbb{Z}\langle Q, u^{16}\rangle.$$

Let $L = \langle u^4\rangle$ be a normal subgroup of order 8 in G, define the idempotents e_i:

$$e_1 = (1 - \widetilde{u^{16}}) \quad e_2 = \widetilde{u^{16}}(1 - \widetilde{u^8}) \quad \text{and} \quad e_3 = \widetilde{u^8}(1 - \widetilde{u^4})$$

and the element

$$\kappa_8 = 8[e_1(u^4v + u^{-4}v^{-1}) + e_2(u^2 + u^{-2}) + e_3(u + u^{-1})] \in \mathbb{Z}\langle u, v\rangle.$$

In the construction one prove a lot of identities, use some pullback diagrams, construct intermediate units λ and γ and finally find the desired unit t. This unit and its inverse are given by the following equations (we use the notation of Proposition 3.1.3):

$$\begin{aligned} t &= (1-\widetilde{L})(1-\widetilde{Q})(r_0\kappa_q + s_0\kappa_8) + \widetilde{L}(1-\widetilde{Q}) + (1-\widetilde{L})\widetilde{Q}(qr_0w^4 + s_0\kappa_8) + \widetilde{L}\widetilde{Q}w^4\theta^2 \\ t^{-1} &= (1-\widetilde{L})(1-\widetilde{Q})(r_0\kappa_q - s_0\kappa_8) + \widetilde{L}(1-\widetilde{Q}) + (1-\widetilde{L})\widetilde{Q}(qr_0w^4 - s_0\kappa_8) + \widetilde{L}\widetilde{Q}w^4\theta^{-2} \end{aligned}$$

The philosophy

We now give a short introduction to the philosophy of the counterexample. It will be vague, but longer explenations will follow in chapter 5 and subsection 6.2.1 .

Let G be a finite solvable group, and G a group basis of $\mathbb{Z}G$. The basis result of the theory is that a finite group basis H can be discribed by a 1-cocycle ρ of a certain Cech cohomolgy class depending only on G, with $H \cong G$ if and only if ρ is a coboundery.

For the purposes of the work of Hertweck, the special case where the order of G is divided by exactly two primes p and r suffices. Then, let $N_1 = O_{\acute{p}}(G)$ and $N_2 = O_{\acute{r}}(G)$ be the maximal normal subgroup of G whose order is prime to p, respectively to r. Note that $N_1 \cap N_2 = 1$. The cocycle ρ is a conjugacy class preserving automorphism δ_c of G/N_1N_2 and H is isomorphic to a pullback $G(\delta_c)$.

$$\begin{array}{ccc} G & \longrightarrow & G/N_2 \\ \downarrow & & \downarrow{\scriptstyle \pi_1} \\ G/N_1 & \xrightarrow[\pi_2]{} & G/N_1N_2 \end{array} \qquad \begin{array}{ccc} G(\delta_c) & \longrightarrow & G/N_2 \\ \downarrow & & \downarrow{\scriptstyle \pi_1 \cdot \delta_c} \\ G/N_1 & \xrightarrow[\pi_2]{} & G/N_1N_2 \end{array}$$

The group-theoretical obstruction is that $G(\delta_c) \cong G$ if and only if there are automorphisms $\sigma_1 \in \mathrm{Aut}(G/N_1)$ and $\sigma_2 \in \mathrm{Aut}(G/N_2)$ which induce automorphisms $\overline{\sigma}_1$ and $\overline{\sigma}_2$ of $\overline{G} = G/N_1N_2$ such that $\delta_c = \overline{\sigma}_1 \cdot \overline{\sigma}_2^{-1}$. So we are doing in fact litle deformations so that the groups still stay the same.

The question remains how to realize δ_c. In other words, how can a group basis H with $H \cong G(\delta_c)$ be constructed? For this the normalizer problem will come in play.

3.2 Zassenhaus Conjectures

3.2.1 Link with (ISO)

We have discussed the isomorphism problem

$$\mathbb{Z}G \cong \mathbb{Z}H \Longrightarrow G \cong H.$$

It has a positive answer for nilpotent groups and metabelian groups. Roggenkamp and Scott proved the nilpotent case, and by doing so, they equally proved the second Zassenhaus Conjecture. In the mid sixties, Zassenhaus made seemingly very strong conjectures. We discuss these conjectures and their relationship with (ISO). As before, the groups G will be finite. All automorphisms of $\mathbb{Z}G$ are normalized with respect to ϵ_G, the augmentation associated to the group basis G.

Conjecture 2 *(Zassenhaus, 1974)*

(ZC1) *If $u \in V(\mathbb{Z}G), o(u) < \infty$ then $u \sim_{\mathbb{Q}G} g$, for some $g \in G$.*

(ZC2) *If H is a finite subgroup such that $\mathbb{Z}G = \mathbb{Z}H$, $\epsilon_G(H) = 1$ then $\alpha^{-1}H\alpha = G$, for some $\alpha \in \mathcal{U}(\mathbb{Q}G)$.*

(ZC3) *If H is a finite subgroup of $V(\mathbb{Z}G)$ then $\alpha^{-1}H\alpha \subseteq G$ for some $\alpha \in \mathcal{U}(\mathbb{Q}G)$.*

(Aut) *If $\theta \in Aut(\mathbb{Z}G)$ then there exists $\beta \in Aut(G)$ and $\alpha \in \mathcal{U}(\mathbb{Q}G)$ such that $\theta(g) = \alpha^{-1}g^{\beta}\alpha$ for all $g \in G$*

One has to consider rational conjugation in the conjecture because if one only consider conjugation in $\mathbb{Z}G$ then a counterexample can already be found in $\mathbb{Z}S_3$ (REF). Let we begin by discussing the implications between these conjectures and also the corelation with (ISO). First remember the following lemma that is proved in G.Higman's dissertation, [43].

Lemma 3.2.1 *If H is a finite subgroup of $V(\mathbb{Z}G)$ then the elements of H are linear independent over $\mathbb{Z}$. Moreover, $|H|$ is a divisor of $|G|$. Finally, if $|H| = |G|$ then $\mathbb{Z}G = \mathbb{Z}H$.*

So (ZC3) concerns any finite subgroup of $V(\mathbb{Z}G)$, (ZC2) deals with maximal order finite subgroups, whereas (ZC1) has to do with cyclic subgroups of $V(\mathbb{Z}G)$. Thus the first point of the following proposition is clear.

Proposition 3.2.2 *1. (ZC3) $\Longrightarrow$ (ZC1) and (ZC2).*

2. (ZC2) $\Longrightarrow$ (ISO).

Proof. Suppose H is a finite group and that $\theta : \mathbb{Z}H \to \mathbb{Z}G$ is an isomorphism. Then, by lemma 3.2.1, $\mathbb{Z}G = \mathbb{Z}H^\theta$. Therefore, by (ZC2), $H^\theta = \alpha^{-1}G\alpha$ for a suitable $\alpha \in \mathcal{U}(\mathbb{Q}G)$. We deduce that $H \cong H^\theta = \alpha^{-1}G\alpha \cong G$. □

This implication is historically very important, because Roggenkamp and Scott -in their breakthrough- proved (ZC2) for nilpotent groups (REF). Further we have the following implications.

Proposition 3.2.3

(ZC2) $\Longrightarrow$ *(Aut)*

(Aut) + (ISO) $\Longrightarrow$ *(ZC2)*

Proof. (1) Suppose (ZC2). Let $\theta \in \mathrm{Aut}(\mathbb{Z}G)$. Then, by lemma 3.2.1, $\mathbb{Z}G = \mathbb{Z}G^\theta$. By (ZC2), $G^\theta = \alpha^{-1}G\alpha$ for some $\alpha \in \mathcal{U}(\mathbb{Q}G)$. Thus, for every $g \in G$ there exists a g_1 such that

$$\theta(g) = \alpha^{-1}g_1\alpha, \quad g_1 \in G.$$

Clearly, the mapping $g \mapsto g_1$ is an automorphism of G and (Aut) follows.

(2) Let H and G be finite groups such that $\mathbb{Z}G = \mathbb{Z}H$. Then by (ISO) there is an isomorphism θ between G and H. By (Aut) there exists an $\alpha \in \mathbb{Q}G$ and $\sigma \in \mathrm{Aut}(G)$ such that $\theta(g) = \alpha^{-1}g^\sigma\alpha$. Consequently, $H = \alpha^{-1}G\alpha$. □

3.2.2 Survey

The utility of the thirth and second Zassenhaus conjecture is obvious, since they imply (ISO) and it gives clearly a new light on the whole story. Roggenkamp and Scott proved (ZC2) for nilpotent groups (REF).For arbitrary finite groups they gave a counterexample (REF) using the bimodule techniques of Weiss (REF). A metabelian group of order $2^6.3.5.7$ provided a counterexample. However a counterexample of smaller order to (ZC2) has been given by Hertweck, [6]. Moreover, he made no use of the complicated bimodule theory of Weiss. His counterexample is of order 1440 and will be discussed in section 6.3. We survey some positive results.

Theorem 3.2.4 *Let A be an abelian group and P a p-group for some prime p. Then (Aut) has a positive answer for*

1. *S_n (Peterson). (REF)*
2. *$AwrS_n$ (Giambruno-Sehgal-Valenti). (REF)*
3. *$PwrS_n$ if p is odd (Giambruno-Seghal). (REF)*
4. *$PwrS_n$ if p is 2(Parmenter-Sehgal). (REF)*

5. $S_k wr S_n$ (Valenti). (REF)

The conjecture (ZC1) has been proved for metacylic groups $\langle a\rangle \rtimes \langle x\rangle$ with $(o(a), o(x)) = 1$ by Polcino Milies-Ritter-Sehgal. Valenti proved that (ZC3) also hold for these groups and one can even change $\langle x\rangle$ in a arbitrary finite abelian group X. Concerning the above metacylic groups, recently Angel Del Rio and S.K sehgal has proven a bit stronger result, see [12]. By $\pi(G)$ we mean the set of primes that divides $|G|$ and if G is a nilpotent group then G_p denotes the Sylow p-subgroup of G and $G_{p'}$ the product of the Sylow q-subgroups G_q with $q \in \pi(G) \setminus \{p\}$.

Theorem 3.2.5 *Let G be a finite group and assume $G = AX$ for A a cyclic normal subgroup and X an abelian subgroup of G. Assume additionally that $\pi(A) \cap \pi(X)$ has at most one element and if such a element, say p, exists then A_p and $X_{p'}$ commute elementwise. Then every torsion unit of $V(\mathbb{Z}G)$ is conjugate in $\mathbb{Q}G$ to an element in G*

The next result of Martin Hertweck, [7], don't fit in the above result of Del Rio and Sehgal:

Proposition 3.2.6 *If $G = A \rtimes X$ with A a p-group, X abelian and $(|A|, |X|) = 1$ the conjecture (ZC1) holds.*

For p-groups Weiss proved even a stronger result than (ZC3). This has a really far reaching proof in which he found incredible results about permutation lattices. The reader can find proof of these results in [14]. For those who find finitness boring: you can state previous conjectures also for infinite groups. In this case a counterexample to (ZC2),(ZC1) and (ISO) are known. For the counterexample to (ZC2) see [14] and for the one to (ZC1) see [16].

3.3 Normal complements

3.3.1 Link with (ISO)

In [14] gives a very nice list of 56 research problems. In this chapter we are especialy interested in Problem 29 of the list. We explain its usefulness for (ISO).

Conjecture 3 *(problem 29)*

Suppose that G is a finite nilpotent group. Then G has a normal complement N in $V(\mathbb{Z}G)$, i.e $V(\mathbb{Z}G) = N \rtimes G$ for a normal subgroup N of $V(\mathbb{Z}G)$.

We recall a classical theorem of G.Higman (REF)

Theorem 3.3.1 *If A is a finite abelian group then $V(\mathbb{Z}A) = A \times \mathcal{U}_2(\mathbb{Z}A)$ where $\mathcal{U}_2(\mathbb{Z}A) = \mathcal{U}(\mathbb{Z}A) \cap (1 + \Delta^2(A))$ is a free abelian group.*

There are two parts to this theorem. The first says that the torsion units are trivial, i.e. they belong to A. The second part concerns the direct decomposition. In the noncommutative situation the question is whether there exists a normal torsion free group N so that we have a semidirect product $V(\mathbb{Z}G) = N \rtimes G$. In other words:

1. Does the inclusion $G \to V(\mathbb{Z}G)$ split?
2. If a splitting exists, is its kernel torsion free?

The following Proposition shows that these qustions are really relevant for (ISO).

Proposition 3.3.2 *1. An affirmative answer to questions 1 and 2 implies an affirmative answer to (ISO).*

2. For finite nilpotent groups, an affirmative answer to question 2 implies an affirmative answer to (ISO).

Proof. Let $\theta : \mathbb{Z}G \to \mathbb{Z}H$ be an normalized isomorphism. Write $V(\mathbb{Z}G) = N \rtimes G$. For $h \in H$ and $\theta^{-1}(h) = ng,\ n \in N,\ g \in G$ we define $\alpha(h) = g$. Then α is a homomorphism from H to G.

1. In this case, $\ker(\alpha) = \{h \in H \ : \ \theta^{-1}(h) \in N\} = 1$ as N is torsion free. Thus $G \cong H$ as they both have the same order.
2. Assume now that G is a nilpotent group. Suppose that P is a Sylow p-subgroup of G. Then by the normal subgroup correspondence (Theorem 1.1.1) $\theta(\hat{P}) = (\hat{P}_1)$ for some $P_1 \lhd H$ with $|P_1| = |P|$. Thus the Sylow

p-subgroups of H are normal for all p and thus H is nilpotent. Since H is nilpotent, its centre is not trivial. Consequently, if $\mathrm{Ker}(\alpha) \neq 1$ then $\mathrm{Ker}(\alpha) \cap \mathcal{Z}(H) \neq 1$. Let z be a non-trivial element in $\mathrm{Ker}(\alpha) \cap \mathcal{Z}(H)$. Now remind Theorem 1.3.3 that states that all central torsion units in $\mathbb{Z}G$ are trivial. Thus $\theta^{-1}(z)$, being a torsion element in the centre of $\mathbb{Z}G$, belongs to G. Thus $\theta^{-1}(z) \in G \cap N = 1$ and therefore $z = 1$, a contradiction. Hence $G \cong H$.

□

The second part may seem less of interest for us, since (ISO) is proved for nilpotent groups. But showing the question about normal complements could pave a more general way.

3.3.2 Survey

The questions were answered affirmatively for circle groups of nilpotent rings by Sandling [22] and Passman-Smith [49] who also handled groups having an abelian subgroup of index 2. The latter was greatly extended by Cliff-Sehgal-Weiss (see below and [50]). A first case where they found a normal complement to G in $V(\mathbb{Z}G)$ is when $\mathbb{Z}(G/A)$ has only trivial units with A an abelian normal group. A central technique in proving that next result, is the "Whitcomb argument"(see section 30 of [14]). More generally Cliff-Sehgal-Weiss proved the following (the interested reader can find proof in section 31,32 and 33 of [14]).

Theorem 3.3.3 *Cliff-Sehgal-Weiss,[50]*

Let G be a finite group having an abelian normal subgroup A, such that either

1. *G/A is abelian of exponent dividing 4 or 6 or*
2. *G/A is abelian of odd order.*

Then G has a normal torsion-free complement in $V(\mathbb{Z}G)$.

The problem remains open in general. However for a finitely generated (not necessarily finite) nilpotent group of class two an affirmative answer is known. It is due to Sandling [23] and Losey [51].

Theorem 3.3.4 *Sandling and Losey*

Let G be a finitely generated nilpotent group of class two. Then there exists a normal subgroup N of $V(\mathbb{Z}G)$ so that $V(\mathbb{Z}G) = N \rtimes G$. Moreover, N is torsion free.

One can also prove, see [14, p. 182]

Theorem 3.3.5 *Let A be a normal abelian subgroup of a finite nilpotent group G. Then $\mathcal{U}(1+\Delta(G)\Delta(A))$ is torsion free.*

For the moment we have several nice results, but counterexamples are also known. They are: $C_{72} \rtimes C_8, C_{241} \rtimes C_{10}$, some $PSL(n,q)'s$ (see [26, 24]) and $G = C_{41} \rtimes C_8$. Proof of the last one can be found in Section 35 of [14].

3.4 Normalizer problem

3.4.1 Survey

Let H be a subgroup of a group G. By $N_G(H)$ we denote the normalizer of H in G, i.e.

$$N_G(H) = \{g \in G \ : \ g^{-1}Hg = H\}.$$

So $H \triangleleft G$ if and only if $N_G(H) = G$.

Conjecture 4 *Normaliser problem*

Let G be a group. Then

$$N_{\mathcal{U}(\mathbb{Z}G)}(G) = G.\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)).$$

Obvious $G.\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)) \subseteq N_{\mathcal{U}(\mathbb{Z}G)}(G)$ for any group G. These are called the trivial normalizators. The conjecture says that G lies very rigidly in the unit group $\mathcal{U}(\mathbb{Z}G)$. The Normalizer problem has been proved for finite nilpotent groups and for groups of odd order. This conjecture has played a very big role in the counterexample to (ISO). Hertweck attacked (ISO) through the normalizer problem. He first discovered two counterexamples to the normaliser problem and use thse to construct a counterexample to (ISO). We formulate the counterexample of smallest order and a proof will follow in section 6.1.

Theorem 3.4.1 *Hertweck*

There is a finite group G with a non-inner group automorphism τ, and $t \in V(\mathbb{Z}G)$ such that $g\tau = g^t$ for all $g \in G$, i.e $t \in N_{\mathcal{U}(\mathbb{Z}G)}(G) \setminus G.\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$. The group G has order $2^{25}.97^2$, a normal Sylow 97-subgroup and is metabelian.

Remark that the group G in this counterexample and in the counterexample of (ISO) are not the same. This G has derived length 2 and the G from $X = G \rtimes \langle c \rangle$ in (ISO)'s counterexample have derived length 3. Nevertheless, the main ingredients for the proof of Theorem 3.1.2 will already appear in the proof of Theorem 3.4.1, with many of the details entirely parallel. By increasing the derived length, Hertweck was able to use a slightly smaller Sylow 2-subgroup for the group G in Theorem 3.1.2. The latter group is, for the most part, simpler in structure and provides a good introduction to the group G in 3.1.2. Beyond this expository advantage, the group G in Theorem 3.4.1 allows us hope to find a counterexample to (ISO) with a group X of derived length 3. Before we begin to discuss the proof of the counterexample and the correlation with (ISO), we state several positive results to the Normalizer problem and afterwards prove the normalizer problem for finite nilpotent groups.

Theorem 3.4.2 *The normalizer problem has a positive answer for the following groups*

1. *If G is a finite group and has a normal Sylow 2-subgroup (Jacowski-Marciniak, 1987, [52]).*
2. *If G is a simple finite group (Feit, Seits, 1988, REF)*
3. *If G is a locally nilpotent group (Jespers, Juriaans, de Miranda, Rogerio, 2002, [53, Theorem 2.4])*
4. *If the finite normal subgroups of G have a normal Sylow 2-subgroup (Hertweck, 2004,[9, Corollary 19.11])*
5. *If G is a finite Frobenius group (Petit Lobão, Polcino Milies, 2002, [54, Theorem 3.1])*
6. *If G is a finite group such that the intersection of all its non-normal subgroups is non-trivial (Li, Parmenter and Sehgal, 1999, [55, Theorem 1])*

The result of Jacowski and Marciniak also includes finite nilpotent groups. We will prove this particular case. Let's proof a first result towards this.

Proposition 3.4.3 (Coleman) *Let P be a p-group contained in a finite group G. Set $\mathcal{U} = \mathcal{U}(\mathbb{Z}G)$ and suppose that $u \in N_{\mathcal{U}}(G)$. Then there exists $y \in G$ such that $u^{-1}gu = y^{-1}gy$ for all $g \in P$.*

Proof. For $g \in G$ define $\phi(g) = u^{-1}gu$. Because u is in the normalizator of G, $\phi(g)$ is again in G. Write $u = \sum_{x\in G} u(x)x$. Since $u = g^{-1}u\phi(g)$ we have that $\sum_{x\in G} u(x)x = \sum_{x\in G} u(x)g^{-1}x\phi(g)$. Thus g acts on the set G by $\sigma_g(x) = g^{-1}x\phi(g)$ and the function $u : G \to \mathbb{Z}$ given by $x \mapsto u(x)$ is constant on the orbits of this action. Let $g \in P$, so P acts on the set G. The orbits of this action are of length a power of p. Applying the augmentation map we obtain that

$$\pm 1 = \epsilon(u) = \sum c_i p^{v_i},$$

where p^{v_i} is the length of the orbit of g_i and $u(g_i) = c_i$ ($\pm 1 = \epsilon(u)$ because ϵ is an homomorphism and thus $\mathcal{U}(\mathbb{Z}G) = \mathcal{U}(\mathbb{Z}) \times V(\mathbb{Z}G) = \pm V(\mathbb{Z}G)$). It follows that there exists an orbit of length one, that is to say, there exists an $x \in G$ such that $\sigma_g(x) = x$ for all $g \in P$. This implies that $g^{-1}x\phi(g) = x$, and thus $\phi(g) = x^{-1}gx$ for all $g \in P$ as claimed. □

Theorem 3.4.4 *Let G be a finite nilpotent group. then $N_{\mathcal{U}}(G) = GZ(\mathcal{U})$.*

Proof. Write $G = \prod P_i$ as a product of Sylow p_i-subgroups. Let $u \in N_{\mathcal{U}}(G)$. Then by Proposition 3.4.3, there exists $x_i \in G$ such that $u^{-1}gu = x_i^{-1}gx_i$ for $g \in P_i$. We can pick $x_i \in P_i$ It follow that $u^{-1}gu = x^{-1}gx$ for all $g \in G$ with $x = \prod x_i$. □

Let $u \in N_{\mathcal{U}}(G)$ and write $conj(u)(g) = u^{-1}gu$ for $g \in G$. Then $conj(u)$ is an automorphism of G. Since G is finite the order of $conj(u)$ is finite. Krempa proved the following proposition.

Proposition 3.4.5 (Krempa) *Let $u \in N_{\mathcal{U}}(G)$. Then $conj(u)^2$ is inner, i.e. $u^2 \in G.Z(\mathcal{U})$.*

In fact, Krempa proved a more general result, see the sentence after Conjecture 5. With this we can easily prove the normalizer problem for groups of odd order.

Theorem 3.4.6 (Jacowski and Marciniak) *The Normalizer problem has a positive answer for finite groups of odd order.*

Proof. Take $u \in N_{\mathcal{U}}(G)$ and define $\phi = \text{conj}(u)$. By Proposition 3.4.5, ϕ^2 is conjugation by a $g \in G$; $\phi^s = 1$ for some odd s. By Bézout there exists a $l, t \in \mathbb{Z}$ such that $2l + st = 1$, $\phi = \phi^{2l+st} = (\phi^2)^l.(\phi^s)^t = \phi^{2l}$ is conjugation by g^l. □

In fact, as stated in Theorem 3.4.2, Jackowski and Marciniak have proved the Normalizer problem for groups having a normal Sylow 2-subgroup. This of course extends the two previous results. One thing is nowadays clear, automorphisms of G and $\mathbb{Z}G$ will play an important role in trying to prove or disprove (ISO). We develop this idea.

Even if we are interested in the integral case,we formulate the next part for more general rings R. Let G be a finite group, R an integral domain of characteristic 0. If no prime divisor of $|G|$ is invertible in R, we shall say that R is G-adapted. Examples of G-adapted rings are $\mathbb{Z}, \mathbb{Z}_{(p)}$ and $\mathbb{Z}_\pi$. The last one is the intersection of the localizations $\mathbb{Z}_{(p)} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b\}$ at the ideal (p) with $p \in \pi(G)$. This ring is more comfortable than $\mathbb{Z}$ itself, since it has only finitely many maximal ideals, and the same is true for the group ring $\mathbb{Z}_\pi G$. We formulate the sequel for arbitrary G-adapted rings and especially $\mathbb{Z}$, because those localizations give rise to more possibilities than the integers $\mathbb{Z}$. In the past the ring $\mathbb{Z}_\pi$ gave a lot of insight in the integral case and in that context one talks about local-global theories. If one is interested in the properties of G which are determined by the module category $\mathbb{Z}G$-Mod, the ring $\mathbb{Z}_\pi G$ is even the better setting since the following statements are equivalent: there is an equivalence $\mathbb{Z}G - mod \equiv \mathbb{Z}H - mod$ of module categories; there is an isomorphism $\mathbb{Z}_\pi G \cong \mathbb{Z}_\pi H$ of rings; there is an equivalence $\mathbb{Z}_\pi G - mod \equiv \mathbb{Z}_\pi H - mod$.

We identify group automorphisms of G with the R-algebra automorphisms of RG normalizing the group basis G. Let

$$Aut_R(G) = \{\phi \in \text{aut}(G) \ : \ \phi = \text{conj}(u) \text{ for some } u \in \mathcal{U}(RG)\}.$$

Note that for a G-adapted ring $\text{Aut}_R(G)$ is contained in $\text{Aut}_c(G)$, the group of conjugacy class preserving automorphisms of G (REF). Some authors, such as

Hertweck in his ph.d thesis, prefer to call these automorphisms central Automorphisms. This is due to the fact that these groupautomorphisms, induce central automorphisms of the group rings (in the ring theoretic sense, i.e. fixing the center elementwise). The quotient $\mathrm{Aut}_R(G)/\mathrm{Inn}(G)$, denoted by $\mathrm{Out}_R(G)$, has two natural interpretations. It is the kernel of the natural map $\mathrm{Out}(G) \to \mathrm{Out}(RG)$, and it is isomorphic to $N_{\mathcal{U}}(G)/G.Z(\mathcal{U})$ (the reader should be able to see this easily). In particular, $\mathrm{Out}_R(G) = \{1\}$ means that there are no non-obious units in RG which normalize G. With this we reformulate the Normaliser problem.

Conjecture 5 *If G is a finite group then $Out_{\mathbb{Z}}(G) = 1$.*

In fact J.Krempa proved that $\mathrm{Out}_{\mathbb{Z}}(G)$ is an elementary abelian 2-group, for any finite group G ([52, Theorem 3.2]). It is also known that each prime divisor of the order of $\mathrm{Aut}_c(G)$ also divides $|G|$. For a group G whose generalized Fitting subgroup is a p-group, and an integral domain S in which p is not invertible, Hertweck proved that $\mathrm{Out}_S(G) = 1$. ([10, 4.2.4]).

M.Mazur established a connection of the normalizer problem to the isomorphism problem for infinite groups, [56]. It was the following.

Theorem 3.4.7 (Mazur) *Let G be a group and $\alpha_0, \beta_0 \in Aut(G)$, and let $\alpha, \beta : C_\infty = \langle x \rangle \to Aut(G)$ the homomorphisms determined by $x \mapsto \alpha_0$ and $x \mapsto \beta_0$. then*

1. *$G \rtimes_\alpha C_\infty \cong G \rtimes_\beta C_\infty$ if and only if $\alpha_0\beta_0^{-1}$ is an inner automorphism of G.*
2. *$R[G \rtimes_\alpha C_\infty] \cong R[G \rtimes_\beta C_\infty]$ if and only if $\alpha_0\beta_0^{-1}$ is an inner ring automorphism of RG.*

This was used by Roggenkamp and Zimmermann together with results concerning outer group automorphisms that become inner in an integral group ring ([20]) to find a counterexample to the Isomorphism Problem for infite polycyclic groups, [18]. A modified construction works for finite groups too. But before citing these results, we introduce some notations and definitions and related problems.

Let R be a commutative ring and Λ an R-order on which a finite group H acts via an R-algebra homomorphism $\iota : RH \to \Lambda$ (i.e $\lambda^h = \lambda^{h\iota}$ for all $h \in H$). A multiplicative 1-cocycle on H with values in Λ is a map $\mu : H \to \Lambda$ satistfying $\mu(gh) = \mu(g)^h.\mu(h)$ for all $g, h \in H$. Such a μ is called a 1-coboundary provided there exists a unit $u \in \Lambda$ such that $\mu(h) = u^{-h}.u$ for all $h \in H$.

For any automorphism $\gamma \in \mathrm{Aut}(G)$ and $u \in RG$ one defines the norm $N_\gamma(u)$ of u with respect to γ by

$$N_\gamma(u) = u^{\gamma^{n-1}} \ldots . u^\gamma . u$$

where n is the order of γ. If $N_\gamma(u) = 1$, then $\mu(\gamma) = u$ defines a (multiplicative) 1-cocycle $\mu : \langle\gamma\rangle \to RG$ and conversely. Note that if $N_\gamma(u)$ is a unit of finite

order, there is a cyclic group $\langle c\rangle$ of finite order, acting via γ on RG (i.e $x^c = x\gamma$ for all $x \in RG$), such that $\mu(c) = u$ defines a 1-cocycle $\mu : \langle c\rangle \to RG$.

From now on let R be a G-adapted ring. We are interesed in cocycles $\langle c\rangle \to RG$ with values in $\mathcal{N}_{\mathcal{U}(RG)}(G)$. The following problems are of interest in our context.

Problem. Give examples of triples (G, u, γ) where G is a finite group, the unit $u \in \mathcal{N}_{\mathcal{U}(RG)}(G)$ induces a non-inner automorphism $\alpha = \mathrm{conj}(u)$ of G of order m and $\gamma \in \mathrm{Aut}(G)$ such that one of the following holds.

1. (P 1) $N_\gamma(u)$ is finite order.
2. (P 2) $N_\gamma(u)$ is finite order, and $\overline{\gamma}$ and $\overline{\alpha\gamma}$ are not conjugate in $\mathrm{Out}(G)$.
3. (P 3) $N_\gamma(u^m)$ is of finite order.

Remark 3.4.8

- *(P 1), and in particular (P 2), are very difficult problems. If (P 2) is solved, it is possible to construct non-isomorphic groups X and Y with isomorphic group rings, $RX \cong RY$ (see Theorem 3.4.9 and Proposition 3.4.10). If G and γ have odd order, the groups X and Y may be chosen to have odd order, too.*
- *As shown in section 6.2, problem (P 2) is solved by Hertweck with G of even order.*

One can wonder if there is a connection between the problems, in particular between (P 1) and (P 3). The connection is the following. Assume that (P 3) is solved, and that the $u\gamma^i$, $i \in \mathbb{N}$ commute pairwise (this happens for example when γ normalizes $\langle a\rangle$). Then $N_\gamma(u)$ has finite order and (P 1) is solved. However, note that if γ acts coprime on $\langle\alpha\rangle$, we will not get a solution of (P 2) in that way.

Let us look for a practicable approach to (P 3). Given G and $u \in \mathcal{N}_{\mathcal{U}(RG)}(G)$ inducing a non-inner automorphism $\alpha = \mathrm{conj}(u)$ of G of order m, the central unit u^m may be calculated in the form c^m for some central unit c of KG, where K is some field containing R. The question, then, is whether there exists a central unit z of RG and $\gamma \in \mathrm{Aut}(G)$ so that $N_\gamma(cz)$ is of finite order and γ acts on $\langle\alpha\rangle$ (for then we could replace u by uz, thus giving a solution of (P 1)).

We now cite and prove some results relating (P 2) to (ISO). These proofs give information on how to construct non-isomorphic groups. The first result was obtained in the Ph.D of Herweck [10] and the second one is written down in his Habilitationschrift [9]. But first remark that for any group K, $\kappa \in \mathrm{Aut}(K)$ of order r, and a cyclic group $\langle x\rangle$ whose order is divisible by r, we may define the semidirect product $S = K \rtimes \langle x\rangle$ with x acting via κ, i.e $k^x = k\kappa$ for all $k \in K$. In this case, we also write $S = K \rtimes_\kappa \langle x\rangle$.

Theorem 3.4.9 *Let G be a finite group. Let $\tau \in Aut(G)$ and $t \in V(\mathbb{Z}G)$ such that $g\tau = g^t$ for all $g \in G$. Assume that there is a $\gamma \in Aut(G)$ such that*

(1) $t\,\gamma = t^{-1}$;

(2) γ is not conjugate to an automorphism of the coset $\tau\langle\gamma\rangle$ in $Out(G)$.

Let $\langle c\rangle$ be a finite cyclic group whose orders is divisible by the order of γ and $\tau\gamma$, so the groups $G_\gamma = G \rtimes_\gamma \langle c\rangle$ and $G_{\tau\gamma} = G \rtimes_{\tau\gamma} \langle c\rangle$ can be defined, where c acts on G via γ and $\tau\gamma$, respectively. Then the integral group rings $\mathbb{Z}G_\gamma$ and $\mathbb{Z}G_{\tau\gamma}$ are isomorphic. However, the order of c can be chosen such that the groups G_γ and $G_{\tau\gamma}$ are not isomorphic.

Proof. We first show that $o(tc) = o(c)$. Consider tc as an element of $\mathbb{Z}G_\gamma$. From (1) we extract that $(tc)^2 = c^2$. In particular, tc is of finite order and we only have to show that that neither tc, neither c have odd order.

Assume that tc or c is of odd order. Then $t^2 = 1$ since $t^{tc} = t^{-1} = t^c$ by (1) and the well known result that elements of odd order only can invert elements of order ≤ 2. As t normalizes G, it follows that $\langle G, t\rangle$ is a finite subgroup of $V(\mathbb{Z}G)$. By (2), τ is a non-inner automorphism of G, so $\langle G, t\rangle$ has order strictly greater than $|G|$. But the order of finite subgroups of $V(\mathbb{Z}G)$ must divide the order of G , so tc and c have the same order.

It follows that $G_{\tau\gamma}$ is isomorphic to the subgroup $\langle G, tc\rangle$ of $V(\mathbb{Z}G_\gamma)$, so the integral group rings $\mathbb{Z}G_\gamma$ and $\mathbb{Z}G_{\tau\gamma}$ are isomorphic.

Also, it follows that γ and $\tau\gamma$ have the same order, say, n. Denote the order of G by m. Let c be of order nm^2 and suppose that an isomorphism $\phi : G_\gamma \to G_{\tau\gamma}$ exists. Let $K = \langle c^{nm}\rangle$, a central subgroup of G_τ of order m. Then $K\phi = K$ as $c^n\phi \in G \times \langle c^n\rangle$. Since $G\phi \subseteq G \times K$, there is $\theta \in \mathrm{Aut}(G)$ with $g\phi \in g\theta \cdot K$ for all $g \in G$. Let $c\phi = xc^r$ for some $x \in G$ and $r \in \mathbb{N}$. Note that r is odd since ϕ is surjective. For each $g \in G, g\gamma\phi \in g\gamma\theta \cdot K$, as well as $g\gamma\phi = (g^c)\phi = g\phi^{c\phi} \in (g\theta)^x(\tau\gamma)^r \cdot K$. Consequently $\gamma \cdot \theta = \theta \cdot \mathrm{conj}(x) \cdot (\tau\gamma)^r$ as automorphisms of G. Finally, $(\tau\gamma)^r = \tau \cdot \gamma^r$ as r is odd, so $\gamma^\theta = \mathrm{conj}(x) \cdot \tau\gamma^r$ and this contradicts (2). □

However, it should be remarked that condition (ii) of this proposition seems to be difficult to verify in practice. Now we state a result in the same spirit but with a slithly different construction.

Proposition 3.4.10 *Let G be a finite group, $\gamma \in Aut(G)$ and $u \in \mathcal{N}_{\mathcal{U}(RG)}(G)$ such that $N_\gamma(u)$ is of finite order. Set $\alpha = conj(u) \in Aut(G)$ and assume further that $\overline{\gamma}$ and $\overline{\alpha\gamma}$ are not conjugate in $Out(G)$. Then there are non-isomorphic groups X and Y such that $RX \cong RY$ and these groups are semidirect products $(G \times C_r) \rtimes C_n$, where n is the product of the order γ and $N_\gamma(u)$, and r is a prime with $(r, n|G|) = 1$ such that C_n acts faithfully on C_r.*

Proof. Let n be the product of the orders of γ and $N_\gamma(u)$. If m denotes the order of γ, then $(\gamma\alpha)^m = \mathrm{conj}(N_\gamma(u))$, so $\gamma^n = id$ and $(\gamma\alpha)^n = id$. Let $\langle c\rangle$ be a cyclic group of order n. Choose a cyclic group $\langle a\rangle$ of prime order r with $(r, n|G|) = 1$ such that n divides $r-1$ (what can be done by Dirichlet's theorem on primes in arithmetic progressions, see Theorem A.0.4), and let $\langle\mu\rangle$ be an automorphism of A of order n. The groups X and Y are given as

$$X = (G \times A) \rtimes_{(\gamma\times\mu)} \langle c\rangle \text{ and } Y = (G \times A) \rtimes_{(\gamma\alpha\times\mu)} \langle c\rangle.$$

Assume that $X \cong Y$ and fix an isomorphism $\phi : X \to Y$. Clearly $A\phi = A$, as A is a normal Hall subgroup of X and Y. It follows that $(GA)\phi = C_X(A)\phi = C_Y(A) = GA$, so $G\phi = G$. Note that the assumption on a and μ implies that there are $x \in G$ and $a \in A$ such that $c\phi = xac$. Thus for all $g \in G$,

$$g(\gamma.\phi) = (g^c)\phi = (g\phi)^{(c\phi)} = (g\phi.\mathrm{conj}(x))^c = g(\phi.\mathrm{conj}(x).\alpha.\gamma),$$

so $\phi|_G^{-1}.\gamma.\phi|_G = \mathrm{conj}(x).\alpha.\gamma$, contradicting the assumption that $\overline{\gamma}$ and $\overline{\alpha\gamma}$ are not conjugate in $\mathrm{Out}(G)$. Hence X and Y are non-isomorphic.

Note that $(cu)^m = c^m N_\gamma(u)$ in RX (where m is the order of γ), so $cu \in RX$ has order n, and it is easy to see that the subgroup $U = \langle G, M, cu\rangle$ of $\mathcal{U}(RX)$ is isomorphic to Y, and that $RU = RX$. This proves $RX \cong RY$. □

We make some final remarks on the above proof and proposition.

Remark 3.4.11

- *It is difficult to verify the non-conjugacy of $\overline{\gamma}$ and $\overline{\alpha\gamma}$ in concrete situations. To prove that X and Y are non-isomorphic it is better to use an obsctruction theory through projective limits as we will outline in chapter 5.*

- *The just mentioned obstruction theory also give information on how the group X should look like. As an example, assume that $X = Q \rtimes P$ is a semidirect product of a normal Sylow q-subgroup q and a sylow p-subgroup P. Let $R = Z_{\pi(X)}$ and $RX = RY$. It is known that the images of X and Y in RP and in $RX/O_p(X)$ are conjugate by rational units u and v, respectively (see F^*-theorem, Theorem 5.2.9, REF), which give rise to a class-preserving automorphism $\delta = conj(\overline{uv}^{-1}) \in Aut(P/O_p(X))$. The groups X and Y are isomorphic if and only if δ can be written as the product of two automorphisms, one induced from an automorphism of RP, the other induced from an automorphism of $RX/O_p(X)$. In particular, if $Out_c(P/O_p(X)) = 1$, then $X \cong Y$.*

The previous pages showed that we are interested in cocycles with values in commutative group rings. A first example will be used to construct the counterexample to the isomorphism problem for integral group rings. We will come back on it, after the counterexample, subsection 6.2.6.

3.4.2 Coleman automorphisms

A Coleman automorphism of a finite group G is an automorphism of G whose restriction to any Sylow subgroup of G equals the restriciton of some inner automorphism of G. These automorphisms has been introduced in [8, 11]. We write $\mathrm{Aut}_{Col}(G)$ for the group of Coleman automorphisms of G. The inner automorphisms clearly are a normal subgroup of the Coleman automorphisms. We define the outer-Coleman automorphisms as $\mathrm{Out}_{Col}(G) = \mathrm{Aut}_{Col}(G)/Inn(G)$. Due to the Ward-Coleman lemma, Coleman automorphisms occur naturally in the study of the normalizer of a finite group G in the units of its integral group rings $\mathbb{Z}G$:

Proposition 3.4.12 *(Ward-Coleman Lemma)*

Let G be a finite group, P a p-subgroup of G for some prime p, R a commutative ring such that $pR \neq R$. Then

$$\mathcal{N}_{U(RG)}(P) = \mathcal{N}_G(P)C_{U(RG)}(P).$$

This result means that a unit $u \in U(RG)$ of the group ring RG normalizing P acts by conjugation on P like a group element $g \in G$. Also, $\mathrm{Aut}_R(G) \leq \mathrm{Aut}_{Col}(G)$ and thus are of interest for the normalizer problem. Coleman automorphisms have been studied in their own right in [9, 11] by Hertweck and Kimmerle.

3.4.3 Central units

We now remark that the normalizer problem also is a problem about certain central units.

For if $t \in N_{\mathcal{U}(RG)}(G)$, we may take a cyclic group $\langle x \rangle$ of the same order as $\tau := \mathrm{conj}(t)$ and form the semidirect product $G_\tau := G \rtimes_\tau \langle x \rangle$ with respect to τ, i.e. $g^x = g^t$ for all $g \in G$. Then tx^{-1} is a central unit in RG_τ because both t and x are units and $g^{tx^{-1}} = g^t.g^{x^{-1}} = g^x.g^{x^{-1}} = g^e = g$.

We remark that if the above t is already a central unit, then x is trivial and so $G_\tau = G$. So this is not a interesting case. If t is an element of G, then tx^{-1} is a torsion central unit of $\mathbb{Z}G$. Remember that all the central torsion units of $\mathbb{Z}G$ are trivial (Theorem 1.3.3). If the normalizer problem has a positive answer, then the trivial normalizers one are the only normalizators of G in $\mathcal{U}(\mathbb{Z}G)$. Thus under the hypothesis that the normalizer problem has a positive answe we should find no non-trivial central units of the form tx^{-1}. This gives a new light on the normalizer problem.

Finite groups with only trivial central units have been classified by Ritter and Sehgal in [57] as follows.

Theorem 3.4.13 *Let G be a finite group. All central units of $\mathbb{Z}G$ are trivial if and only if for every $x \in G$ and every natural number j, relatively prime to $|G|$, $x^j \sim x$ or $x^j \sim x^{-1}$.*

One can show that this means that group G will have a lot of $\mathbb{R}$-characters. For a proof we refer to [14, p. 22]. From this result it follows that, in general, there do exist central units of infinite order in integral group rings of finite groups. Aleev constructed all central units of $\mathbb{Z}A_5$ and $\mathbb{Z}A_6$. Also, Li and Parmenter independently constructed all central units of $\mathbb{Z}A_5$ (REF).

Almost no constructions of central units are known. Jespers, Parmenter and Sehgal gave a recipe for constructing central units in $\mathbb{Z}G$, if G is nilpotent. This is done as follows.

Let G be a finite group which is nilpotent of class n. Let $\mathcal{Z}_i$ denote the i^{th} term of the upper central series of G. Then $\mathcal{Z}_n = G$. For an element $g \in G$, let $b \in \mathbb{Z}\langle g \rangle$ be a Bass cyclic unit. Recursively one defines.

$$b_1 = b, \quad b_i = \prod_{h \in \mathcal{Z}_i} b_{i-1}^h \quad \text{for } 2 \leq i \leq n.$$

We notice that $b_i \in \mathcal{Z}(\mathbb{Z}\langle \mathcal{Z}_i, g \rangle)$ by induction and also that the conjugates in the product commute. Thus b_i is well defined. For $i = n$ we get, b_n an element of the centre of $\mathbb{Z}G$. It has been proven in [4] that the units so constructed generate a subgroup of finite index in the centre of $\mathcal{U}(\mathbb{Z}G)$. Note that the previous construction can be modified and improved by considering the subnormal series $\langle g \rangle \triangleleft \langle \mathcal{Z}_1, g \rangle \triangleleft \ldots \triangleleft \langle \mathcal{Z}_n, g \rangle = G$ and taking in each step conjugates in a transversal for $\mathcal{Z}_i$ in $\mathcal{Z}_{i-1}$. Then both constructions differ by a power. The constructions remain valid when starting with an arbitrary unit u in $\mathbb{Z}G$ with support in an abelian subgroup.

Very recent by Jespers, Van Gelder, Olteanu and Del Río proved (REF) a generalization of above theorem of Jespers-Parmenter-Sehgal. A construction is given for a subgroup in the set of Bass units of $\mathbb{Z}G$ that is of finite index in $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ for G a finite abelian-by-supersolvable group G such that every cyclic subgroup of order not a divisor of 4 and 6 is subnormal in G. It is clear that this class of groups contains the finite nilpotent groups, the dihedral groups $D_{2n} = \langle x, y \mid x^n = 1 = y^2, yxy = x^{-1} \rangle$ and the generalized quaternion groups $Q_{2n} = \langle x, y \mid x^{2n} = 1 = y^4, x^n = y^2, y^{-1}xy = x^{-1} \rangle$. We brievly mention their construction and some obtained results.

Let $u \in \mathcal{U}(\mathbb{Z}\langle g \rangle)$, for $g \in G$ or order not a divisor of 4 or 6. Consider a subnormal series $\mathcal{N}$: $N_0 \triangleleft N_1 \triangleleft N_2 \triangleleft \ldots \triangleleft N_m = G$. Further, define

$$c_0^{\mathcal{N}}(u) = u \text{ and } c_i^{\mathcal{N}}(u) = \prod_{h \in T_i} c_{i-1}^{\mathcal{N}}(u)^h,$$

where T_i is a transversal for N_i in N_{i-1}. One can prove that the construction is independent of the order of the conjugates in the product expression. Furthermore

the final step in the construction is a central unit in $\mathbb{Z}G$. This is denoted by $c^{\mathcal{N}}(u)$. The authors of the construction proved following theorem.

Theorem 3.4.14 *(REF) Let G be a finite abelian-by-supersolvable group such that every cyclic subgroup of order not a divisor of 4 or 6, is subnormal in G. Then the group generated by the Bass units of $\mathbb{Z}G$ contains a subgroup of finite index in $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$.*

From this theorem two interesting corollaries are extracted.

Corollary 3.4.15 *Let G be a finite abelian-by-supersolvable group such that every cyclic subgroup of order not a divisor of 4 or 6, is subnormal in G. For each such cyclic subgroup $\langle g \rangle$, fix a subnormal series $\mathcal{N}_g$ from $\langle g \rangle$ to G. Then*

$$\langle c^{\mathcal{N}_g}(b_g) \mid b_g \text{ a Bass unit based on } g, g \in G \rangle$$

is of finite index $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$.

For finite nilpotent groups of class n, we can of course always take the subnormal series $\mathcal{N}_g : \langle g \rangle \triangleleft \langle Z_1, g \rangle \triangleleft \ldots \triangleleft \langle Z_n, g \rangle = G$. Since the constructions $c^{\mathcal{N}_g}(b)$ and b_n only differ on a power, one can deduce the Jespers-Parmenter-Sehgal result. With these central unit constructions the authors also constructed a basis for a free abelian subgroup of finite index in $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$.

3.4.4 Normalizer on subgroups

In this section we mention at a generalization of the normalizer problem. For facilitate the notation, we write $U = \mathcal{U}(\mathbb{Z}G)$. One says that a subgroup H of G has the normalizer property if

$$N_U = N_G(H)C_U(H).$$

We abbreviate this by $(NP : H \leq G)$. Remark that $(NP : 1 \leq G)$ holds always and $(NP : G \leq G)$ is simply the classical normalizer problem $N_U(G) = G.Z(U)$. One can look at the normalizer property from two points of view. First, fix the subgroup H and go through all the overgroups G. Secondly, fix the group G and go through all the subgroups H. In the first situation, positive resuts for $(NP : H \leq G)$ holds in the following cases.

Proposition 3.4.16

- *H is a p-group (Wald, 1960, REF).*
- *H is cyclic (Andreas Bächle, REF).*
- *$H \triangleleft G$, $|H| = pq$ with p and q primes (Andreas Bächle, REF).*
- *$H \triangleleft G$, H is torsion-free abelian (Andreas Bächle, REF).*

No other results seem to be known if one fixes H.

Let us now fix G and go through all the subgroups H of G. This problem is called the 'subgroup normalizer proprety'. Explicitly:

$$(SNP : G) \Longleftrightarrow \forall H \leq G : \ (NP : H \leq G)$$

The survey of the other conjectures teach us that the nilpotent groups somehow behave well. This is also the case here. If G_1 and G_2 are two nilpotent groups, then $(SNP : G_1 \times G_2)$ holds if and only if $(SNP : G_1)$ and $(SNP : G_2)$ holds.

Theorem 3.4.17 *(REF) For G a periodic locally nilpotent group $(SNP : G)$ holds, and thus in particular for finite nilpotent groups.*

The proof goes through the following lemmas and typical cohomology arguments.

Lemma 3.4.18 *Let $K \leq G$, $C \leq Z(G)$. Then*

$$(NP : KC \leq G) \Longrightarrow (NP : K \leq G).$$

and

Lemma 3.4.19 *Let $1 \longrightarrow C \hookrightarrow G \longrightarrow \overline{G} \longrightarrow 1$ be a central extension, C torsion-free, $C \leq L \leq G$ and $|\overline{L}| < \infty$. Then*

$$(NP : \overline{L} \leq \overline{G}) \Longrightarrow (NP : C \leq G).$$

An other positive result is the following

Proposition 3.4.20 *Let G be a finitly generated nilpotent group. Then $(NP : H \leq G)$ holds for finite $H \leq G$.*

One would like to dropp the restriction of finitness on H. In the following case this is possible.

Proposition 3.4.21 *Let G be a nilpotent group of class 2 with torsion-free center. Then $(SNP : G)$ holds.*

Other families are known and also these proofs are due to Andreas Bächle.

Proposition 3.4.22 *The following groups G satisfy $(SNP : G)$*

- *G is of square-free order,*
- *G has an abelian subgroup of index 2,*
- *G is of order $|G| = pqr$ with p, q, r, eventuelly equal, primes.*

Remark that most groups of less then or equal to order 50 falls under one of these families.

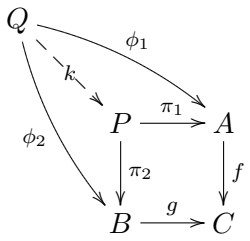
4 Some Pullback Diagrams

In this chapter, we introduce pullback diagrams describing the integral group ring $\mathbb{Z}G$ of a finite group G. They naturally show up in the presence of normal subgroups of G. We first lay out the general setting.

Let $\mathcal{C}$ a category, $A, B, C \in \mathrm{Ob}(\mathcal{C})$ and $f \in \mathrm{Hom}_{\mathcal{C}}(A, C), g \in \mathrm{Hom}_{\mathcal{C}}(B, C)$. Then an object $P \in \mathrm{Ob}(\mathcal{C})$ is called the pullback of f and g if there are morphisms $\pi_1 \in \mathrm{Hom}_{\mathcal{C}}(P, A)$ and $\pi_2 \in \mathrm{Hom}_{\mathcal{C}}(P, B)$ such that

$$\begin{array}{ccc} P & \xrightarrow{\pi_1} & A \\ \downarrow{\scriptstyle \pi_2} & & \downarrow{\scriptstyle f} \\ B & \xrightarrow{g} & C \end{array}$$

is a commutative diagram and for every other triple (Q, ϕ_1, ϕ_2) with $f \circ \phi_1 = g \circ \phi_2$ there is a morphism $k \in \mathcal{C}(Q, P)$ such that $\pi_2 \circ k = \phi_2$ and $\pi_1 \circ k = \phi_1$.



We gave a specific example. Let R be an arbitrary ring, I and J ideals of R such that $I \cap J = \{0\}$. Then R is the pullback of the natural maps $\sim: R/J \to R/(I+J)$ and $- : R/I \to R/(I+J)$. So the diagram

$$\begin{array}{ccc} R & \longrightarrow & R/I \\ \downarrow & & \downarrow{\scriptstyle -} \\ R/J & \xrightarrow{\sim} & R/(I+J) \end{array}$$

commutes and R is in some sense unique to do this. One easily checks that $P = \{(r+I, s+J) \in (R/I, R/J) \mid \overline{r+I} = \widetilde{s+J}\}$ is the pullback of $\sim: R/J \to R/(I+J)$ and $- : R/I \to R/(I+J)$. Thus we only have to show that $R \cong P$. Consider the ringhomomorphism $\phi : R \to P : r \mapsto (r+I, r+J)$. In order to show that ϕ is injective, assume that $\phi(r_1) = \phi(r_2)$ then $r_1 - r_2 \in I \cap J = \{e\}$. Thus $r_1 = r_2$. To show that ϕ is surjective, assume $(r_1 + I, r_2 + J) \in P$. Then

$r_1 - r_2 \in I + J$. So there exist $i \in I, j \in J$ such that $r_1 - r_2 = i + j$. Take $r = r_1 - i = r_2 + j$. Then $\phi(r) = (r_1 + I, r_2 + I)$ as desired. Thus R is indeed the pullback.

Some authors, also call R the fibre product. The above tells us that if one has elements in R/I and R/J that are maped to the same element in $R/(I + J)$ then there is a unique element in R projecting to the previous elements in R/I and R/J. We deduce immediatly the follewing very useful proposition.

Proposition 4.0.23 *Let R be a ring and I and J ideals of R with $I \cap J = \emptyset$. Then the following diagram of natural maps is commutative*

$$\begin{array}{ccc} \mathcal{U}(R) & \longrightarrow & \mathcal{U}(R/I) \\ \downarrow & & \downarrow{\scriptstyle -} \\ \mathcal{U}(R/J) & \xrightarrow{\sim} & \mathcal{U}(R/(I+J)) \end{array}$$

and $\mathcal{U}(R) \cong \{(u_1, u_2) \in (\mathcal{U}(R/I), \mathcal{U}(R/J)) \mid \overline{u_1} = \widetilde{u_2}\}$.

This idea will often be used in the thesis. To prove that an element is a unit we will go through two natural projections and show that the projections are equal modulo an ideal.

Analogous to the ring-case we can prove that G is the pullback of $\sim: G/N_2 \to G/N_1N_2$ and $- : G/N_1 \to G/N_1N_2$, where N_1 and N_2 are normal subgroups of G with $N_1 \cap N_2 = \{1\}$.

We will often associate the following pullback diagrma to a normal subgroup K of a finite group G

$$\begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \mathbb{Z}(G/K) \\ \downarrow & (*) & \downarrow \\ \mathbb{Z}G/(\hat{K}) & \longrightarrow & (\mathbb{Z}/|K|\mathbb{Z})(G/K) \end{array}$$

This is indeed a pullback diagram because $\mathbb{Z}(G/K) \cong \mathbb{Z}G/\Delta(G, K)$. That the common quotient looks like that follows from $0 = \hat{K} = \sum_{k \in K} k = \sum_{k \in K} 1 = |K|$.

Let $L, Q \triangleleft G$. Denote by Γ the image of $\mathbb{Z}G$ under he natural map $\kappa : \mathbb{Z}G \to \mathbb{Z}(G/L) \oplus \mathbb{Z}(G/Q)$. The kernel of this map is clearly $T = \Delta(G, L) \cap \Delta(G, Q)$. Define $\Lambda = \mathbb{Z}(G)/S$ with $S = (L^+, Q^+)$. We have the following pullback diagrams:

$$\begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \Gamma \\ \downarrow & (**) & \downarrow \\ \Lambda & \longrightarrow & \Omega \end{array} \qquad \text{and} \qquad \begin{array}{ccc} \Gamma & \longrightarrow & \mathbb{Z}(G/Q) \\ \downarrow & (***) & \downarrow \\ \mathbb{Z}(G/L) & \longrightarrow & \mathbb{Z}(G/LQ) \end{array}$$

If L and Q are of coprime order, the common quotient Ω in $(**)$ has a particular nice description. This was proved by Roggenkamp and Scott [25, Theorem 2.1]. Herweck found a shorter proof in his Habilitationschrift [9, Theorem 7.1].

Theorem 4.0.24 *(Roggenkamp, Scott) Let $N_1, \ldots, N_r$ be normal subgroups of a finite group G with N_j and N_k of coprime order for all $j \neq k$. Set $R_i = R/|N_i|R$. The following diagram of natural maps is commutative and has exact rows.*

$$\begin{array}{ccccccc} 0 & \longrightarrow & \bigcap_i I(G,N_i) & \longrightarrow & \mathbb{Z}G & \longrightarrow & \bigoplus_i \mathbb{Z}G/N_i \\ & & \| & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \bigcap_i I(G,N_i) & \longrightarrow & \frac{\mathbb{Z}G}{\sum_i (\mathbb{Z}G)\hat{N}_i} & \longrightarrow & \bigoplus_i \frac{\mathbb{Z}_iG/N_i}{\sum_{j\neq i}(\mathbb{Z}_iG/N_i).\hat{N}_j} \longrightarrow 0 \end{array}$$

Moreover in their proof they showed that Ω equals $\oplus_i \Lambda_{\hat{i}}/n_i\Lambda_{\hat{i}}$ with $\Lambda_{\hat{i}} = \Lambda(G/N_i, N_1, \ldots, \hat{N}_i, \ldots, N_k)$ and $\Lambda(G, N_1, \ldots, N_k) = \mathbb{Z}G(\prod_i(1-\tilde{N}))$. In this thesis we will only be interested in the case of 2 components. We formulate the above theorem for this special case.

Theorem 4.0.25 *(Roggenkamp, Scott) Let G be a finite group with normal subgroups L and Q of coprime order. The following diagram of natural maps is commutative and her rows are exact.*

$$\begin{array}{ccccccc} 0 & \longrightarrow & \Delta(G,L)\cap\Delta(G,Q) & \longrightarrow & \mathbb{Z}G & \xrightarrow{\kappa} & \mathbb{Z}(G/L)\oplus\mathbb{Z}(G/Q) \\ & & \| & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \Delta(G,L)\cap\Delta(G,Q) & \longrightarrow & \mathbb{Z}G/(\hat{L},\hat{Q}) & \xrightarrow{\pi} & \frac{\mathbb{Z}(G/L)}{(Q^+,|L|)} \oplus \frac{\mathbb{Z}(G/Q)}{(L^+,|Q|)} \longrightarrow 0 \end{array}$$

Proof. Note $T = \Delta(G,L)\cap\Delta(G,Q)$ and $S = (\hat{L},\hat{Q})$. Since $(|L|,|Q|) = 1$, the map π is sujective. It remains to show that $T \cong S + T/S = ker(\pi)$, that is, $S + T = (S + \Delta(G,L)) \cap (S + \Delta(G,Q))$. The inclusion "'$\subseteq$"' is obvious. From

$$|Q| \cdot (S + \Delta(G,L)) \cdot (1-\widetilde{L})(1-\widetilde{Q}) = \Delta(G,L) \cdot (|Q| - \hat{Q}) \subseteq T,$$

and

$$|Q| \cdot (Q + \Delta(G,L)) \cdot (1 - (1-\widetilde{L})(1-\widetilde{Q})) = |Q| \cdot S + \Delta(G,L) \cdot \hat{Q} \subseteq S$$

it follows that $|Q| \cdot (S + \Delta(G,L)) \subseteq S + T$. The same holds with roles of L and Q reversed. This shows the other inclusion, since $(|L|,|Q|) = 1$. □

The diagram $(***)$ fits into a larger diagram. It can be extended to the right and to the bottom by a diagram of type $(*)$:

$$\begin{array}{ccccc} \Gamma & \longrightarrow & \mathbb{Z}(G/Q) & \longrightarrow & \mathbb{Z}(G/Q)/(L^+) \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{Z}(G/L) & \longrightarrow & \mathbb{Z}(G/LQ) & \longrightarrow & (\mathbb{Z}/|L|\mathbb{Z})(G/LQ) \\ \downarrow & & \downarrow & & \\ \mathbb{Z}(G/L)/(Q^+) & \longrightarrow & (\mathbb{Z}/|Q|\mathbb{Z})(G/LQ) & & \end{array}$$

This argument will be used in the proofs of the counterexample. It also gives more information on the way we will have to construct the counterexample:

Assume that there is $\tau \in \mathrm{Aut}_{\mathbb{Z}}(G)$ which is minimal in the sense that there are $x \in G/L$ and $y \in G/Q$ such that τ induces the inner group automorphisms $\mathrm{conj}(x)$ and $\mathrm{conj}(y)$ on G/L and G/Q respectively. Note that $z = \overline{xy}^{-1}$ is central in the common quotient $\overline{G} = G/LQ$. If τ induces an inner automorphism of Γ, there must be central units u and v of $\mathbb{Z}(G/L)$ and $\mathbb{Z}(G/Q)$ respectively, such that $z = \overline{uv}^{-1}$ in $\mathbb{Z}(G/LQ)$. Using the extended diagram, it is easily seen that this happens if there is a central unit $c \in \mathbb{Z}(G/LQ)$ such that $c \equiv z \bmod |Q|$.

Let $C_{10} = \langle x \rangle$ be the cyclic group of order 10. As an illustration of the Pullback technic and the theorem of Roggenkamp and Scott we calculate the unit group of $\mathbb{Z}C_{10}$. This has been done by Aleev, in [33] but his calculation is somewhat special and occupies, including some corollaries, about 15 pages.

By Theorem 4.0.25 we have the following commutative diagram.

$$\begin{array}{ccc} \mathbb{Z}C_{10} & \longrightarrow & \mathbb{Z}C_5 \oplus \mathbb{Z}C_2 \\ \downarrow & & \downarrow \\ \frac{\mathbb{Z}C_{10}}{(\hat{C}_5,\hat{C}_2)} & \longrightarrow & \frac{\mathbb{F}_2C_5}{(\hat{C}_5)} \oplus \frac{\mathbb{F}_5C_2}{(\hat{C}_2)} \end{array}$$

which can be written as

$$\begin{array}{ccc} \mathbb{Z}C_{10} & \longrightarrow & \mathbb{Z}C_5 \oplus \mathbb{Z}C_2 \\ \downarrow & & \downarrow \\ \mathbb{Z}[\zeta_{10}] & \longrightarrow & \mathbb{F}_2(\zeta_5) \oplus \mathbb{F}_5 \end{array}$$

By ζ_n we denote a primitive n^{th} root of unity and remark that $\mathbb{Z}[\zeta_{10}] = \mathbb{Z}[\zeta_5]$. Note that we obtain a pullback diagram if we replace $\mathbb{Z}C_5 \oplus \mathbb{Z}C_2$ by the pullback Γ over the augmentation maps ϵ, that is, $\Gamma = \{(s,t) \mid (s,t) \in \mathbb{Z}C_5 \oplus \mathbb{Z}C_2 \text{ and } \epsilon(s) = \epsilon(t)\}$.

Clearly the image of $\mathcal{U}(\mathbb{Z}C_2)$ in $\mathbb{F}_5$ is $\{\pm 1\}$. Let $\zeta_5 = \exp(2\pi i/5)$. Then

$$\omega = -\zeta_5^2 - \zeta_5^3 = \frac{1+\sqrt{5}}{2}$$

is a fundamental unit of $\mathbb{Z}[\zeta_5]$ and $\mathcal{U}(\mathbb{Z}[\zeta_5]) = \langle -\zeta_5 \rangle \times \langle \omega \rangle$. Let $\overline{x}$ be the image of x under the map $\mathbb{Z}C_{10} \to \mathbb{Z}C_5$. Then it is well known (and rather easy to see) that

$$\mathcal{U}(\mathbb{Z}C_5) = \langle \overline{x} \rangle \times \langle -1 + \overline{x}^2 + \overline{x}^3 \rangle$$

Let $\zeta_{10} = -\zeta_5$. Then $1 + \zeta_{10}^2 - \zeta_{10}^3 = 1 + \zeta_5^2 + \zeta_5^3 = \frac{1-\sqrt{5}}{2}$ us a fundamental unit of $\mathbb{Z}[\zeta_{10}]$ (This choice will yield the generators for the unit group given by Aleev).

Let $w \in \mathcal{U}(\mathbb{Z}C_{10})$. Multiplying w with a trivial unit, and inverting w if necessary, we may assume that for some $n \geq 0$, the elements w and $(1 + x^2 - x^3)^n$

have the same image in $\Lambda = \mathbb{Z}C_{10}/(\hat{C}_5, \hat{C}_2)$. The following table lists the relevant congruences, where $\Phi_i(x)$ denotes the i-th cyclotomic polynomial.

n	$(1+x^2-x^3)^n$	$(1+x^2-x^3)^n$	$(-1+x^2+x^3)^n$
	mod $(\Phi_5(x), 2)$	mod $(\Phi_2(x), 5)$	mod $(\ \Phi_5(x), 2\ )$
1	$1+x^2+x^3$	3	$1+x^2+x^3$
2	x^2+x^3	-1	x^2+x^3
3	1	2	1

It follows that $n \neq 1$ and that there are units $u, v \in V(\mathbb{Z}C_{10})$, defined via the first diagram of the proof as indicated below.

$$\begin{array}{ccc} u & \longmapsto & ((-1+x^2+x^3)^2, x) \\ \downarrow & & \downarrow \\ (1+x^2-x^3)^2 & \longmapsto & (1+x^2+x^3, -1) \end{array} \qquad \begin{array}{ccc} v & \longmapsto & ((-1+x^2+x^3)^3, 1) \\ \downarrow & & \downarrow \\ 1 & \longmapsto & (1,1) \end{array}$$

Moreover, it easily follows that $w = u^i v^j$ for some uniquely determined $i, j \in \mathbb{Z}$. Hence

$$\mathcal{U}(\mathbb{Z}C_{10}) = \langle -1 \rangle \times \langle x \rangle \times \langle u \rangle \times \langle v \rangle.$$

We give the units u, v explicitly (they coincide with the units given by Aleev):

$$\begin{aligned} u &= 2 + (x + x^5 + x^9) - (x^2 + x^3 + x^7 + x^8), \\ u^{-1} &= 2 + (x^3 + x^5 + x^7) - (x + x^4 + x^6 + x^9), \\ v &= -3 - 4x^5 - (x + x^4 + x^6 + x^9) + 3(x^2 + x^3 + x^7 + x^8), \\ v^{-1} &= -3 - 4x^5 - (x^2 + x^3 + x^7 + x^8) + 3(x + x^4 + x^6 + x^9), \end{aligned}$$

5 Projective Limits

Guided by possible applications to the Zassenhaus conjecture and the isomorphism problem we will in this chapter touch upon the following problems in group theory.

- Given a finite group G, what are the the possibilities to represent G as a subgroup of a direct product?
- Describe the structure of the subgroups of a direct product in terms of the subgroups of the direct factors.

In [29] Kimmerle and Roggenkamp deals with the first question. More precisely, they investigate when a group G can be written as a projective limit. We begin with writing general definitions and results concerning these questions, and then we explain the parts of [29] that are of interest to deal with the problems dealt within this thesis.

5.1 General notions + survey

Let $G_1, \ldots, G_n$ be finite groups. A subgroup of the direct product $D = G_1 \times \ldots \times G_n$ is called a subdirect product of the G_i if the projections are surjective. This also make sense for infinite groups and infinitely many factors. The definitions in the sequal also, but since we are only interested in finite groups we don't go further on it. Remak was the first who investigated in a series of papers, [34, 35, 36, 37], how a finite group G can be written as subdirect product, and introduced the terminology that will follow in this subsection.

We should have notions of buildings blocks, as for example the role of the prime numbers in $\mathbb{N}$ or the irreducible representations in representationtheory.

Definition 5.1.1 *The finite group G is subdirectly indecomposable if it is not a subgroup of the direct product of two groups of smaller order.*

Let G be a subgroup of $D = G_1 \times \ldots \times G_n$. The projection of G to G_i is called the i-th subdirect factor and the kernel of the projection of G to $G_{\hat{i}} = G_1 \times \ldots G_{i-1} \times G_{i+1} \times \ldots \times G_n$ the i-th block component. If the i-th block

component is trivial then the i-th subdirect factor is superfluous. Remark that in this case G is a subdirect product of $G_{\hat{i}}$. A last definition.

Definition 5.1.2 *The embedding $G \hookrightarrow D$ is called an economic subdirect decomposition if each G_i is subdirectly indecomposable and not superfluous.*

For the further of this subsection we give a survey of several results concerning subdirect products. None of these results will be used later in this thesis, but it can always we useful to know witch research has been done. The only paper that we will explain is the one of Roggenkamp and Kimmerle [29] (in subsection 5.2).

Remak, [34], studied subdirect products of two factors and showed that these are in fact pullbacks. He proved also that a group G is subdirectly indecomposable if and only if G has exactly one nontrivial minimal normal subgroup. In [36], Remak described a method of how to obtain an economic subdirect decomposition for a given group, and showed that all such decompositions are obtained in that way. Thus one can always look at an economic subdirect decomposition of G. The socle of G is the direct product of the minimal normal subgroups of the factors of such a decomposition. Based on his work of [34], Remak proved in [35] further results on subdirect products, depending on the properties of the socle of a group. In [37] he related certain subgroups of a subdirect product with three factors.

If G is the subdirect product of groups $G_i, i \in I$, then Loonstra gave a criterion (REF) for when there exist a group F and homomorphisms $\alpha_i : G_i \to F$ such that G consists of those tupels $(g_i)_{i\in I}$ with $g_i\alpha_i = g_j\alpha_j$ for all $i, j \in I$.

If $N_1, \ldots N_n$ are normal subgroups of G whose intersection is trivial, then G is a subdirect product of the groups G/N_i in a natural way. We may also form a projective limit associated with G and the N_i, in which G embeds. Kimmerle and Roggenkamp gave a criterion for when G is isomorphic to this projective limit.

Bryce and Cossey investigated (REF) fitting classes which are closed with respect to forming subdirect products. Verkinkov showed (REF) that finite subdirect products can be made iterating the familiar (pullback) construction of subdirect products with two subdirect factors, and uses this construction to describe those formations of finite groups whose subformations are all closed under taking subnormal subgroups.

As mentioned, there is a 'well known' description of all subgroups of the direct product of two finite groups. Seemingly, it is open whether there is a similar description of the subgroups of direct products of more then two finite groups. Thévenaz (REF) describes the maximal subgroups of the direct product G^n of n copies of a group G. In particular, if G is perfect (this means that the commutator of G equals G, equivalently that G posses no non-trivial abelian quotients) then any maximal subgroup of G^n is the inverse image of a maximal

subgroup of G^2 for some projection $G^n \to G^2$ onto two factors, and if G is perfect and finite then the number of maximal subgroups of G^n is a quadratric function of n. Also, he deduces a theorem of Wiegold about the growth behavior of the number of generators of G^n.

5.2 Writing as projective limit

This section is based on [29] and [9].

We will deal with the Isomorphism problem, the Zassenhaus conjecture and certain p-versions of the Zassenhaus conjecture from a conceptional point of view, by defining a style cohomology set, which yields obstructions for the above conjectures to be true.

5.2.1 Introduction

We will describe a finite group G as a projective limit with respect to certain families of normal subgroups $\{N_i\}_{1\leq i\leq n}$, i.e.

$$G \cong \{(g_1, \ldots, g_n) \mid g_i \in G_i = G/N_i : g_i = g_j \text{ in } G/(N_iN_j)\}.$$

(i.e. G is a subdirect product of the groups G/N_i). Later on, it will be shown that this can be done provided $\cap N_i = 1$ and for every $p \in \pi(G)$ there is an index i with $(p, |N_i|) = 1$. This applies in particular when $N_i = O_{\dot{p}_i}(G)$ the maximal normal subgroup with order relative prime to p_i in G. If G is the projective limit of the quotients G_i, then the projective limit $\Gamma_G = \gamma_G(\{G_i\})$ of the group rings $\mathbb{Z}G_i$ does not coincide with $\mathbb{Z}G$. It is in general a relatively small proper quotient of $\mathbb{Z}G$. However, it nevertheless reflects many properties of the integral group ring and we will see that this projective limit seems to be an interesting substitute for the integral group ring. We recall the conjectures that are of interest for us.

Conjecture 6 *Let G and H be finite groups. Assume that*

$$\mathbb{Z}G = \mathbb{Z}H \text{ or that } \Gamma_G = \Gamma_H$$

as augmented algebras (thus the equality is compatible with the augmentations).

1. *The Isomorphism Problem asks whether there exists an isomorphism $\rho : G \to H$.*

2. *The p-version of the second Zassenhaus conjecture asks whether in addition a $\rho = \rho_P$ can be chosen in such a way that its restriction to a Sylow p-subgroup P is given by conjugation with an element $a_P \in \mathcal{U}(\mathbb{Q}G)$, $a_P \in \mathbb{Q} \otimes_{\mathbb{Z}} \Gamma_G$ resp.*

3. *We shall say that the p-version of the second Zassenhaus conjecture holds simultaneously for all p if there exists an isomorphism $\rho : G \to H$ such that its restriction to every Sylow subgroup S is given by conjugation with an element $a_S \in \mathcal{U}(\mathbb{Q}G)$, $a_S \in \mathbb{Q} \otimes_{\mathbb{Z}} \Gamma_G$ resp., where a_S will in general depend on S.*

4. *The Zassenhaus conjecture asks whether the above element a_P can be chosen to be independent of p for all primes p, i.e whether G and H are conjugate in $\mathbb{Q}G$, $\mathbb{Q} \otimes_{\mathbb{Z}} \Gamma_G$ resp.*

The main result will give an explicit description of H in terms of G provided $\mathbb{Z}G = \mathbb{Z}H$ as augmented algebras, in case G is soluble. We will show that G is the projective limit of the groups $G_i = G/O_{\acute{p}_i}(G)$. Put $G_{ij} = G/(O_{\acute{p}_i}(G) \cdot O_{\acute{p}_j}(G))$. Denote the projective limit (an exact definition is given in next subsection) of the group rings $\mathbb{Z}G_i$ by $\Gamma_G(\mathcal{O}_0)$. Assume we are given a cocycle $\rho = (\rho_{ij})$ of conjugacy class preserving automorphisms ρ_{ij} of G_{ij} (in subsection 7.2.2 we give exact definitions). Then

$$G(\rho) = \{(g_i) \in \prod_{1 \le i \le n} G_i \mid \rho_{ij}(g_j G_{ij}) = (g_i G_{ij})\}$$

is a group. In subsection 7.2.2 we elaborate on the question of when G and $G(\rho)$ are isomorphic. One of the main results in [29] is the following.

Theorem 5.2.1 *Assume that $\Gamma_G(\mathcal{O}_0) = \Gamma_H(\mathcal{O}_0)$ as augmented algebras and that G is soluble. Then the Zassenhaus conjecture holds for the group rings $\mathbb{Z}G_i$ and there exists a cocycle ρ such that $H \cong G(\rho)$.*

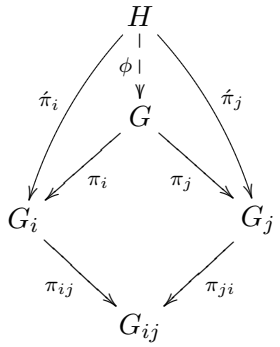
The hypothesis of above theorem is in particular satisfied if $\mathbb{Z}G = \mathbb{Z}H$. So the result shows that then $H = G(\rho)$ which shows in particular that G and H share many properties. The theorem is also used to construct two non isomorphic groups G and H as projective limits such that the projective limits of the corresponding group rings are semi-locally isomorphic (i.e. $\mathbb{Z}_{\pi(G)}G \cong \mathbb{Z}_{\pi(H)}$). All the semi-local counterexamples are important, since they paved possible ways to the counter example constructed by Hertweck.

5.2.2 General results

Let G_i and G_{ij} be finite groups with $G_{ij} = G_{ji}$ and $G_{ii} = G_i$, for all $1 \le i, j \le n$. Let $\pi_{ij} : G_i \to G_{ij}$ be epimorphisms (with π_{ii} the identity mapping). The projective limit of the groups G_i with respect to the homomorphisms π_{ij} is the subgroup

$$\begin{aligned} G &= projlim_{1 \le i,j \le n}(G_i, \pi_{ij}) \\ &= \{(g_1, \ldots, g_n) \in \textstyle\prod_{i=1}^n G_i \mid g_i \pi_{ij} = g_j \pi_{ji} \text{ for all } 1 \le i, j \le n\} \end{aligned}$$

of the direct product of the G_i (and thus is a special subdirect product). The projection $\pi_i : G \to G_i$ onto the i-th component is clearly a homorphism, and $\pi_i\pi_{ij} = \pi_j\pi_{ji}$ for all i, j. The projective limit G has the following universal property: whenever there is a group G and homomorphisms $\acute{\pi}_i : H \to G_i$ such that $\acute{\pi}_i\pi_{ij} = \acute{\pi}_j\pi_{ji}$ for all i, j then there is a unique homomorphism $\phi : H \to G$ making the following diagrams commutative.



Let G be a finite group, and let $N_1, \ldots N_n$ be normal subgroups of G. Put $G_i = G/N_i$, $G_{ij} = G/N_iN_j$, and let $\pi_{ij} : G_i \to G_{ij}$ be the natural maps. Then we write

$$\hat{G} = projlim_{1\leq i,j\leq n}(G_i, \pi_{ij}).$$

There is a map

$$\gamma : G \to \hat{G} : g \to (g_i = g \cdot N_i)_{1\leq i\leq n}$$

which has kernel $\cap_{1\leq i\leq N}N_i$. Thus γ is injective if and only if $\cap_{1\leq i\leq n}N_i = 1$.

In general it is not so easy to determine when the map γ is surjective. This is surely the case if $n = 2$, since then G is the pullback of G/N_1 and G/N_2 over $G/(N_1N_2)$. An example for which γ is not surjective is Kleins four group $\langle a : a^2\rangle \times \langle b : b^2\rangle$ Klein's four group with $N_1 = \langle a\rangle$, $N_2 = \langle b\rangle$ and $N_3 = \langle ab\rangle$.

There is however a situation, which is relevant to the Isomorphism problem for which γ is surjective.

Lemma 5.2.2 *Let G be a finite group an let $\{N_i\}_{1\leq i\leq n}$ be a family of normal subgroups of G. Assume that*

1. $\cap_{1\leq i\leq n}N_i = \{1\}$,
2. *for every prime divisor p of $|G|$ there is at least one index $i = i(p)$ such that $(p, |N_{i(p)}|) = 1$.*

Then G is the projective limit of $\{G/N_i\}_{1\leq i\leq n}$, i.e. γ is an isomorphism.

Proof. Clearly

$$\hat{G} = \{(g_1N_1, \ldots, g_iN_i, \ldots, g_nN_n) \mid g_i \equiv g_j \bmod N_iN_j\}.$$

The image of $\gamma : G \to \hat{G}$ is the group

$$\{(gN_1, \ldots, gN_n) \mid g \in G\}.$$

Set $x = (g_1N_1, \ldots g_nN_n) \in \hat{G}$ an element of $Im(\gamma)$. We nood to show that all cosets g_iN_i have a common representative. Say that there are $n-k$ cosets with the same representative. We use induction on k to prove that $x \in Im(\gamma)$ and thus that γ is a surjection. If $k = 0$ then it is done by definition of γ. Assume that the statement is true for every element in $\hat{G}$ with $n-(k-1)$ identical representatives. If necessary after renumbering, we may assume that we are given the element

$$x = (g_1N_1, \ldots, g_kN_k, gN_{k+1}, \ldots, gN_n).$$

Because γ is a group homomorphism we may assume that

$$x = (g_1N_1, \ldots, g_kN_k, \underbrace{N_{k+1}, \ldots, N_n}_{n-k \text{ copies}}).$$

We may also assume that x has order p^m for a prime number p. So in particular all components of x have this order. We now have to distinguish two cases:

1. There is an index $k+1 \leq j \leq n$ such that $(p, |N_j|) = 1$. We show that $g_1 \in N_1$. By the definition of $\hat{G}$ we get that $g_1 \in N_1N_j$. If we consider the natural homomorphism $\rho : N_1N_j \to (N_jN_1)/N_1 \cong N_j/(N_j \cap N_1)$, then $\rho(g_1) = 1$ since g_1 is a p-element and N_j has order prime to p. Thus $g_1 \in Ker(\rho) = N_1$, as desired.

2. The prime number p divides $|N_j|$ for all $k+1 \leq j \leq n$. Now we invoke the essential second hypothesis: there must exist an index $1 \leq i \leq k$ such that $(p, |N_i|) = 1$. Now, a similar argument as above shows that $g_i \in N_j$ for every $k+1 \leq j \leq n$ and $g_i \in N_i$. So $x = (g_1N_1, \ldots, N_i, \ldots, g_kN_k, N_{k+1}, \ldots, N_n)$.

□

This yields naturally to the following open problem, formulated by Hertweck in his Habilitationschrift [9].

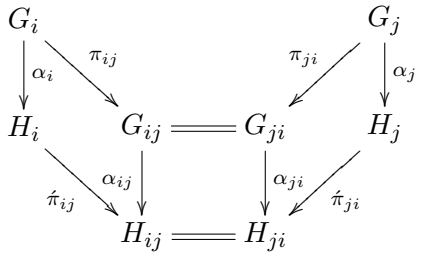
Problem. Let $D_1, \ldots D_n$ be normal subgroups of G such that $G \hookrightarrow \prod_{i=1}^n G/D_i$ is an economic subdirect decomposition of G. Is then $G \cong projlim_{1 \leq i,j \leq n}(G/D_i)$?

Remark that the above conditions are satisfied for a finite group G, if $\{N_i = O_{p_i'}(G)\}_{1 \leq i \leq n}$, where $\{p_i\}_{1 \leq i \leq n}$ runs over all prime divisors of $|G|$. Here we take $N_{i(p)} = N_i$. We denote this family of normal subgroups by $\mathcal{O}_0$.

So we already know a case of when a group G can be viewed as a projective limit. Since we are, above all, interested in the Isomorphism Problem, we have to consider homomorphisms between projective limits. A homomorphism between projective limits (with the same index set)

$$G = projlim_{1 \leq i,j \leq n}(G_i, \pi_{ij}) \text{ and } H = projlim_{1 \leq i,j \leq n}(H_i, \acute{\pi}_{ij})$$

is in fact the obvious thing. This means, a family of homomorphisms $\alpha_i : G_i \to H_i$ such that $\pi_i\alpha_i\acute{\pi}_{ij} = \pi_j\alpha_j\acute{\pi}_{ji}$ for all i, j. By the universal property, this family determines uniquely a homomorphism $G \to H$. One can use a simplier criterium to determine when a family $(\alpha_i)_{1\leq i,j\leq n}$ is a homomorphism of projective limits. If the kernel of π_{ij} is contained in the kernel of $\alpha_i\acute{\pi}_{ij}$ for all i, j then the α_i induces homomorphisms $\alpha_{ij} = G_{ij} \to H_{ij}$, and $(\alpha_i)_{1\leq i\leq n}$ is a homomorphism of projective limits if $\alpha_{ij} = \alpha_{ji}$ for all i, j which is also necessary condition if all maps π_i, π_{ij} are surjective (and we made this assumptions earlier on in this thesis):



In this thesis we assume that a homomorphism between projective limits is understood in this stricter sense.

As mentioned in the introduction the goal is to describe one group basis in function of the other. For this the notion of twisted group basis is primordial. So we briefly discuss the concept of twisted projective limits in connection with the Zassenhaus conjecture and the Isomorphism problem.

Let $N_1, \ldots, N_n$ still be normal subgroups of the finite group G. Set $G_i = G/N_i$, $G_{ij} = G/N_iN_j$, and let $\pi_{ij} : G_i \to G_{ij}$ be the natural maps. Given a family σ of automorphisms $\sigma_{ij} \in \mathrm{Aut}(G_{ij})$, the projective limit

$$\hat{G}(\sigma) = projlim_{1\leq i,j\leq n}(G_i, \pi_{ij}\sigma_{ij})$$

is called a twisted projective limit. The interest in these groups arises from the following theorem, that is proved by Roggenkamp and Kimmerle [29, Theorem 7].

Theorem 5.2.3 *Let G be a finite solvable group, and set $\hat{G} = projlim_{p\in\pi(G)}(G/O_{p'}(G))$. If H is a group basis of $\mathbb{Z}G$, then $H \cong \hat{G}(\sigma)$ for a family σ of class-preserving automorphisms.*

For proving this theorem, we have to introduce a notion of cocycle. This is done in the following 2 defintions.

Definition 5.2.4 *For a finite group G denote the subgroup of $Aut(G)$ consisting of those automorphisms $\gamma \in Aut(G)$ such that for every p and for every p-power element $g \in G$ the elements g and $\gamma(g)$ are conjugate in G by $Aut_p(G)$. Finally we denote by $Aut_c(G)$ the subgroup consisting of those automorphisms such that $\gamma(g)$ and g are conjugate for every $g \in G$.*

For the further admit that G is the projective limit of a family normal subgroups $\{N_i\}_{1\leq i\leq n}$ such that the normal subgroups N_i are characteristic (the family $\mathcal{O}_0$ showed that this isn't a restrictive condition). We write $G_i = G/N_i$ and $G_{ij} = G/(N_iN_j)$ with natural homomorphisms

$$\phi_i : G \to G_i \text{ and } \phi_{ij} : G_i \to G_{ij}.$$

We use the notation $\underline{G}$ for G, if we want to stress that we view G as a projective limit.

Definition 5.2.5

- *The cocycles are defined as*

$$Z(\underline{G}, \underline{Aut_*(G)}) = \{(\rho_{ij})_{1\leq i,j\leq n} \mid \rho_{ij} \in Aut_*(G_{ij}), \rho_{ii} = id, \rho_{ij}^{-1} = \rho_{ji}\},$$

  where $Aut_*(-)$ stands for $Aut(-)$, $Aut_c(-)$ or for $Aut_p(-)$.

- *Let $\rho_i \in Aut_*(G_i)$. This induces an automorphism $\overline{\rho_i}$ of $Aut_*(G_{ij})$. It is easily seen that the following defines an equivalence relation on $Z(\underline{G}, \underline{Aut_*}(G))$:*

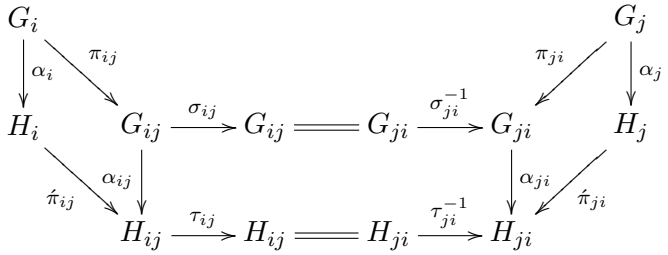
$$(\rho_{ij}) = (\sigma_{ij}) \text{ if and only if } \overline{\rho}_i \cdot \rho_{ij} \cdot \overline{\rho}_j^{-1} = \sigma_{ij}$$

  for $\rho_i \in Aut_*(G_i), \rho_j \in Aut_*(G_j)$ respectively. . If (ρ_{ij}) is a cocycle then $(\overline{\rho}_i \cdot \rho_{ij} \cdot \overline{\rho}_j^{-1})$ is a cocycle for $\rho_i \in Aut_*(G_i), 1 \leq i \leq n$. The set formed by these equivalence classes is denoted by $\check{H}(\underline{G}, \underline{Aut_*(G)})$. The class of the identity consists of the coboundaries:

$$B(\underline{G}, \underline{Aut_*(G)}) = \{(\rho_{ij}) \in Z(\underline{G}, \underline{Aut_*(G)} \mid \rho_{ij} = \overline{\rho}_i \cdot \rho_j^{-1} \text{ for } \rho_i \in Aut_*(G_i)\}$$

Again we discuss homomorphisms, between twisted projective limits. Let H be another finite group, and let $M_1, \ldots, M_n$ be normal subgroups of H. Set $H_i = H/M_i$, $H_{ij} = H/M_iM_j$. Let $\acute{\pi}_{ij} : H_i \to H_{ij}$ be the natural maps, and let τ be a family of automorphisms $\tau_{ij} \in \mathrm{Aut}(H_{ij})$.

If a family α of homomorphisms $\alpha_i : G_i \to H_i$ induce homomorphisms $\alpha_{ij} : G_{ij} \to H_{ij}$ such that the following diagram commutes:



i.e. if $\alpha_{ij}(\tau_{ij}\tau_{ji}^{-1}) = (\sigma_{ij}\sigma_{ji}^{-1})\alpha_{ji}$ for all i, j then α is a homomorphism of projective limits $\hat{G}(\sigma) \to \hat{H}(\tau)$.

For a family of automorphisms $\sigma_{ij} \in \mathrm{Aut}(G_{ij})$, we are thus led to consider the family of automorphisms $\delta_{ij} = \sigma_{ij}\sigma_{ji}^{-1}$. The collection $\delta = (\delta_{ij})_{1\leq i,j\leq n}$ is a cocycle. A cocycle δ is a coboundary if there is a family of automorphisms $\alpha_i \in \mathrm{Aut}(G_i)$ which induce automorphisms α_{ij} of G_{ij} such that $\alpha_{ij}\delta_{ij} = \alpha_{ji}$ for all i, j. Remark that this is the case if and only if there exists an isomorphism (of projective limits) between $\hat{G}$ and $\hat{G}(\tau)$, where $\tau = (\tau_{ij})$ is such that $\tau_{ij} = \delta_{ij}$ if $i < j$ and $\tau_{ij} = id$ otherwise.

Remark that if G and H are solvable groups and $\alpha : G \to H$ is a homomorphism (of abstract groups), then α is also a homomorphism between the projective limits $\hat{G} = projlim_{p\in\pi(G)}(G/O_{p'}(G))$ and $\hat{H} = projlim_{p\in\pi(H)}(H/O_{p'}(H))$ in the above sense. The same holds for homomorphisms of abstract groups between twisted projective limits $\hat{G}(\sigma)$ and $\hat{H}(\tau)$. Roggenkamp and Kimmerle proved following lemma.

Lemma 5.2.6 *Given a cocycle $\rho = (\rho_{ij}) \in Z(\underline{G}, \underline{Aut_*(G)})$. Then*

$$G(\rho) = \{(g_i) \in \prod_{1\leq i\leq n} G_i \mid \rho_{ij}\phi_{ji}(g_j = \phi_{ij}(g_i)\}$$

is a group.

We will now turn our attention to the Isomorphsm problem, the p-version of the Zassenhaus conjecture and the second Zassenhaus conjecture. We already know that in general the second Zassenhaus conjecture is not true. However, no counterexample is known for the p-version of the Zassenhaus conjecture.

It is often useful to rephrase the Zassenhaus conjecture and its p-version as follows.

Lemma 5.2.7 *Assume that $\mathbb{Z}G \cong \mathbb{Z}H$ as augmeted algebras. Then the clas ssum correspondence implies that one has for the class sums K_g of G and K_h of H a correspondcence $K_{\beta(g)} = K_g$ for a bijection $\beta : G \to H$*

1. *The Zassenhaus conjecture is true for $\mathbb{Z}G$ if and only if the map β can be chosen to be a groupisomorphism.*

2. *The p-version of the Zassenhaus conjecture holds if and only if there is an isomorphism $\rho = \rho_P : G \to H$ of groups sucht that for all p-power elements $g \in G$ ons has $K_{\beta(g)} = K_{\rho(g)}$.*

An advantage of the p-version of the Zassenhaus conjecture is that the projective ring limits suffice.

Proposition 5.2.8 *Assume that $\mathbb{Z}G = \mathbb{Z}H$ as augmented algebras. Let $\mathcal{N}^0$ be a family of subgroups for G as defined in 5.2.2. Then there exists a family $\mathcal{M}^0$ of normal subgroups for H such that $\Gamma_G(\mathcal{N}^0) = \Gamma_H(\mathcal{M}^0)$ as projective limits. Then*

the p-version of the Zassenhaus conjecture holds for the pair of group bases G and H of $\mathbb{Z}G$ if and only if it holds for the images of G and H in $\Gamma_G(\mathcal{N}^0)$ under the natural map $\phi : \mathbb{Z}G \to \Gamma_G(\mathcal{N}^0)$.

Remind that the hypotheses are satisfied if $N_i = O_{p_i'}(G)$ or if $N_1 = O_{p'}(G)$ and $N_2 = O_p(G)$. Later on we show that the proposition is not valid for the Zassenhaus conjecture. We recall a far reaching result concerning the Isomorphism problem (see [30], [31]) that is a particular case of the so called F^*-theorem.

Theorem 5.2.9 *Assume that for some prime p the group G has a normal p-subgroup N such that $C_G(N)$ is contained in N (this condition is in particular satisfied if G is soluble and $O_{p'}(G) = 1$). If $\mathbb{Z}G = \mathbb{Z}H$, then the Zassenhaus conjecture holds. Thus there exists $a \in \mathbb{Q}G$ (a is even p-adically a unit in $\mathbb{Z}_pG$) such that $aGa^{-1} = H$.*

Let the groups $G = projlim(G/N_i)$ and $H = projlim(G/M_i)$ be given as projective limits. Assume that $\Gamma_G(\mathcal{N}^0) = \Gamma_H(\mathcal{M}^0)$ as projective limits. We are going to discuss the connections between the various situations arond the Isomorphism problem for the quotients $\mathbb{Z}(G/N_i)$ and for $\Gamma_G(\mathcal{N}^0)$.

1. Lets say that the Isomorphism problem has a positive answer for the various rings $\mathbb{Z}G_i$. So there exists an isomorphism $\sigma_i : G_i \to H_i$. We get induced isomorphisms
$$\sigma_{ij} = \overline{\sigma_i}\,\overline{\sigma_j^{-1}} : H_{ij} \to H_{ij} \text{ with } \sigma = (\sigma_{ij}) \in Z(\underline{H}, \underline{Aut(H)}).$$
2. If the p-version of the Zassenhaus conjecture has a positive answer for the various rings $\mathbb{Z}G_i$ then we obtain in a similar a cocycle $\sigma = (\sigma_{ij})$ in $Z(\underline{H}, \underline{Aut_p(H)})$.
3. If the Zassenhaus conjecture has a positive answer for the various rings $\mathbb{Z}G_i$ then in a similar way we obtain a cocycle $\sigma = (\sigma_{ij})$ in $Z(\underline{H}, \underline{Aut_c(H)})$.

Following result was obtained by Roggenkamp and Kimmerle.

Theorem 5.2.10 *Assume that $\Gamma_G(\mathcal{N}^0) = \Gamma_H(\mathcal{M}^0)$.*

1. *The groups G and H are isomorphic if and only if the cocycle from above lies in $B(\underline{H}, \underline{Aut(H)})$.*
2. *Under the assumptions of part 2 of above, the p-version of the Zassenhaus conjecture is true for $\Gamma_G(\mathcal{N}^0) = \Gamma_H(\mathcal{M}^0)$ if and only if $(\sigma_{ij}) \in B(\underline{H}, \underline{Aut_p(H)})$. Under the assumptions of 5.2.8, the p-version of the Zassenhaus conjecture holds for the pair G and H of group bases $\mathbb{Z}G$.*
3. *Under the assumption of Part 3 of above, the Zassenhaus conjecture holds for $\Gamma_G(\mathcal{N}^0) = \Gamma_H(\mathcal{M}^0)$ if and only if $(\sigma_{ij}) \in B(\underline{H}, \underline{Aut_c(H)})$.*

By 5.2.9 the assumptions of the third part are satisfied for $\mathcal{N}^0 = \mathcal{O}$. This yields following corollary.

Corollary 5.2.11 *Assume that G is soluble and that $\mathbb{Z}G = \mathbb{Z}H$ as augmented algebras. If the cocycle σ lies in $B(\underline{H}, \underline{Aut_p(H)})$, then the p-version of the Zassenhaus conjecture holds for $\mathbb{Z}G$.*

Corollary 5.2.12 *Assume that G is a soluble group.*

1. *Let $\Gamma_G(\mathcal{O}) = \Gamma_H(\mathcal{O})$ and assume that the groups H_{ij} are abelian. Then the Zassenhaus conjecture holds for $\Gamma_G(\mathcal{O})$.*
2. *Admit that $\mathbb{Z}G = \mathbb{Z}H$ and that the groups H_{ij} are abelian. Then the p-version of the Zassenhaus conjecture holds for $\mathbb{Z}G$.*

In order to apply these results to special classes of groups we have to discuss questions of when automorphisms of quotient groups can be lifted. But this go beyond the scope of the presented work. It can be found back in [29]. From these 'lifting results' they also prove the following result.

Proposition 5.2.13 *Assume that G is a pullback*

$$\begin{array}{ccc} G & \longrightarrow & G_1 \\ \downarrow & & \downarrow \\ G_2 & \longrightarrow & G_0 \end{array}$$

with $G_i = G/N_i$.

1. *If the Zassenhaus conjecture holds for $\mathbb{Z}G_i$, then the p-version of the Zassenhaus conjecture is true for $\mathbb{Z}G_i$. In particular the Isomorphism problem has a positive answer for $\mathbb{Z}G$, provided for every central isomorphism γ of G_0, thee exist a $\rho_i \in Aut(G_i)$ such that $\rho_1 \rho_2^{-1} = \gamma$. This latter condition is satisfied if $M_1 = Ker(G_1 \to G_0)$ is abelian and semisimple as $\mathbb{Z}G_0$-module or the charateristic of M_1 is prime to $|G|$.*
2. *Assume that the p-version of the Zassenhaus conjecture holds for $\mathbb{Z}G_i$ and assume that every p-central automorphism γ of G_0 (i.e. $\gamma \in Aut_p(G_0)$) can be written as*

   $$\rho_1 \rho_2^{-1} = \gamma \text{ for } \rho_i \in Aut(G_i).$$

   Then the p-version of the Zassenhaus conjecture holds for $\mathbb{Z}G$. In particular the Isomorphism problem has a positive answer for $\mathbb{Z}G$.

We now describe G in terms of H and the cocycle $\sigma = (\sigma_{ij})$, with $\sigma_{ij} = \overline{\sigma_i}\,\overline{\sigma_j^{-1}} : H_{ij} \to H_{ij}$.

Theorem 5.2.14 *Assume that $\Gamma_0 = \Gamma_G(\mathcal{O}) = \Gamma_H(\mathcal{O})$ as augmented algebras (and thus also as projective limits). Let the cocycle $\sigma \in Z(\underline{H}\underline{Aut_c(H)})$. Then $H(\sigma) = \{(h_i)_{1\leq i\leq n} \mid h_i \in H_i,\ \sigma_{ij}\phi_{ij}(h_i) = \phi_{ji}(h_j)\}$ and $G \cong H(\sigma)$.*

Proof. Since $\Gamma_G(\mathcal{O}) = \Gamma_H(\mathcal{O})$ we get induced equations $\mathbb{Z}G_i = \mathbb{Z}H_i$. However, $O_{p_i'}(G_i) = 1$ and so by 5.2.9 there are automorphisms σ_i of $\mathbb{Z}G_i = \mathbb{Z}H_i$ which leave the centre elementwise fixed and map G_i and H_i. Thus the cocycle $\sigma = (\sigma_{ij}) = (\overline{\sigma_i}\overline{\sigma_j^{-1}})$ lies in $Z(\underline{H}, \underline{Aut_c(H)})$. Recall that $H(\sigma) = \{(h_i)_{1\leq i\leq n} \mid h_i \in H_i, \sigma_{ij}\phi_{ij}(h_i) = \phi_{ji}(h_j)\}$, where as always $\phi_{ij} : \mathbb{Z}G_i \to \mathbb{Z}G_{ij}$ are the induced maps. We know that

$$G = \{(g_i)_{1\leq i\leq n} \mid \phi_{ij}(g_i) = \phi_{ji}(g_j)\}.$$

The map $\rho : G \to H(\sigma)$ defined by $\rho((g_i)_{1\leq i\leq n}) = (\sigma_i(g_i))_{1\leq i\leq n}$ is then an isomorphism. In fact the condition $\phi_{ij}(g_i) = \phi_{ji}(g_j)$ translates to $\phi_{ij}\sigma_i(g_i) = \overline{\sigma_i}\,\overline{\sigma_j^{-1}}\phi_{ji}(g_j)$. So we have constructed the desired isomorphism. □

Assume that $\mathbb{Z}G \cong \mathbb{Z}H$ as augmented algebras for G a finite soluble group. Then also H is soluble and, as mentioned earlier, $\Gamma_G(\mathcal{O}) = \Gamma_H(\mathcal{O})$. So the conclusion of the theorem says that $G \cong H(\sigma)$ for the associated cocycle σ.

5.2.3 The case n=2

In the counterexample to the Isomorphism, Hertweck deals with a family of normal subgroups $\mathcal{N}$ consisting of only 2 subgroups. For facilitate the comprehension of that chapter, we resume and formulate the obstruction theory for such a family.

Let G be a finite group, and let $N_1, N_2 \triangleleft G$ with $N_1 \cap N_2 = 1$. Set $\overline{G} = G/N_1N_2$. Then we have the following pullback diagram

$$\begin{array}{ccc} G & \xrightarrow{\pi_2} & G/N_2 \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \rho_2} \\ G/N_1 & \xrightarrow{\rho_1} & \overline{G} \end{array}$$

Let $\sigma \in \mathrm{Aut}(\overline{G})$. We form the triwsted pullback H of the maps $\rho_1\sigma$ and ρ_2:

$$\begin{array}{ccccc} H & & \xrightarrow{\tau_2} & & G/N_2 \\ {\scriptstyle \tau_1}\downarrow & & & & \downarrow{\scriptstyle \rho_2} \\ G/N_1 & \xrightarrow{\rho_1} & \overline{G} & \xrightarrow{\sigma} & \overline{G} \end{array}$$

Then we have the following group-theoretical condition for when G and H are isomorphic.

Proposition 5.2.15 *With G and H given as above, suppose that each surjective homomorphism $G \to G/N_i$ has kernel N_i. Then $G \cong H$ if and only if there are $\phi_i \in Aut(G/N_i)$ inducing automorphisms $\overline{\phi_i}$ of $\overline{G}$, such that $\sigma = \overline{\phi_1}^{-1}\overline{\phi_2}$.*

In last section we gave no proves of the obstruction theory results. Because this is of main importance in the further chapters, we sketch a proof for this case. **Proof.** Let $\phi : G \to H$ be an isomorphism. By assumption $\phi\tau_i$ has kernel N_i, so here is a $\phi_i \in \mathrm{Aut}(G/N_i)$, with $\phi\tau_i = \pi_i\phi_i$.

Let $K = N_1\pi_2$, which is the kernel of ρ_2. Then $(K\phi_2)\rho_2 = N_1\pi_2\phi_2\rho_2 = N_1\phi\tau_2\rho_2 = N_1\phi\tau_1\sigma = (N_1\pi_1)\phi_1\rho_1\sigma = 1$, so ϕ_2 stabilizes the kernel of ρ_2 and there is a $\overline{\phi_2} \in \mathrm{Aut}(\overline{G})$ with $\phi_2\rho_2 = \rho_2\overline{\phi_2}$. Similarly, we get that $\overline{\phi_1} \in \mathrm{Aut}(\overline{G})$ with $\phi_1\rho_1 = \rho_1\overline{\phi}_1$. Hence we have the following diagram, in which every square is commutative.

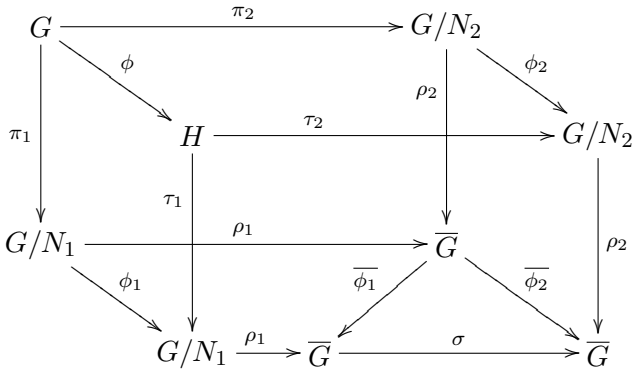


Diagram chasing shows that the triangle is also commutative:

$$\pi_1\rho_1\overline{\phi_1}\sigma = \pi_1\phi_1\rho_1\sigma = \phi\tau_1\rho_1\sigma = \phi\tau_2\rho_2 = \pi_2\phi_2\rho_2 = \pi_2\rho_2\overline{\phi_2} = \pi_1\rho_1\overline{\phi_2},$$

so $\overline{\phi_1}\sigma = \overline{\phi_2}$ as $\pi_1\rho_1$ is surjective. conversely, given ϕ_i as above, $G \cong H$ follows from the universal property of the pullback □

Remark 5.2.16 *1. In the proof of the counterexamples the proposition is used for $N_i = O_{p_i}(G)$ for different primes p_1 and p_2.*

2. In the special situation when N_1 has a complement K in G containing N_2, the group H has a convenient description as the semidirect product $N_1 \ltimes_\sigma K$, i.e $n^k = n^{\overline{k}\sigma}$ for all $n \in N_1, k \in K$ (so in some sense the action of K on N_1 is twisted by σ). This because following diagram is commutative.

$$\begin{array}{ccccc} N_1 \ltimes_\sigma K & \xrightarrow{(id,\rho_1)} & N_1 \ltimes_\sigma \overline{G} & \xrightarrow{(id,\sigma)} & N_1 \ltimes \overline{G} = G/N_2 \\ \downarrow{\scriptstyle \tau_1} & & & & \downarrow{\scriptstyle \rho_2} \\ G/N_1 = K & \xrightarrow{\rho_1} & \overline{G} & \xrightarrow{\sigma} & \overline{G} \end{array}$$

6 Counterexamples

6.1 To the Normalizer problem

6.1.1 Introduction

A construction is given of a finite group G such that the elements of $G.Z(\mathcal{U}(\mathbb{Z}G))$ are not the only units normalizing G. This is equivalent with proving that $Out_{\mathbb{Z}}(G)$ is not trivial. So we need a non-inner group automorphism τ of G that becomes inner over $\mathbb{Z}G$. The content of this chapter is based on [10, Kapitel 4]. We begin by defining the group that will yield the counterexample.

The group G is a semidirect product of a Sylow 2-subgroup P and a normal subgroup Q. The Sylow 2-subgroup P is a semidirect product

$$P = (\langle u : u^{32} \rangle \times \langle v : v^4 \rangle \times \langle w : w^8 \rangle \times \langle h : h^{256} \rangle) \rtimes (\langle a : a^{64} \rangle \times \langle g : g^2 \rangle),$$

with the action of a and g defined by

- $u \in Z(P)$,
- $v^a = u^{16}v,\ w^a = u^4 w$ and $h^a = h^5$,
- $v^g = v^{-1}u^{-8},\ [w, g] = 1$ and $[h, g] = 1$.

One can easily verify that $Z(P) = \langle u, h^{64} \rangle$. Let $K = \langle u, v, g, h, a^8 w \rangle$. One easily checks with the relations that $K \lhd P$ and $P/K = \langle \overline{a} \rangle \cong C_{64}$ since $w^{-1} = a^8$ in P/K (and thus by going through $\langle a \rangle$ one also finds $\langle w \rangle$ back). Let $Q = \mathbb{F}_{97} \oplus \mathbb{F}_{97}$ as additive groups. The group G is the semidirect product $G = Q \rtimes P$ with $[Q, K] = 1$ and a acts (faithfully) on Q by multipliction on the right with the matrix $A = \begin{bmatrix} 0 & 1 \\ \zeta & 0 \end{bmatrix}$, where ζ is a fixed primitive 32^{nd}-root of unity of $\mathbb{F}_{97}$. So $C_P(Q) = K$. The group G is metabelian, because of the normal abelian subgroup $\langle Q, v^2, u^4, h^4 \rangle$. The latter, are the minimal elements such that in quotient with these all the relations in P become trivial. This making of P a direct product of cyclic groups. Obviously the order of G is $2^{25}.97^2$.

The automorphism $\tau \in \mathrm{Aut}(G)$ that will yield the counterexample is given by $a\tau = u^{16}a$ and $x\tau = x$ for all $x \in \langle Q, u, v, w, g, h \rangle$. This is a non-inner

automorphism. This is shown a bit later, but first we remark the following:

$$\tau|_P = \mathrm{conj}(w^4)|_P.$$

Since $wx = xw$ for all $x \in \{u, v, w, k\}$, we only have to check $\mathrm{conj}(w^4)(a)$ and $\mathrm{conj}(w^4)(g)$.

$$\begin{aligned} \mathrm{conj}(w^4)(a) &= a(u^4w)^{-4}w^4 \\ &= au^{-16} \\ &= au^{16} \\ &= u^{16}a \\ &= \tau(a) \end{aligned}$$

and $\mathrm{conj}(w^4)(g) = w^{-4}gw^4 = gw^{-4}w^4 = g = \tau(g)$.

This automorphism τ is a non-inner automorphism: We prove this by contradiction,i.e. assume that it is inner. Thus $\tau = \mathrm{conj}(x)$ for some $x \in P$ since $P\tau = P$. This yields $x \in Z(P)w^4 \cap C_P(Q) = \langle u, h^{64}\rangle \cap K = \{1\}$, a contradiction.

With this the setting of the story is outlined. The next step is to create a unit in $\mathbb{Z}G$. As explained in the previous chapters, we have to split the group ring in two 'easier' group rings. Explicitly, we will look at the pullback diagram $(**)$ of Chapter 4 with $L = \langle u^4 \rangle$.

$$\begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \Gamma \\ \downarrow & (**) & \downarrow \\ \Lambda & \longrightarrow & \frac{\mathbb{Z}(G/L)}{(\hat{Q},|L|)} \oplus \frac{\mathbb{Z}(G/Q)}{(\hat{L},|Q|)} \end{array}$$

So we have to construct units γ and λ in respectively Γ and Λ. The unit γ from Γ will be a surprising walk through the following diagram already mentionned in the Chapter 4.

$$\begin{array}{ccccc} \Gamma & \longrightarrow & \mathbb{Z}(G/Q) & \longrightarrow & \mathbb{Z}(G/Q)/(\hat{L}) \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{Z}(G/L) & \longrightarrow & \mathbb{Z}(G/LQ) & \longrightarrow & (\mathbb{Z}/|L|\mathbb{Z})(G/LQ) \\ \downarrow & & \downarrow & & \\ \mathbb{Z}(G/L)/(\hat{Q}) & \longrightarrow & (\mathbb{Z}/|Q|\mathbb{Z})(G/LQ) & & \end{array}$$

So the construction of γ will go through two steps. First one creates a γ_1 in $\mathcal{U}(\mathbb{Z}(G/L))$ and a second one for a γ_2 in $\mathcal{U}(\mathbb{Z}(G/Q))$. Afterwards, we look at Λ. The creation of λ in Λ will only be a single step. Finally a last short step is devoted to the final unit in $\mathbb{Z}G$.

6.1.2 Step 1

We construct a unit $\gamma_1 \in \mathbb{Z}(G/L)$. For this let $q = |Q|$ and consider the diagram

$$\begin{array}{ccc} \mathbb{Z}(G/L) & \longrightarrow & \mathbb{Z}(G/LQ) \\ \downarrow & & \downarrow \\ \mathbb{Z}(G/L)/(\hat{Q}) & \longrightarrow & (\mathbb{Z}/q\mathbb{Z})(G/LQ) \end{array} .$$

Where $q = |Q|$. We take in the lower horizontal arrow $1 \mapsto 1$. This can seem a bit illusionary, but in some sense it is logical given that this diagram is the farest reaching diagram in the splitting up program. To avoid finding trivial elements at the end, we will not take 1 in $\mathbb{Z}(G/LQ)$ (otherwise the whole diagram would become trivial and the element γ_2 in $\mathbb{Z}(G/Q)$ would probably be to weak to have the expected effect on the element γ in Γ). Before citing the unit from $\mathbb{Z}(G/LQ)$ we have to define some element. This will be built as product of power of units that are well known.

Units of the group ring $\mathbb{Z}C_8$

Let $\langle w \rangle$ be a cyclic group of order 8. It is known, [15, p. 251], that the normalized unit group of the integral group ring $\mathbb{Z}\langle w \rangle$ is the direct product of the cyclic group $\langle w \rangle$ and the unit $\nu = 2 - w^4 + (1 - w^4)(w + w^{-1})$. It will be more convenient to rewrite this element as:

$$\nu = \widetilde{w^4} + (1 - \widetilde{w^4})(3 + 2(w + w^{-1})).$$

One can check that $(1 - \widetilde{w^4})(w + w^{-1})^2 = 2(1 - \widetilde{w^4})$. We show this by pullback arguments: Let ϵ a primitive 8-th primitive root of unity. Then $(\epsilon + \epsilon^{-1})^2 = \epsilon^2 + \epsilon^{-2} + 2 = \sqrt{-1} - \sqrt{1} + 2 = 2$. One have following pullback

$$\begin{array}{ccc} \mathbb{Z}\langle w \rangle & \longrightarrow & \mathbb{Z}\langle w \rangle/(w^+) \cong \mathbb{Z}[\epsilon] \\ \downarrow & & \downarrow \\ \mathbb{Z}\langle w \rangle/\langle w^4 \rangle & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})(\langle w \rangle/\langle w^4 \rangle) \cong \mathbb{F}_2(C_4) \end{array}$$

Since $(1 - \widetilde{w^4})(w + w^{-1})^2$ and $2(1 - \widetilde{w^4})$ can play the role of x in the following pullback diagram

$$\begin{array}{ccc} x & \longrightarrow & (\epsilon + \epsilon^{-1})^2 = 2 \\ \downarrow & & \downarrow \\ 0 & \longrightarrow & 0 \end{array}$$

we have that they must be equal. This equality shows that ν corresponds to the unit $3 + 2\sqrt{2}$ of $\mathbb{Z}[\sqrt{2}] = \mathbb{Z}[(\epsilon + \epsilon^{-1})]$. A crucial observation is given by the following proposition.

Proposition 6.1.1 *Let $x, y \in \mathbb{Z}$ with $x^2 - 2y^2 = 1$. Let p be a prime, and $m, n \in \mathbb{N}$ such that $p^m | x$ and $2^n | y$. Then*

$$\theta = \widetilde{w^4} + (1 - \widetilde{w^4})(x + y(w + w^{-1}))$$

is a unit in $\mathbb{Z}\langle w \rangle$, the inverse given by $\theta^{-1} = \widetilde{w^4} + (1 - \widetilde{w^4})(x + y(w + w^{-1}))$. Moreover,

$$\theta^2 \equiv w^4 \ mod\ p^m \quad and \quad \theta^2 \equiv 1 \ mod\ 2^n.$$

Proof. By the pullback diagram

$$\begin{array}{ccc} \theta & \longrightarrow & x + y(w + w^{-1}) \\ \downarrow & & \downarrow \\ 1 & \longrightarrow & 1 \end{array}$$

we see that θ is a unit in $\mathbb{Z}\langle w \rangle$. Since $(x + y(w + w^{-1}))^{-1} = x - y(w + w^{-1})$ and $1^{-1} = 1$, the invers of θ is indeed given as in the statement of the proposition. The congruences follow from

$$\begin{aligned} \theta^2 &= \widetilde{w^4} + (1 - \widetilde{w^4})[x^2 + 2y^2 + 2xy(w + w^{-1})] \\ &= \widetilde{w^4} + (1 - \widetilde{w^4})[2x^2 - 2 + 1 + 2xy(w + w^{-1})] \\ &= 1 + (x^2 - 1)(1 - w^4) + (1 - w^4)xy(w + w^{-1}) \\ &= 1 + 2y^2(1 - w^4) + xy(1 - w^4)(w + w^{-1}) \\ &= w^4 + x^2(1 - w^4) + xy(1 - w^4)(w + w^{-1}) \end{aligned}$$

The first equality holds because $\tilde{G}(1 - \tilde{G}) = 0$ for every group G, $\widetilde{w^4}, 1 - \widetilde{w^4}$ are idempotents in $\mathbb{Q}\langle w \rangle$ and due to $(1 - \widetilde{w^4})(w + w^{-1})^2 = 2(1 - \widetilde{w^4})$. The second and fourth equality follow from $x^2 - 2y^2 = 1$ and the third is simply working out the definition of the idempotents. From the fourth equalition we deduce the congruence $\theta^2 \equiv 1 \bmod 2^n$ and by the last one we deduce $\theta^2 \equiv w^4 \bmod p^n$. □

Lemma 6.1.2 *Let $x, y \in \mathbb{Z}$. Let p be an odd prime, and $m, n \in \mathbb{N}$ be such that $p^m | x$ and $2^n | y$. Then $(x + y\sqrt{2})^p = \acute{x} + \acute{y}\sqrt{2}$ for some $\acute{x}, \acute{y} \in \mathbb{Z}$ with $p^{m+1} | \acute{x}$ and $2^n | \acute{y}$.*

Proof. It follows at once from the binomial expansion of $(x + y\sqrt{2})^p$ that we may take

$$\begin{aligned} \acute{x} &= \tbinom{p}{1} 2^{(p-1)/2} x y^{p-1} + \tbinom{p}{3} 2^{(p-3)/2} x^3 y^{p-3} + \ldots + \tbinom{p}{p-2} 2 x^{p-2} y^2 + \tbinom{p}{p} x^p, \\ \acute{y} &= \tbinom{p}{0} 2^{p/2} + \tbinom{p}{2} 2^{(p-2)/2} x^2 y^{p-2} + \ldots + \tbinom{p}{p-3} 2 x^{p-3} y^3 + \tbinom{p}{p-1} x^{p-1} y. \end{aligned}$$

□

Since $(3+2\sqrt{2})^4 = 577 + 8.51\sqrt{2}$ we obtain from Proposition 6.1.1 (applied with $x = 577$ and $y = 8.51$) that $\nu^8 \equiv 1 \bmod 8$. With an mathematical computer program one can check that $p = 97$ is the smallest prime p for which there exists a $k \in \mathbb{N}$ such that $(3+2\sqrt{2})^k = pr + 8s\sqrt{2}$ for some $r, s \in \mathbb{Z}$. In the case of $p = 97$ the corresponding k is 12. These numbers explain the q and power of ν in next corollary.

Corollary 6.1.3 *Let q be some natural power of the prime 97. Then*

$$\theta := \nu^{12q} = \widetilde{w^4} + (1 - \widetilde{w^4})(qr_0 + 8s_0(w + w^{-1}))$$

for some $r_0, s_0 \in \mathbb{Z}$. Moreover,

$$qr_0 \equiv 1 \ mod\ 8 \tag{6.1}$$

$$(qr_0)^2 - 2(8s_0)^2 = 1 \tag{6.2}$$

$$\theta^2 \equiv w^4 \ mod\ q \tag{6.3}$$

$$\theta^2 \equiv 1 \ mod\ 8 \tag{6.4}$$

Proof. That an r_0 and s_0 exist follows from Lemma 6.1.2. These also satisfies (6.1) because $(3+2\sqrt{2})^4 \equiv 1 \bmod 8$. The equality (6.2) follows immediately from $(3+2\sqrt{2})^n = a + b\sqrt{2}$ with $a^2 - 2b^2 = 1$ for every $n \in \mathbb{N}$. The latter can be proved by an easy induction argument as follow.

For $n = 1$ it is obvious. Asume that $(3+2\sqrt{2})^n = a + b\sqrt{2}$ with $a^2 - 2b^2 = 1$. Then

$$\begin{aligned}(3+2\sqrt{2})^{n+1} &= (a+b\sqrt{2})(3+2\sqrt{2}) \\ &= (3a+4b) + (3b+2a)\sqrt{2}\end{aligned}$$

and $(3a+4b)^2 - 2(3b+2a)^2 = a^2 - 2b^2 = 1$. Thus the inductionstep is done.

The congruences (6.3) and (6.4) now follow from (6.2) combined with Proposition 6.1.1. □

This element θ will play a crucial role and explains the number 97 in the counterexamples. We want to underline that this is the smallest number satisfiying some aritmethic equation. But as we will explain at the end of the chapter, Hertweck paved the way for a whole family of counterexamples. The smallest of this family, being the counterexamples explained in this chapter.

The unit of step 1

Let us now come back to the main question. We want a unit in $\mathbb{Z}(G/LQ)$ that is equal to 1 modulo q. By (6.3) such an element is $w^4\theta^2$. Thus there is a

unit γ_1 of $\mathbb{Z}(G/L)$ which maps to 1 in $\mathbb{Z}(G/L)/(\hat{Q})$ and to the image of $w^4\theta^2$ in $\mathbb{Z}(G/LQ)$. Since the images of w and θ in $\mathbb{Z}(G/LQ)$ are central elements, γ_1 is a central unit (thus conjugation by γ_1 on G/L agrees with τ, which induces the identity there). This concludes step 1.

6.1.3 Step 2

In this step we make a unit γ_2 in $\mathbb{Z}(G/Q)$. Look at the expanded diagram of the beginning of the chapter. We see that it in the left lower corner it has to be projected to the unit $w^4\theta^2$. A unit in the right upper corner still has to be found. For this one should wonder how $w^4\theta^2$ behaves in $(\mathbb{Z}/8\mathbb{Z})(G/LQ)$. By (6.4) the element $w^4\theta^2$ maps to the image of w^4 in $(\mathbb{Z}/8\mathbb{Z})(G/LQ)$. So the unit that we need to create in $\mathbb{Z}(G/Q)/(\hat{L})$ has to contain a term aw^4, where a is an integer that is send to 1 modulo 8. For example qr_0w^4. This will not suffice at the end to end up with a counterexample. So we will add a term to qr_0w^4 that belongs to $\Delta(G,L)$. For this we will use the simple components of $\mathbb{Q}L$.

Let e_i be the idempotents of $\mathbb{Q}L$ defined by $u^{16}e_1 = -e_1, u^8e_2 = -e_2, u^4e_3 = -e_3$ and $e_1 + e_2 + e_3 = 1 - \widetilde{L}$. So

$$e_1 = 1 - \widetilde{u^{16}}, \qquad e_2 = \widetilde{u^{16}}(1 - \widetilde{u^8}), \quad \text{and} \quad e_3 = \widetilde{u^8}(1 - \widetilde{u^4}). \tag{6.5}$$

Define now the element κ_8.

$$\kappa_8 = 8[e_1(u^4v + u^{-4}v^{-1}) + e_2(u^2 + u^{-2}) + e_3(u + u^{-1})] \in \mathbb{Z}\langle u, v\rangle \tag{6.6}$$

By the form of the common quotient, we obviously we must know how κ_8 interacts with the group elements of G and how it behaves modulo $\Delta(G,L)$. For later purposes we also investigate how the square of κ_8 looks like.

Proposition 6.1.4 *The following equations hold.*

$$x\kappa_8 = \kappa_8(x\tau) \text{ for all } x \in G \tag{6.7}$$

$$\kappa_8 \in \Delta(G,L) \tag{6.8}$$

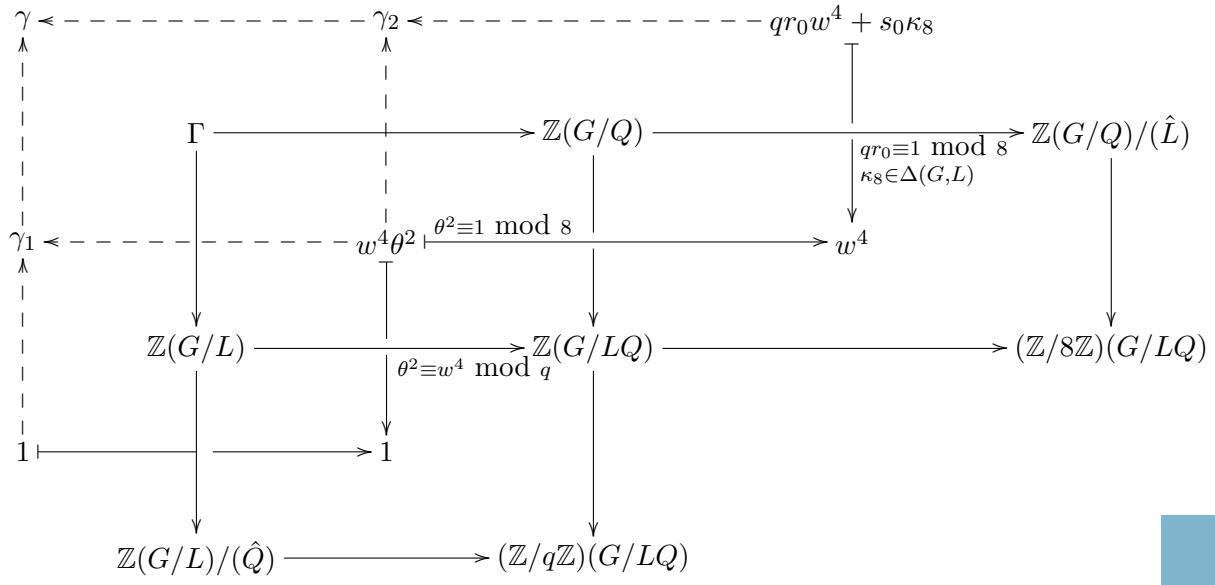
$$\kappa_8^2 = 2.8^2 - 16.\hat{L} \tag{6.9}$$

Proof. Because $[Q,K] = 1$ we only have to verify equation (6.7) for $x = a$ and $x = g$. Take $x = g$. One calculate that $(u^4v+u^{-4}v^{-1})g = (u^4gv^g+u^{-4}g(v^{-1})^g) = g(u^{-4}v^{-1} + u^4v)$. This together with $u \in \mathcal{Z}(G)$ yield $g\kappa_8 = \kappa_8 g = \kappa_8(g\tau)$. Now, take $x = a$. Remaind that $va = au^{16}v$ and $a\tau = u^{16}a$. With this in mind, equation (6.7) is clear. Before beginning the calculations for the equation (6.9), recall that $uv = vu$ and $\{e_1, e_2, e_3\}$ is a set of orthogonal central idempotents.

$$\begin{aligned}
\tfrac{\kappa_8^2}{8^2} &= e_1(u^4v + u^{-4}v^{-1})^2 + e_2(u^2 + u^{-2})^2 + e_3(u + u^{-1})^2 \\
&= e_1v^2(u^8 + u^{24}) + e_2(u^4 + u^{28}) + e_3(u^2 + u^{30}) + 2 - \tfrac{1}{4}.\hat{L} \\
&= v^2(u^8e_1 - u^8e_1) + (u^4e_2 - u^4e_2) + (u^2e_3 - u^2e_3) + 2 - \tfrac{1}{4}.\hat{L} \\
&= 2 - \tfrac{1}{4}.\hat{L}
\end{aligned}$$

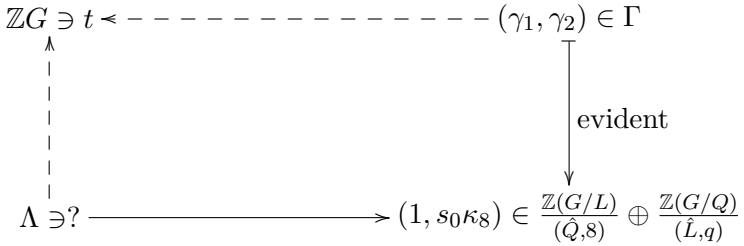
For (6.8) remark that the image of e_1, e_2 and e_3 in $\mathbb{Q}(G/L)$ is 0. □

Hertweck have chosen u to be of order 32 because of (6.9). By (6.1) and (6.8) the element $qr_0w^4 + s_0\kappa_8$ maps to the image of w^4 in $(\mathbb{Z}/8\mathbb{Z})(G/LQ)$. Since $(qr_0w^4 + s_0\kappa_8)(qr_0w^4 - s_0\kappa_8) = q^2r_0^2 - s_0^2.2.8^2 - s_0^2.16.\hat{L} \equiv 1 \bmod (\hat{L})$ by (6.2) and (6.9), the image of $qr_0w^4 + s_0\kappa_8$ in $\mathbb{Z}(G/Q)/(\hat{L})$ is a unit. So by the typical pullback argument there is a unit $\gamma_2 \in \mathbb{Z}(G/Q)$ which maps to the image of $w^4\theta^2$ in $\mathbb{Z}(G/LQ)$ and to the image of $qr_0w^4 + s_0\kappa_8$ in $\mathbb{Z}(G/Q)/(\hat{L})$. By (6.7), and the fact that τ induces the inner automorphism $\mathrm{conj}(\overline{w}^4)$ of G/Q, τ induces the inner automorphism $\mathrm{conj}(\gamma_2)$ of $\mathbb{Z}(G/Q)$. The desired unit γ is the unit of Γ which maps to γ_1 in $\mathbb{Z}(G/L)$ and to γ_2 in $\mathbb{Z}(G/Q)$. Summarized we have the diagram



6.1.4 Step 3

In the introduction of this section we splitted $\mathbb{Z}G$ in the rings Γ and $\Lambda = \mathbb{Z}G/(\hat{L}, \hat{Q})$. In step 2 we found a unit in Γ. Thus only the projection Λ remains. For the moment the situation is the following.



Before discovering the final unit t, we have to construct the element ? in Λ. It will contain (at least) a term $s_0\kappa_8$. But this is not sufficient since that $\kappa_8 \in \Delta(G, L)$ and thus projects to 0 in $\frac{\mathbb{Z}(G/L)}{(\hat{Q},8)}$ and not to 1. We will have to add a multiple of a so called element κ_q.

By looking at the definition of the element κ_q, equation (6.10), it may be astonishing to define such an element. But for those knowing Clifford theory and the results of [20] it will not come completely by surprise because the group G has been designed so that Clifford theory can be applied to show that τ induces an inner automoprihsm on $(1-\widetilde{Q})\cdot\mathbb{Z}[\frac{1}{97}]G$ and the conjugating element can be given explicitely.

Let $\mathcal{I}$ be the set of primitive idempotents of $\mathbb{Z}[\frac{1}{97}]Q$ except $\widetilde{Q}$. Remark that the elements of $\mathcal{I}$ correspond to the nontrivial cyclic subgroups of Q, since Q is abelian. Since the matrix $A=\begin{bmatrix}0 & 1\\ \zeta & 0\end{bmatrix}$ does not have eigenvalues over the prime field, the element a fixes no idempotents of $\mathcal{I}$ (by definition of the action of a on Q) and it follows easily that $\mathcal{I}$ is a disjoint union of sets E and F with $E^a=F$, and $E^x=E$ for all $x\in\langle Q,K,a^2\rangle$. Denote by E^+ and F^+ the sum of the idempotents in E and F, respectively, and let $q=97^2$, the order of Q. Define:

$$\kappa_q = q(E^+ + u^{16}F^+)\in\mathbb{Z}\langle Q,u^{16}\rangle, \tag{6.10}$$

We need several observations about this element.

Proposition 6.1.5 *The element κ_q satisfies:*

$$x\kappa_q = \kappa_q(x\tau) \text{ for all } x\in G \tag{6.11}$$

$$\kappa_q \in I(G,Q), \tag{6.12}$$

$$\kappa_q \equiv q \ mod(I(G,L),\hat{Q}) \tag{6.13}$$

$$\kappa_q^2 = q^2 - q\cdot\hat{Q} \tag{6.14}$$

Proof. The set $\mathcal{I}$ consists of central idempotents and $[Q,K]=1$. Also τ is the identity on G except for the element a there $a\tau=u^{16}a$. All this combined with $G/K\cong\langle a\rangle$ show that we only have to verify (6.11) for $x=a$. This is easly seen by observing that the action of a interchange E and F of place and so you have to take u^{16} out te find κ_q back. The other equations are obvious because $\widetilde{Q}$ is the only idempotent not in $\mathcal{I}$. □

Since $qr_0\equiv 1 \bmod 8$ and $\kappa_8\in I(G,L)$, we know that $r_0\kappa_q+s_0\kappa_8\in\Lambda$ is send to $(1,s_0\kappa_8)$ in the common quotient. The only question that remains, is whether this element is a unit in Λ or not. This is done in the next proposition.

Proposition 6.1.6 *Let κ_8 and κ_q be as before. These satisfy:*

$$\kappa_8\kappa_q = \kappa_q\kappa_8 \tag{6.15}$$

and

$$(r_0\kappa_q+s_0\kappa_8)(r_0\kappa_q-s_0\kappa_8)\equiv 1 \ mod\ (\hat{L},\hat{Q}).$$

Proof. The kappa's commute because $u \in Z(P)$ and v commutes with Q. Further

$$\begin{aligned}(r_0\kappa_q + s_0\kappa_8)(r_0\kappa_q - s_0\kappa_8) &= r_0^2\kappa_q^2 - s_0^2\kappa_8^2 \\ &= -r_0^2 q\hat{Q} - s_0.16.\hat{L} + r_0^2q^2 - s_0^2.2.8^2 \\ &\equiv 1 \bmod (\hat{L}, \hat{Q})\end{aligned}$$

In the second step we used (6.14) and (6.9). In the last step we used (6.2). □

Hence the image λ of $r_0\kappa_q + s_0\kappa_8$ in $\Lambda = \mathbb{Z}G/(\hat{L}, \hat{Q})$ is a unit and τ induces the inner automorphism $\mathrm{conj}(\lambda)$ of Λ by 6.7 and 6.11.

6.1.5 Step 4

From Theorem 4.0.25, (6.1), (6.12), (6.13) and (6.7) it follows that the units λ and γ give rise to a unit t of $\mathbb{Z}G$. This is illustrated in the following diagram

$$\begin{array}{ccc} \mathbb{Z}G \ni t & \prec\!\!- - - - - - - - - - - - - - - - - - - & (\gamma_1, \gamma_2) \in \Gamma \\ \vdots & \text{image calculated using } \kappa \in I(G,L),\ \kappa_q \equiv q \bmod (I(G,L), \hat{Q}) & \Big\downarrow \text{evident} \\ \Lambda \ni (r_0\kappa_q + s_0\kappa_8) & \xmapsto[\text{and } \kappa_q \in I(G,Q)]{qr_0 \equiv 1 \bmod 8} & (1, s_0\kappa_8) \in \frac{\mathbb{Z}(G/L)}{(\hat{Q},8)} \oplus \frac{\mathbb{Z}(G/Q)}{(\hat{L},q)} \end{array}$$

Altogether we have shown that $\tau = \mathrm{conj}(t)$ and so the proof is finished. For the moment we formally constructed a unit, but we can describe it precisly.

Proposition 6.1.7 *The unit t and its invers are given by:*

$$\begin{aligned} t &= (1-\widetilde{L})(1-\widetilde{Q})(r_0\kappa_q + s_0\kappa_8) + \widetilde{L}(1-\widetilde{Q}) + (1-\widetilde{L})\widetilde{Q}(qr_0w^4 + s_0\kappa_8) + \widetilde{L}\widetilde{Q}w^4\theta^2 \\ t^{-1} &= (1-\widetilde{L})(1-\widetilde{Q})(r_0\kappa_q - s_0\kappa_8) + \widetilde{L}(1-\widetilde{Q}) + (1-\widetilde{L})\widetilde{Q}(qr_0w^4 - s_0\kappa_8) + \widetilde{L}\widetilde{Q}w^4\theta^{-2} \end{aligned} \tag{6.16}$$

Proof. We first have to construct γ_1 and γ_2. We can do this by the isomorphism that we created to prove that a ring R is the pullback of $\sim: R/J \to R/I + J$ and $- : R/I \to R/I + J$. But there is a easier method by remarking the following: $1 - \widetilde{L} = 0$ and $\widetilde{L} = 1$ in $\mathbb{Z}(G/L)$. Also, $1 - \widetilde{L} = 1$ and $\widetilde{L} = 0$ in $\mathbb{Z}G/(\hat{L})$.

By using these remarks and the fact that γ_i is unique sending to the corners of their respective diagram (look at the expanded diagram of the end of Step 2) we see the following.

- $\gamma_1 = (1 - \widetilde{Q}) + \widetilde{Q}w^4\theta^2$
- $\gamma_2 = (1 - \widetilde{L})(qr_0w^4 + s_0\kappa_8) + \widetilde{L}w^4\theta^2$

Since the inverse of $w^4\theta^2$ and $(qr_0w^4 + s_0\kappa_8)$ are respectively $w^4\theta^{-2}$ and $qr_0w^4 - s_0\kappa_8$. We also find:

- $\gamma_1^{-1} = (1 - \widetilde{Q}) + \widetilde{Q}w^4\theta^{-2}$
- $\gamma_2^{-1} = (1 - \widetilde{L})(qr_0w^4 - s_0\kappa_8) + \widetilde{L}w^4\theta^{-2}$

The nice behaviour of the central idempotents combined with $(r_0\kappa_q + s_0\kappa_8)(s_0\kappa_q - s_0\kappa_8) \equiv 1 \bmod (\hat{L}, \hat{Q})$ delivers the cited form of t and t^{-1}. □

6.2 Counterexample to (ISO)

Hertweck found in 1999 and published in 2001 the following counterexample to the famous Isomorphism Problem.

Theorem 6.2.1 *There is a finite solvable group X, which is a semidirect product of a normal subgroup G and a cyclic subgroup $\langle c \rangle$, such that*

1. *There is a non-inner group automorphism τ of G, and $t \in V(\mathbb{Z}G)$, such that $g\tau = g^t$ for all $g \in G$.*
2. *In $\mathbb{Z}X$ we have that $t^c = t^{-1}$, that is the element c inverts the element t.*
3. *The group $Y = \langle G, tc \rangle$ is a group basis of $\mathbb{Z}X$ which is not isomorphic to X.*
4. *The group X has order $2^{21}.97^{28}$, a normal Sylow 97-subgroup and derived length 4.*

Let begin by explaining the philosphy behind the counterexample.

6.2.1 The philosophy

The idea is to split the group G in two quotients G_i and G_j:

$$\begin{array}{ccc} G & \longrightarrow & G_i \\ \downarrow & & \downarrow \\ G_j & \longrightarrow & G_{ij} \end{array}$$

where G_{ij} is the common quotient, such that the quotients satisfy the Isomorphism problem. Once this is done, we try to pullback the results to G. We will see that this is possible, but some obstruction will be created. This technique goes through projective limits. So before trying to create some obstruction theory, we have to know how and when we can see G as a projective limit of the quotients. For this, we introduce some notations and definitions.

First recall the categorical definition of a projective limit. Let $\mathcal{C}$ be any category, $(I, \leq)$ a partially ordered set, $\{A_i : i \in I\}$ a set of objects in $\mathcal{C}$ and $\{f_{i,j} : A_j \to A_i : i \leq j \in I\}$ a set of morphisms in $\mathcal{C}$. The set $\{A_i, f_{i,j} : i \leq j \in I\}$ is called a projective system if the maps satisfy the following conditions:

1. $f_{i,i} = Id$
2. $f_{i,k} = f_{i,j} \circ f_{j,k},\ i \leq j \leq k$

The projective limit associated to the above projective system is

$$limproj\{A_i, f_{i,j}\} = \{(a_i)_{i\in I} \in \prod_{i\in I} A_i : a_i = f_{i,j}(a_j), i \leq j \in I\}.$$

Now, let G be a finite group and let $\mathcal{N} = \{N_i \mid 1 \leq i \leq n\}$ be a family of normal subgroups. We write $\phi_i : G \to G/N_i = G_i$ for the natural mapping. Note by $\mathcal{P}_n = \mathcal{P}(\{1, \leq, n\})$ the powerset of $\{1, \ldots, n\}$. We partially order it by inclusion. For $S \in \mathcal{P}_n$ we set

$$G_S = G/(\prod_{i\in S} N_i) \text{ and } \phi_S : G \to G_S$$

denotes the natural projection. For $S \subseteq T$ we have a corresponding induced homomorphism $\phi_{S,T} : G_S \to G_T$. Then the set

$$\{G_S, \phi_{S,T} \mid S \in \mathcal{P}_n, S \subseteq T\}$$

is clearly a projective system. Form the projective limit $\hat{G} = limproj_{S\in\mathcal{P}_n}(G_S, \phi_{S,T})$. For simplicity reasons we shall write G_i for $G_{\{i\}}$ and $G_{ij} = G_{\{i,j\}}$. Write also ϕ_{ij} for $\phi_{i,\{i,j\}}$. Then $\phi_{ij} \neq \phi_{ji}$ for $i \neq j$, but $G_{ij} = G_{ji}$ and $G_{ii} = G_i$. As mentioned above, we are looking for criteria such that G is isomorphic to $\hat{G}$. In this setting of mind, define the homomorphism

$$\gamma : G \to \hat{G} : g \to (g_i = g \cdot N_i)_{1\leq i\leq n},$$

which has kernel $\cap_{1\leq i\leq N} N_i$. Thus γ is injective if and only if $\cap_{1\leq i\leq n} N_i = \{1\}$. If $n = 2$ and $N_1 \cap N_2 = \{1\}$ then γ is surely surjective, since then G is the pullback of G/N_1 and G/N_2 over $G/(N_1.N_2)$. More general we have

Lemma 6.2.2 *Let G be a finite group an let $\{N_i\}_{1\leq i\leq n}$ be a family of normal subgroups of G. Assume that*

1. $\cap_{1\leq i\leq n} N_i = \{1\}$,
2. *for every prime divisor p of $|G|$ there is at least one index $i = i(p)$ such that $(p, |N_{i(p)}|) = 1$.*

Then γ is an isomorphism, thus G is the projective limit of $\{G/N_i\}_{1\leq i\leq n}$.

It is important to remark that the above conditions are satisfied for a finite group G (which order is divisible by at least two primes), if one take $\mathcal{O}_0 = \{N_i = O_{p_i'}(G)\}_{1\leq i\leq n}$, where $\{p_i\}_{1\leq i\leq n}$ runs over all prime divisors of $|G|$. Here we take $N_{i(p)} = N_i$. So from now on we can consider G as a projective limit of some family of normal subgroups $\{N_i\}$ with N_i a characteristic subgroup (this has the advantage that a $\rho_i \in \mathrm{Aut}(G_i)$ induces a map $\overline{\rho_i}$ of G_{ij}). When we see G rather as a projective limit then a abstract group we note $\underline{G}$. The obstruction theory will consist of some cocycles and cobounderies.

Definition 6.2.3
- *The elements of the set* $Z(\underline{G}, \underline{Aut(G)}) = \{(\rho_{ij})_{1\leq i,j\leq n} \mid \rho_{ij} \in Aut(G_{ij}), \rho_{ii} = id, \rho_{ij}^{-1} = \rho_{ji}\}$ *are called cocycles.*
- *The elements of* $B(\underline{G}, \underline{Aut(G)}) = \{(\rho_{ij}) \in Z(\underline{G}), \underline{Aut(G)} \mid \rho_{ij} = \overline{\rho}_i \cdot \rho_j^{-1}$ *for* $\rho_i \in Aut(G_i)\}$ *are called cobounderies.*

Let us now continue into the philosophy of the counterexample. We already splitted the group G in quotients G_i. Assume that they satisfy the Isomorphism problem. So for each group basis H_i of $\mathbb{Z}G_i$ there exist an isomorphism $\sigma_i : G_i \to H_i$. Because G is the projective of normal characteristic groups, σ_i induces a homomorphism $\overline{\sigma_i} : G_{ij} \to H_{ij}$. Define the induced isomorphisms

$$\sigma_{ij} = \overline{\sigma_i}\,\overline{\sigma_j^{-1}} : H_{ij} \to H_{ij} \text{ with } \sigma = (\sigma_{ij}) \in Z(\underline{H}, \underline{Aut(H)}).$$

The obstruction is the following.

Theorem 6.2.4 *Assume that* $\mathbb{Z}G = \mathbb{Z}H$.

The groups G *and* H *are isomorphic if and only if the cocycle from above lies in* $B(\underline{H}, \underline{Aut(H)})$.

Consequently, we have to know when the quotients satisfy (ISO). The F^*-theorem gives a solution in that direction.

Theorem 6.2.5 (F^*-theorem) *REF.*

Let G *be a finite group which has a normal* p*-subgroup* N *containing its own centralizer, i.e.* $C_G(N) \subseteq N$. *Let* H *be a group basis of* $\mathbb{Z}G$. *Then* H *and* G *are* p*-adicly conjugate (i.e. by a unit of* $\mathbb{Z}_p(G)$ *the group ring over the* p*-adic numbers* $\mathbb{Z}_p$*).*

In particular H and G are isomorphic. Thus the group G satisfies (ISO). In fact one can proof that being p-adic conjugate implies being conjugate in the localization $\mathbb{Z}_{(p)} = \{\frac{a}{b} | a, b \in \mathbb{Z}$ and $p \nmid b\}$ and therefore in $\mathbb{Q}$ (REF). Hence the second Zassenhaus conjecture holds. Now remark that a solvable group G with $O_{p'} = \{1\}$ satisfies the conditions of the F^*-theorem. Consequently, for an arbitrary solvable group G and some prime divisior p of $|G|$, the quotient $G/O_{p'}$ falls unders the F^*-theorem. All the above results in a family of normal subgroups that gives place to quotients satisfying (ISO) and that permit us to form an obstruction theory for G satisfying (ISO). We 'only' have to find an appropriate cocycle.

The proof will clearly go through several steps. A first step will be devoted to the construction of the group. In the second step we start the group theoretical obstruction. So we will construct a non-trivial cocycle. In step 3, the normalizer problem is put forward. This step will mainly consist of reproducing all the steps

of the counterexample to the Normalizer Problem but with the new group. This yielding the first two parts of Theorem 6.2.1. Finally, step 4 will unify all the previous steps and will complete the proof of Theorem 6.2.1.

6.2.2 Step 1

Let us begin with the structure of the group X of Theorem 6.2.1. Due to the result of Jacowski and Marciniak the group X have to posses a non-normal Sylow 2-subgroup. The number 97 have showed to be useful, so X is a semidirect product $Q \rtimes P$ with a normal Sylow 97-Sylow subgroup Q and a Sylow 2-subgroup P. As explained in the obstruction theory, somehow the miracle have to appear in the common quotient. More precisely, the common quotient have to posses a non-inner, central automorphism. In the last century research has been done in the existance of groups with such an automorphism. The first example has been found by G.E.Wall in 1947, see [38]. It is the semidirect product $\langle w\rangle \rtimes \langle b\rangle \times \langle c\rangle)$ with action $w^b = w^{-1}$ and $w^c = w^5$ (later on this is the group $\overline{H}$).

Since 1947, there was a flow of examples but the one of Wall is still a very good one. It is not only a very small group, it also posses other very good propreties such as a faithfull irreducible representation. Despite this, Roggenkamp and Scott used an other group in their first semi-local counterexample, [25]. However they putted forward in [25] that the group of Wall could give a global counterexample. Probably Hertweck read it, because the common quotient will be almost the group of Wall (see the group $\overline{P}$ on next page). This already demystifie a bit the structure of the Sylow 2-subgroup P. After the proof of the counterexample we will do some final remarks with inter alia some extra examples of groups possesing a non-inner central automorphism.

Construction of P

$$P = \left(\langle u : u^{32}\rangle \times \langle v : v^4\rangle \times \langle w : w^8\rangle\right) \rtimes \left(\langle a : a^{128}\rangle \times \langle b : b^2\rangle \times \langle c : c^8\rangle\right),$$

the actions of a, b and c are given by:

- $u^a = u,\ v^a = u^{16}v$ and $w^a = u^4w$;
- $x^b = x^{-1}$ and $x^c = x^5$ for alle $x \in \langle u, v, w\rangle$.

The element a acts the same on $\langle u, v, w\rangle$ as in the counterexample to the normalizer problem, but has larger order. Note that the element u is no longer central.

Construction of Q

The normal Sylow 97-Subgroup Q of X is the direct product of normal subgroups N and M of X, defined as follows. Let $D = (\langle d_3\rangle \times \langle d_2\rangle) \rtimes \langle d_1\rangle \cong C_{97}^{(2)} \rtimes C_{97}$

with $d_2^{d_1} = d_3 d_2$ and $[d_3, d_1] = 1$ and let $R = D \times D = D^{(2)}$. Also define $N = R^{(4)}$. The group M is the additive group of the finite field $\mathbb{F}_{97^4}$. That we take the power 4 is explained afterwars by the action of a on M. That this group M have to be added in the sylowsubgroup Q can be seen the best by a semi-local analysis of the group. We will come back on this in a later chapter.

Action of P on Q

The largest normal 2-subgroup of X is $O_2(X) = C_P(Q) = \langle u, v, c^2 \rangle$ (and so the action of u and v is defined). Let $\overline{X} = X/O_2(X)$. Then $\overline{P} = \langle \overline{a} \rangle \times \overline{H}$ with $H = \langle w, b, c \rangle$ and $\overline{H} = C_8 \rtimes (C_2 \times C_2) = C_8 \rtimes Aut(C_8)$ (this will be proven later on). The subgroup H of P centralizes M, and a operates on M via multiplication with a fixed primitive 128^{th}-root of unity of $\mathbb{F}_{97^4}$ (the power 4 is the least power such that a 128-th root of unity exists in the field). For the action on the elements of N, we have to define some automorphisms.

An automorphism $\delta \in Aut(D)$ of order 64 is given by

$$\delta : \begin{cases} d_1 & \mapsto & d_2^{19} \\ d_2 & \mapsto & d_1 \\ d_3 & \mapsto & d_3^{-19} \end{cases}$$

Because $(d_2\delta)^{d_1\delta} = d_1^{d_2^{19}} = d_3^{-19} d_1 = d_3\delta \cdot d_2\delta$ this indeed defines an automorphism. From $19^{16} \equiv -1 \bmod 97$ it follows that

$$\delta^{16} : \begin{cases} d_1 & \mapsto & d_1^{19^8} \\ d_2 & \mapsto & d_2^{19^8} \\ d_3 & \mapsto & d_3^{-1} \end{cases} \quad \text{and} \quad \delta^{32} : \begin{cases} d_1 & \mapsto & d_1^{-1} \\ d_2 & \mapsto & d_2^{-1} \\ d_3 & \mapsto & d_3 \end{cases}$$

So δ has indeed order 64 and an automorphism $\rho \in \mathrm{Aut}(R)$ of order 128 is defined by $(x, y)\rho = (y, x\delta)$ for all $x, y \in D$. The operation of P on N is defined by

$$\begin{aligned} (r_1, r_2, r_3, r_4)^a &= (r_1\rho, r_2\rho, r_3\rho, r_4\rho), \\ (r_1, r_2, r_3, r_4)^w &= (r_4\rho^{64}, r_1, r_2, r_3), \\ (r_1, r_2, r_3, r_4)^b &= (r_1, r_4\rho^{64}, r_3\rho^{64}, r_2\rho^{64}), \\ (r_1, r_2, r_3, r_4)^c &= (r_1, r_2\rho^{64}, r_3, r_4\rho^{64}), \end{aligned}$$

for all $(r_1, r_2, r_3, r_4) \in N$ and u, v centralize $R^{(4)}$. That this is indeed a well defined action can be seen with the (irreducible) representation Ψ of $\overline{H}$ over $\mathbb{F}_{97}$:

$$\overline{w}\Psi = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{bmatrix}, \quad \overline{b}\Psi = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}, \quad \overline{c}\Psi = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

Because if for $h \in H$ all entries of the matrix $\overline{h}\Psi$ which are equal to -1 are replaced by ρ^{64}, then h acts on $N = R^{(4)}$ by "multiplication" from the right with this modified matrix. The group X is now completely fixed.

Proposition 6.2.6 *The group X has derived length 4.*

Proof. We assert that $X' = Q\langle u^2, v^2, w^2\rangle$, $X'' = N$ and $X''' = \langle d_2\rangle \times \langle d_1\rangle$. For this, we recall that the commutator subgroup is the smallest subgroup such that the factor group is abelian. So we must look at what we have to kill out to become abelian. Since $x^b = x^{-1}$ for all $x \in \langle u, v, w\rangle$, we get that $\langle u^2, v^2, w^2\rangle \subseteq X'$. Since the action of a on M is fixed point-free, we also have that $M \subseteq X'$. Since $d_2^{d_1} = d_3 d_2$ we also have that $d_3 \in X'$. The equation $(r_1, \ldots, r_4)^c = (r_1, r_2\rho^{64}, r_3, r_4\rho^{64})$ shows that d_1^2 and d_2^2 are in X'. Finally $(r_1, \ldots, r_4)^w = (r_4\rho^{64}, r_1, r_2, r_3)$ shows that in fact d_1 and d_2 are elements of X'. Alltogether have $Q\langle u^2, v^2, w^2\rangle \subseteq X'$. Moreover, this is sufficient to become abelian. So we are done.

For X'' look at $(r_1, \ldots, r_4)^w = (r_4\rho^{64}, r_1, r_2, r_3)$. The 3-th commutator subgroup X''' is calculated by considering the only non-trivial action $d_2^{d_1} = d_3 d_2$. □

We point out some other properties of the group X. The automorphism δ^{16} induces fixed-point free automorphism on $Z(D)$ and also on $D/Z(D)$, and δ^{32} induces the identity on $Z(D)$ and inverts the elements of $D/Z(D)$. Analogous statements hold for ρ^{32} and ρ^{64}, and it follows that

$$a^{32} \text{ induces fixed-point free automorphisms on } Z(Q) \text{ and on } Q/Z(Q) \quad (6.17)$$

$$a^{64} \text{ induces the identity on } Z(N) \quad (6.18)$$

Let $\tilde{R} = R/Z(R) \cong C_{97}^{(4)}$, and let $f_1, \ldots, f_4 \in R$ with $\tilde{R} = \langle \tilde{f}_1, \ldots, \tilde{f}_4\rangle$. Then $N/Z(N)$, as $\mathbb{F}_{97}\overline{H}$-module, is the direct sum of the four 4-dimensional modules $\langle(\tilde{r_1}, \ldots, \tilde{r_4} \mid r_i \in \langle f_k\rangle\rangle,\ k = 1, \ldots, 4$, all of them being isomorphic to the faithful irreducible module corresponding to the representation Ψ. Hence

$$End_{\overline{H}}(N/Z(N)) \cong Mat_4(\mathbb{F}_{97}). \quad (6.19)$$

6.2.3 Step 2

In this section we will work out the group-theoretical obstruction. So we will make a nontrivial cocycle δ_c and finally prove that this can give rise to non-isomorphic group baes. All this will consist of 4 lemma's.

Let $X^* = X/QO_2(X)$. Note that we can identify X^* with $\overline{P} = \langle\overline{a}\rangle \times \overline{H}$. We exhibit the class preserving non-inner automorphisms of $\overline{H}$.

Lemma 6.2.7 *There are automorphisms ζ_c and ψ of $\overline{H}$. The first defined by $\overline{w}\zeta_c = \overline{w}$, $\overline{b}\zeta_c = \overline{b}$ and $\overline{c}\zeta_c = \overline{w}^4\overline{c}$. The second by $\overline{w}\psi = \overline{wc}$, $\overline{b}\psi = \overline{bc}$ and $\overline{c}\psi = \overline{c}$. The outer automorphism group of $\overline{H}$ is $\langle\zeta_c, \psi\rangle/Inn(\overline{H})$, and is isomorphic to $C_2 \times C_2$. The automorphism ζ_c is a class preserving automorphism.*

Proof. For simplicity, we will omit the bars. So $H = \langle w \rangle \rtimes (\langle b \rangle \times \langle c \rangle) \cong C_8 \rtimes (C_2 \times C_2)$ with $w^b = w^{-1}$ and $w^c = w^5$. Thus the automorphisms ζ_c and ψ of H are defined as

$$\zeta_c : \begin{cases} c & \mapsto & w^4c \\ b & \mapsto & b \\ w & \mapsto & w \end{cases} \quad \text{and } \psi : \begin{cases} c & \mapsto & c \\ b & \mapsto & bc \\ w & \mapsto & wc \end{cases}$$

Both automorphisms are clearly of order 2. One can wonder how ζ_c and ψ interact. For example do they commute? Thus we calculate $[\zeta_c, \psi]$:

$$\begin{aligned} c &\xrightarrow{\zeta_c} w^4c \xrightarrow{\psi} (wc)^4c = w^4c \xrightarrow{\zeta_c} c \xrightarrow{\psi} c \\ b &\xrightarrow{\zeta_c} b \xrightarrow{\psi} bc \xrightarrow{\zeta_c} bw^4c \xrightarrow{\psi} bc(wc)^4c = bw^4 \\ w &\xrightarrow{\zeta_c} w \xrightarrow{\psi} wc \xrightarrow{\zeta_c} w^5c \xrightarrow{\psi} (wc)^5c = w^5 \end{aligned}$$

Here we used that $(wc)^2 = wccw^5 = w^6$ and so $(wc)^4 = w^4$. So

$$[\zeta_c, \psi] : \begin{cases} b & \mapsto & bw^4 \\ c & \mapsto & c \\ w & \mapsto & w^5 \end{cases}$$

Also $b^{w^2c} = cbw^2w^2c = bw^4$, $c^{w^2c} = ccw^{-10}w^2c = c$ and $w^{w^2c} = ccw^5 = w^5$. So $[\zeta_c, \psi] = \mathrm{conj}(w^2c)$. This means that ζ_c and ψ commute in $\mathrm{Out}(H)$. Now, we show thas these maps are not in $Inn(G)$. One can verify that the non-trivial conjugacy classes of H are as follows:

classes of elements of order 2:	$\{w^4\}$, $\langle w^4 \rangle c$, $\langle w^2 \rangle b$, $\langle w^2 \rangle wb$, $\langle w^2 \rangle bc$;
classes of elements of order 4:	$\langle w^4 \rangle w^2$, $\langle w^4 \rangle w^2c$, $\langle w^2 \rangle wbc$;
classes of elements of order 8:	$\langle w^2 \rangle w$, $\langle w^2 \rangle wc$.

If we let act ζ_c on all the conjugacy classes, we easily find out that it is a class preserving automorphism of H. Moreover it is non-inner. Indeed, $c\zeta_c = w^4c = \mathrm{conj}(zw)$, where $z \in C_H(c) = \langle b, w^2 \rangle$ and $(bc)\zeta_c = w^4bc$. Further $(bc)^{w^i} = w^{-i}w^{-5i}bc = w^{2i}bc = (w^{2i}bc)^c = (bc)^{w^ic}$ and $(bc)^{w^ib} = (w^{2i}bc)^b = w^{-2i}bc = w^{6i}bc = (w^{6i}bc)^c = (bc)^{w^ibc}$. Hence $c\zeta_c$ is conjugation with odd powers of w and in $(bc)\zeta_c$ we need conjugation with even powers of w. So ζ_c is indeed not-inner.

We also remark that ψ is non-central, because $(w^2b)\psi = (wc)^2bc = w^6bc \notin \langle w^2 \rangle b$.

Let $\theta \in \mathrm{Aut}(H)$. It remains to show that $\theta \in \langle \zeta_c, \psi \rangle \mathrm{Inn}(H)$. Since w is of order 8 it is possible to modify θ by an inner automorphism such that either 1) $w\theta = w$ or 2) $w\theta = wc$. Moreover in the first case $c\theta = w^4c$ and in the second one $c\theta = c$. Replacing θ by $\theta\zeta_c$ in the first case and by $\theta\psi$ in the latter, we can even assume that $w\theta = w$ and $c\theta = c$. Moreover, the class of wb is fixed by θ,

since it is the only class of elements of order 2 and length 4 whose elements do not commute with the fixed point c of θ. Consequently $w(b\theta) = (wb)\theta \in \langle w^2\rangle wb$ and thus $b\theta \in \langle w^2\rangle b$. So there are 4 possible choices for the image of b. In every case, one can easily transform θ in $Out(H)$ to ζ_c. Thus $\theta \in \langle\zeta_c\rangle \mathrm{Inn}(H)$. □

Define the automorphism $\delta_c = \mathrm{id} \times \zeta_c$ of X^*. So $\overline{a}\delta_c = \overline{a}$ and $\overline{h}\delta_c = \overline{h}\zeta_c$ for all $h \in H$. The next two lemmas establish that δ_c is a nontrivial cocycle.

Lemma 6.2.8 *Let $\phi \in Aut(P)$. Assume that ϕ fixes $O_2(X)$ (thus ϕ induces an automorphism $\overline{\phi}$ of $\overline{P}$). Assume further that $\overline{\phi}$ fixes $\overline{H}$. Then $\overline{\phi}|_{\overline{H}}$ is an inner automorphism.*

Proof. Assume that $\overline{\phi}|_{\overline{H}}$ is an outer automorphism. Suppose that $\overline{\phi}|_{\overline{H}} = \psi$ or $\overline{\phi}|_{\overline{H}} = \zeta_c\psi$. Then $\overline{b\phi} = \overline{b}\overline{c}$, but the order of b is 2 and the order of any preimage of $\overline{b}\overline{c}$ in P is at least 8, a contradiction. By Lemma 6.2.7, we may assume that $\overline{\phi}|_{\overline{H}} = \zeta_c$. We have to reach a contradiction. By definition of ζ_c and the form of the factor group $\overline{X} = X/O_2(X) = X/\langle u, v, c^2\rangle$ there are $r_i, s_i, t_i \in \mathbb{Z}$ with

$$a\phi = u^{r_1}v^{r_2}c^{2r_3}w^{4r_4}a^{2r_5+1}, \qquad b\phi = u^{s_1}v^{s_2}c^{2s_3}b, \qquad c\phi = u^{t_1}v^{t_2}w^4c^{2t_3+1}.$$

The form of $a\phi$ is explained by the facts that $\overline{P} = \langle\overline{a}\rangle \times \overline{H}$ and $\overline{H}\phi = \overline{H}$ and thus $\overline{a}\overline{\phi}$ is send on a generator of $\langle\overline{a}\rangle$. The largest part of the proof will consist of showing that the r_i, s_i, t_i can be taking in a specific form which will easily give rise to a contradiction.

Let $n, m \in \mathbb{Z}$. By definition $uc = cu^5$ and so $u^{13}c = cu$. This implies that $c^nu^m = u^{m.13^n}.c^n$ and so $(u^mc^n)^2 = u^{m(1+13^n)}c^{2n}$. By $k||l$ we mean that k is a divisor of l and no higher power of k is a divisor of l. Since $13^n \equiv_4 1$ we have that $2||1 + 13^n$. This implies that the order of u^mc^n is the maximum of the orders of u^m and c^n. Hence $c^4\phi = (u^{t_1}c^{2t_3+1})^4$ implies that $u^{t_1}c^{2t_3+1}$ has order 8 and thus, since u has order 32, that (i)$4|t_1$. Working out the relation $b\phi.c\phi = (bc)\phi = (cb)\phi = c\phi.b\phi$ delivers the equation

$$u^{s_1-t_1.13^{2s_3}}v^{s_2-t_2}w^4bc^{2s_3+2t_3+1} = u^{t_1+s_1.13^{2t_3+1}}v^{s_2+t_2}w^4bc^{2s_3+2t_3+1}.$$

Bring all the elements over to the left side of the equality and group the elements of the same type together. Then we obtain $u^{s_1(1-13^{2t_3+1})-t_1(13^{2s_3}+1)}v^{-2t_2} = 1$. This implies that (ii) $2|t_2$ and

$$s_1\underbrace{(1-13^{2t_3+1})}_{4||} \equiv \underbrace{t_1}_{4|\ (by\ (i))}\ \underbrace{(1+13^{2s_3})}_{2|} \bmod 32$$

(That $4||(1-13^{2t_3+1})$ follows from $13^{2t_3+1} \equiv_4 1$ and $13^{2t_3+1} \equiv_8 5^{2t_3}5 \equiv_8 5$). The congruence implies that (iii) $2|s_1$. Working out the relation $b\phi \cdot a\phi = a\phi \cdot b\phi$ gives

$$u^{s_1-r_1.13^{2s_3}}v^{s_2-r_2}w^{4r_4}a^{2r_5+1}bc^{2s_3+2r_3} = u^{r_1+s_1.13^{2r_3}+16s_2}v^{s_2+r_2}w^{4r_4}a^{2r_5+1}bc^{2s_3+2r_3}.$$

Again by regrouping the elements we find that (iv)$2|r_2$ and

$$\underbrace{s_1}_{2|\ (by\ (iii))}\ \underbrace{(1-13^{2s_3})}_{8|} \equiv r_1 \underbrace{(1+13^{2s_3})}_{2||} + 16s_2 \bmod 32.$$

The underbraces are modulo calculations similar to the previous ones. These implie that (v)$8|r_1$.

From (i)-(v) it follows that the r_i, t_i may be chosen such that

$$a\phi = u^{8r_1}v^{2r_2}c^{2r_3}w^{4r_4}a^{2r_5+1} \qquad \text{and} \qquad c\phi = u^{4t_1}v^{2t_2}w^4c^{2t_3+1}.$$

The element $a\phi$ commutes with u^4 (because $c^{2r_3}u^4 = u^{4.5^{2r_3}}c^{2r_3} = u^{4.25}c^{2r_3} = u^4c^{2r_3}$), $v^2 (\in Z(P))$ and c (because $u^{8r_1}c = cu^{40r_1} = cu^{8r_1}$), but not with w^4 (due to $aw^4 = u^{-16}wa$). So $[a\phi, c\phi] \neq 1$, but this is a contradiction since $[a, c] = 1$. □

It is in the proof of the next claim that we need that Q is non-abelian

Lemma 6.2.9 *Let $\phi \in Aut(\overline{X})$ and denote the induced automorphism on X^* by ϕ^*. Then $\overline{H}\phi^* = \overline{H}$ and $\phi^*|_{\overline{H}} \notin \zeta_c \cdot Inn(\overline{H})$.*

Proof. By the Sylow theorems, all the Sylow 2-subgroups are conjugated. Therefore we may modify $\overline{\phi}$ by an inner automorphism such that $\overline{P}\phi = \overline{P}$. Clearly, the center $\overline{M} \times Z(\overline{N})$ of $\overline{Q}$ is ϕ-invariant. The element $\overline{a}^{64}$ inverts the elements of $\overline{M}$ and centralizes $Z(\overline{N})$ by (6.18). Furthermore, $\overline{a}^{64}\phi = \overline{a}^{64}$ as $\overline{P} = \langle\overline{a}\rangle \times \overline{H}$ and $\overline{H}$ has exponent 8, the map $\overline{\phi}$ sends $\overline{a}$ on a other generator, say $\overline{a}^{2k+1}$. Therefore $\overline{a}^{64}\overline{\phi} = \overline{a}$. With this we easily prove that $\overline{M}\phi = \overline{M}$:

We know that $\overline{M\phi} \subseteq \overline{M} \times Z(\overline{N})$. Assume that there exist a $\overline{m}, \overline{m}_2 \in \overline{M}$ and a $1 \neq \overline{n} \in \overline{N}$ such that $\overline{m\phi} = \overline{m}_2.\overline{n}$. Since $(\overline{m\phi})^{\overline{a}^{64}} = (\overline{m}^{\overline{a}^{64}})\overline{\phi}$, we get that $\overline{m}_2^{-1}.\overline{n} = \overline{m}_2^{-1}.\overline{n}^{-1}$. Thus $\overline{a} = \overline{a}^{-1}$, but N has no elements of even order. This yields that $\overline{n} = 1$. So $\overline{M\phi} = \overline{M}$.

Consequently, $\overline{H}\phi = C_{\overline{P}}(\overline{M})\overline{\phi} = C_{\overline{P}}(\overline{M}) = \overline{H}$, and the first part of the lemma is proved.

Moreover, $\overline{w}^4\overline{a}^{64}\overline{\phi} = \overline{w}^4\overline{a}^{64}$ and $\overline{w}^4\overline{a}^{64}$ centralizes $\overline{N}$ $((r_1, \dots r_4)^{\overline{w}^4\overline{a}^{64}} = (r_1\overline{\phi}^{64}, \dots, r_4\overline{\phi}^{64})^{\overline{a}^{64}} = (r_1, \dots, r_4))$ and inverts the elements of $\overline{M}$ (because $\overline{w}^{64}$ commutes with $\overline{M}$). Analogues to before we prove that $\overline{N\phi} = \overline{N}$:

Assume that there exists a $\overline{n} \in \overline{N}$ and $\overline{x} \notin \overline{N}$ such that $\overline{n}\phi = \overline{x}$, then $(\overline{n}\phi)^{\overline{w}^4\overline{a}^{64}} = (\overline{n}^{\overline{w}^{54}\overline{a}^{64}})\phi$. This yield the contradiction $\overline{x}^{\overline{w}^4\overline{a}^{64}} = \overline{x}$. So $\overline{N\phi} = \overline{N}$.

In particular, ϕ induces an automorphism of $\overline{N}\,\overline{H}$. Let $\tilde{X} = X/O_2(X)Z(Q)$. Since $d_3 \in Z(Q)$ the normal subgroup $\tilde{N}$ is elementary abelian. Consider it as a $\mathbb{F}_{97}\tilde{H}$-module. Note that we may identify $\tilde{H}$ with $\overline{H}$.

By (6.19), $\mathrm{End}_{\tilde{H}}(\tilde{N}) \cong \mathrm{Mat}_4(\mathbb{F}_{97})$. As $\tilde{R} \cong \mathbb{F}_{97}$, also $\mathrm{End}(\tilde{R}) \cong \mathrm{Mat}_4(\mathbb{F}_{97})$. Thus $\mathrm{Aut}_{\tilde{H}}(\tilde{N}) \cong \mathrm{Aut}(\tilde{R})$. For any $\mu \in \mathrm{Aut}(\tilde{R})$ there is $\beta \in \mathrm{Aut}(\tilde{N}\tilde{H})$ defined

by $x\beta = x$ for all $x \in \tilde{H}$ and

$$(\tilde{r_1}, \dots \tilde{r_4})\beta = (\tilde{r_1}\mu, \dots, \tilde{r_4}\mu) \text{ for all } r_i \in R.$$

For any $\beta \in \mathrm{Aut}(\tilde{N}\tilde{H})$ fixing $\tilde{H}$ element-wise, which implies $\beta|_{\tilde{N}} \in \mathrm{Aut}_{\tilde{H}}(\tilde{N})$, there is a $\mu \in \mathrm{Aut}(\tilde{R})$ so that above equation holds.

The automorphism $\zeta_c \in \mathrm{Aut}_c(\overline{H})$ can be extended to an automorphism $\hat{\zeta_c} \in \mathrm{Aut}(\tilde{N}\tilde{H})$. To prove this, set

$$Z_c = (\overline{w} + \overline{w}^{-1})\Psi = \begin{bmatrix} 0 & 1 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & 1 & 0 \end{bmatrix} \in \mathrm{GL}(4, 97)$$

Since $\overline{h}(\overline{w} + \overline{w}^{-1}) = (\overline{w} + \overline{w}^{-1})\overline{h}\zeta_c$ for every $h \in H$ (this is easily checked on the basis elements $\overline{c}, \overline{b}$ and $\overline{w}$), we have that $\overline{h}\Psi \cdot Z_c = Z_c \cdot \overline{h}\zeta_c\Psi$ for all $h \in H$. Thus an automorphism $\hat{\zeta_c} \in \mathrm{Aut}(\tilde{N}\tilde{H})$ is defined by $x\hat{\zeta_c} = x\zeta_c$ for all $x \in \tilde{H}$ and

$$(\tilde{r_1}, \dots, \tilde{r_4})\hat{\zeta_c} = (\tilde{r_2}\tilde{r_4}^{-1}, \tilde{r_1}\tilde{r_3}, \tilde{r_2}\tilde{r_4}\mu, \tilde{r_1}^{-1}\tilde{r_3}) \text{ for all } r_i \in R.$$

Suppose that $\phi^*|_{\overline{H}} \in \zeta_c.Inn(\overline{H})$. For any $r, s \in R$ with $\tilde{r} = \tilde{s}\mu : (\overline{s}, 1, 1, 1)\overline{\phi} \in (1, \overline{r}, 1, \overline{r}^{-1}) \cdot Z(\overline{N})$ and $[(\overline{s}, 1, 1, 1), \overline{N}]\overline{\phi} = [(1, \overline{r}, 1, \overline{r}^{-1}), \overline{N}]$. Hence

$$\langle [(\overline{s}, 1, 1, 1), \overline{N}]\overline{\phi} \ : \ s \in R\rangle = \langle [(1, \overline{r}, 1, \overline{r}^{-1}), \overline{N}] \ : \ r \in R\rangle$$

but the groups on each side of the equality have different orders. This is a contradiction. So $\overline{\phi}|_{\overline{H}} \neq \zeta_c$ □

We are ready to formulate the final result of this section. Recall that $\delta_c = \mathrm{id} \times \zeta_c \in \mathrm{Aut}(X^*)$. From now on, we let $\breve{X} = X/Q$. Note that X is the pullback

$$\begin{array}{ccc} X & \longrightarrow & \overline{X} = X/O_2(X) \\ \downarrow & & \downarrow \\ X/Q = \breve{X} & \longrightarrow & X^* \end{array}$$

Lemma 6.2.10 *Let B be a group basis of $\mathbb{Z}X$. Assume that there exist normalized ring automorphisms $\phi_1 \in Aut_n(\mathbb{Z}\overline{X})$ and $\phi_2 \in Aut_n(\mathbb{Z}\breve{X})$, each mapping the image of X onto the image of B. Assume further that ϕ_2 induces an automorphism ϕ_2^* of $\mathbb{Z}X^*$. The automorphism ϕ_1 induces an automorphism ϕ_1^* of $\mathbb{Z}X^*$. Hence $\phi_1^*{\phi_2^*}^{-1}$ is a group automorphism of X^*. If $\phi_1^*\phi_2^{*-1} = \delta_c$, then B and X are not isomorphic*

Proof. Since Q is a normal Sylow 97-subgroup it is characteristic in X. Thus ϕ_1 induces an automorphism ϕ_1^* of $\mathbb{Z}X^*$. Assume that there is $\alpha \in \mathrm{Aut}(\mathbb{Z}X)$

with $X\alpha = B$. Also by the normal subgroup correspondence (Theorem 1.1.1), α induces automorphisms $\alpha_1 \in Aut(\mathbb{Z}\overline{X})$ and $\alpha_2 \in \mathrm{Aut}(\mathbb{Z}\breve{X})$ (Since Q is normal, it is the unique 97-Sylow subgroup and so the correspondance can be applied). These induce automorphisms α_1^* and α_2^* of $\mathbb{Z}X^*$. The latter are equal since X is a pullback. Let $\sigma_i = \phi_i\alpha_i^{-1}$. Then $\sigma_1 \in \mathrm{Aut}(\overline{X})$ and $\sigma_2 \in \mathrm{Aut}(\breve{X})$ and due to the normal subgroup correspondence σ_i induces an automorphism σ_i^* of X^*. Assume that $\phi_1^*\phi_2^{*-1} = \delta_c$. Then

$$\sigma_1^*\sigma_2^{*-1} = \phi_1^*\alpha_1^{*-1}\alpha_2^*\phi_2^{*-1} = \phi_1^*\phi_2^{*-1} = \delta_c.$$

By Lemma 6.2.9, σ_1^* fixes $\overline{H}$ and $\sigma_1^*|_{\overline{H}} \notin \zeta_c \cdot \mathrm{Inn}(\overline{H})$. We already have that $\sigma_1^*\sigma_2^{*-1} = \delta_c$, σ_1^* and δ_c fixes $\overline{H}$. This implies that σ_2^* fixes $\overline{H}$. So by 6.2.8 $\sigma_2^*|_{\overline{H}} \in \mathrm{Inn}(\overline{H})$. Consequently $\sigma_1^*\sigma_2^{*-1}|_{\overline{H}} \neq \zeta_c$ and $\sigma_1^*\sigma_2^{*-1} \neq \delta_c$, a contradiction. □

6.2.4 Step 3

We will bring back to life the normalizer problem and prove the first two parts of Theorem 6.2.1.

The group G is the subgroup $\langle Q, u, v, w, a, b\rangle$ of X. So $X = G \rtimes \langle c\rangle$. Let $S = \langle u, v, w, a, b\rangle$, a Sylow 2-subgroup of G. The automorphism $\tau \in \mathrm{Aut}(G)$ is defined by $x\tau = x$ for all $x \in \langle Q, u, v, w, b\rangle$ and $a\tau = u^{16}a$ (note the similarities with the τ of the counterexample to the normalizer problem). Easy verifications show that

$$\tau|_S = \mathrm{conj}(w^4)|_S$$

With analogous arguments as in the counterexample to the normalizer problem we show that τ is a non-inner group automorphism. Indeed, assume that there exist a $s \in S$ such that $\tau = \mathrm{conj}(s)$. Then

$$s \in w^4Z(S) \cap C_S(Q) = w^4\langle u^{16}, v^2, a^8\rangle \cap \langle u, v\rangle = \emptyset,$$

a contradiction. A unit $t \in V(\mathbb{Z}G)$ will be constructed with $g\tau = g^t$ for all $g \in G$ and $t^c = t^{-1}$.

Lemma 6.2.11 *Let $\mathcal{I}$ be the set of central primitive idempotents of $\mathbb{Q}Q$ except ϵ_Q. No idempotent from $\mathcal{I}$ is fixed by an element of the coset $\overline{a}\overline{H}$. Thus $\mathcal{I}$ is the disjoint union of sets E and F with $E^{\overline{a}} = F$ and $E^{\overline{x}} = E$ for all $x \in H$.*

Proof. The following is a list of mutual orthogonal central idempotents of $\mathbb{Q}Q$ which add up to $1 - \widetilde{Q}$.

1. $\widetilde{U}(1 - \widetilde{Z(Q)})$, where U is a subgroup of index 97 in $Z(Q)$;
2. $\widetilde{V}(1 - \widetilde{Q})$, where V is a subgroup of index 97 in Q containing $Z(Q)$.

Assume that there is a $h \in H$ such that $\overline{a}\overline{h}$ fixes one of these idempotents. Then, as $Q/Z(Q)$ and $Z(Q)$ are semisimple $\mathbb{F}_{97}\langle\overline{a}\overline{h}\rangle$-modules. One of these modules contains a 1-dimensional $\mathbb{F}_{97}\langle\overline{a}\overline{h}\rangle$-submodule. However since H has exponent 8 and $\overline{a}$ commutes with $\overline{H}$, we have that $(\overline{a}\overline{h})^{32} = \overline{a}^{32}$ and thus this submodule is a trivial $\langle\overline{a}^{32}\rangle$-module. This contradicts with (6.17). Consequently, no idempotent from $\mathcal{I}$ is fixed by an element of $\overline{a}\overline{H}$. From this we also deduce that $\mathcal{I}$ is a disjoint union of sets E and F as claimed. □

Choose sets E and F with the properties stated in the Lemma. As in the proof of the counterexample to the normalizer problem let $q = 97^{28}$ be the order of the normal Sylow 97-subgroup Q of G. Define as before

$$\kappa_q = q(E^+ + u^{16}F^+) \in \mathbb{Z}\langle Q, u^{16}\rangle$$

Let $L = \langle u^4\rangle$, a normal subgroup of order 8 of G. Define, as before, idempotents e_i of $\mathbb{Q}L$ defined by $u^{16}e_1 = -e_1, u^8e_2 = -e_2, u^4e_3 = -e_3$ and $e_1 + e_2 + e_3 = \eta_L$. So

$$e_1 = 1 - \widetilde{u^{16}}, \qquad e_2 = \widetilde{u^{16}}(1 - \widetilde{u^8}), \quad \text{and} \quad e_3 = \widetilde{u^8}(\widetilde{u^4}).$$

Again, the element κ_8 is defined as

$$\kappa_8 = 8[e_1(u^4v + u^{-4}v^{-1}) + e_2(u^2 + u^{-2}) + e_3(u + u^{-1})] \in \mathbb{Z}\langle u, v\rangle$$

Finally, let $\theta \in \mathbb{Z}\langle w\rangle, r_0$ and s_0 as in Corollary 6.1.3. So,

$$\theta := \nu^{12q} = \widetilde{w^4} + (1 - \widetilde{w^4})(qr_0 + 8s_0(w + w^{-1}))$$

with $r_0, s_0 \in \mathbb{Z}$ such that

1. $qr_0 \equiv 1 \bmod 8$,
2. $(qr_0)^2 - 2(8s_0)^2 = 1$,
3. $\theta^2 \equiv w^4 \bmod q$,
4. $\theta^2 \equiv 1 \bmod 8$.

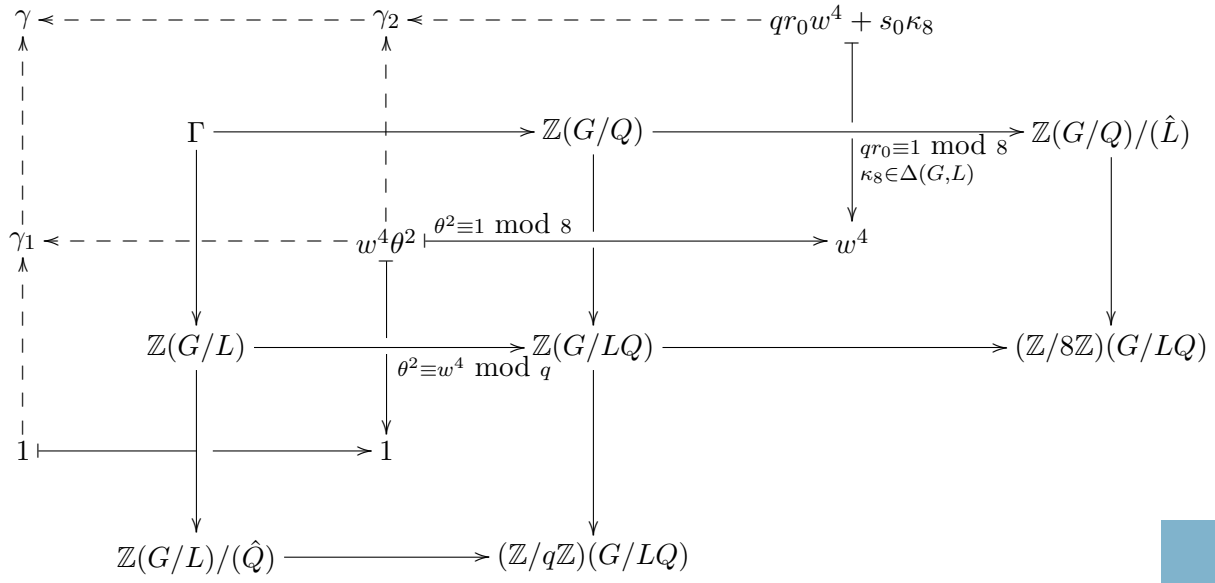
We recall a list of equations obtained in the counterexample to the normalizer problem. By looking carefully at the proofs of all these, we remark that they still hold.

1. $x\kappa_q = \kappa_q(x\tau)$ for all $x \in G$
2. $\kappa_q \in I(G, Q)$,
3. $\kappa_q \equiv q \bmod(\Delta(G, L), \hat{Q})$
4. $\kappa_q^2 = q^2 - q \cdot \hat{Q}$

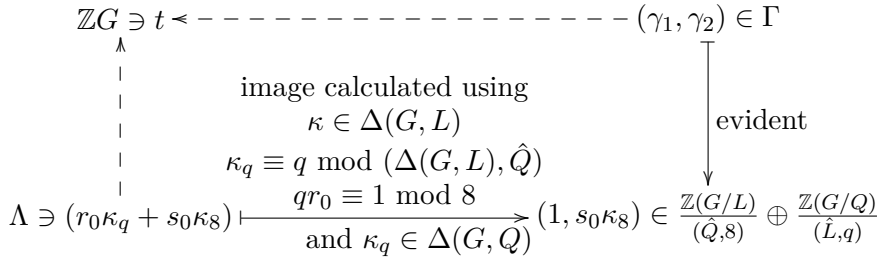
5. $x\kappa_8 = \kappa_8(x\tau)$ for all $x \in G$
6. $\kappa_8 \in \Delta(G, L)$
7. $\kappa_8^2 = 2.8^2 - 16.\hat{L}$
8. $\kappa_8\kappa_q = \kappa_q\kappa_8$
9. $(r_0\kappa_q + s_0\kappa_8)(r_0\kappa_q - s_0\kappa_8) \equiv 1 \bmod (\hat{L}, \hat{Q})$.

By the last equation the image λ of $r_0\kappa_q + s_0\kappa_8$ in $\Lambda = \mathbb{Z}G/(L^+, Q^+)$ is a unit and τ induces the inner automorphism $\mathrm{conj}(\lambda)$ of Λ by the first and fifth equation.

A unit γ is, again, constructed by going through the collection of three pullback diagrams:



The units λ and γ together with all the above equations, give again raise to a unit t of $\mathbb{Z}G$ such that $\tau = \mathrm{conj}(t)$:



Similar arguments as in the normalizer problem counterexample yield the unit t and its invers are given by the following.

$$\begin{aligned} t &= (1-\widetilde{L})(1-\widetilde{Q})(r_0\kappa_q + s_0\kappa_8) + \widetilde{L}(1-\widetilde{Q}) + (1-\widetilde{L})\widetilde{Q}(qr_0w^4 + s_0\kappa_8) + \widetilde{L}\widetilde{Q}w^4\theta^2, \\ t^{-1} &= (1-\widetilde{L})(1-\widetilde{Q})(r_0\kappa_q - s_0\kappa_8) + \widetilde{L}(1-\widetilde{Q}) + (1-\widetilde{L})\widetilde{Q}(qr_0w^4 - s_0\kappa_8) + \widetilde{L}\widetilde{Q}w^4\theta^{-2} \end{aligned}$$

This time we need some additional propreties of θ, κ_8 and κ_q. We omit the proof, because it simply consist of working out the definitions.

Lemma 6.2.12 *The elements θ, κ_8 and κ_q satisfy the following identities:*

$$\theta^c = \theta^{-1}, \qquad \kappa_8^c = -\kappa_8 \quad \text{and} \quad \kappa_q^c = \kappa_q.$$

And consequently $t^c = t^{-1}$.

6.2.5 Step 4

With this unit t of $\mathbb{Z}X$ we are able to construct another group basis. Define $Y = \langle G, tc \rangle$. Because $(tc)^2 = c^2$, we know that Y is a finite subgroup of $\mathrm{V}(\mathbb{Z}X)$ of the same order as X. So by Lemma 3.2.1 Y is a group basis of $\mathbb{Z}X$.

Recall that we write $\overline{X} = X/O_2(X)$, $\breve{X} = X/Q$ and $X^* = X/QO_2(X)$. The next lemma in combination with Lemma 6.2.10 shows that the groups X and Y are not isomorphic and Theorem 6.2.1 follows.

Lemma 6.2.13 *Set $K = \langle Q, w, a, b \rangle$ and $S = \langle u, v, w, a, b \rangle$. There are automorphisms*

- *$\phi_1 \in Aut(\mathbb{Z}\overline{X})$ defined by $\overline{x}\phi_1 = \overline{x}$ for all $x \in K$ and $\overline{c}\phi_1 = \overline{t}\overline{c}$.*
- *$\phi_2 \in Aut(\mathbb{Z}\breve{X})$ defined by $\breve{x}\phi_2 = \breve{x}$ for all $x \in S$ and $\breve{c}\phi_2 = \breve{w}^4\breve{t}\breve{c}$.*

Both automorphisms map the image of X to the image of Y and induce automorphisms of $\mathbb{Z}X^*$. The automorphism $\phi_1^*\phi_2^{*-1} \in Aut(\mathbb{Z}X^*)$ is induced from the group automorphism $\delta_c = id \times \zeta_c$ of X^*.

Proof. We have $\overline{X} = \overline{K} \rtimes \langle \overline{c} \rangle$. The element $\overline{t}$ centralizes $\overline{K}$, since τ induces the identity on $\overline{K}$. Because $t^c = t^{-1}$ the element $\overline{t}\overline{c}$ has the same order as $\overline{c}$, namely 2. Hence ϕ_1 is an automorphism. We have $\breve{X} = \breve{S} \rtimes \langle \breve{c} \rangle$. The element $\breve{w}^4\breve{t}$ centralizes $\breve{S}$, because the automorphism of $\breve{X}$ induced by τ is given by conjugation with $\breve{w}^4$. The element $\breve{w}^4\breve{t}\breve{c}$ has the same order as $\breve{c}$, namely 8. Hence ϕ_2 is an automorphism. Since $\breve{w}^4\breve{c}\phi_2 = \breve{t}\breve{c}$, we have obviously have that $\phi_1^*\phi_2^{*-1} = \delta_c$. □

6.2.6 Concluding remarks

Remark 1. We know that the second Zassenhaus conjecture (which asserts that the group bases of $\mathbb{Z}G$ are rationally conjugate) and the Isomorphism problem are not true in general. However, one can formulate a block version of these conjectures. Namely, that for any group basis H of $\mathbb{Z}G$, the projections of G and H on each block of the semisimple rational group algebra $\mathbb{Q}G$ are conjugate within the units of the component in the case of (ZC2). The Isomorphism problem becomes: two group bases of $\mathbb{Z}G$ are isomorphic with G in each component of $\mathbb{Q}G$. Also the known counterexamples to (ZC2) and (ISO) are not counterexamples to these block versions. We will show that Hertweck's counterexample is not a

counterexample in this case. More precisely, the projections of X and Y on each block of the rational group algebra $\mathbb{Q}X$ are conjugate within the units of the block. Conceptionally this follows from a semilocal analysis of the counterexample involving central automorphisms. One of $\mathbb{Q}P$ and one of $\mathbb{Q}T$ where T is the inertia group of E^+, which induce on each block a group automorphism. This goes beyond the scope of the thesis. That is why we content ourselves with listing explicitely conjugating units.

In $\mathbb{Q}X$ there is a decomposition $\sum_{i=1}^{6} f_i = 1$ with central idempotents

$$\begin{array}{lll} f_1 = \widetilde{L}\widetilde{Q} & f_2 = \widetilde{L}(1-\widetilde{Q}) & f_3 = (\widetilde{L})\widetilde{Q}, \\ f_4 = \widetilde{u^{16}}(1-\widetilde{L})\widetilde{Q} & f_5 = (1-\widetilde{u^{16}})\widetilde{v^2}(1-\widetilde{Q}) & f_6 = (1-\widetilde{u^{16}})\widetilde{u^{16}v^2}(1-\widetilde{Q}). \end{array}$$

We give rational group ring elements $\mu_i, \mu_i^{'}$ such that $f_i\mu_i^{'}\mu_i = f_i$ and $f_i\mu_i^{'}X\mu_i = f_iY$. Note that

$$\begin{array}{lll} f_1tc = f_1w^4\theta^2c, & f_2tc = f_2c, & f_3tc = f_3(w^4qr_0 + s_0\kappa_8)c, \\ f_4tc = f_4(qr_0 + s_0\kappa_8), & & f_itc = f_i(qr_0(E^+ - F^+) + s_0\kappa_8)c, \ i = 5,6 \end{array}$$

We may take $\mu_1 = \theta^{-1}, \mu_1^{'} = \theta$ and $\mu_2 = \mu_2^{'} = 1$. Somewhat harder to find are

$$\mu_3 = \frac{4s_0}{qr_0 - 1} - \frac{1}{32}w^4\kappa_8 \text{ and } \mu_3^{'} = 16s_0 + \frac{qr_0 - 1}{8}w^4\kappa_8.$$

Let

$$\beta_{\pm} = \pm\frac{4s_0}{qr_0 - 1} - \frac{1}{32}\kappa_8 \text{ and } \beta_{pm}^{'} = \pm 16s_0 + \frac{qr_0 - 1}{8}\kappa_8.$$

It is tedious but straightforward to check that $(1-\widetilde{L})\cdot\beta_{pm}^{'}\beta_{pm} = (1-\widetilde{L})$ and $(1-\widetilde{L})\cdot\beta_{pm}^{'}c\beta_{pm} = (1-\widetilde{L})\cdot(qr_0 \pm s_0\kappa_8)c$ and that we may take

$$\begin{array}{rcl} \mu_4 & = & \beta_+ \\ \mu_4^{'} & = & \beta_+^{'} \\ \mu_5 & = & [\beta_+(\widetilde{v} + (u^4+u^{-4})(1-\widetilde{v}))E^+] - [\beta_-((1-\widetilde{v}) + (u^4+u^{-4})\widetilde{v})F^+] \\ \mu_5^{'} & = & [\beta_+^{'}(\widetilde{v} + \frac{1}{2}(u^4+u^{-4})(1-\widetilde{v}))E^+] - [\beta_-^{'}((1-\widetilde{v}) + \frac{1}{2}(u^4+u^{-4})\widetilde{v})F^+] \\ \mu_6 & = & [\beta_+(\widetilde{u^8v} + (u^4+u^{-4})(1-\widetilde{u^8v}))E^+] - [\beta_-((1-\widetilde{u^8v}) + (u^4+u^{-4})\widetilde{u^8v})F^+] \\ \mu_6^{'} & = & [\beta_+^{'}(\widetilde{u^8v} + \frac{1}{2}(u^4+u^{-4})(1-\widetilde{u^8v}))E^+] - [\beta_-^{'}((1-\widetilde{u^8v}) + \frac{1}{2}(u^4+u^{-4})\widetilde{u^8v})F^+] \end{array}$$

Remark 2. One might ask whether there are counterexamples of odd order, since the known examples are of even order. In the semi-local case the constraint of even drops, so it may be possible to also find a odd global counterexample.

Remark 3. In the introductory chapter on the normalizer problem we outlined the importance of cocycles (in the part of subsection 3.4.1 behind Theorem 3.4.7) and it let to problems (P1)-(P3) and triples $(G, u\gamma)$. In the previous counterexample we constructed such a cocycle. We put more clearly forward the triple. Let $G = \langle w \rangle$ be the cyclic group of order 8, and let γ be the automorphism of G of order 2 defined by $w\gamma = w^5$. Then for the unit

$$\nu = \widetilde{w^4} + (1-\widetilde{w^4})(3 + 2(w + w^{-1})) \in \mathcal{U}(\mathbb{Z}G),$$

we have $N_\gamma(\nu) = 1$ (see middle of subsection 3.4.1 for the definitioin of the map N_γ), which simply means that γ inverts ν. For each $n \geq 2$, there are prime powers p^a and r^b such that $\nu^n \equiv 1 \bmod p^a$ and $\nu^n \equiv w^4 \bmod r^b$. We list the prime powers for some values of n in the following table.

n	2	3	4	5	6	7	8	$\cdots$	24
p^a	2	7	$2^2, 3$	41	$2, 5, 7$	239	$2^3, 3, 17$	$\cdots$	$2^3, 3^2, 5, 7, 11, 17, 1153$
r^b	3	5	17	29	$3^2, 11$	13^2	577	$\cdots$	$97, 577, 13729$

As we already mentioned before, the prime 97 is the smallest prime r such that there is $n \in \mathbb{N}$ with $\nu^n \equiv 1 \bmod 8$ and $\nu^n \equiv w^4 \bmod r$, and that this is the reason why the groups from the counterexamples are divisble by 97.

Next, we present an example of a triple where G and γ are of odd order. Let $G = \langle x \rangle$ be a cyclic group of order 7, and let γ be the automorphism of G of order 3 defined by $x\gamma = x^2$. Let ζ be a primitive 7^{th} root of unity. Then $a = -1 - \zeta - \zeta^6$ is a unit in $\mathbb{Z}[\zeta]$ with $a^{21} \equiv 1 \bmod 7$. Hence

$$\begin{aligned} u &= \widetilde{G} + (1 - \widetilde{G})(-1 - x - x^6)^{21} \\ &= -6910567 - 4308668(x + x^6) + 1537746(x^2 + x^5) + 6226206(x^3 + x^4) \end{aligned}$$

is a unit in $\mathbb{Z}G$ with $N_\gamma(u) = 1$.

Remark 4. One of the main ingredients of the proof was the group with non-inner, class preserving automorphism in the common quotient. Further research could consist of beginning with another example. That's why we mention here some other examples.

1. Let H be a 2-Sylow subgroup of the linear group $\mathrm{GL}(3, 4)$ (this is a group of order 64 and derived length 2). This group was used by Roggenkamp and Scott in their semi-local counterexample to the second Zassenhaus conjecture and $\mathrm{Out}_c(H) \cong C_2^{(4)}$.

2. The next example was found by Soriano, [39]. His example is the following group S:

   $$S = \langle w, b, c : w^8 = b^4 = c^2 = 1, [b, c] = 1, w^b = w^{-1}, w^c = w^5, w^4b^2 = 1 \rangle.$$

   The non-inner, class preserving automorphism ζ_c is again given by $c\zeta_c = w^4c, b\zeta_c = b$ and $w\zeta_c = w$. The group of Soriano and the group of Wall have the same charactertable, but the faithfull irreducible representation of S isn"t in $\mathbb{Q}$ (the Shür index over $\mathbb{Q}$ is 2) and the corresponding simple component of $\mathbb{Q}S$ is a matrixring over the Quaternionalgebra $\mathbb{H}$.

6.3 Counterexample to Zassenhaus

As some illustration of Hertwecks technics from the previous chapters, we give the least known counterexample to the automorphism version of the Zassenhaus

conjectures. This chapter is based on [6] The Second Zassenhaus conjecture says that each two group bases of $\mathbb{Z}G$ are conjugate by a unit in $\mathbb{Q}G$. By the Skolem-Noether theorem (see Theorem A.0.6) the Zassenhaus conjecture asserts that G can be mapped onto any group basis of $\mathbb{Z}G$ by a central ring automorphism of $\mathbb{Z}G$ (this is an automorphism fixing the center element-wise). Therefore we say that an augmentation preserving automorphism α of $\mathbb{Z}G$ has a Zasenhaus factorization if it is the composition of a group automorphism of G (extended to a ring automorphism) and a central automorphism. Roggenkamp and Scott produced a metabelian group G of order 2880 such with an augmentation preserving automorphism α of $\mathbb{Z}G$ which has no Zassenhaus factorization. And thus G and $G\alpha$ are group bases of $\mathbb{Z}G$ which are not rationally conjugate. Their construction of the automorphism α is explicit in the semilocal situation. To show that their example is also a global counterexample, they developed some kind of a general theory. This using Picard groups and Milnor's Mayer Vietoris sequence. (see [32]) The counterexample of Hertweck uses way more easy technics (namely, those similar to the other counterexamples of Hertweck). In fact we will give a counterexample to the assertion (AUT) which is implied by the second Zassenhaus conjecture:

(AUT) assume that α is a an augmentation preserving automorphism of $\mathbb{Z}G$. Then α is the composition of a group automorphism of G and conjuagation with a unit in $\mathbb{Q}G$ that normalizes $\mathbb{Z}G$.

Due to the Skolem-Noether theorem this is equivalent with:

α is the composition of a group automorphism (more precisely, an automorphism of $\mathbb{Z}G$ induced by an automorphism of the group G) and a central ring automorphism of $\mathbb{Z}G$.

Such a composition is called a Zassenhaus factorization. We will prove the following.

Theorem 6.3.1 *(M.Hertweck, 2002) There is a metabelian group G of order 1440 ($= 2^5.3^2.5$) and an automorphism α of $\mathbb{Z}G$ which has no Zassenhaus factorization.*

We begin with writing down the philosphy behind the proof (this is somehow the obstruction theory of the previous chapters).

6.3.1 Philosophy outline

The group G will be a pullback

$$\begin{array}{ccc} G & \longrightarrow & G_5 \\ \downarrow & & \downarrow \\ G_3 & \longrightarrow & H \end{array}$$

where the maps are surjective, and the subscripts 3 and 5 reflects structural details of the two groups which are the buildingblock of the story (the kernel of the horizontal map to H is of order 3 and the corresponding vertical kernel is of order 5). Form also the following pullback of rings

$$\begin{array}{ccc} \Gamma & \longrightarrow & \mathbb{Z}G_5 \\ \downarrow & & \downarrow \\ \mathbb{Z}G_3 & \longrightarrow & \mathbb{Z}H \end{array}$$

As mentioned in earlier chapters, the $\mathbb{Z}$-order Γ is only a relative small image of the group ring $\mathbb{Z}G$. Nevertheless, it will be very usefull. Suppose now that we have an automorphism α of $\mathbb{Z}G$ that behaves well with respect to the projections on $\mathbb{Z}G_3$ and $\mathbb{Z}G_5$. Thus inducing automorphisms α_3 and α_5 respectively. Assume that both have a Zassenhaus conjecture. This means that

$$\begin{aligned} \alpha_3 &= \beta_3\delta_3 \\ \alpha_5 &= \beta_5\delta_5 \end{aligned}$$

where β_i is a groupalgebra automorphism of $\mathbb{Z}G_i$ induced by a group automorphism and δ_i a central automorphism. The central automorphisms δ_i induce automorphisms of $\mathbb{Z}H$. Thus the β_i also and consequently β_i induces an automorphism of the group H.

Consider now the automorphism $\sigma = \beta_5^{-1}\beta_3$ of the group H. This is a central group automorphism. Suppose α is compatible with the Zassenhaus conjecture, i.e is has a Zassenhaus conjecture $\alpha = \beta\delta$, where β is a group automorphism of $\mathbb{Z}G$ and δ is a central automorphism. Then $\beta^{-1}\beta_3 = \delta\delta_3^{-1}$ is a central group automorphism of G_3, and $\beta^{-1}\beta_5$ is a central group automorphism of G_5. Put $\rho_3 = \beta^{-1}\beta_3$ and $\rho_5 = \beta^{-1}\beta_5$. Each of the central group automorphisms ρ_3, ρ_5 induces an automorphism of the group H and on H we have that

$$\alpha = \beta_5^{-1}\beta_3 = \rho_5^{-1}\rho_3.$$

Alltogether we found that:

If α is compatible with the Zassenhaus conjecture,then the central group automorphisms σ of H must be the product of automorphisms of H induced by central group automorphisms of G_3 and G_5.

6.3.2 The proof

The group G is the semidirect product $G = (M \times N \times Q) \rtimes W$, with

- $W = \langle w : w^8\rangle \rtimes (\langle b : b^2\rangle \times \langle c : c^2\rangle)$, with $w^b = w^{-1}$ and $w^c = w^5$;
- $M = \langle m : m^5\rangle,\ N = \langle n : n^3\rangle$ and $Q = \langle q : q^3\rangle$;
- $C_W(m) = \langle wc, b\rangle,\ C_W(n) = \langle w^2, b, c\rangle$ and $C_W(q) = \langle w, b\rangle$

Remark that again the group of Wall is used (i.e the group W) and that the centralizers are subgroups of index 2 in W. We proved in Lemma 6.2.7 that the group W has a non-inner class-preserving automorphism δ of order 2, which maps c to w^4c and b and w are fixed. Simultaneously we showed that $\mathrm{Out}(W) \cong C_2 \times C_2$. We extend this automorphism to an automorphism σ of G:

$$\sigma : \begin{cases} c \mapsto w^4 c \\ b, w, m, n, q \text{ fixed} \end{cases}$$

Define

$$G_3 = G/M, \qquad G_5 = G/N \text{ and } H = G/MN.$$

Note that we may identify G_3 with NQW, G_5 with MQW and H with QW.

Lemma 6.3.2 *The automorphism σ induces an inner automorphism of $\mathbb{Z}[\frac{1}{2}]H$, given by conjugation with the unit*

$$\mu = \widetilde{w^4} + (1 - \widetilde{w^4})(w + w^{-1}) \in \mathbb{Z}[\frac{1}{2}]\langle w \rangle.$$

Proof. It is wellknown that it is a unit (it follows from $(1 - \widetilde{w^4})(w + w^{-1})^2 = 2(1 - \widetilde{w^4})$ and this was proven earlier). One easily checks that $x\mu = \mu(x\sigma)$ for the generators x of H. □

This together with the next lemma, shows that σ is a candidate for the obstruction theory. We write $x \nsim y$ to indicate that the group elements x and y are not conjugate.

Lemma 6.3.3 *The subgroups G_3 and G_5 have trivial central outer group automorphisms. Thus*

$$Out_c(G_3) = 1 \quad \textit{and} \quad Out_c(G_5) = 1.$$

Proof. Let $\phi \in \mathrm{Aut}_c(NQW)$. We have to show that $\phi \in \mathrm{Inn}(NQW)$. We may assume that $w\phi = w, b\phi = b$ and either $c\phi = c$ or $c\phi = w^4c$. From $qw \nsim q^{-1}w$ it follows that $q\phi = q$. If $c\phi = c$, then $nb \sim n^{-1}b$ implies that $\phi = id$. So assume that $c\phi = w^4c$. From $[n, c] = 1$ it follows that nc and $(nc)\phi$ are conjugate in W. As $c^w = w^4c$. As $c^w = w^4c = c\phi$ and $C_W(c) = C_W(n)$, it follows that $n\phi = n^w = n^{-1}$, yielding the contradction $nb \nsim n^{-1}b = (nb)\phi$.

Similar for $\phi \in \mathrm{Aut}_c(MQW)$. Again, we may assume that $w\phi = w, b\phi = b$ and either $c\phi = c$ or $c\phi = w^4c$. From $qw \nsim q^{-1}w$ it follows that $q\phi = q$. If $c\phi = c$, then $mwc \nsim m^{-1}wc$ implies that $\phi = id$. So assume that $c\phi = w^4c$. From $[m, wc] = 1$ it follows that mwc and $(mwc)\phi$ are conjugate in W. As wc and w^5c $(= (wc)\phi)$ are not conjugate in $C_W(m)$, $m\phi = m^{-1}$. From $[mqb, b] = 1$ it follows that mqb and $(mqb)\phi$ $(m^{-1}qb)$ are conjugate in W. Hence $m^x = m^{-1}$ for some $x \in C_W(q) \cap C_W(b) = \langle w^4, b \rangle \subseteq C_W(m)$, a contradiction. □

We will need following observation: Let x and y be elements of a group with $y^x = y^{-1}$. Then $(y - y^{-1})x = -x(y - y^{-1})$. One can prove that σ induces a central automorphism of $\Lambda = \mathbb{Z}G(M^+, N^+)$, but since it is not crucial for the construction for α we will omit the proof. Again we define Γ as the image of $\kappa : \mathbb{Z}G \to \mathbb{Z}G_3 \oplus \mathbb{Z}G_5$ and construct associated pullbacks diagrams

$$\begin{array}{ccc} \Gamma & \longrightarrow & \mathbb{Z}G_5 \\ \downarrow & & \downarrow \\ \mathbb{Z}G_3 & \longrightarrow & \mathbb{Z}H \end{array} \quad \text{and} \quad \begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \Gamma \\ \downarrow & & \downarrow \\ \Lambda & \longrightarrow & \Omega \end{array}.$$

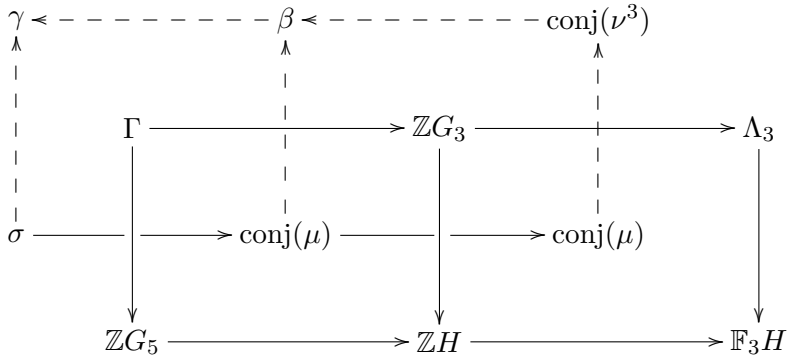
Note that N and M can be viewed as normal subgroups of G_3 and G_5 respectively. Denote by Λ_3 and Λ_5 following quotients:

$$\Lambda_3 = \mathbb{Z}G_3/(\hat{N}) \quad \text{and} \quad \Lambda_5 = \mathbb{Z}G_5/(\hat{M}).$$

By Theorem 4.0.25 the ring Ω equals $\Lambda_3/5\Lambda_3 \oplus \Lambda_5/3\Lambda_5$. We still note ν for the unit $\widetilde{w^4} + (1 - \widetilde{w^4})(3 + 2(w + w^{-1}))$ of $\mathbb{Z}\langle w\rangle$. The invers is given by $\widetilde{w^4} + (1 - \widetilde{w^4})(3 - 2(w + w^{-1}))$. From $\nu^3 = \widetilde{w^4} + (1 - \widetilde{w^4})(90 + 70(w + w^{-1}))$ it follows that

$$\begin{array}{rcll} \nu^3 & \equiv & \widetilde{w^4} - (1 - \widetilde{w^4}) = w^4 & \mod 5\mathbb{Z}\langle w\rangle, \\ \nu^3 & \equiv & \mu & \mod 3\mathbb{Z}[\frac{1}{2}]\langle w\rangle, \end{array}$$

The automorphism σ of G induces automorphisms of G_5 and H which, for simplicity, we denote by the same symbol. At the beginning we proved that $\sigma = \mathrm{conj}(\mu)$ on H, so $\sigma = \mathrm{conj}(\nu^3)$ on $\mathbb{F}_3(H)$ and there is $\gamma \in \mathrm{Aut}(\Gamma)$, inducing σ on $\mathbb{Z}G_5$ and a central automorphism β on $\mathbb{Z}G_3$ as shown below.



As $\nu^3 \equiv w^4 \mod 5$ and $w^4 \in Z(G)$,

$$\gamma \textit{ induces the identity on } \Lambda_3/5\Lambda_3 \textit{ and induces } \sigma \textit{ on } \Lambda_5/3\Lambda_5.$$

In Λ, the group element mn corresponds to a primitive 15^{th} root of unity, so the image t of $mn - (mn)^{-1}$ in Λ is a unit in Λ. The binomial expansion gives $(mn - (mn)^{-1})^{15} = 1 - (\sum_{i=1}^{14}(-1)^i\binom{15}{i}(mn)^{2i}) - 1$ and for $1 \le i \le 14$ it follows from $\binom{15}{1} \equiv 1 \mod 2$ and $\binom{15}{i} + \binom{15}{i+1} = \binom{16}{i+1} \equiv 0 \mod 2$ that $\binom{15}{i} \equiv 1 \mod 2$. Hence $(mn - (mn)^{-1})^{15} \equiv 1 + \hat{M}\hat{N} \equiv 1 \mod 2$ and consequently $t^{15} \in 1 + 2\Lambda$.

Note the image of $m - m^{-1}$ in $\mathbb{Q}\Lambda$ by u. Because m is a 5-th root of unity, the element u is invertible. The image of $n - n^{-1}$ in $\mathbb{Q}\Lambda$ will be noted by v. One can verify that $\mathrm{conj}(u)$ and $\mathrm{conj}(v)$ of Λ is given by the following maps

$$\mathrm{conj}(u) : \begin{cases} c \mapsto -c \\ w \mapsto -w \\ b, m, n, q \text{ fixed} \end{cases}$$

$$\mathrm{conj}(v) : \begin{cases} w \mapsto -w \\ b, c, m, n, q \text{ fixed} \end{cases}$$

Note that Λ can be written as the pull-back

$$\begin{array}{ccc} \Lambda & \longrightarrow & (1 - \widetilde{w^4})\Lambda \\ \downarrow & & \downarrow \\ \widetilde{w^4}\Lambda & \longrightarrow & \overline{\Lambda} \end{array}$$

By using $2\widetilde{w^4} \in \Lambda$ in the diagram, we get that $2 = 0$ in $\overline{\Lambda}$. The automorphism $\mathrm{conj}(v)\mathrm{conj}(t^{15})$ of Λ induces an automorphism ϕ of $(1 - \widetilde{w^4})\Lambda$, which in turn induces the identity on $\overline{\Lambda}$ due to the form of $\mathrm{conj}(v)$ and $t^{15} \in 1 + 2\Lambda$. It follows that there is an automorphism λ of Λ which induces ϕ on $(1 - \widetilde{w^4})\Lambda$ and the identity on $\widetilde{w^4}\Lambda$. The elements $mn - (mn)^{-1}$ and $n - n^{-1}$ map to the same element in $\mathbb{Z}G_3$ and it follows that the inner automorphism $\mathrm{conj}(t)$ and the automorphism $\mathrm{conj}(v)$ induce the same automorphism on $(1 - \widetilde{w^4})\Lambda_3/5\Lambda_3$. Similarly, $mn - (mn)^{-1}$ and $m - m^{-1}$ map to the same element in $\mathbb{Z}G_5$, so that $\mathrm{conj}(t)$ and $\mathrm{conj}(u)$ induce the same automorphism on $(1 - \widetilde{w^4})\Lambda_5/3\Lambda_5$. As $\mathrm{conj}(v)\mathrm{conj}(u)$ and σ induce the same automorphism of $(1 - \widetilde{w^4})\Lambda$ ($w^4 = -1$ in $(1 - \widetilde{w^4})\Lambda$)). It follows that

λ induces the identity on $\Lambda_3/5\Lambda_3$ and induces σ on $\Lambda_5/3\Lambda_5$.

Using the given description of $\mathbb{Z}G$ as a pull-back, it follows from the italic centralized remarks that there is an automorphism α of $\mathbb{Z}G$ inducing γ on Γ and λ on Λ.

As γ induces σ on $\mathbb{Z}G_5$ (which implies that α preserves the augmentation), and a central automorphism on $\mathbb{Z}G_3$. It follows from Lemma 6.3.3 and the introductory philosophy that α has no Zassenhaus factorization. Consequently we proved the theorem.

7 Possible further research

The last chapters probably revealed a lot of open problems to the reader. We remind you of several open problems is the problem list of Sehgal in [14].

Problem.10 Is (ZC1) true for S_n?

Problem.11 Is (ZC3) true for S_n?

Since Roggenkamp-Scott gave a counterexample to (ZC2) he suggest: **Problem.12** (ZC1) for finite solvable groups.

Problem.13 Is (Aut) true for A_n?

Problem.14 (ZC1),(ZC2),(ZC3) for A_n?

Problem.15 (Aut) for $G = AwrS_n$ when A is finite nilpotent.

Problem.16 (ISO) for $G = AwrS_n$ when A is finite nilpotent.

Problem.27 Give a "‘ good proof"’ of the following Theorem of Cliff-Sehgal-Weiss: Suppose that G is finite group with $A \triangleleft G$ and both A and G/A abelian. Then $\mathcal{U}(1 + \Delta(G)\Delta(A))$ is torsion free.

If one finds a reasonable proof of the above result then it may be possible to generalize it to the following, which is easy proveded G is nilpotent.

Problem.28 Suppose that G is finite having a normal abelian subgroup. Then $\mathcal{U}(1 + \Delta(G)\Delta(A)$ is torsion free.

Problem.29 Suppose that G is finite nilpotent. Does G have a normal complement N in $V(\mathbb{Z}G)$, namely $V(\mathbb{Z}G) = N \rtimes G$?

Problem.30 Problem.29 for finite nilpotent class three groups.

Problem.31 Does there exist a normal torsion free complement to G in $V(\mathbb{Z}G)$ if G is nilpotent of class two?

Problem.38 Does (ZC1) hold for infinite nilpotent groups?

Problem.39 Does (ZC1) hold for the free product $G = C_{m_1} * C_{m_2} * \ldots * C_{m_n}$?

We have to remark that Problem.43 (= the normaliser problem) is not up to date. Since Hertweck found a counterexample recently.

Problem.46 Let G be an infinite nilpotent group. Does (ISO) hold?

A Appendix

A numbertheoretical theorem that we will need is following theorem of Dirichlet. Also refered to as 'Dirichlet's theorem on aritmetic progressions' in most literature.

Theorem A.0.4 (Theorem of Dirichlet on aritmetic progressions) *Let a, d two positive coprime integers. There there exists infintely many primes p such that*

$$p \equiv a \ mod \ d$$

Thus the aritmetic progression $a, a+d, a+2d, \ldots, a+nd, \ldots$ contains infintely many primes.

In section 6.3 we need the theorme of Skolem-Noether. For this we first remind the definition of a simple K-algebra and a central simple K-algebra.

Definition A.0.5 *1. a K-algebra A is called simple if it is a simple ring.*

2. a simple K-algebra a is a central simple K-algebra if A is finite dimensional over K and the natural embedding $K \to \mathcal{Z}(A)$ gives an isomorphism $K \cong \mathcal{Z}(A)$.

Remark that each simple algebra is a central simple algebra over its center. With this we state the theorem [3].

Theorem A.0.6 (Skolem-Noether) *(REF) Let B be a simple K-subalgebra of a central simple K-algebra A. Then every isomorphism of K-algebras $\phi : B \to B' \subseteq A$ can be extended to an inner automorphism of A, that is, there exists an element $a \in A$ such that*

$$\phi(b) = aba^{-1}, \forall b \in B.$$

Following corollary is used regularly in literature.

Corollary A.0.7 *Let a be a central simple K-algebra, and let ϕ be an automorphism of A which fixes each element of K.1. Then ϕ is an inner automorphism.*

Bibliography

Bibliography

[1] Eric Jespers, Gabriela Olteanu and Angel Del Rio, Rational Group Algebras of Finite Groups: from Idempotents to Units of Integral Group Rings, 2010, Algebras and representation theory

[2] A.Olivieri, del Rio, J.J. Simon, On monomial characters and central idempotents of rational group algebras, communications in Algebra 32 (2004), 1531-1550.

[3] Charles W. Curtis and Irving Reiner, Methodes of Representation Theory with applications to finite groups and orders Volume 1, Wiley-interscience publication, 1981, ISBN: 0-471-18994-4

[4] E. Jespers, M.M. Parmenter and S.K.Sehgal, Central units of integral group rings of nilpotent groups, Proc. Amer. Math. Soc. **124** (1996), 1007-1012.

[5] Martin Hertweck, A Counterexample to the Isomorphism Problem for Integral Group Rings, Ann.of Math. (2) 154 (2001),no.1,115-138.

[6] Martin Hertweck, Another counterexample to a conjecture of Zassenhaus, Contributations to Algebra and Geometry, Volume 43 (2002), No.2, 513-520.

[7] Martin Hertweck, on torsion units of some integral group rings

[8] Martin Hertweck, Class-preserving automorphisms of finite groups, J.Algebra **241** (2001), no.1, 1-26

[9] Martin Hertweck, Contributions to the integral representation theory of groups, Habilitationsschrift, 2004.

[10] Martin Hertweck, Eine Lösung des Isomorphieproblems für ganzzahlige Gruppenringe von endlichen Gruppen, Ph.D thesis, University of Stuttgart, 1998

[11] Martin Hertweck and Wolfgang Kimmerle, Coleman automorphisms of finite groups, Math.Z **242** (2002), no. 2, 203-215.

[12] Angel Del Rio and S.K.Sehgal, Zassenhaus conjecture (ZC1) on torsion units of integral group rings for some metabelian groups, Arch. Math. (Basel) 86 (2006), no. 5, 392-397.

[13] Sudarshan K.Sehgal, Topics in Group Rings, Marcel Dekker INC., 1978.

[14] Sudarshan K.Sehgal, Units in integral group rings, Longman Scinetific and Technical,1993.

[15] Sudarshan K.Sehgal and Cesar Polcino Milies, An introduction to group rings, Kluwer academic Publishers, 2002.

[16] Sudarshan K. Sehgal, Z. Marciniak, Zassenhaus conjecture and infinite nilpotent groups, J.Algebra, 184, 1996, pp.207-212

[17] K.W.Roggenkamp and L.L.Scott, Isomorphisms of p-adic group rings, Ann. Math. **126** (1987), 593-647.

[18] K.W.Roggenkamp and A.Zimmermann, A counterexample for the isomorphism problem of polycylic groups, J.Pure.Appl.Algebra, **103** (1995), 101-103.

[19] K.W. Roggenkamp, The isomorphism problem for integral group rings of finite groups, Representation theory of finite groups and finite-dimensional algebras, Proc. Conf., Bielfeld/Ger., 1991, Prog.Math. 95, 193-220 (1991).

[20] K.W.Roggenkamp and A.Zimmerman, Outer group automorphisms may become inner in polycylic groups, J. Pure Appl. Algebra, **103** (1995), 101-103.

[21] R. Sandling, The ismorphism problem for group rings, a survey, Proc. 1984 Oberwolfach, conf. on Orders and their Applications, Lecture Notes in Math., no. 1148, Springer, 1985, pp. 256-289

[22] R. Sandling, Group rings of circle and unit groups, Math. Z. **124** (1974), 195-202.

[23] R. Sandling, Dimension subgroups over arbitrary coefficient rings, J. Algebra **21** (1972), 250-265

[24] K.W. Roggenkamp, L.L. Scott, Units in group rings: Splittings and the isomorphism problem, J. Algebra 96 (1985), 397–417.

[25] K.W. Roggenkamp, L.L. Scott, On a conjecture of Zassenhaus or finite group rings, Manuscript, November 1988, 1-60.

[26] K.W. Roggenkamp, L.L. Scott, Units in metabelian group rings: Nonsplitting examples for normalized units, J. Pure Applied Algebra **27** (1983), 299-314.

[27] A. Weiss, Idempotents in group rings, J. Pure Appl. Algebra 16 (1980), 207–213.

[28] G. Janssens, Primitive Central Idempotents of Rational Group algebras, to appear in Journal of Algebra and Its Applications, to appear.

[29] W. Kimmerle and K.W .Roggenkamp, Projective limits of group rings, J.Pure Appl.Algebra, **88** (1993), 119-142.

[30] L.L. Scott, Recent progress on the isomorphism problem, Proc. Symposia in Pure Math., Vol. 47 (1987), 259-274

[31] L.L. Scott, Defect groups and the isomorphism problem, Representations lineaires des groupes finis., Proc. Colloq. Luminy, France (1988), Asterisque 181-182 (1990)

[32] L.L. Scott, On a conjecture of Zassenhaus and beyond, Algebra, Proc .Int. Conf. Memory A.I. Mal'cev, Novosibirsk/USSR, 1989, Contemp. Math. **131**(1) (1992), 325-343.

[33] R.Z.Aleev, Higman's central unit theory, units of integral group rings of finite cyclic groups and Fibonacci numbers, Internat. J. Algebra Comput. **4** (1994), no.3, 309-358

[34] Robert Remak, Über die darstellung der endlichen Gruppen als Untergruppen direkter Produkte, J. Reine Angew. Math., **163** (1930), 1-44.

[35] R. Remak, Über minimale invariante Untergruppen in der Theorie der endlichen Gruppen, J. Reine Angew. Math. **162** (1930), 1-16.

[36] R. Remak, Über die erzugenden invarianten Untergruppen der subdirekten Darstellungen endlicher Gruppen, J.Reine Angew.Math. **164** (1931), 197-242.

[37] R. Remak, Über Untergruppen direkter Produkte von drei Faktoren, J.Reine Angew. Math. **166** (1931), 65-100.

[38] G.E. Wall, Finites groups with class-preserving outer automorphisms, J.London Math., Soc. **22** (1947), 315-320.

[39] M. Soriano, Klassenerhaltende Automorphisms von nicht zefallenden Gruppenerweiterungen, Diplomarbeit, Universität Stuttgart, 1996

[40] E. Noether, Hypercomplexe Grössen und Darstellungtheorie, Math. Z., **30** (1929), 641-692

[41] R. Brauer and E. Noether, Über minimale Zerfällungskörper irreduzibler Darstellungen, Sitz. Preuss. Akad. Wiss. Berlin (1927), 221-228.

[42] R. Brauer, Über Systeme Hypercomplexer Zahlen, Math. Z. **30** (1929), 79-107.

[43] G. Higman, Units of group rings, D.Phil. Thesis, University of Oxford, Oxford, 1940.

[44] I. Kaplansky, Problems in the theory of rings, Nas-NRC Publ. 502, Washington, 1957, pp. 1-3 .

[45] I. Kaplanksy, "Problems in the theory of rings" revisited, Amer. Math .Monthly **77** (1970), 445-454.

[46] D.S. Passman, Infinite Group rings, Marcel Dekker, New York, 1971.

[47] E.C. Dade, Deux groups finis ayant la meme algebre de group sur tout corps, Math. Z. **119** (1971), 345-348.

[48] I. van Gelder, Idempotenten in Groepringen, Master Thesis, Vrije Universiteit Brussel, 2010

[49] D.S. Passman and P.F. Smith, Units in integral group rings, J. Algebra **69** (1981), 213-239.

[50] G.H. Cliff, S.K. Sehgal and A.R. Weiss, Units of integral group rings of metabelian groups, J. Algebra **73** (1981), 167-185.

[51] G. Losey, On the structure of $Q_2(G)$ for finitely generated groups, Canad.J. Math **25** (1973), 353-357.

[52] S. Jackowski, Z. Marciniak, Group automorphisms inducing the identity map on cohomolog, J.Pure and Appl. Algebra **44** (1987), 241-250.

[53] E.Jespers, S.O. Juriaans, J.M. Miranda, and J.R. Rogerio, On the Normalizer Problem, Journal of Algebra **247** (2002), 24-36.

[54] T. Petit Lobão and C. Polcino Milies, The normalizer property for integral group rings of Frobenius groups, Journal of Algebra **256** (2002), no. 1-6.

[55] Yuanlin Li, M. M. Parmenter and S. K. Sehgal, On the Normalizer Property for integral Group Rings, Communications in Algebra **27** (1999), no. 9, 4217-4223.

[56] M. Mazur, On the isomorphism problem for integral group rings of infinite groups, Expositiones Mathematicae **13** (1995), no. 5, 433-445.

[57] J. Ritter and S.K. Sehgal, Construction of units in integral group rings of finite nilpotent groups