A cohomological approach to the classification of p-groups

Inger Christin Borge

Wadham College
University of Oxford

Trinity term 2001

Thesis submitted to the Faculty of
Mathematical Sciences as partial fulfilment
for the degree of Doctor of Philosophy

Abstract

In this thesis we apply methods from homological algebra to the study of finite p-groups. Let G be a finite p-group and let $\mathbb{F}_p$ be the field of p elements. We consider the cohomology groups $\mathrm{H}^1(G, \mathbb{F}_p)$ and $\mathrm{H}^2(G, \mathbb{F}_p)$ and the Massey product structure on these cohomology groups, which we use to deduce properties about G.

We tie the classical theory of Massey products in with a general method from deformation theory for constructing hulls of functors and see how far the strictly defined Massey products can take us in this setting.

We show how these Massey products relate to extensions of modules and to relations, giving us cohomological presentations of p-groups. These presentations will be minimal pro-p presentations and will often be different from the presentations we are used to.

This enables us to shed some new light on the classification of p-groups, in particular we give a "tree construction" illustrating how we can "produce" p-groups using cohomological methods. We investigate groups of exponent p and some of the families of groups appearing in the tree. We also investigate the limits of these methods.

As an explicit example illustrating the theory we have introduced, we calculate Massey products using the Yoneda cocomplex and give 0-deficiency presentations for split metacyclic p-groups using strictly defined Massey products.

We also apply these methods to the modular isomorphism problem, i.e. the problem whether (the isomorphism class of) G is determined by $\mathbb{F}_pG$. We give a new class $\mathcal{C}$ of finite p-groups which can be distinguished using $\mathbb{F}_pG$.

Acknowledgements

Oxford, August 2001

Two roads diverged in a yellow wood,
And sorry I could not travel both

It is Sunday afternoon. The sun is actually shining and I am about to finish this thesis. I start to think back and remember all the people who have had an impact on the work presented within these pages. During my years in Oxford I have talked and met with many people both here and elsewhere, all of whom have inspired and helped me in different ways, both mathematically and otherwise. I intend to mention quite a few of them here.

First of all, I want to thank Dan Segal for being my supervisor and for his insight, encouragement and support! Also, I thank Arnfinn Laudal for introducing me to these methods, and for all his help.

When I applied to Oxford I had no idea of what college to choose, but Wadham seems to have been a very good choice, the staff and students being extremely friendly and helpful. I thank Wadham for providing me with a home away from home and for awarding me a Senior Scholarship.

I wouldn't have been able to come to Oxford without any money, and so I would like to acknowledge the support of the European Commission under a TMR Marie Curie Research Training Grant, contract no. ERBFM-BICT972701.

The staff at the Mathematical Institute has also been very helpful, in particular Keith Gillow, Cathy Hunt, Val Timms, Christine Webb and Brenda Willoughby. I thank Jill Drake especially for her support and help with money-issues. I also thank the academic staff for lots of interesting lectures and seminars and many inspiring conversations.

Thanks to Michael Vaughan-Lee for his interest in the cohomological presentations of p-groups. In particular, I thank him for the presentation (2.24) in example 2.31. As for the work on metacyclic p-groups, this was started off after Martin Bridson pointed out that a group that appeared in my calculations was metacyclic and Dave Benson gave me a reference to cohomological works on these groups. So I thank them for their input and also my thanks to Roger Heath-Brown for his input on the number theory formula that appears in the calculations on metacyclic p-groups (theorem 5.20).

There are many more people to thank, and I must mention Dave Benson again for very valuable discussions and clarifications, also Avinoam Mann and Mike Newman for all their e-mails, especially on the Golod-Shafarevich inequality, Peter Neumann for organising the Kinderseminar and for all his advice, in particular on the art of giving talks, Bob Sandling for sending me his and others' recent work on the modular isomorphism problem, Graeme Segal for his interest and input, and Thomas Weigel for spending several hours discussing Massey products.

Thanks to all those who have taken an interest in my work, which is always very motivating and appreciated. In particular I thank Persi Diaconis, Karin Erdmann, George Glauberman, Peter Kropholler and Ian Leary.

Thanks to Danny Groves, Radha Kessar, Benjamin Klopsch, Dan Quillen, John Rognes, Will Turner, Al Weiss and everyone else who have filled in that little detail and have added to my understanding.

A big thank you to all my fellow students for giving so many interesting talks (and for listening to mine) and for making the studies much more enjoyable. Another thank you goes to Kristoffer Rose and Ross Moore for developing the XY-pic package. All the diagrams in this thesis are made using this package.

Mathematics aside for a moment, I thank my instructors Anita, Cathy, Jane and Maria for counting to 3, 8, 8 and 10 respectively. Without them I wouldn't have had that much energy.

Many thanks also to friends and family for their hospitality, visits and correspondence. Most importantly, I thank my parents David and Lise and my brother Richard for all their advice, love and support.

Two roads diverged in a wood, and I –
I took the one less traveled by,
And that has made all the difference.[1]

---

[1] *From* ROBERT FROST: *"Mountain Interval"(1920), "1. The Road Not Taken"*

Contents

Notation and conventions

$\mathbb{F}_p$	field of p elements, p a prime number
$\mathbb{F}_pG$	modular group algebra
IG	augmentation ideal of $\mathbb{F}_pG$
C_p	cyclic group of order p, written multiplicatively
$\mathbb{Z}/p\mathbb{Z}$	cyclic group of order p, written additively
$\mathcal{D}_i(G)$	modular dimension subgroup series of G, $\mathcal{D}_1(G) = G$
$\mathcal{M}_i(G)$	Jennings series of G, $\mathcal{M}_1(G) = G$
$\Gamma_i(G)$	lower central p-series of G, $\Gamma_0(G) = G$
$(C^\bullet, \partial)$	cocomplex (cochain complex), $\partial^n : C^n \longrightarrow C^{n+1}$
$\ker \partial^n$	n-cocycles
$\operatorname{im} \partial^{n-1}$	n-coboundaries
$\mathrm{H}^*(C^\bullet)$	cohomology of $C^\bullet$, $\mathrm{H}^n(C^\bullet) = \ker \partial^n / \operatorname{im} \partial^{n-1}$
$[x]$	class of x
$\mathrm{H}^*(G, \mathbb{F}_p)$	ordinary mod-p group cohomology of G
$\mathrm{HH}^*(\mathbb{F}_pG, \mathbb{F}_p)$	Hochschild cohomology of $\mathbb{F}_pG$
$\xi_1, \dots, \xi_d$	basis elements for $\mathrm{H}^1(G, \mathbb{F}_p)$
$\eta_1, \dots, \eta_t$	basis elements for $\mathrm{H}^2(G, \mathbb{F}_p)$
T^1	free pro-p group on a dual basis of $\mathrm{H}^1(G, \mathbb{F}_p)$
T^2	free pro-p group on a dual basis of $\mathrm{H}^2(G, \mathbb{F}_p)$
$\langle -, -; 0 \rangle$	Yoneda composition; cup product; 2-fold Massey product
$\langle -; n \rangle$	nth Bockstein operation; p^n-fold restricted Massey product
$\langle \underbrace{-, \dots, -}_{n}; 0 \rangle$	n-fold Massey product
$\{\}$	brackets used for a group presentation
$[a, b]$	denotes $a^{-1}b^{-1}ab$
$[-, \dots, -]$	left-normed commutators, i.e. $[[\cdots[-,-],-,\dots,-],-]$
$\alpha \circ \beta; \alpha\beta$	composition of maps; β first and α first respectively. We will also use $\circ$ for the Alexander-Whitney map.
□	ends a *Proof*
■	ends an **Example** or a **Remark**

Chapter 1

Introduction

Anyone working in the theory of finite p-groups has come to realise that these groups are very complex and difficult. For example writing down presentations is quite a mess. Will we be able to classify finite p-groups?

In this thesis we take a representation theorist's point of view: Let G be a finite p-group and F a field of characteristic p. By studying G's representations over F, what can we say about G? We quote what Jon F. Carlson says in his preface to [9]: "In this situation, all group characters are trivial, the Grothendieck group is trivial and many of the classical techniques of representation theory have no relevance. The only method left open to us is homological algebra."

A lot of work in the theory of finite p-groups has involved the use of homological algebra. However, it seems to the author that there is a lot of material here which is still to be investigated. This thesis is a contribution to this investigation.

For a finite p-group G, the only irreducible representation in characteristic p is the trivial representation $\mathbb{F}_p$, and so to study G using homological algebra we will be using ordinary group cohomology of G with values in $\mathbb{F}_p$, $\mathrm{H}^n(G, \mathbb{F}_p)$ for $n \geq 0$.

The useful thing (and maybe also the confusing thing) about the low-dimensional ($n = 1, 2$) cohomology groups is the fact that there are many different interpretations of these groups. For example, many of the articles one finds on the topic of homological algebra in finite group theory use the fact that the second cohomology group classifies the set of group extensions of G by a G-module.

In **Chapter 2 Cohomology of p-groups** we give an introduction to the mod-p cohomology of p-groups, in particular we will have a closer look at several of the interpretations of $\mathrm{H}^1(G,\mathbb{F}_p)$ and $\mathrm{H}^2(G,\mathbb{F}_p)$. The author acknowledges all the questions that came up during the organising of the Junior Group Theory Seminar on homological algebra. This chapter should hopefully clarify and answer some of them.

The groups $\mathrm{H}^1(G,\mathbb{F}_p)$ and $\mathrm{H}^2(G,\mathbb{F}_p)$ turn out to be the cohomology groups we are interested in. The reason is given by **Theorem 2.30**, telling us that if we let G be a finite p-group, $d(G)$ the minimal number of generators for G and $r(G)$ the minimal number of relations between these generators in the corresponding free pro-p group, then

$$\begin{aligned} d(G) &= \dim_{\mathbb{F}_p} \mathrm{H}^1(G,\mathbb{F}_p); \\ r(G) &= \dim_{\mathbb{F}_p} \mathrm{H}^2(G,\mathbb{F}_p). \end{aligned}$$

We will make extensive use of the theory introduced in chapter 2, for example

- the (as we have discovered) not so well-known result that group cohomology for G and Hochschild cohomology for $\mathbb{F}_pG$ are the same over the trivial module (**Theorem 2.13**);
- the Yoneda cocomplex. The author was introduced to this by A. Laudal as a student in Oslo, and since we will need this cocomplex and haven't found much written work on this, we have included some of the work done on this in Oslo (section **2.5 The Yoneda cocomplex**);
- the various interpretations of $\mathrm{H}^1(G,\mathbb{F}_p)$ and $\mathrm{H}^2(G,\mathbb{F}_p)$, in particular subsection **2.7.5 Relations; finite p-groups as pro-p groups**.

The last point relates to a famous open problem, namely "Does there exist a p-group G such that the minimal number of relations defining G as an abstract group is strictly bigger than the minimal number of relations defining G as a pro-p group?" See [43, page 34]. We end the chapter by giving an example illustrating this problem.

The cohomology groups $\mathrm{H}^n(G, \mathbb{F}_p)$ for $n \geq 0$ introduced in chapter 2 are vector spaces over $\mathbb{F}_p$. **Chapter 3 Massey products** deals with the product structure on the graded vector space $\mathrm{H}^*(G, \mathbb{F}_p)$.

To calculate the cohomology groups we need a dual resolution

$$\mathrm{Hom}_{\mathbb{F}_pG}(F_\bullet, \mathbb{F}_p)$$

where $F_\bullet$ is an $\mathbb{F}_pG$-free resolution of $\mathbb{F}_p$. The dual resolution has a product which induces an algebra structure on $\mathrm{H}^*(G, \mathbb{F}_p)$, usually referred to as the cup product. However, we will use the Yoneda composition as our product. We do this because these two products are the same when we work over the trivial module, and the Yoneda composition is more suited for our purposes.

The next thing to observe is that "An algebra which happens to be the homology of a differential algebra will generally have a very rich internal structure" (quote from May, see [31]). A part of this structure is called the Massey product structure, which can be viewed as higher order analogues of the cup product. Our Massey products are defined in terms of defining systems.

A definition of these products was first given by William S. Massey in 1958, see [30], and then followed on by David Kraines, see [22] (the definition of a defining system is due to him). J. Peter May introduced a generalisation of this construction and defined matric Massey products. These provide us with a complete conceptual description of the differentials in the Eilenberg-Moore spectral sequence, see [32, chapter 8]. By reindexing and taking only (1×1)-matrices, we recover the definition of Massey products.

In chapter 3 we give the definitions we will need from this product structure. We explain this structure for $\mathrm{H}^1(G, \mathbb{F}_p)$ and $\mathrm{H}^2(G, \mathbb{F}_p)$ in the case of the Yoneda cocomplex (section **3.3 Massey products in the Yoneda cocomplex**) and also show how the formulas for the Massey products come out by considering extensions of modules. This is really the Yoneda construction of

Massey products for $\mathrm{H}^1(G, \mathbb{F}_p)$ and $\mathrm{H}^2(G, \mathbb{F}_p)$ (section **3.4 Massey products and extensions**). By doing this we study more closely the fact that finite p-groups are built from the trivial module $\mathbb{F}_p$ using a finite number of extensions.

In the last section of chapter 3, we introduce a mod-p cohomology operation called the Bockstein operation which, for $\mathrm{H}^1(G, \mathbb{F}_p)$ and $\mathrm{H}^2(G, \mathbb{F}_p)$, turns out to be a Massey product too.

In **Chapter 4 Cohomological presentations of p-groups** we build on Laudal's preprint, see [23] and move into a more general context, namely deformation theory. Let us try to explain the bigger picture of our work in chapter 4. The important result is the fact that

- any pro-p group G is the "cokernel" of a morphism

  $$\mathrm{o}_G : \; T^2 \longrightarrow T^1$$

  where T^i is the free pro-p group generated by a dual basis of $\mathrm{H}^i(G, \mathbb{F}_p)$ for $i = 1, 2$. By the "cokernel" of o_G we mean T^1/N where N is the normal closure of $\operatorname{im} \mathrm{o}_G$ in T^1 (as our category is not abelian).

We consider how the morphism o_G is constructed using obstruction theory. Applying a general method from deformation theory for constructing hulls of functors, the idea is then to establish a relationship between the pro-p group G (via o_G) and the Massey product structure on $\mathrm{H}^1(G, \mathbb{F}_p)$ and $\mathrm{H}^2(G, \mathbb{F}_p)$. To establish this in general we will need deformation theoretic definitions of such products. However, we will only use some of this theory in this thesis, and tie it in with the classical theory of Massey products.

The fact that Massey products are differentials in a spectral sequence gives the existence of the products. In the deformation theoretic setting, this fact is replaced by obstruction theory. We will see that the fact that

$$T^1/(T^1)^p[T^1, T^1] \simeq G/G^p[G, G]$$

for p-groups helps us with existence in this case.

Laudal gives a deformation theoretic definition of defining systems for Massey products, which suggests we should call the products we get from these systems something else. We will refer to them as Laudal products (generalised Whitehead products). Whereas Massey products are partially defined functions, the Laudal products are defined on all cohomology classes.

The Massey products live on the dual resolution as a natural construction, and from this construction it is also natural that we will get indeterminacy. This causes problems for us, which we will point out when they appear. This also means that when we start applying this theory, we need to make certain restrictions, which will be discussed further in chapter 4.

The definition of Laudal products gets rid of the indeterminacy, but we can't apply Kraines' result (**Theorem 4.2**) on the correspondence between defining systems for Massey products and certain group homomorphisms, and the fact that the Massey products are obstructions for lifting these homomorphisms.

Another problem is to find coherent defining systems for the Laudal products, as they come from inductive systems. However, if we start with a p-group G, we can choose our defining systems *using* G, and via the Laudal products get out a group H which is Morita equivalent to G. We note that since all simple representations for $\mathbb{F}_p G$ are 1-dimensional, Morita equivalence means $\mathbb{F}_p G \simeq \mathbb{F}_p H$, see [2, Theorem 2.2.6].

As mentioned earlier, we will only use some of this theory, and we have chosen to concentrate on the classical definition of strictly defined Massey products from chapter 3. Combining the mentioned result of Kraines' with Laudal's theory we get a correspondence between certain group relations and these Massey products.

This is done in **Theorems 4.5 and 4.6**, which are the main results in the theoretical part of this thesis. The rest of the thesis (from section 4.3 onwards) is based on these results. These theorems also give a good illustration of the general fact that cohomology classes are obstructions for carrying out certain constructions. After all, homological algebra is there because things aren't as nice as we would like them to be.

We then go on to put the theory into work and consider cohomological presentations of p-groups. We will not make a proper definition of this, but when we say "a group-theoretic presentation" of G, we mean that we can easily read off properties like the centre of G, the commutator subgroup of G, etc. Whereas by "a cohomological presentation" we shall mean that the relations are given by cohomological invariants, like the Massey products, using the correspondence from section **4.2 Strictly defined Massey products and group relations**.

Finding a "new" presentation for a group can sometimes be very useful, as it might tell you something new about the group. For example, many people are interested in 0-deficiency presentations of a group G (number of generators = number of relations), as this is related to the Schur multiplier $\mathrm{H}_2(G, \mathbb{Z})$.

We asked the group-pub-forum@maths.bath.ac.uk the following: "Let G be a finite p-group. Is it true that the deficiency of G is zero iff the Schur multiplier is trivial?" As we will see in chapter 5, it is true for metacyclic groups by Wamsley, see [45]. However, in general it is still an open problem. Trivial Schur multiplier implies that the relation module can be generated by as many elements as there are generators (again by Wamsley), but one might still need more relations to present the group.

Our methods provide us with minimal pro-p presentations and will often have fewer relations than the group-theoretic presentations. Hence, this way we might find 0-deficiency presentations more easily (as in **Example 2.31**).

In fact, the presentations we get will be part of a power-commutator-presentation (PCP), with redundant relations omitted. Now, a PCP is usually what people use when working with finite p-groups. We can get a PCP from our presentation using the p-quotient algorithm in Magma, which uses the lower central p-series. In addition to providing cohomological information, our presentations could also be useful for storage purposes since they are minimal.

Minimal pro-p presentations are also interesting in connection with other problems, for example problems related to the Golod-Shafarevich inequality. We will see an example of this fact along with other examples illustrating what the methods can do in section **4.3 Some examples**.

In section **4.4 A procedure and a tree construction**, we look at a procedure for writing down strictly defined Massey products. In particular we consider a tree construction which helps us to keep track of this procedure and the groups which it produces.

One of the families of p-groups that come out of the tree construction is a family of certain metacyclic p-groups. As we felt we needed to do some heavy calculations to give ourselves and others a better feeling for the Massey products, we decided to study metacyclic p-groups more closely. This is done in **Chapter 5 Metacyclic p-groups**.

Quite a lot of work has been done on metacyclic p-groups by others, but we prove several results and organise the groups into families from our approach's point of view. For example **Theorem 5.11** gives a different 0-deficiency presentation for some of the families. **Theorems 5.23 and 5.24** conclude the cohomolgical calculations on metacyclic p-groups using the Yoneda cocomplex. We admit that we were quite exhausted by the time we finally spotted the pattern of 1-s, 2-s, 3-s etc.

As we have worked on this approach, several interesting problems have emerged as possible roads to take. Once we realised that the Massey products are determined by $\mathbb{F}_pG$, we chose to concentrate on the problem whether (the isomorphism class of) a finite p-group G is determined by $\mathbb{F}_pG$. This has become known as the modular isomorphism problem.

The problem arose in the 1950-s as a natural follow-up to the question posed by Graham Higman in 1940, namely "Does the integral group ring $\mathbb{Z}G$ determine the finite group G?" For a finite p-group G it was shown by Roggenkamp and Scott, see [39], that $\mathbb{Z}G$ determines G. However, it is not true in general, as a counterexample has been provided by Martin Hertweck, see [17].

In 1963, Richard Brauer asked the following question, see [6]: "If two groups G_1 and G_2 have isomorphic group algebras over every ground field Ω, are G_1 and G_2 isomorphic?" Everett Dade gave a counterexample where the groups have order p^3q^6 where p and q are primes such that $q \equiv 1 \pmod{p^2}$, see [11]. So what happens for p-groups? If $\operatorname{char}\Omega \neq p$, there are lots of p-groups G with the same group algebra ΩG, see [37, page 658]. This leaves us with the modular isomorphism problem (which to us means $\Omega = \mathbb{F}_p$), which is still open.

In **Chapter 6 The modular isomorphism problem** we have a look at the history of this problem, where quite a lot of results have been obtained, some very deep. Using our theory we exhibit a new class of groups (**Definition 6.20**) which can be distinguished using $\mathbb{F}_pG$. I.e. we see how far we get with this problem using strictly defined Massey products.

By only using strictly defined Massey products, we have limited ourselves to concentrating on a part of the product structure on $\mathrm{H}^1(G,\mathbb{F}_p)$ and $\mathrm{H}^2(G,\mathbb{F}_p)$ and to calculating a part of the morphism o_G. Even then we encounter various problems, which we consider in section **4.5 Indeterminacy- and well-definedness-considerations**. We will see to what extent we can control these problems and, via some observations we have made, suggest how to overcome them in general.

One suggestion on how to solve the modular isomorphism problem would be to consider the whole product structure on $\mathrm{H}^1(G,\mathbb{F}_p)$ and $\mathrm{H}^2(G,\mathbb{F}_p)$. We would need to find a way to define the products such that we still have control of the various problems occurring, we are able to calculate o_G in general and we don't use the group G.

We end this introduction with an obvious sin of omission, as we have not considered what happens for arbitrary fields of characteristic p in this theory. We can at least point out that the interpretation (3.3.8) of the Bockstein operation as a Massey product uses that we work over $\mathbb{F}_p$.

Chapter 2

Cohomology of p-groups

In this thesis, G will always denote a finite p-group. We begin by giving some basic definitions from homological algebra and defining the groups $\mathrm{H}^n(G, \mathbb{F}_p)$, the mod-$p$ group cohomology of G.

There are many ways of defining these groups, and we will make good use of this fact. We give four definitions here and briefly explain why they are all the same. We then go on to consider what these definitions give us for $\mathrm{H}^1(G, \mathbb{F}_p)$ and $\mathrm{H}^2(G, \mathbb{F}_p)$. Most of the results in this chapter are well-known, and so the reader will be referred to existing literature for the proofs of many of them. We will however include parts of the proof or the whole proof where we have found it appropriate, for example when we haven't found a good proof in the literature or when we want to emphasise an argument.

2.1 Homological algebra

Definition 2.1 *Let R be a ring with 1. A cochain complex $(C^\bullet, \partial)$ over R, or a cocomplex for short, is a family $\{C^n\}_{n\in\mathbb{Z}}$ of R-modules and a family of R-module homomorphisms $\{\, \partial^n : C^n \longrightarrow C^{n+1} \,\}_{n\in\mathbb{Z}}$ such that $\partial^{n+1} \circ \partial^n = 0$ for all $n \in \mathbb{Z}$.*

$$C^\bullet : \; \cdots \longrightarrow C^{n-1} \xrightarrow{\partial^{n-1}} C^n \xrightarrow{\partial^n} C^{n+1} \longrightarrow \cdots$$

Elements in C^n are called n-cochains. Elements in $\ker \partial^n$ are called n-cocycles and elements in $\operatorname{im} \partial^{n-1}$ are called n-coboundaries. The R-module

$$\mathrm{H}^n(C^\bullet) = \ker \partial^n / \operatorname{im} \partial^{n-1}, \quad n \in \mathbb{Z}$$

is called the nth cohomology group of $C^\bullet$. $\mathrm{H}^*(C^\bullet)$ is referred to as the cohomology of $C^\bullet$.

We can similarly define a (chain) complex by introducing subscripts, reversing the arrows and renaming the differentials so that we get $\partial_n : C_n \longrightarrow C_{n-1}$ and the nth homology group of $C_\bullet$ is

$$\mathrm{H}_n(C_\bullet) = \ker \partial_n / \operatorname{im} \partial_{n+1}.$$

We want to study p-groups G using the trivial module $\mathbb{F}_p$ and homological algebra. To do this we need to introduce the modular group algebra $\mathbb{F}_pG$ consisting of elements $\sum_{g\in G} \alpha_g g$, $\alpha_g \in \mathbb{F}_p$, where the multiplication is induced by multiplication in G and addition is defined by collecting coefficients. We will study $\mathbb{F}_pG$ more closely in section 6.1.

Definition 2.2 *An $\mathbb{F}_pG$-free resolution of $\mathbb{F}_p$ is a complex $C_\bullet$ with*

$$C_i = \begin{cases} 0 & \text{for } i < 0 \\ \text{free } \mathbb{F}_pG\text{-module} & \text{for } i \geq 0 \end{cases}$$

and

$$\mathrm{H}_i(C_\bullet) = \begin{cases} \mathbb{F}_p & \text{for } i = 0 \\ 0 & \text{for } i \geq 1. \end{cases}$$

We will need the notions of a morphism between cocomplexes and a homotopy between such morphisms.

Definition 2.3 *Let $(C^\bullet, \partial)$ and $(D^\bullet, \delta)$ be cocomplexes. A morphism ϕ between $C^\bullet$ and $D^\bullet$ is a family $\{ \phi^n : C^n \longrightarrow D^n \}_{n\in\mathbb{Z}}$ of homomorphisms such that ϕ commutes with the differentials, i.e.*

$$\delta^n \circ \phi^n = \phi^{n+1} \circ \partial^n \quad \forall n \in \mathbb{Z}. \tag{2.1}$$

Remark 2.4 By (2.1) we see that ϕ takes cocycles to cocycles and coboundaries to coboundaries, so $\phi : C^\bullet \longrightarrow D^\bullet$ induces a morphism

$$\phi^* : \mathrm{H}^n(C^\bullet) \longrightarrow \mathrm{H}^n(D^\bullet)$$

for all $n \in \mathbb{Z}$. ■

Definition 2.5 *Let ϕ and ψ be morphisms between $C^\bullet$ and $D^\bullet$. A homotopy σ between ϕ and ψ is a family $\{ \sigma^n : C^{n+1} \longrightarrow D^n \}_{n\in\mathbb{Z}}$ such that*

$$\psi^n - \phi^n = \delta^{n-1} \circ \sigma^n + \sigma^{n+1} \circ \partial^n \quad \forall n \in \mathbb{Z}. \tag{2.2}$$

The diagram is

$$\begin{tikzcd}
C^\bullet : & \cdots \arrow[r] & C^{n-1} \arrow[r, "\partial^{n-1}"] \arrow[d, shift right] \arrow[d, shift left] & C^n \arrow[r, "\partial^n"] \arrow[dl, dashed, "\sigma^n"'] \arrow[d, shift right, "\psi^n"'] \arrow[d, shift left, "\phi^n"] & C^{n+1} \arrow[r] \arrow[dl, dashed, "\sigma^{n+1}"'] \arrow[d, shift right] \arrow[d, shift left] & \cdots \\
D^\bullet : & \cdots \arrow[r] & D^{n-1} \arrow[r, "\delta^{n-1}"'] & D^n \arrow[r, "\delta^n"'] & D^{n+1} \arrow[r] & \cdots
\end{tikzcd}$$

We say that $C^\bullet$ and $D^\bullet$ are of the same homotopy type if there exists morphisms $\phi : C^\bullet \longrightarrow D^\bullet$ and $\theta : D^\bullet \longrightarrow C^\bullet$ such that we have a homotopy between $\theta \circ \phi$ and $\mathbf{1}_{C^\bullet}$ and a homotopy between $\phi \circ \theta$ and $\mathbf{1}_{D^\bullet}$.

Recall that $\phi : C^\bullet \longrightarrow D^\bullet$ induces a morphism ϕ^* between the cohomology of $C^\bullet$ and $D^\bullet$, remark 2.4.

Lemma 2.6 *If we have a homotopy between ϕ and ψ, then $\phi^* = \psi^*$.*

Proof: Let $c \in \ker \partial^n$. By (2.2), $\psi^n(c) - \phi^n(c) \in \operatorname{im} \delta^{n-1}$, which is what we want. □

Corollary 2.7 *If $C^\bullet$ and $D^\bullet$ are of the same homotopy type then*

$$\mathrm{H}^n(C^\bullet) \simeq \mathrm{H}^n(D^\bullet) \forall n \in \mathbb{Z}.$$

for all $n \in \mathbb{Z}$. □

These results lead to the following important theorem.

Theorem 2.8 *Any two $\mathbb{F}_pG$-free resolutions of $\mathbb{F}_p$ are of the same homotopy type.*

Proof: This follows from the Comparison Theorem, see [2, page 28]. □

2.2 Mod-p group cohomology; a first definition

We now define mod-p group cohomology of G with values in $\mathbb{F}_p$, $\mathrm{H}^n(G, \mathbb{F}_p)$ for $n \geq 0$. In order to calculate these cohomology groups, we take an $\mathbb{F}_pG$-free resolution $F_\bullet$ of $\mathbb{F}_p$ and apply $\mathrm{Hom}_{\mathbb{F}_pG}(-, \mathbb{F}_p)$ to obtain a cocomplex $(\mathrm{Hom}_{\mathbb{F}_pG}(F_\bullet, \mathbb{F}_p), \delta)$.

We will refer to this cocomplex as the dual resolution (even though it is not itself a resolution). The functor $\mathrm{Hom}_{\mathbb{F}_pG}(-, \mathbb{F}_p)$ does not preserve surjective maps, and will therefore have right-derived functors. The cohomology group $\mathrm{H}^n(G, \mathbb{F}_p)$ is defined as the n-th cohomology group of the dual resolution, i.e. we have the following definition.

Definition 2.9 *We define*

$$\mathrm{H}^n(G, \mathbb{F}_p) = \mathrm{Ext}^n_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p), \tag{2.3}$$

where $\mathrm{Ext}^n_{\mathbb{F}_pG}(-, \mathbb{F}_p)$ is the n-th right-derived functor of $\mathrm{Hom}_{\mathbb{F}_pG}(-, \mathbb{F}_p)$.

Since $\mathrm{Hom}_{\mathbb{F}_pG}((\mathbb{F}_pG)^i, \mathbb{F}_p) \simeq (\mathbb{F}_p)^i$, the mod-$p$ cohomology groups are vector spaces over $\mathbb{F}_p$. An explicit example of a resolution and how to calculate the first two cohomology groups is given in section 5.6.

Lemma 2.10 *The cohomology groups $\mathrm{H}^n(G, \mathbb{F}_p)$, $n \geq 0$, are independent of the choice of resolution of $\mathbb{F}_p$.*

Proof: By theorem 2.8, two resolutions $F_\bullet$ and $F'_\bullet$ of $\mathbb{F}_p$ are of the same homotopy type. Since $\mathrm{Hom}_{\mathbb{F}_pG}(-, \mathbb{F}_p)$ is an additive functor, the cocomplexes

$\mathrm{Hom}_{\mathbb{F}_pG}(F_\bullet, \mathbb{F}_p)$ and $\mathrm{Hom}_{\mathbb{F}_pG}(F'_\bullet, \mathbb{F}_p)$ are also of the same homotopy type, and hence the cohomology groups are independent of the choice of resolution since homotopy equivalent cocomplexes have the same cohomology, by corollary 2.7. □

2.3 Hochschild cohomology; a second definition

As an associative $\mathbb{F}_p$-algebra, $\mathbb{F}_pG$ will also have a cohomology theory. This theory was originally defined by Hochschild, see [19]. We will give the definition here, and refer the reader to the literature for more theory, for example Loday's exposition, see [28].

Definition 2.11 *Let A be an associative k-algebra, k a field, and let Q be an A-bimodule. The Hochschild cocomplex is given by*

$$\begin{tikzcd}
\vdots \arrow[d] \\
C^n(A,Q) = \mathrm{Hom}_k(\underbrace{A \otimes \cdots \otimes A}_{n}, Q) \arrow[d, "\delta^n"'] \\
C^{n+1}(A,Q) = \mathrm{Hom}_k(\underbrace{A \otimes \cdots \otimes A}_{n+1}, Q) \arrow[d] \\
\vdots
\end{tikzcd}$$

where the differential is given by the formula

$$\begin{aligned}
&\delta^n\phi(a_1 \otimes \cdots \otimes a_{n+1}) \\
=&a_1\phi(a_2 \otimes \cdots \otimes a_{n+1}) + \sum_{i=1}^{n}(-1)^i\phi(a_1 \otimes \cdots \otimes a_ia_{i+1} \otimes \cdots \otimes a_{n+1}) \\
+&(-1)^{n+1}\phi(a_1 \otimes \cdots \otimes a_n)a_{n+1}
\end{aligned}$$

for $\phi \in C^n(A, Q)$*,* $a_1, \dots, a_{n+1} \in A$*. The cohomology groups of this cocomplex are the Hochschild cohomology groups, denoted* $\mathrm{HH}^n(A, Q)$*.*

Lemma 2.12 *Let* k *be a field,* A *a* k*-algebra and let* M, N *be right* A*-modules. Then* $\mathrm{Hom}_k(M, N)$ *has an* A*-bimodule structure.*

Proof: Let $\gamma \in \mathrm{Hom}_k(M, N)$, $a \in A$ and $m \in M$. Then $\mathrm{Hom}_k(M, N)$ is a left A-module by $(a\gamma)(m) = \gamma(ma)$, and a right A-module by $(\gamma a)(m) = \gamma(m)a$. □

In our situation, $k = \mathbb{F}_p$, $A = \mathbb{F}_p G$ and $M = N = \mathbb{F}_p$. The group algebra is an augmented algebra via the augmentation map

$$\begin{array}{rcl} \epsilon : \mathbb{F}_p G & \longrightarrow & \mathbb{F}_p \\ \\ \sum_{g \in G} \alpha_g g & \longmapsto & \sum_{g \in G} \alpha_g, \end{array} \tag{2.4}$$

and as such it has yet another cohomology theory defined in terms of Ext-groups. This fact helps us prove the following theorem.

Theorem 2.13 $\mathrm{H}^n(G, \mathbb{F}_p) \simeq \mathrm{HH}^n(\mathbb{F}_p G, \mathbb{F}_p)$ *for* $n \geq 0$*.*

Proof: This follows since $\mathbb{F}_p G$ is an augmented algebra and we work over the trivial module. For details, see [2, page 31] and [3, section 2.11].

We also note that an $\mathbb{F}_p$-basis for $\otimes^n \mathbb{F}_p G$ is G^n, and so the Hochschild cocomplex $C^*(\mathbb{F}_p G, \mathbb{F}_p)$ can be recognised as the dual bar resolution, given in definition 2.26, and we can apply lemma 2.10. □

2.4 n-extensions; a third definition

An interpretation of $\mathrm{Ext}^n_A(M, N)$ for A a ring and M, N A-modules has been given by Yoneda, see [18, page 148].

Definition 2.14 *Let* $\mathrm{E}^n_A(M, N)$ *be the set of equivalence classes of* n*-extensions* *of M by N, i.e.*

$$\mathrm{E}^n_A(M,N) = \{0 \to N \to E_1 \to \cdots \to E_n \to M \to 0\}\Big/ \sim$$

where $E_1, \dots, E_n$ are A-modules, the sequence is exact and $\sim$ is defined as follows: Let η and η' be two n-extensions.

$n = 1$: *We say $\eta \sim \eta'$ if there exists ϕ such that the following diagram is commutative.*

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] \arrow[d, equal] & E \arrow[r] \arrow[d, "\phi"] & M \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & N \arrow[r] & E' \arrow[r] & M \arrow[r] & 0
\end{tikzcd} \tag{2.5}$$

$n \geq 2$: *We say $\eta \sim \eta'$ if there exists a chain of n-extensions $\eta = \eta_0, \eta_1, \dots$ $\dots, \eta_k = \eta'$ such that we have a commutative diagram*

$$\begin{tikzcd}
\eta : & 0 \arrow[r] & N \arrow[r] \arrow[d, equal] & E_1 \arrow[r] \arrow[d] & \cdots \arrow[r] & E_n \arrow[r] \arrow[d] & M \arrow[r] \arrow[d, equal] & 0 \\
\eta_1 : & 0 \arrow[r] & N \arrow[r] \arrow[d, equal] & E_1^1 \arrow[r] & \cdots \arrow[r] & E_n^1 \arrow[r] & M \arrow[r] \arrow[d, equal] & 0 \\
\eta_2 : & 0 \arrow[r] & N \arrow[r] \arrow[d, equal] & E_1^2 \arrow[r] \arrow[u] \arrow[d] & \cdots \arrow[r] & E_n^2 \arrow[r] \arrow[u] \arrow[d] & M \arrow[r] \arrow[d, equal] & 0 \\
& & \vdots \arrow[d, equal] & \vdots \arrow[d, shift left, "or"] & & \vdots \arrow[d, shift left, "or"] & \vdots \arrow[d, equal] & \\
\eta' : & 0 \arrow[r] & N \arrow[r] & E_1' \arrow[r] \arrow[u, shift left] & \cdots \arrow[r] & E_n' \arrow[r] \arrow[u, shift left] & M \arrow[r] & 0.
\end{tikzcd} \tag{2.6}$$

We have the following result giving us yet another definition of our cohomology groups, which is a corollary of theorem 9.1. in [18] (natural equivalence of functors).

Theorem 2.15 *We have an isomorphism*

$$\mathrm{Ext}^n_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p) \simeq \mathrm{E}^n_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p).$$

Proof: To calculate $\mathrm{Ext}^n_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$ we only need a resolution $F_\bullet$ of length n (see first part of theorem 2.24). If we are given an n-extension of $\mathbb{F}_p$ by $\mathbb{F}_p$, we use the Comparison Theorem to get a chain map between these resolutions, which will provide us with an element in $\mathrm{Ext}^n_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$. Conversely, from a resolution of length n we form a push-out diagram to get an n-extension. For details, see [18, page 150]. □

2.5 The Yoneda cocomplex; a fourth definition

In this section we will introduce the Yoneda cocomplex $\mathrm{Hom}^{(\bullet)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet)$, which contains a lot of information about the $\mathbb{F}_pG$-modules. The cohomology of this cocomplex also turns out to be the group cohomology of G.

Note that we will use the following notation for composing maps: If we write $\phi \circ \psi$, we mean "use ψ first". If we write $\phi\psi$, we mean "use ϕ first".

We start with an $\mathbb{F}_pG$-free resolution of $\mathbb{F}_p$, $F_\bullet \twoheadrightarrow \mathbb{F}_p$.

Definition 2.16 *We define the Yoneda cocomplex* $\mathrm{Hom}^{(\bullet)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet)$ *by*

$$\mathrm{Hom}^{(i)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet) = \prod_{n\in\mathbb{Z}} \mathrm{Hom}_{\mathbb{F}_pG}(F_n, F_{n-i}), \quad i \geq 0,$$

and 0 otherwise, i.e. an element ϕ^i in the i-th component of $\mathrm{Hom}^{(\bullet)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet)$ *for $i \geq 0$ is a family of maps $\{\phi^i_j\}_{j\in\mathbb{Z}}$ in the following ladder diagram.*

$$\begin{tikzcd}
\cdots \arrow[r, "\delta_{n+1}"] & F_{n+1} \arrow[r, "\delta_n"] \arrow[d, "\phi^i_{n+1}"] & F_n \arrow[r, "\delta_{n-1}"] \arrow[d, "\phi^i_n"] & F_{n-1} \arrow[r, "\delta_{n-2}"] \arrow[d, "\phi^i_{n-1}"] & \cdots \\
\cdots \arrow[r, "\delta_{n-i+1}"] & F_{n-i+1} \arrow[r, "\delta_{n-i}"] & F_{n-i} \arrow[r, "\delta_{n-i-1}"] & F_{n-i-1} \arrow[r, "\delta_{n-i-2}"] & \cdots
\end{tikzcd}$$

The differential in $\mathrm{Hom}^{(\bullet)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet)$

$$\begin{tikzcd}
\vdots \arrow[d] & \\
\prod_{n\in\mathbb{Z}} \mathrm{Hom}_{\mathbb{F}_pG}(F_n, F_{n-i}) \arrow[d, "\partial^i"] & \phi^i \arrow[d, mapsto] \\
\prod_{n\in\mathbb{Z}} \mathrm{Hom}_{\mathbb{F}_pG}(F_n, F_{n-i-1}) \arrow[d, "\partial^{i+1}"] & \partial^i(\phi^i) \arrow[d, mapsto] \\
\prod_{n\in\mathbb{Z}} \mathrm{Hom}_{\mathbb{F}_pG}(F_n, F_{n-i-2}) \arrow[d] & \partial^{i+1}(\partial^i(\phi^i)) \\
\vdots &
\end{tikzcd}$$

is defined by the formula

$$\boxed{\partial^i(\phi^i_n) = \delta_{n-1}\phi^i_{n-1} - (-1)^i\phi^i_n\delta_{n-i-1},} \tag{2.7}$$

with the diagram

$$\begin{tikzcd}
\cdots \arrow[r] & F_n \arrow[rr, "\delta_{n-1}"] \arrow[dr, "\phi^i_n"'] \arrow[drrr, dashed, "\partial^i(\phi^i_n)"] & & F_{n-1} \arrow[r] \arrow[dr, "\phi^i_{n-1}"] & \cdots & \\
& \cdots \arrow[r] & F_{n-i} \arrow[rr, "\delta_{n-i-1}"'] & & F_{n-i-1} \arrow[r] & \cdots
\end{tikzcd}$$

We check that this gives us a cocomplex:

Lemma 2.17 *$\partial^{i+1} \circ \partial^i = 0$ for $i \geq 0$.*

Proof: Consider

$$\begin{tikzcd}
\cdots \arrow[r] & F_n \arrow[r, "\delta_{n-1}"] \arrow[d, dashed] \arrow[dr, "\partial^i(\phi^i_n)"'] \arrow[drr, "\partial^{i+1}(\partial^i(\phi^i_n))"] & F_{n-1} \arrow[r, "\delta_{n-2}"] \arrow[d, dashed] & F_{n-2} \arrow[r] \arrow[d, dashed] & \cdots \\
\cdots \arrow[r] & F_{n-i} \arrow[r, "\delta_{n-i-1}"'] & F_{n-i-1} \arrow[r, "\delta_{n-i-2}"'] & F_{n-i-2} \arrow[r] & \cdots
\end{tikzcd}$$

where the broken arrows are the components of ϕ^i. We calculate that

$$\begin{aligned}
&(\partial^{i+1} \circ \partial^i)(\phi^i_n) \\
=&\partial^{i+1}(\delta_{n-1}\phi^i_{n-1} - (-1)^i(\phi^i_n\delta_{n-i-1})) \\
=&\delta_{n-1}(\delta_{n-2}\phi^i_{n-2} - (-1)^i\phi^i_{n-1}\delta_{n-i-2}) \\
&\quad - (-1)^{i+1}(\delta_{n-1}\phi^i_{n-1} - (-1)^i(\phi^i_n\delta_{n-i-1}))\delta_{n-(i+1)-1} \\
=&(\underbrace{\delta_{n-1}\delta_{n-2}}_{=0}\phi^i_{n-2} - (-1)^i(\delta_{n-1}\phi^i_{n-1}\delta_{n-i-2})) \\
&\quad - (-1)^{i+1}(\delta_{n-1}\phi^i_{n-1}\delta_{n-i-2} + \phi^i_n\underbrace{\delta_{n-i-1}\delta_{n-i-2})}_{=0} \\
=&0.
\end{aligned}$$

□

The cohomology of this cocomplex will be referred to as Yoneda cohomology of $\mathbb{F}_pG$. The next result combined with definition 2.9 tells us that Yoneda cohomology for $\mathbb{F}_pG$ is the same as group cohomology for G.

Theorem 2.18 *$\mathrm{H}^i(\mathrm{Hom}^{(\bullet)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet), \partial^\bullet) \simeq \mathrm{Ext}^i_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$ for all $i \geq 0$.*

Proof: We need to show that

$$\mathrm{H}^i(\mathrm{Hom}^{(\bullet)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet), \partial) \simeq \mathrm{H}^i(\mathrm{Hom}_{\mathbb{F}_pG}(F_\bullet, \mathbb{F}_p), \delta).$$

Let $\phi \in \mathrm{Hom}^{(\bullet)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet)$. Then in particular we have the maps

$\{\, F_i \xrightarrow{\phi^i_i} F_0 \,\}_{i\geq 0}$, and also $F_0 \overset{\rho}{\twoheadrightarrow} \mathbb{F}_p$. Composing these gives us a map

$$\begin{tikzcd}
\mathrm{Hom}^{(\bullet)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet) \arrow[d, "\Phi"] & \phi \arrow[d, mapsto] \\
\mathrm{Hom}_{\mathbb{F}_pG}(F_\bullet, \mathbb{F}_p) & \{\phi^i_i\rho\}_{i\geq 0}.
\end{tikzcd} \tag{2.8}$$

We must show that Φ induces an isomorphism on the level of cohomology. For this we need to know what a cocycle in $\mathrm{Hom}^{(i)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet)$ is.

Take $\phi^i \in \mathrm{Hom}^{(i)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet)$ such that $\partial^i\phi^i = 0$, and consider the diagram

$$\begin{tikzcd}
\cdots \arrow[r, "\delta_{n+1}"] & F_{n+1} \arrow[r, "\delta_n"] \arrow[d, "\phi^i_{n+1}"] \arrow[dr, dashed, "0"] & F_n \arrow[r, "\delta_{n-1}"] \arrow[d, "\phi^i_n"] \arrow[dr, dashed, "0"] & F_{n-1} \arrow[r, "\delta_{n-2}"] \arrow[d, "\phi^i_{n-1}"] & \cdots \\
\cdots \arrow[r, "\delta_{n-i+1}"] & F_{n-i+1} \arrow[r, "\delta_{n-i}"] & F_{n-i} \arrow[r, "\delta_{n-i-1}"] & F_{n-i-1} \arrow[r, "\delta_{n-i-2}"] & \cdots
\end{tikzcd}$$

Hence we get commutative or anticommutative diagrams, depending on what i is. Now, Φ sends ϕ^i to $\phi^i_i\rho$ in $\mathrm{Hom}_{\mathbb{F}_pG}(F_i, \mathbb{F}_p)$, so we need to show that $\phi^i_i\rho$ is a cocycle. Consider $\mathrm{Hom}_{\mathbb{F}_pG}(F_\bullet, \mathbb{F}_p)$:

$$\begin{tikzcd}
\cdots & \mathrm{Hom}_{\mathbb{F}_pG}(F_{i+1}, \mathbb{F}_p) \arrow[l] & \mathrm{Hom}_{\mathbb{F}_pG}(F_i, \mathbb{F}_p) \arrow[l, "\delta^i"'] & \mathrm{Hom}_{\mathbb{F}_pG}(F_{i-1}, \mathbb{F}_p) \arrow[l, "\delta^{i-1}"'] & \cdots \arrow[l]
\end{tikzcd}$$

Then $\delta^i(\phi^i_i\rho) = \delta_i\phi^i_i\rho$ is the broken arrow in the following diagram.

$$\begin{tikzcd}
\cdots \arrow[r, "\delta_{i+1}"] & F_{i+1} \arrow[r, "\delta_i"] \arrow[r, dashed, shift right] \arrow[drr, "\phi^i_{i+1}"] & F_i \arrow[r, "\delta_{i-1}"] \arrow[drr, "\phi^i_i"] \arrow[drrr, dashed] & F_{i-1} \arrow[r] & \cdots & \\
\cdots \arrow[r, "\delta_3"'] & F_3 \arrow[r, "\delta_2"'] & F_2 \arrow[r, "\delta_1"'] & F_1 \arrow[r, "\delta_0"'] & F_0 \arrow[r, two heads, "\rho"'] & \mathbb{F}_p
\end{tikzcd}$$

We see that the broken arrow is the zero-map by exactness, so $\phi^i_i\rho$ is an

i-cocycle, hence we have found a map

$$\mathrm{H}^i(\mathrm{Hom}^{(\bullet)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet)) \xrightarrow{\quad\Phi\quad} \mathrm{H}^i(\mathrm{Hom}_{\mathbb{F}_pG}(F_\bullet, \mathbb{F}_p))$$

$$\ker \partial^i / \operatorname{im} \partial^{i-1} \xrightarrow{\quad\Phi\quad} \ker \delta^i / \operatorname{im} \delta^{i-1},$$

sending the cocycle ϕ^i to $\phi^i_i\rho$ modulo $\operatorname{im}\delta^{i-1}$.

This map is well-defined: Let $\xi, \xi' \in \ker \partial^i$ be two representatives of the same cohomology class. By the definition of ∂ in (2.7), $\xi - \xi'$ can be split into two components. When we apply Φ, one of the components vanish by exactness, and we get that $\Phi(\xi - \xi') \in \operatorname{im}\delta^{i-1}$.

We claim that Φ is surjective and injective:

Φ is surjective Let $\overline{\phi_i} \in \mathrm{Hom}_{\mathbb{F}_pG}(F_i, \mathbb{F}_p)$ such that $\delta^i(\overline{\phi_i}) = \delta_i\overline{\phi_i} = 0$.

$$\begin{tikzcd}
F_{i+1} \arrow[r, "\delta_i"] \arrow[rrd, bend right=50, "0"'] & F_i \arrow[rd, dashed, "\exists\ \phi^i_i"'] \arrow[rrd, "\overline{\phi_i}"] & & \\
& & F_0 \arrow[r, two heads, "\rho"'] & \mathbb{F}_p
\end{tikzcd}$$

The map ϕ^i_i exists such that $\phi^i_i\rho = \overline{\phi_i}$ because F_i is free, hence projective. We claim that ϕ^i_i can be lifted to give us $\phi^i_{i+1} \in \mathrm{Hom}^{(i)}_{\mathbb{F}_pG}(F_{i+1}, F_1)$ with $\partial^i(\phi^i_{i+1}) = 0$:

$$\begin{tikzcd}
F_{i+1} \arrow[rr, "\delta_i"] \arrow[rd, dashed, "\phi^i_{i+1}"'] \arrow[rdd, bend right=50] & & F_i \arrow[d, "\phi^i_i"'] \arrow[rrd] & & \\
& F_1 \arrow[r, "\delta_0"] \arrow[d] & F_0 \arrow[rr, two heads, "\rho"] & & \mathbb{F}_p \\
& \ker\rho \arrow[ru, hook] & & &
\end{tikzcd}$$

The 0-map from the previous diagram gives us a factorisation via $\ker\rho$ which gives the existence of ϕ^i_{i+1} since F_{i+1} is free, hence projective.

Since this is a lifting, we have commutative diagrams, and so $\partial^i(\phi^i_{i+1}) = 0$. This process continues to give us $\phi^i \in \mathrm{H}^i(\mathrm{Hom}^{(i)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet))$.

Φ is injective Let $\phi^i \in \ker \partial^i$ such that $\phi^i_i\rho = 0$, i.e. $\phi^i \in \ker \Phi$. We need to show $\phi^i \in \operatorname{im} \partial^{i-1}$, which again follows from yet another picture.

$$\begin{tikzcd}
\cdots \arrow[r, "\delta_i"] & F_i \arrow[rr, "\delta_{i-1}"] \arrow[dr, dashed, "\exists"'] \arrow[drr, "\phi^i_i"] \arrow[drrr, "0"] \arrow[ddr, bend right] & & \cdots & \\
& & F_1 \arrow[r, "\delta_0"'] \arrow[d] & F_0 \arrow[r, two heads, "\rho"'] & \mathbb{F}_p \\
& & \ker\rho \arrow[ur, hook] & &
\end{tikzcd}$$

☐

The following lemma will be referred to in chapter 3.

Lemma 2.19 $\partial(\phi^i\psi^j) = \partial(\phi^i)\psi^j + (-1)^i\phi^i\partial(\psi^j)$.

Proof: From the picture

$$\begin{tikzcd}
F_n \arrow[rr, "\delta_{n-1}"] \arrow[dr, "\phi^i_n"'] \arrow[drrr, dotted, "\partial^i(\phi^i_n)"] \arrow[ddrrrr, dashed] \arrow[ddrr, bend right, "\phi^i_n\psi^j_{n-i}"'] & & F_{n-1} \arrow[dr, "\phi^i_{n-1}"] & & \\
& F_{n-i} \arrow[rr, "\delta_{n-i-1}"'] \arrow[dr, "\psi^j_{n-i}"'] \arrow[drrr, dotted, "\partial^j(\psi^j_{n-i})"'] & & F_{n-i-1} \arrow[dr, "\psi^j_{n-i-1}"] & \\
& & F_{n-i-j} \arrow[rr, "\delta_{n-i-j-1}"] & & F_{n-i-j-1}
\end{tikzcd}$$

we see that we need to show that

$$\partial^{i+j}(\phi^i_n\psi^j_{n-i}) = \partial^i(\phi^i_n)\psi^j_{n-i-1} + (-1)^i\phi^i_n\partial^j(\psi^j_{n-i}),$$

which is done by using the formula for ∂ in (2.7). ☐

2.6 Interpretations of $\mathrm{H}^{\mathbf{1}}(\mathbf{G}, \mathbb{F}_{\mathbf{p}})$:

2.6.1 Extensions

The group $\mathrm{E}^1_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$ from section 2.4 is the group of equivalence classes of 1-extensions, usually called extensions, which refers both to the short-exact sequence itself and the module in the middle of the sequence. So

$$\mathrm{E}^1_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p) = \{0 \to \mathbb{F}_p \to E \to \mathbb{F}_p \to 0\}/\sim$$

where two sequences

$$0 \longrightarrow \mathbb{F}_p \longrightarrow E \longrightarrow \mathbb{F}_p \longrightarrow 0 \quad \text{and} \quad 0 \longrightarrow \mathbb{F}_p \longrightarrow E' \longrightarrow \mathbb{F}_p \longrightarrow 0$$

are equivalent iff $E \simeq E'$, since $\mathbb{F}_p$ has no automorphisms as an $\mathbb{F}_pG$-module.

From theorem 2.15, $\mathrm{E}^n_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$ will have an abelian group structure. The group operation uses the maps $\Delta_{\mathbb{F}_p} : \mathbb{F}_p \longrightarrow \mathbb{F}_p \oplus \mathbb{F}_p$ where $\Delta_{\mathbb{F}_p}(a) = (-a, a)$ and $\nabla_{\mathbb{F}_p} : \mathbb{F}_p \oplus \mathbb{F}_p \longrightarrow \mathbb{F}_p$ which sends (a_1, a_2) to $a_1 + a_2$. If we have two extensions

$$\xi : \quad 0 \longrightarrow \mathbb{F}_p \xrightarrow{\mu} E \xrightarrow{\epsilon} \mathbb{F}_p \longrightarrow 0\,; \tag{2.9}$$

$$\xi' : \quad 0 \longrightarrow \mathbb{F}_p \xrightarrow{\mu'} E' \xrightarrow{\epsilon'} \mathbb{F}_p \longrightarrow 0\,, \tag{2.10}$$

in $\mathrm{E}^1_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$, then $\xi + \xi'$ will be the extension

$$\xi + \xi' : \quad 0 \longrightarrow \mathbb{F}_p \xrightarrow{\alpha} E'' \xrightarrow{\beta} \mathbb{F}_p \longrightarrow 0 \tag{2.11}$$

where $E'' = \{(e, e') \in E \oplus E' | \epsilon(e) = \epsilon'(e') \text{ and } \mu(1) = \mu'(1)\}$, and where $\alpha = (\mu, \mu') \circ \Delta_{\mathbb{F}_p}$ and $\beta = \nabla_{\mathbb{F}_p} \circ (\epsilon, \epsilon')$.

2.6.2 Derivations

We defined $\mathrm{H}^1(G, \mathbb{F}_p) = \mathrm{Ext}^1_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$, and by theorem 2.15, we can look at elements in $\mathrm{H}^1(G, \mathbb{F}_p)$ as being (isomorphism classes of) extensions of the trivial module $\mathbb{F}_p$ by $\mathbb{F}_p$. Such an extension will in a natural way give us a derivation (a map satisfying Leibniz' rule under the appropriate module-structure), which we will now prove. The method will be generalised when we come to the Yoneda construction for Massey products in the next chapter.

Lemma 2.20 *Let A be a k-algebra with M and N (right) A-modules. An extension of M by N will give us a derivation from A to* $\mathrm{Hom}_k(M,N)$*.*

Proof: We start with an extension

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r, "\mu"] & E \arrow[r, "\epsilon"] & M \arrow[r] \arrow[l, dashed, bend left, "\sigma"] & 0
\end{tikzcd}$$

where σ is k-linear and such that $\epsilon \circ \sigma = id_M$. We use σ to introduce the isomorphism ψ such that the following diagram commutes

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r, "\mu"] \arrow[dr, "\iota"'] & E \arrow[r, "\epsilon"] & M \arrow[r] \arrow[l, dashed, bend left, "\sigma"] & 0 \\
& & N \oplus M \arrow[u, "\simeq", "\psi"'] \arrow[ur, "\pi"'] & &
\end{tikzcd}$$

hence $\psi(n,m) = \mu(n) + \sigma(m)$, for $n \in N, m \in M$. So we think of E as a vector space over k and we want to find an A-module-structure on $N \oplus M$. Let $(n,m)a = (\alpha,\beta)$, where $a \in A$. To find α and β, we use ψ and get

$$\begin{aligned}
& (\mu(n)+\sigma(m))a \\
= \; & \mu(n)a + \sigma(m)a \\
= \; & \mu(na) + \sigma(m)a \\
= \; & \mu(na) + \sigma(ma) - \sigma(ma) + \sigma(m)a
\end{aligned}$$

since μ is an A-module homomorphism, and σ is not. By compensating for the fact that σ is not an A-module homomorphism, we have got a new element $\boxed{\phi(a)(m) = -\sigma(ma) + \sigma(m)a}$. We see that $\epsilon(\phi(a)(m)) = 0$, so $\phi(a)(m) \in N$

by exactness. This means that

$$(\alpha,\beta)=(na+\sigma(m)a-\sigma(ma),ma)=(na+\phi(a)(m),ma), \tag{2.12}$$

where $\phi(a)\in\mathrm{Hom}_k(M,N)$ and $\phi\in\mathrm{Hom}_k(A,\mathrm{Hom}_k(M,N))$.

We claim that $\phi\in\mathrm{Der}_k(A,\mathrm{Hom}_k(M,N))$. To show this we use the A-bimodule structure of $\mathrm{Hom}_k(M,N)$ from lemma 2.12. Let $a,b\in A$, $m\in M$. Then

$$\begin{aligned}\phi(ab)(m)&=\sigma(m)ab-\sigma(m(ab))\\&=\sigma(m)ab-\sigma(ma)b+\sigma(ma)b-\sigma(m(ab))\\&=\phi(a)(m)b+\phi(b)(ma)\\&=\phi(a)b(m)+a\phi(b)(m),\end{aligned}$$

hence ϕ is a derivation. □

More generally we will have

$$\mathrm{Der}_A(A,\mathrm{Hom}_k(M,N))\big/\,\mathrm{Ider}_A(A,\mathrm{Hom}_k(M,N))\simeq\mathrm{HH}^1(A,\mathrm{Hom}_k(M,N)),$$

where $\mathrm{Ider}_A(A,\mathrm{Hom}_k(M,N))$ denotes the inner derivations ($ad(a)$ for $a\in A$), see [28, page 38], and so using our various definitions we get

Lemma 2.21 $\mathrm{H}^1(G,\mathbb{F}_p)\simeq\mathrm{Der}_{\mathbb{F}_p}(\mathbb{F}_p[G],\mathbb{F}_p)/\,\mathrm{Ider}_{\mathbb{F}_p}(\mathbb{F}_p[G],\mathbb{F}_p)$.

Proof: This can be obtained without going via the Hochschild cocomplex, see for example [18, page 195] (although these are all different sides to the same story). □

2.6.3 Generators

Since $\mathbb{F}_p$ is a trivial module, the inner derivations in lemma 2.21 are already zero. Moreover, a derivation d will be a group homomorphism:

$$\begin{array}{rccc} d: & \mathbb{F}_p[G] & \longrightarrow & \mathbb{F}_p\\ & g_1g_2 & \longmapsto & d(g_1)+d(g_2),\end{array}$$

i.e. $\mathrm{Der}_{\mathbb{F}_p}(\mathbb{F}_p[G],\mathbb{F}_p) = \mathrm{Hom}_{\mathbb{F}_p}(G,\mathbb{F}_p^+)$. We see that d factorises via $[G,G]$, and also via G^p for finite p-groups, and hence

$$\mathrm{H}^1(G,\mathbb{F}_p) \simeq (G/[G,G]G^p)^*. \tag{2.13}$$

So the first cohomology group is the dual of the Frattini quotient of G. We therefore get

Theorem 2.22 *Let G be a finite p-group, then* $\dim_{\mathbb{F}_p} \mathrm{H}^1(G,\mathbb{F}_p)$ *is the minimal number of generators for G.*

Proof: See also [43, page 29]. □

2.7 Interpretations of $\mathrm{H}^2(\mathbf{G},\mathbb{F}_\mathbf{p})$:

2.7.1 2-extensions

The second cohomology group $\mathrm{H}^2(G,\mathbb{F}_p) = \mathrm{Ext}^2_{\mathbb{F}_pG}(\mathbb{F}_p,\mathbb{F}_p)$ can be interpreted as the group of equivalence classes under $\sim$ of 2-extensions with a group operation similar to that of $\mathrm{E}^1_{\mathbb{F}_pG}(\mathbb{F}_p,\mathbb{F}_p)$ in section 2.6 where $\eta+\eta'$ now will be the extension

$$\eta+\eta' : \quad \begin{tikzcd} 0 \arrow[r] & \mathbb{F}_p \arrow[r] & E_1'' \arrow[r] & E_2'' \arrow[r] & \mathbb{F}_p \arrow[r] & 0 \end{tikzcd} \tag{2.14}$$

where E_2'' is the pull-back of E_2 and E_2' over $\mathbb{F}_p$ and E_1'' is the quotient of the push-out of E_1 and E_1' under $\mathbb{F}_p$ by the skew diagonal copy of $\mathbb{F}_p$.

Whereas the zero element in $\mathrm{E}^1_{\mathbb{F}_pG}(\mathbb{F}_p,\mathbb{F}_p)$ corresponds to the direct sum $\mathbb{F}_p\oplus\mathbb{F}_p$, in other words, elements in $\mathrm{H}^1(G,\mathbb{F}_p)$ are obstructions to the module extension being split, the zero element in $\mathrm{E}^2_{\mathbb{F}_pG}(\mathbb{F}_p,\mathbb{F}_p)$ is not that straightforward, and we will point it out later.

2.7.2 Group extensions

Results about the structure of groups using homological algebra often make use of the next theorem, and so this is probably the result most people are familiar with when it comes to cohomological methods in group theory.

Theorem 2.23 *The cohomology group* $\mathrm{H}^2(G,\mathbb{F}_p)$ *classifies the equivalence classes of group extensions, i.e. short-exact sequences*

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{F}_p \arrow[r] & E \arrow[r] & G \arrow[r] & 1 \end{tikzcd} \tag{2.15}$$

where E *is a group.*

Proof: See [46, pp. 182]. ☐

From this we get that the zero element in $\mathrm{H}^2(G,\mathbb{F}_p)$ corresponds to the semidirect product $\mathbb{F}_p \rtimes G$, i.e. elements in $\mathrm{H}^2(G,\mathbb{F}_p)$ are obstructions to the group extension (2.15) being split. In general, $\mathrm{H}^2(G,A)$ classifies group extensions with abelian kernels A.

2.7.3 Certain module extensions

Instead of writing out the proof of theorem 2.23, we choose to include the (typical homological algebra-) proof of the next theorem. The corollary of this theorem is another useful result and tells us that elements in $\mathrm{H}^2(G,\mathbb{F}_p)$ can be considered as equivalence classes of module extensions

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{F}_p \arrow[r] & E \arrow[r] & IG \arrow[r] & 0 \end{tikzcd}$$

of the augmentation ideal IG by $\mathbb{F}_p$. The augmentation ideal is defined as the kernel of the augmentation map given in (2.4).

Theorem 2.24 *Let* $(F_\bullet,\delta)$ *be an* $\mathbb{F}_pG$*-free resolution of* $\mathbb{F}_p$ *and let* K *be the kernel of* δ_{n-1}*. Then*

(i) *the following sequence is exact*

$$\begin{tikzcd} \mathrm{Hom}_{\mathbb{F}_pG}(F_{n-1},\mathbb{F}_p) \arrow[r] & \mathrm{Hom}_{\mathbb{F}_pG}(K,\mathbb{F}_p) \arrow[r] & \mathrm{H}^n(G,\mathbb{F}_p) \arrow[r] & 0; \end{tikzcd}$$

(ii) for $m \geq n+2$ *we have*

$$\mathrm{H}^m(G, \mathbb{F}_p) \simeq \mathrm{Ext}^{m-n-1}_{\mathbb{F}_pG}(K, \mathbb{F}_p).$$

Proof: From the following diagram we see that $\cdots \longrightarrow F_{n+1} \longrightarrow F_n \longrightarrow 0$ can be considered as a free resolution $F'_\bullet$ for K:

$$\begin{tikzcd}
\cdots \arrow[r] & F_{n+1} \arrow[r, "\delta^{n+1}"] & F_n \arrow[rr, "\delta^n"] \arrow[dr] & & F_{n-1} \arrow[r, "\delta^{n-1}"] & \cdots \arrow[r, "\delta_1"] & F_0 \arrow[r, "\epsilon"] & \mathbb{F}_p \arrow[r] & 0. \\
 & & & K \arrow[ur, "\mu"'] & & & & &
\end{tikzcd}$$

Applying $\mathrm{Hom}_{\mathbb{F}_pG}(-, \mathbb{F}_p)$ to $F'_\bullet$ we get the exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_{\mathbb{F}_pG}(K, \mathbb{F}_p) \arrow[r, "\overline{\partial}"] & \mathrm{Hom}_{\mathbb{F}_pG}(F_n, \mathbb{F}_p) \arrow[r, "\partial^n"] & \mathrm{Hom}_{\mathbb{F}_pG}(F_{n+1}, \mathbb{F}_p)
\end{tikzcd}$$

where the ∂-s are induced from the δ-s. We now put this together with the dual resolution for $\mathbb{F}_p$, and apply the Snake Lemma, see [18, page 121] to get the following commutative diagram (the dual resolution of $\mathbb{F}_p$ is marked with dotted arrows)

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_{\mathbb{F}_pG}(F_{n-1}, \mathbb{F}_p) \arrow[r, "\simeq"] \arrow[d, "\mu^*"] & \mathrm{Hom}_{\mathbb{F}_pG}(F_{n-1}, \mathbb{F}_p) \arrow[r] \arrow[d, dotted, "\partial^{n-1}"] & 0 \arrow[d] \\
0 \arrow[r] & \mathrm{Hom}_{\mathbb{F}_pG}(K, \mathbb{F}_p) \arrow[r, "\overline{\partial}"] \arrow[d] & \mathrm{Hom}_{\mathbb{F}_pG}(F_n, \mathbb{F}_p) \arrow[r, dotted, "\partial^n"] \arrow[d] & \mathrm{Hom}_{\mathbb{F}_pG}(F_{n+1}, \mathbb{F}_p) \arrow[d, "\simeq"] \\
0 \arrow[r] & \operatorname{coker} \mu^* \arrow[r] \arrow[d] & \operatorname{coker} \partial_{n-1} \arrow[r, "\alpha"] \arrow[d] & \mathrm{Hom}_{\mathbb{F}_pG}(F_{n+1}, \mathbb{F}_p) \arrow[d] \\
 & 0 & 0 & 0
\end{tikzcd}$$

If we can show that $\operatorname{coker} \mu^* = \mathrm{H}^n(G, \mathbb{F}_p)$, we are done. Diagram-chasing tells us that

$$\operatorname{coker} \mu^* = \ker \alpha \simeq \ker \partial^n / \operatorname{im} \partial^{n-1} = \mathrm{H}^n(G, \mathbb{F}_p),$$

and so we get (i).

For (ii) we observe that the resolution for $\mathbb{F}_p$ (which is used for calculating $\mathrm{H}^i(G,\mathbb{F}_p),\ i \geq 0$) and the resolution for K (which is used for calculating $\mathrm{Ext}^j_{\mathbb{F}_pG}(K,\mathbb{F}_p),\ j \geq 0$) differ by $n-1$ free $\mathbb{F}_pG$-modules. ☐

Corollary 2.25 $\mathrm{H}^2(G,\mathbb{F}_p) \simeq \mathrm{Ext}^1_{\mathbb{F}_pG}(IG,\mathbb{F}_p)$.

Proof: We have the short-exact sequence

$$\begin{tikzcd} 0 \arrow[r] & IG \arrow[r] & \mathbb{F}_pG \arrow[r, "\epsilon"] & \mathbb{F}_p \arrow[r] & 0, \end{tikzcd}$$

so if we put $K = IG$ in theorem 2.24 we get that for $m \geq 2$,

$$\mathrm{H}^m(G,\mathbb{F}_p) \simeq \mathrm{Ext}^{m-1}_{\mathbb{F}_pG}(IG,\mathbb{F}_p).$$

☐

2.7.4 Obstructions to lifting group homomorphisms

We have mentioned two explicit cocomplexes for calculating $\mathrm{H}^n(G,\mathbb{F}_p)$ in sections 2.3 and 2.5, but we haven't mentioned the bar resolution, which a lot of people usually think of when it comes to group cohomology. The bar resolution $B_\bullet$ is the simplicial way of doing group cohomology, and the reason why we haven't mentioned it yet is that it is much more of a theoretical tool rather than a practical tool. However, there is one interpretation of $\mathrm{H}^2(G,\mathbb{F}_p)$ which comes out easily from this resolution, so we will give the cocomplex arising from $B_\bullet$ here.

Definition 2.26 *The dual bar resolution* $B^\bullet(G,\mathbb{F}_p)$ *is the cocomplex*

$$\begin{tikzcd} \cdots \arrow[r] & \mathrm{Maps}(G^n,\mathbb{F}_p) \arrow[r, "\delta^n"] & \mathrm{Maps}(G^{n+1},\mathbb{F}_p) \arrow[r] & \cdots \end{tikzcd}$$

with

$$\begin{aligned}&\delta^n(\phi)(g_1, \ldots, g_{n+1})\\ =&\phi(g_2, \ldots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i \phi(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) + (-1)^{n+1} \phi(g_1, \ldots, g_n)\end{aligned}$$

where ϕ *is a map from* G^n *(as a set) to* $\mathbb{F}_p$*.*

In particular,

$$\delta^1 \phi(g_1, g_2) = \phi(g_2) - \phi(g_1 g_2) + \phi(g_1) \tag{2.16}$$

and

$$\delta^2 \phi(g_1, g_2, g_3) = \phi(g_2, g_3) - \phi(g_1 g_2, g_3) + \phi(g_1, g_2 g_3) - \phi(g_1, g_2). \tag{2.17}$$

The situation to which our next interpretation of $\mathrm{H}^2(G, \mathbb{F}_p)$ relates is the diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{F}_p \arrow[r, "\iota"] & H_1 \arrow[r, "\pi"] & H_2 \arrow[r] & 1 \\
& & & G \arrow[u, "\phi"'] \arrow[ul, dashed, "\phi'"] &
\end{tikzcd} \tag{2.18}$$

where H_1, H_2 are groups and the sequence is exact.

Theorem 2.27 *To each diagram* (2.18) *one associates a specific cohomology class* $\mathrm{obs}_G(\phi) \in \mathrm{H}^2(G, \mathbb{F}_p)$ *such that* $\mathrm{obs}_G(\phi) = 0$ *iff there exists a group homomorphism* ϕ' *making the diagram* (2.18) *commutative.*

Proof: Let σ be a section from H_2 to H_1 (as sets), $g_1, g_2 \in G$ and consider the map ψ defined by

$$\psi(g_1, g_2) = \sigma(\phi(g_1 g_2)) \sigma(\phi(g_2))^{-1} \sigma(\phi(g_1))^{-1}. \tag{2.19}$$

Then $\psi \in \mathrm{Maps}(G \times G, \mathbb{F}_p)$ since ϕ is a homomorphism. Moreover, using (2.17) and (2.19), we check that $(\delta^2 \psi)(g_1, g_2, g_3) = 1$, and so we can let $\mathrm{obs}_G(\phi) = [\psi]$.

Assume $\mathrm{obs}_G(\phi) = 0$. Then $\psi \in \mathrm{im}\, \delta^1$, and so there exists $\alpha \in \mathrm{Maps}(G, \mathbb{F}_p)$

such that $\delta^1\alpha = \psi$. Define

$$\phi'(g) = \sigma(\phi(g))\alpha(g).$$

Then since we have a central extension, we find that ϕ' is a group homomorphism, and $\pi(\phi'(g)) = \phi(g)$.

Conversely, suppose we have ϕ' such that the diagram (2.18) commutes. We need to show that $\mathrm{obs}_G(\phi)$ is zero as an element of $\mathrm{H}^2(G, \mathbb{F}_p)$, i.e. it is "$\delta^1$ of something". So we have to find an element $\gamma \in \mathrm{Maps}(G, \mathbb{F}_p)$ such that $\delta^1\gamma = \psi$. Let $\gamma(g) = \phi'(g)\sigma(\phi(g))^{-1}$. Then we can check that $\pi(\gamma(g)) = 1$, so $\gamma \in \mathrm{Maps}(G, \mathbb{F}_p)$, and $\psi(g_1, g_2) = \gamma(g_1)\gamma(g_1 g_2)^{-1}\gamma(g_2)$, which was what we wanted. ☐

Note that this fits in well with theorem 2.23:

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{F}_p \arrow[r] \arrow[d, equal] & H_1 \arrow[r, "\pi"] & H_2 \arrow[r] & 1 \\
0 \arrow[r] & \mathbb{F}_p \arrow[r] & E \arrow[r, dotted] \arrow[u, dotted] & G \arrow[r] \arrow[u, "\phi"'] \arrow[ul, dashed, "\phi'"'] & 1
\end{tikzcd}$$

where E is the pull-back of (π, ϕ), and so by its properties will give a group extension of G by $\mathbb{F}_p$. If ϕ' exists, $E \simeq \mathbb{F}_p \rtimes G$.

2.7.5 Relations; finite p-groups as pro-p groups

The next theorem includes theorem 2.22 and is important for what is to come. It tells us that $r := \dim_{\mathbb{F}_p} \mathrm{H}^2(G, \mathbb{F}_p)$ is the minimal number of relations defining G as a pro-p group, i.e. an inverse limit of finite p-groups. The minimal number of relations defining G as an abstract group is greater or equal to r, but it is not known if we have equality. The difference lies in the following lemma, which we will need in the proof of the theorem.

Lemma 2.28 *Let G be a pro-p group, and let K and L be normal subgroups of G such that $L \leq K$ and $K = L[K, G]K^p$. Then $K = L$.*

Proof: See [48, page 239]. ☐

Theorem 2.30 will tell us that we are dealing with a minimal pro-p presentation for G, so we need to say a few words about pro-p presentations:

Consider a minimal presentation of G, i.e. a short-exact sequence

$$\begin{tikzcd} 1 \arrow[r] & R \arrow[r] & F \arrow[r] & G \arrow[r] & 1 \end{tikzcd}$$

where F is a free group on a minimal generating set for G. We form the inverse limit

$$\hat{F} = \lim_{\longleftarrow N\in\mathcal{N}} F/N, \quad \text{where } \mathcal{N} = \Big\{ N \lhd F \Big| \; |F:N| = p^r, \text{ some } r \Big\}.$$

Then $\hat{F}$ is a free pro-p group, and since free groups are residually finite p-groups (see [16, page[57]), $F \longrightarrow \hat{F}$ is injective. If we define

$$\hat{R} = \lim_{\longleftarrow N\in\mathcal{N}} R/N,$$

with $\mathcal{N}$ as the set of normal subgroups of R with pth power index, we get a short-exact sequence of pro-p groups (the maps are continuous homomorphisms):

$$\begin{tikzcd} 1 \arrow[r] & \hat{R} \arrow[r] & \hat{F} \arrow[r] & G \arrow[r] & 1, \end{tikzcd} \qquad (2.20)$$

which gives us a minimal pro-p presentation of G. The universal property of a pro-p group is that it maps onto all the finite p-groups in the inverse system of which it is the limit.

For a finite p-group we can make the following definition

Definition 2.29 *Let G be a finite p-group. A minimal pro-p presentation for G is a presentation of an abstract group of which the largest p-quotient is isomorphic to G.*

We will give an example of this after the theorem.

Theorem 2.30 *Let G be a finite p-group, $d(G)$ the minimal number of generators for G and $r(G)$ the minimal number of relations between these gen-*

erators in the corresponding free pro-p group. Then

$$d(G) = \dim_{\mathbb{F}_p} \mathrm{H}^1(G,\mathbb{F}_p); \tag{2.21}$$

$$r(G) = \dim_{\mathbb{F}_p} \mathrm{H}^2(G,\mathbb{F}_p). \tag{2.22}$$

Proof: Statement (2.21) is just theorem 2.22.

To prove (2.22), let G be a pro-p group such that $\mathrm{H}^1(G,\mathbb{F}_p)$ and $\mathrm{H}^2(G,\mathbb{F}_p)$ are finite and let

$$1 \longrightarrow \ker\pi \longrightarrow F \xrightarrow{\pi} G \longrightarrow 1 \tag{2.23}$$

be a (finite) minimal presentation of G. We want to show that

$$d_F(\ker\pi) = \dim_{\mathbb{F}_p} \mathrm{H}^2(G,\mathbb{F}_p),$$

where by $d_F(\ker\pi)$ we mean the least cardinality of a generating set for $\ker\pi$ as a normal subgroup of F.

To every short-exact sequence of groups, we get a 5-term exact sequence connecting the cohomology in dimensions 1 and 2 (use the Lyndon-Hochschild-Serre spectral sequence or see [18, page 202]). The presentation 2.23 gives us the sequence

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^1(G,\mathbb{F}_p) \arrow[r, "\alpha"] & \mathrm{H}^1(F,\mathbb{F}_p) \arrow[r, "\beta"] & \mathrm{H}^1(\ker\pi,\mathbb{F}_p)^F \arrow[dll, rounded corners, to path={ -- ([xshift=2ex]\tikztostart.east) |- ([yshift=-3ex]\tikztostart.south) \tikztonodes -| ([xshift=-2ex]\tikztotarget.west) -- (\tikztotarget)}, "\gamma"] \\
& \mathrm{H}^2(G,\mathbb{F}_p) \arrow[r, "\delta"] & \mathrm{H}^2(F,\mathbb{F}_p) &
\end{tikzcd}$$

where $\mathrm{H}^2(F,\mathbb{F}_p) = 0$ since F is a free group. From 2.22 we have that $\dim_{\mathbb{F}_p} \mathrm{H}^1(G,\mathbb{F}_p) = d(G)$. Also, $\dim_{\mathbb{F}_p} \mathrm{H}^1(F,\mathbb{F}_p) = d(F) = d(G)$.

We claim that $\dim_{\mathbb{F}_p} \mathrm{H}^1(\ker\pi,\mathbb{F}_p)^F = d_F(\ker\pi)$. Let us write K for $\ker\pi$. We know that $d_F(K) = d_F(K/\Phi(K))$ and by 2.13 we also have $\mathrm{H}^1(K,\mathbb{F}_p)^F \simeq$

$\mathrm{Hom}_{\mathbb{F}_p}(K/\Phi(K),\mathbb{F}_p)^F$. Now

$$\begin{aligned}\mathrm{Hom}_{\mathbb{F}_p}(K/\Phi(K),\mathbb{F}_p)^F &= \mathrm{Hom}_F(K/\Phi(K),\mathbb{F}_p)\\ &= \mathrm{Hom}_{\mathbb{F}_p}(K/[K,F]K^p,\mathbb{F}_p)\end{aligned}$$

since F acts on K by conjugation and acts trivially on $\mathbb{F}_p$. We now apply lemma 2.28 to get $\dim_{\mathbb{F}_p}(K/[K,F]K^p) = d_F(K)$ (let L be the normal subgroup of F generated by a generating set for $K/[K,F]K^p$), hence the claim (the dual has the same dimension).

And so we get

$$\begin{aligned}&d(F)\\ =&d(G)+\dim\mathrm{im}\,\beta\\ =&d(G)+\dim\ker\gamma\\ =&d(G)+d_F(\ker\pi)-\dim\mathrm{im}\,\gamma\\ =&d(G)+d_F(\ker\pi)-\dim\mathrm{H}^2(G,\mathbb{F}_p).\end{aligned}$$

As $d(G)=d(F)$, the result follows. □

To illustrate the difference between a pro-p presentation and a presentation for G we give the following example, which was found when we ran different cohomological presentations on Magma.

Example 2.31 We consider the group G_6 for $p=3$ from Burnside's list of groups of order p^4, see [7]. The "usual" presentation for this group is

$$G=\{x,y|x^{27}=1,y^3=1,[x,y]=x^9\}.$$

From a certain combination of Massey products we get the following presentation (will be explained in section 4.3.2):

$$H=\{x,y|x^3=1,y^9[x,y]=1\},$$

which has order $3^4{\cdot}37$. The largest p-quotient of this is isomorphic to G, so the presentation of H gives a pro-p presentation of G. However, the presentation of G has three relations and H has two. The question is therefore “Does G have a presentation as an abstract group of order 81 with only two relations?” The answer is yes (Michael Vaughan-Lee):

$$K = \{x, y | x^{27} = y^3, [x, y] = x^9\}. \tag{2.24}$$

See appendix A for a Magma-session showing this example. ■

In the rest of this thesis we will alternate between the various definitions and interpretations introduced in this chapter. We hope the reader will be forgiving when we don’t always refer back to the relevant result.

Chapter 3

Massey products

The basis for this chapter lies in the proof of lemma 2.10: Take an $\mathbb{F}_pG$-free resolution $F_\bullet$ of $\mathbb{F}_p$. Then the dual resolution $\mathrm{Hom}_{\mathbb{F}_pG}(F_\bullet, \mathbb{F}_p)$ will be homotopy equivalent to any other dual resolution of $\mathbb{F}_p$, and they will give the same cohomology groups.

Both the dual resolution and the cohomology $\mathrm{H}^*(G, \mathbb{F}_p)$ will be graded vector spaces over $\mathbb{F}_p$. Moreover, as we will see in this chapter, both the dual resolution and the cohomology carry an algebra structure. But whereas the algebra $\mathrm{H}^*(G, \mathbb{F}_p)$ will be strictly associative and graded-commutative, the dual resolution will only be associative and graded-commutative up to homotopy. The extra information we get from this fact is encoded in a very rich internal product structure called Massey products (from the associativity) and Steenrod operations (from the commutativity).

In the previous chapter we introduced several dual resolutions used for finding the graded vector space $\mathrm{H}^*(G, \mathbb{F}_p)$, and in this chapter we will see what the product structure looks like in these different situations. The multiplication on $\mathrm{H}^*(G, \mathbb{F}_p)$ is usually called the cup product. This is a universal construction, and all the products we introduce will be the same as this, and will have the same properties.

Because of theorem 2.30, we will concentrate on $\mathrm{H}^1(G, \mathbb{F}_p)$ and $\mathrm{H}^2(G, \mathbb{F}_p)$. This is also the reason why we only consider Massey products and not Steenrod operations, since Steenrod operations, save the Bockstein, don't do anything as operations from $\mathrm{H}^1(G, \mathbb{F}_p)$ to $\mathrm{H}^2(G, \mathbb{F}_p)$ ($\mathcal{P}^0$ is the identity operation, see [3, page 138]).

3.1 The algebra structure on $\mathrm{H}^*(\mathbf{G},\mathbb{F}_\mathbf{p})$

First we need to define what we mean by a graded-commutative differential graded algebra over $\mathbb{F}_p$. We note that if H^* is a graded vector space over $\mathbb{F}_p$ then $\mathrm{H}^* \otimes_{\mathbb{F}_p} \mathrm{H}^*$ becomes a graded vector space by

$$(\mathrm{H}^* \otimes_{\mathbb{F}_p} \mathrm{H}^*)^n = \bigoplus_{i+j=n} \mathrm{H}^i \otimes_{\mathbb{F}_p} \mathrm{H}^j \,.$$

Definition 3.1 *The graded vector space* H^* *over* $\mathbb{F}_p$ *is called a graded algebra over* $\mathbb{F}_p$ *if it has a multiplication* α*, i.e. a linear mapping*

$$\alpha_{i,j}: \quad \mathrm{H}^i \otimes_{\mathbb{F}_p} \mathrm{H}^j \longrightarrow \mathrm{H}^{i+j} \quad \textit{for all } i, j$$

such that α *is associative, i.e. the following diagram is commutative*

$$\begin{tikzcd}
\mathrm{H}^* \otimes_{\mathbb{F}_p} \mathrm{H}^* \otimes_{\mathbb{F}_p} \mathrm{H}^* \arrow[r, "\alpha\otimes 1"] \arrow[d, "1\otimes\alpha"'] & \mathrm{H}^* \otimes_{\mathbb{F}_p} \mathrm{H}^* \arrow[d, "\alpha"] \\
\mathrm{H}^* \otimes_{\mathbb{F}_p} \mathrm{H}^* \arrow[r, "\alpha"] & \mathrm{H}^* .
\end{tikzcd}$$

The graded algebra H^* *is called graded commutative if*

$$x \cdot y = (-1)^{ij} y \cdot x \tag{3.1}$$

for $x \in \mathrm{H}^i$, $y \in \mathrm{H}^j$ *and* $x \cdot y$ *denotes* $\alpha(x, y)$*. And it is said to be a differential graded algebra if it has a differential* δ *such that*

$$\delta(x \cdot y) = \delta(x) \cdot y + (-1)^i x \cdot \delta(y). \tag{3.2}$$

Remark 3.2 Let $(A^\bullet, \delta)$ be a differential graded algebra and let $\mathrm{H}^* = \mathrm{H}^*(A^\bullet)$. The formula (3.2) tells us that the product on $(A^\bullet, \delta)$ induces a well-defined product on H^*:

If x, y are cocycles then $\delta(x) = \delta(y) = 0$, hence $\delta(x \cdot y) = 0$ and so $x \cdot y$ is a cocycle. Also, the product of a cocycle and a coboundary (or vice versa) is a coboundary (e.g. $\delta(x)$ is a coboundary; if y is a cocycle then $\delta(y) = 0$, so $\delta(x) \cdot y = \delta(x \cdot y)$ which is a coboundary). ■

The various cocomplexes from chapter 2 will be differential graded algebras and so by remark 3.2 we get an algebra structure on $\mathrm{H}^*(G, \mathbb{F}_p)$.

3.1.1 The Yoneda composition

We will now introduce the algebra structure on $\mathrm{H}^*(G, \mathbb{F}_p)$. More proofs and details will be given in sections 3.3 and 3.4.

Take $\xi = [\phi], \xi' = [\phi'] \in \mathrm{E}^1_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$, represented by

$$0 \longrightarrow \mathbb{F}_p \longrightarrow E \longrightarrow \mathbb{F}_p \longrightarrow 0 \quad \text{and} \quad 0 \longrightarrow \mathbb{F}_p \longrightarrow E' \longrightarrow \mathbb{F}_p \longrightarrow 0$$

respectively. Then we can form the splice of these short-exact sequences to get a 2-extension:

$$\begin{tikzcd}
\phi: & 0 \arrow[r] & \mathbb{F}_p \arrow[r] & E \arrow[r] \arrow[drr, dashed] & \mathbb{F}_p \arrow[r] \arrow[d, equal] & 0 & & \\
\phi': & & & 0 \arrow[r] & \mathbb{F}_p \arrow[r] & E' \arrow[r] & \mathbb{F}_p \arrow[r] & 0
\end{tikzcd}$$

This map is well-defined (the equivalence relation is isomorphism), bilinear, associative and anti-symmetric, see [2], and is called the Yoneda composition

$$\langle -, -; 0 \rangle : \quad \mathrm{Ext}^1_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p) \otimes \mathrm{Ext}^1_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p) \longrightarrow \mathrm{Ext}^2_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p). \qquad (3.3)$$

The anti-symmetry tells us that if we splice ϕ and ϕ' then the 2-extension we get is an additive inverse to the 2-extension obtained from splicing ϕ' and ϕ.

A couple of words about the notation, which might seem unfamiliar to the reader: This notation will fit in well with the notation we will use for the Massey products, and where we can think of the Yoneda composition as being the 2-fold Massey product.

We mention that the Yoneda composition is defined not only for $\mathrm{H}^1(G, \mathbb{F}_p)$ and $\mathrm{H}^2(G, \mathbb{F}_p)$, but on the cohomology in all dimensions, i.e.

$$\langle -, -; 0\rangle : \quad \mathrm{H}^n(G, \mathbb{F}_p) \otimes \mathrm{H}^m(G, \mathbb{F}_p) \longrightarrow \mathrm{H}^{n+m}(G, \mathbb{F}_p),$$

splicing an n-extension with an m-extension. This gives us a product structure on $\mathrm{H}^*(G, \mathbb{F}_p)$, making it into an associative, graded-commutative ring with unit, referred to as the cohomology ring.

Recall definition 2.26 of the dual bar resolution. From this we can define the cup product,

$$\begin{array}{ccc} \mathrm{Maps}(G^n, \mathbb{F}_p) \otimes \mathrm{Maps}(G^m, \mathbb{F}_p) & \longrightarrow & \mathrm{Maps}(G^{n+m}, \mathbb{F}_p) \\ (\phi, \psi) & \longmapsto & \phi \circ \psi \end{array}$$

where $\phi \circ \psi(g_1, \ldots, g_{n+m})$ is given by the Alexander-Whitney map, i.e.

$$\phi \circ \psi(g_1, \ldots, g_{n+m}) = \phi(g_1, \ldots, g_n)\psi(g_{n+1}, \ldots, g_{n+m}). \tag{3.4}$$

The reader is referred to [1, chapter 7] for more details on the cup product construction. This product is the same as the Yoneda composition, see [2, page 53]. So we can think of the product on $\mathrm{H}^*(G, \mathbb{F}_p)$ as composing maps, and on $\mathrm{H}^1(G, \mathbb{F}_p)$ and $\mathrm{H}^2(G, \mathbb{F}_p)$ it will be antisymmetric, since in general it is graded commutative.

If we use the differential formula in definition 2.26, we can show that the dual bar resolution is a differential graded algebra, i.e.

$$\partial^{n+m}(\phi \circ \psi) = (\partial^n \phi) \circ \psi + (-1)^n \phi \circ (\partial^m \psi).$$

We will see what the product structure looks like in the Yoneda cocomplex, and also in the theory of n-extensions, after we have introduced Massey products.

3.2 Massey products; the classical way

A dual resolution of $\mathbb{F}_p$ is a differential graded algebra with an associative product $\langle -,-;0\rangle$. Since this product is well-defined on cohomology classes, we use this notation both for a product between cochains and a product between cocycles.

We will now see how we can generalise this product and construct higher order analogues called Massey products. This construction holds for any differential graded algebra with an associative pairing.

For the definitions given here (for $\mathrm{H}^1(G,\mathbb{F}_p)$ and $\mathrm{H}^2(G,\mathbb{F}_p)$) we have used Kraines[22], May[31] and Dwyer[13]. We will follow Kraines' procedure for defining the Massey products, but will use 1-s on the diagonal in the defining systems, as Dwyer does. Also, Dwyer and Kraines differ by a sign, and on this we will follow Kraines. The ∂ refers to the differential in a dual resolution for $\mathbb{F}_p$.

Definition 3.3 *Let* $\xi_1,\ldots,\xi_s \in \mathrm{H}^1(G,\mathbb{F}_p)$ *and let* $\phi_1,\ldots,\phi_s$ *be cocycle representatives of* $\xi_1,\ldots,\xi_s$ *respectively. A collection of 1-cochains*

$$M = \{m_{ij} | 1 \leq i < j \leq s+1, (i,j) \neq (1,s+1)\}$$

is said to be a defining system for the cochain product $\langle \phi_1,\ldots,\phi_s;0\rangle$ *if*

$$m_{i,i+1} = \phi_i \qquad \text{for } i = 1,\ldots,s; \tag{3.5}$$

$$\partial m_{ij} = \sum_{k=i+1}^{j-1} -\langle m_{ik}, m_{kj};0\rangle \qquad \text{for } j \neq i+1. \tag{3.6}$$

The value of M*, denoted* $v(M)$*, is the 2-cocycle*

$$v(M) = \sum_{k=2}^{s} -\langle m_{1k}, m_{k,s+1};0\rangle.$$

To see that $v(M)$ is a 2-cocycle we use (3.5), (3.6) and the fact that $\langle -,-;0\rangle$

is bilinear and associative. Let us check that $\partial(v(M)) = 0$ for $s = 3$:

$$\begin{aligned}
\partial(v(M)) = {} & -\partial\langle m_{12}, m_{24}; 0\rangle - \partial\langle m_{13}, m_{34}; 0\rangle \\
= {} & -(\langle \partial(m_{12}), m_{24}; 0\rangle - \langle m_{12}, \partial(m_{24}); 0\rangle \\
& \quad + \langle \partial(m_{13}), m_{34}; 0\rangle - \langle m_{13}, \partial(m_{34}); 0\rangle) \\
= {} & \langle m_{12}, \langle m_{23}, m_{34}; 0\rangle; 0\rangle - \langle\langle m_{12}, m_{23}; 0\rangle, m_{34}; 0\rangle \\
= {} & 0.
\end{aligned}$$

Note that a defining system can be viewed as an $(s+1) \times (s+1)$-matrix

$$\begin{pmatrix}
1 & m_{12} & \cdots & m_{1s} & \\
0 & 1 & \ddots & \ddots & m_{2,s+1} \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & 1 & m_{s,s+1} \\
0 & \cdots & \cdots & 0 & 1
\end{pmatrix}.$$

The top right-hand corner will be the value of the defining system.

On the level of cochains, we make the following definition:

Definition 3.4 *The s-fold (cochain) product $\langle \phi_1, \ldots, \phi_s; 0\rangle$ is defined if there is a defining system for it. If it is defined then we define $\langle \phi_1, \ldots, \phi_s; 0\rangle$ to be the set of cohomology classes v such that there exists an M with $v(M)$ representing v.*

Because of the following theorem, Massey products are well-defined on cohomology classes:

Theorem 3.5 *The operation $\langle \phi_1, \ldots, \phi_s; 0\rangle$ depends only on the cohomology classes of $\phi_1, \ldots, \phi_s$.*

Proof: Given a defining system $M = (m_{ij})$ for $\langle \phi_1, \ldots, \phi_s; 0\rangle$, we define a defining system M' for $\langle \phi_1, \ldots, \phi_t + \partial a, \ldots \phi_s; 0\rangle$ for a a 0-cochain, by changing the t-th column and the $(t+1)$-st row of M:

$$\begin{pmatrix} \ddots & & & \vdots & & \\ & 1 & m_{t-1,t} & m_{t-1,t+1} + \langle m_{t-1,t}, a; 0\rangle & m_{t-1,t+2} & \\ \cdots & 0 & 1 & m_{t,t+1} + \partial a & m_{t,t+2} - \langle a, m_{t+1,t+2}; 0\rangle & \cdots \\ & 0 & 0 & 1 & m_{t+1,t+2} & \\ & 0 & 0 & 0 & 1 & \\ & & & \vdots & & \ddots \end{pmatrix}.$$

We check that M' is a defining system using the properties of $\langle -, -; 0\rangle$.

Moreover, $v(M)$ and $v(M')$ will be the same for $1 < t < s$ and for $t = 1$ and $t = s$ they will differ by a coboundary, so

$$\langle \phi_1, \ldots, \phi_s; 0\rangle \subset \langle \phi_1, \ldots, \phi_t + \partial a, \ldots \phi_s; 0\rangle.$$

For the reverse inclusion, we have given an M' and construct M in the similar way as before. □

Hence we define a defining system for the s-fold Massey product $\langle \xi_1, \ldots, \xi_s; 0\rangle$ to be a defining system for $\langle \phi_1, \ldots, \phi_s; 0\rangle$, and

$$\langle \xi_1, \ldots, \xi_s; 0\rangle = \langle \phi_1, \ldots, \phi_s; 0\rangle$$

as subsets of $\mathrm{H}^2(G, \mathbb{F}_p)$.

For particularly nice Massey products, we will always have a defining system. These are called strictly defined Massey products, and are the products we will be interested in:

Definition 3.6 *We say that* $\langle \xi_1, \ldots, \xi_s; 0\rangle$ *is strictly defined if each*

$$\langle \xi_i, \ldots, \xi_j; 0\rangle \quad \textit{for} \quad 1 \leq j - i \leq s - 2$$

is defined and contains only zero.

Example 3.7 The product $\langle \xi_1, \xi_2; 0\rangle$ is always defined and contains only one cohomology class, namely $[-\langle \xi_1, \xi_2; 0\rangle]$.

The 3-fold product $\langle\xi_1,\xi_2,\xi_3;0\rangle$ is defined if and only if the products $\langle\xi_1,\xi_2;0\rangle$ and $\langle\xi_2,\xi_3;0\rangle$ are both zero. In general, every defined 3-fold product is seen to be strictly defined.

Suppose $\langle\xi_1,\xi_2;0\rangle = 0$ and $\langle\xi_2,\xi_3;0\rangle = 0$, and let m_{13}, m_{24} be such that $\partial^1 m_{13} = \langle\xi_1,\xi_2;0\rangle$ and $\partial^1 m_{24} = \langle\xi_2,\xi_3;0\rangle$ (such m_{13} and m_{24} exist since the products are 0 as elements in $\mathrm{H}^2(G,\mathbb{F}_p)$). A defining system for $\langle\xi_1,\xi_2,\xi_3;0\rangle$ is

$$\begin{pmatrix} 1 & m_{12} & m_{13} & \\ 0 & 1 & m_{23} & m_{24} \\ 0 & 0 & 1 & m_{34} \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and the formula is

$$\langle\xi_1,\xi_2,\xi_3;0\rangle = -\langle m_{12}, m_{24};0\rangle - \langle m_{13}, m_{34};0\rangle.$$

For the 4-fold product $\langle\xi_1,\xi_2,\xi_3,\xi_4;0\rangle$ to be strictly defined, we need that the products $\langle\xi_1,\xi_2;0\rangle, \langle\xi_2,\xi_3;0\rangle, \langle\xi_3,\xi_4;0\rangle, \langle\xi_1,\xi_2,\xi_3;0\rangle$ and $\langle\xi_2,\xi_3,\xi_4;0\rangle$ are all zero. ■

We note that the definition of a Massey product will not give us a unique cohomology class, but rather a set of such classes. This means we naturally have indeterminacy, which we need to deal with.

Definition 3.8 *The indeterminacy of the Massey product* $\langle\xi_1,\ldots,\xi_s;0\rangle$ *is defined by*

$$\mathrm{In}\langle\xi_1,\ldots,\xi_s;0\rangle = \{x-y \mid x,y\in\langle\xi_1,\ldots,\xi_s;0\rangle\}.$$

Example 3.9 Example 3.7 showed that $\langle\xi_1,\xi_2;0\rangle$ has no indeterminacy, as it only contains one cohomology class.

Let us calculate $\mathrm{In}\langle\xi_1,\xi_1,\xi_1;0\rangle$. Suppose $\langle\xi_1,\xi_1;0\rangle = 0$, let m_1 be a cocycle representative for ξ_1 and m_2 be a 1-cochain such that $\partial^1 m_2 = -\langle\xi_1,\xi_1;0\rangle$. A different choice for m_2 would be $m_2' = m_2 + a$ where a is a 1-cocycle, since

$\partial^1(m_2 - m_2') = 0$. So two defining systems for $\langle \xi_1, \xi_1, \xi_1; 0\rangle$ are

$$M = \begin{pmatrix} 1 & m_1 & m_2 & \\ 0 & 1 & m_1 & m_2 \\ 0 & 0 & 1 & m_1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } M' = \begin{pmatrix} 1 & m_1 & m_2 & \\ 0 & 1 & m_1 & m_2 + a \\ 0 & 0 & 1 & m_1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

We have

$$\begin{aligned} v(M') = & -\langle m_1, m_2 + a; 0\rangle - \langle m_2, m_1; 0\rangle \\ = & -\langle m_1, m_2; 0\rangle - \langle m_1, a; 0\rangle - \langle m_2, m_1; 0\rangle, \end{aligned}$$

which differs from $v(M)$ by the element $\langle m_1, a; 0\rangle$. We see that

$$\mathrm{In}\langle \xi_1, \xi_1, \xi_1; 0\rangle = \bigcup_{a \in \mathrm{H}^1(G, \mathbb{F}_p)} \langle \xi_1, a; 0\rangle.$$

If $\mathrm{H}^1(G, \mathbb{F}_p)$ is 1-dimensional and $|G| \neq 2$, $\mathrm{In}\langle \xi_1, \xi_1, \xi_1; 0\rangle = 0$, and we can talk about the Massey product as a unique element. ■

We will see what sort of problems the indeterminacy gives us in section 4.5.

Remark 3.10 We summarise some facts:

1) The Massey product of a particular ordered set is defined if there is a defining system for it. Hence it will not always exist.

2) The Massey product may contain more than one element, but in certain cases we can restrict the defining system so that the Massey product for particular ordered sets contains a unique element.

3) Submatrices of M will define subproducts (Massey products of shorter length). In order for $\langle \xi_1, \ldots, \xi_s; 0\rangle$ to be defined it is necessary that each of these Massey subproducts contain zero. If they contain zero and only zero, then $\langle \xi_1, \ldots, \xi_s; 0\rangle$ is said to be strictly defined.

4) The Massey products can be made to satisfy lots of properties, and we refer the reader to [22] and [31] for details. We mention that scalar

multiplication by invertible elements behave as you expect, as we will need this.

■

3.3 Massey products in the Yoneda cocomplex

We will now see what the products look like in the Yoneda cocomplex $(\mathrm{Hom}^{(\bullet)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet), \partial)$ from section 2.5.

First, we consider the cup product

$$\langle -, -; 0\rangle : \quad \mathrm{Ext}^1_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p) \otimes \mathrm{Ext}^1_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p) \longrightarrow \mathrm{Ext}^2_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p).$$

If $\phi^n \in \mathrm{Hom}^{(n)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet)$, $\psi^m \in \mathrm{Hom}^{(m)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet)$, then we can define the product

$$\begin{aligned}\mathrm{Hom}^{(n)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet) \otimes \mathrm{Hom}^{(m)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet) &\longrightarrow \mathrm{Hom}^{(n+m)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet)\\ (\phi^n, \psi^m) &\longmapsto \phi^n\psi^m,\end{aligned}$$

where the obvious subscripts of $F_\bullet$ must match to get a legal composition. Lemma 2.19 tells us that this product makes the Yoneda cocomplex into a differential graded algebra. We now consider the case $n = m = 1$ and drop the superscripts.

Let $\xi_1, \xi_2 \in \mathrm{Ext}^1_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$, and let $F_\bullet \twoheadrightarrow \mathbb{F}_p$ be an $\mathbb{F}_pG$-free resolution for $\mathbb{F}_p$, i.e.

$$\begin{tikzcd}\mathbb{F}_p & F_0 \arrow[l, two heads, "\rho"'] & F_1 \arrow[l, "\delta_0"'] & F_2 \arrow[l, "\delta_1"'] & \cdots \arrow[l]\end{tikzcd}$$

Elements in $\mathrm{Ext}^1_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$ has representatives in $\mathrm{Hom}^{(1)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet) \supseteq \ker \partial^1$, so if we let $\psi = \{\psi_i\}_{i \geq 1} \in \ker \partial^1$ be such a representative, we get the following commutative diagram:

$$\begin{tikzcd}
\mathbb{F}_p & F_0 \arrow[l, two heads, "\rho"'] & F_1 \arrow[l, "\delta_0"'] \arrow[dl, "\psi_1"'] & F_2 \arrow[l, "\delta_1"'] \arrow[dl, "\psi_2"'] & F_3 \arrow[l, "\delta_2"'] \arrow[dl, "\psi_3"'] & \cdots \arrow[l] \\
\mathbb{F}_p & F_0 \arrow[l, two heads, "\rho"] & F_1 \arrow[l, "\delta_0"] & F_2 \arrow[l, "\delta_1"] & F_3 \arrow[l, "\delta_2"] & \cdots \arrow[l]
\end{tikzcd}$$

We let $(\psi_1) = \{(\psi_1)_i\}_{i\geq 1}$ and $(\psi_2) = \{(\psi_2)_i\}_{i\geq 1}$ be representatives for ξ_1 and ξ_2 respectively.

Remark 3.11 In our case F_1 will be $(\mathbb{F}_pG)^d$ where d is the minimal number of generators for G. The standard basis for F_1 will also be a basis for $\mathrm{Hom}_{\mathbb{F}_pG}(F_1, F_0)$, and so $(\psi_1)_1$ and $(\psi_2)_1$ can be chosen to be the standard basis for F_1. We only need to check that this choice gives us cocycles. For this, we see from the diagram (where $d = 2$)

$$\begin{tikzcd}
\mathbb{F}_p & F_0 \arrow[l, two heads, "\rho"'] & F_1 \arrow[l, "\delta_0"'] \arrow[dl, shift right, "(\psi_1)_1"'] \arrow[dl, shift left, "(\psi_2)_1"] & F_2 \arrow[l, "\delta_1"'] \arrow[dl, shift right, "(\psi_1)_2"'] \arrow[dl, shift left, "(\psi_2)_2"] & F_3 \arrow[l, "\delta_2"'] \arrow[dl, shift right, "(\psi_1)_3"'] \arrow[dl, shift left, "(\psi_2)_3"] & \cdots \arrow[l] \\
\mathbb{F}_p & F_0 \arrow[l, two heads, "\rho"'] & F_1 \arrow[l] & F_2 \arrow[l] & F_3 \arrow[l] & \cdots \arrow[l]
\end{tikzcd} \tag{3.7}$$

and (2.8) that we need

$$\delta_1(\psi_1)_1\rho = 0,$$

$$\delta_1(\psi_2)_1\rho = 0,$$

which depends on the differentials in our resolution. ■

To find $(\psi_1)_i$ and $(\psi_2)_i$ for $i > 1$, we need to lift $(\psi_1)_1$ and $(\psi_2)_1$ to get commutative diagrams, and so these can again be calculated using the differentials in the resolution.

Finally, we know that the product $\langle \xi_1, \xi_2; 0\rangle$ corresponds to composing maps, and as it is an element in $\mathrm{Ext}^2_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$, we need to compose our maps with ρ. Hence we get the diagram

$$\begin{tikzcd}
\mathbb{F}_p & F_0 \arrow[l, two heads] & F_1 \arrow[l] & F_2 \arrow[l] \arrow[dl, "(\psi_1)_2"'] \arrow[dl, "(\psi_2)_2"] & \cdots \arrow[l] \\
\mathbb{F}_p & F_0 \arrow[l, two heads] & F_1 \arrow[l] \arrow[dl, "(\psi_1)_1"'] \arrow[dl, "(\psi_2)_1"] & F_2 \arrow[l] & \cdots \arrow[l] \\
\mathbb{F}_p & F_0 \arrow[l, two heads, "\rho"'] & F_1 \arrow[l] & F_2 \arrow[l] & \cdots \arrow[l]
\end{tikzcd}$$

and the formulas

$$\begin{aligned}
\langle \xi_1, \xi_1; 0\rangle &= (\psi_1)_2(\psi_1)_1\rho, \\
\langle \xi_1, \xi_2; 0\rangle &= (\psi_1)_2(\psi_2)_1\rho, \\
\langle \xi_2, \xi_1; 0\rangle &= (\psi_2)_2(\psi_1)_1\rho, \\
\langle \xi_2, \xi_2; 0\rangle &= (\psi_2)_2(\psi_2)_1\rho.
\end{aligned}$$

If we have products that are 0 (as elements in $\operatorname{Ext}^2_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$), we know that we will get 3-fold Massey products. So let $\langle \xi_1, \xi_1; 0\rangle = 0$, say. Then there exists $\phi = \{\phi_i\}_{i\geq 1} \in \operatorname{Hom}^{(1)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet)$ such that $\partial\phi = (\psi_1)_2(\psi_1)_1$, so consider

$$\begin{tikzcd}
\mathbb{F}_p & F_0 \arrow[l, two heads] & F_1 \arrow[l] \arrow[ddl, dashed, "\phi_1"'] & F_2 \arrow[l, "\delta_1"'] \arrow[dl, "(\psi_1)_2"'] \arrow[ddll, squiggly, "(\psi_1)_2(\psi_1)_1"] \arrow[ddl, dashed, "\phi_2"] & \cdots \arrow[l] \\
\mathbb{F}_p & F_0 \arrow[l, two heads] & F_1 \arrow[l] \arrow[dl, "(\psi_1)_1"] & F_2 \arrow[l] & \cdots \arrow[l] \\
\mathbb{F}_p & F_0 \arrow[l, two heads] & F_1 \arrow[l, "\delta_0"] & F_2 \arrow[l] & \cdots \arrow[l]
\end{tikzcd}$$

We calculate ϕ_1 and ϕ_2 using the formula

$$\delta_1\phi_1 - \phi_2\delta_0 = (\psi_1)_2(\psi_1)_1,$$

and then we have what we need to calculate the 3-fold Massey product $\langle \xi_1, \xi_1, \xi_1; 0\rangle$. We have seen that the formula for this product is

$$\langle \xi_1, \xi_1, \xi_1; 0\rangle = ((\psi_1)_2\phi_1 + \phi_2(\psi_1)_1)\rho.$$

Hence we get the diagram

$$\begin{tikzcd}
\mathbb{F}_p & F_0 \arrow[l, two heads] & F_1 \arrow[l] & F_2 \arrow[l] \arrow[dl, "(\psi_1)_2"'] \arrow[ddll, dashed, bend left] & \cdots \arrow[l] \\
\mathbb{F}_p & F_0 \arrow[l, two heads] & F_1 \arrow[l] \arrow[dl, "\phi_1"'] & F_2 \arrow[l] \arrow[dl, "\phi_2"'] \arrow[ddll, dashed, bend left] & \cdots \arrow[l] \\
\mathbb{F}_p & F_0 \arrow[l, two heads] & F_1 \arrow[l] \arrow[dl, "(\psi_1)_1"'] & F_2 \arrow[l] & \cdots \arrow[l] \\
\mathbb{F}_p & F_0 \arrow[l, two heads, "\rho"'] & F_1 \arrow[l] & F_2 \arrow[l] & \cdots \arrow[l]
\end{tikzcd}$$

Remember that to get $\langle \xi_1, \xi_1, \xi_1; 0\rangle$ as an element in $\mathrm{Ext}^2_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$, we need to compose with ρ.

Let us also show the diagram for calculating the 4-fold Massey product, as we now need to involve quite a few lower order Massey products. So assume $\langle \xi_1, \xi_1, \xi_1; 0\rangle$ is 0 (as an element in $\mathrm{Ext}^2_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$). Then there exists $\mu = \{\mu_i\}_{i\geq 1} \in \mathrm{Hom}^{(1)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet)$ such that $\partial\mu = (\psi_1)_2\phi_1 + \phi_2(\psi_1)_1$, i.e. we get

$$\begin{tikzcd}
\mathbb{F}_p & F_0 \arrow[l, two heads] & F_1 \arrow[l] \arrow[dddl, dashed, "\mu_1"'] & F_2 \arrow[l, "\delta_1"'] \arrow[dddll, squiggly, "(\psi_1)_2\phi_1+\phi_2(\psi_1)_1"'] \arrow[dddl, dashed, "\mu_2"] & \cdots \arrow[l] \\
\mathbb{F}_p & F_0 \arrow[l, two heads] & F_1 \arrow[l] & F_2 \arrow[l] & \cdots \arrow[l] \\
\mathbb{F}_p & F_0 \arrow[l, two heads] & F_1 \arrow[l] & F_2 \arrow[l] & \cdots \arrow[l] \\
\mathbb{F}_p & F_0 \arrow[l, two heads] & F_1 \arrow[l, "\delta_0"] & F_2 \arrow[l] & \cdots \arrow[l]
\end{tikzcd}$$

To calculate $\langle \xi_1, \xi_1, \xi_1, \xi_1; 0\rangle$ we have the formula

$$\langle \xi_1, \xi_1, \xi_1, \xi_1; 0\rangle = ((\psi_1)_2\mu_1 + \phi_2\phi_1 + \mu_2(\psi_1)_1)\rho$$

which gives us the following diagram:

$$\begin{tikzcd}
\mathbb{F}_p & F_0 \arrow[l, two heads] & F_1 \arrow[l] & F_2 \arrow[l] \arrow[dl, "(\psi_1)_2"'] \arrow[dl, dashed, bend left=10] & \cdots \arrow[l] \\
\mathbb{F}_p & F_0 \arrow[l, two heads] & F_1 \arrow[l] \arrow[dl, "\mu_1"'] \arrow[dl, dashed, bend left=10] & F_2 \arrow[l] & \cdots \arrow[l] \\
\mathbb{F}_p & F_0 \arrow[l, two heads] & F_1 \arrow[l] & F_2 \arrow[l] \arrow[dl, "\phi_2"'] \arrow[dl, dashed, bend left=10] & \cdots \arrow[l] \\
\mathbb{F}_p & F_0 \arrow[l, two heads] & F_1 \arrow[l] \arrow[dl, "\phi_1"'] \arrow[dl, dashed, bend left=10] & F_2 \arrow[l] & \cdots \arrow[l] \\
\mathbb{F}_p & F_0 \arrow[l, two heads] & F_1 \arrow[l] & F_2 \arrow[l] \arrow[dl, "\mu_2"'] \arrow[dl, dashed, bend left=10] & \cdots \arrow[l] \\
\mathbb{F}_p & F_0 \arrow[l, two heads] & F_1 \arrow[l] \arrow[dl, "(\psi_1)_1"'] \arrow[dl, dashed, bend left=10] & F_2 \arrow[l] & \cdots \arrow[l] \\
\mathbb{F}_p & F_0 \arrow[l, two heads, "\rho"'] & F_1 \arrow[l] & F_2 \arrow[l] & \cdots \arrow[l]
\end{tikzcd}$$

Using the formula for the Massey products, we now have a way of calculating these products using the Yoneda cocomplex. This will be put into use in section 5.6.

3.4 Massey products and extensions

In this section we will see how we can get the formulas for the Massey products by looking at extensions of modules. This can be viewed as the Yoneda cocomplex construction for $\mathrm{H}^1(G, \mathbb{F}_p)$ and $\mathrm{H}^2(G, \mathbb{F}_p)$.

Again, we will do this a bit more generally, so let A be a k-algebra (for us $k = \mathbb{F}_p$, $A = \mathbb{F}_p[G]$) and let $(V_i)_{i=1}^n$ be the family of the irreducible A-modules (for us $V_i = \mathbb{F}_p$ for all i). Lemma 2.12 tells us that $\mathrm{Hom}_k(V_i, V_j)$ has an A-bimodule structure for $i, j \in \{1, \dots, n\}$. We will use the Hochschild cocomplex $C^*(A, \mathrm{Hom}_k(V_i, V_j), \delta)$ in this section.

We have seen that Massey products are well-defined on cohomology classes so let $\xi_{ij} \in \mathrm{Ext}^1_A(V_i, V_j)$. Since ξ_{ij} is a 1-cocycle, it is also a derivation. The derivation will be called ψ_{ij}.

Now take $\xi_{jk} \in \mathrm{Ext}^1_A(V_j, V_k)$ with the corresponding derivation ψ_{jk}, and consider the Yoneda composition of ξ_{ij} and ξ_{jk}. We want to check that this is an element in $\mathrm{Ext}^2_A(V_i, V_k)$. We know that it corresponds to taking the composition, i.e. $\langle \xi_{ij}, \xi_{jk}; 0\rangle(a \otimes b) = \psi_{ij}(a)\psi_{jk}(b)$ so $\langle \xi_{ij}, \xi_{jk}; 0\rangle$ has a representative in $C^2(A, \mathrm{Hom}_k(V_i, V_k))$. Let $a, b, c \in A$, then we can check that $\delta^2\langle \xi_{ij}, \xi_{jk}; 0\rangle(a \otimes b \otimes c)(v_i) = 0$ using the Hochschild differential, the bimodule structure from lemma 2.12 and Leibniz' rule:

$$\begin{aligned}
& \delta^2\langle \xi_{ij}, \xi_{jk}; 0\rangle(a \otimes b \otimes c)(v_i) \\
= \;& a\langle \xi_{ij}, \xi_{jk}; 0\rangle(b \otimes c)(v_i) - \langle \xi_{ij}, \xi_{jk}; 0\rangle(ab \otimes c)(v_i) \\
& + \langle \xi_{ij}, \xi_{jk}; 0\rangle(a \otimes bc)(v_i) - \langle \xi_{ij}, \xi_{jk}; 0\rangle(a \otimes b)c(v_i) \\
= \;& (a(\psi_{ij}(b)\psi_{jk}(c)))(v_i) - \psi_{jk}(c)(a\psi_{ij}(b)(v_i)) - \psi_{jk}(c)(\psi_{ij}(a)b(v_i)) \\
& + b\psi_{jk}(c)(\psi_{ij}(a)(v_i)) + \psi_{jk}(b)c(\psi_{ij}(a)(v_i)) - ((\psi_{ij}(a)\psi_{jk}(b))c)(v_i) \\
= \;& \psi_{jk}(c)(\psi_{ij}(b)(v_i a)) - \psi_{jk}(c)(\psi_{ij}(b)(v_i a)) - \psi_{jk}(c)(\psi_{ij}(a)(v_i)b) \\
& + \psi_{jk}(c)(\psi_{ij}(a)(v_i)b) + \psi_{jk}(b)(\psi_{ij}(a)(v_i))c - \psi_{jk}(b)(\psi_{ij}(a)(v_i))c \\
= \;& 0.
\end{aligned}$$

What we have seen so far is that by starting with an extension

$$\begin{tikzcd} 0 \arrow[r] & V_j \arrow[r] & E_{ij} \arrow[r] & V_i \arrow[r] & 0 \end{tikzcd}$$

and by looking at the A-module structure on E_{ij}, we get a derivation ψ_{ij}. Then we add an extension E_{jk} and show that the splicing of these short-exact sequences gives an element in $\mathrm{Ext}^2_A(V_i, V_k)$ and the formula for the cup product. Using (2.12) in the proof of lemma 2.20, we see that the module structure on E_{ij} is given by

$$(v_j, v_i)a = (v_j a + \psi_{ij}(a)(v_i), v_i a).$$

Now consider the following diagram.

$$\begin{tikzcd}
 & \xi_{ij} & & & & \\
 & 0 \arrow[d] & & & & \\
0 & V_j \arrow[l] \arrow[d] \arrow[rr, dashed, bend left, "\psi_{jk}"] & E_{jk} \arrow[l] \arrow[d, hook] & V_k \arrow[l] \arrow[d, equal] & 0 \arrow[l] & \xi_{jk} \\
0 & E_{ij} \arrow[l] \arrow[d] & E_{ijk} \arrow[l] & V_k \arrow[l] \arrow[d, equal] & 0 \arrow[l] & \\
0 & V_i \arrow[l] \arrow[d] \arrow[uu, dashed, bend left, "\psi_{ij}"] & E_{ik} \arrow[l] & V_k \arrow[l] & 0 \arrow[l] & \\
 & 0 & & & &
\end{tikzcd}$$

Let us see what we need to have an A-module structure on E_{ijk}: As a vector space over k, $E_{ijk} \simeq (V_k \times V_j) \times V_i$, and since $E_{jk} \hookrightarrow E_{ijk}$ we know that

$$(v_k, v_j, 0)a = (v_k a + \psi_{jk}(a)(v_j), v_j a, 0).$$

Consider $(0, 0, v_i)a = (\bullet, \psi_{ij}(a)(v_i), v_i a)$ and put $\bullet = \psi_{ijk}(a)(v_i)$. Does there exist an element ψ_{ijk} such that we get an A-module structure on E_{ijk}? We need that

$$(0, 0, v_i)(a_1 a_2) = ((0, 0, v_i)a_1)a_2 \tag{3.8}$$

for $a_1, a_2 \in A$ and $v_i \in V_i$.
The left hand side in (3.8):

$$\begin{aligned}&(0, 0, v_i)(a_1 a_2)\\ =&(\psi_{ijk}(a_1 a_2)(v_i), \psi_{ij}(a_1 a_2)(v_i), v_i(a_1 a_2))\end{aligned}$$

The right hand side in (3.8):

$$\begin{aligned}&((0,0,v_i)a_1)a_2\\=&(\psi_{ijk}(a_1)(v_i),\psi_{ij}(a_1)(v_i),0)a_2+(0,0,v_ia_1)a_2\\=&(\psi_{ijk}(a_1)(v_i)a_2+\psi_{jk}(a_2)(\psi_{ij}(a_1)(v_i)),\psi_{ij}(a_1)(v_i)a_2,0)\\+&(\psi_{ijk}(a_2)(v_ia_1),\psi_{ij}(a_2)(v_ia_1),(v_ia_1)a_2)\end{aligned}$$

We see that the 3^{rd} coordinates are equal since V_i is an A-module, and the 2^{nd} coordinates are equal since ψ_{ij} is a derivation. This is typical for these calculations; all coordinates except one will be equal by the construction in the previous steps. So consider the 1^{st} coordinates:

$$\begin{aligned}&\psi_{ijk}(a_1a_2)(v_i)\\=&\psi_{ijk}(a_1)(v_i)a_2+\psi_{jk}(a_2)(\psi_{ij}(a_1)(v_i))+\psi_{ijk}(a_2)(v_ia_1)\\=&\psi_{ijk}(a_1)a_2(v_i)+\psi_{ij}\circ\psi_{jk}(a_1,a_2)(v_i)+a_1\psi_{ijk}(a_2)(v_i)\end{aligned}$$

which implies that

$$\begin{aligned}&\langle\psi_{ij},\psi_{jk};0\rangle(a_1,a_2)(v_i)\\=&-(a_1\psi_{ijk}(a_2)(v_i)-\psi_{ijk}(a_1a_2)(v_i)+\psi_{ijk}(a_1)a_2(v_i))\\=&-\delta^1\psi_{ijk}(a_1,a_2)(v_i).\end{aligned}$$

Conclusion: An A-module structure on E_{ijk} is given by

$$(v_k,v_j,v_i)a=(v_ka+\psi_{jk}(a)(v_j)+\psi_{ijk}(a)(v_i),v_ja+\psi_{ij}(a)(v_i),v_ia)$$

where $-\delta^1\psi_{ijk}(a_1,a_2)(v_i)=\psi_{ij}\circ\psi_{jk}(a_1,a_2)(v_i)$.

Let us assume that the product between ξ_{ij} and ξ_{jk} is zero, i.e. is δ of ψ_{ijk}, so that we have a module structure on E_{ijk}. Now we add a third extension

ξ_{kl} (extending V_k by V_l) and consider the following 3-dimensional diagram.

$$\begin{tikzcd}
 & & V_j \arrow[ddd, tail] & & & E_{jk} \arrow[lll, two heads] \arrow[lll, dotted, two heads, shift right=1.5] \arrow[ddd, hook, two heads] \arrow[dddlll, dashed, two heads, bend right] & & & V_k \arrow[lll, tail] \arrow[lll, dashed, tail, shift right=1.5] \arrow[ddd, equal] \\
 & E_{jl} \arrow[ur, two heads] & & & E_{jkl} \arrow[ur, two heads] \arrow[ddd, hook] \arrow[ddr, squiggly, two heads] & & & E_{kl} \arrow[lll, tail] \arrow[ur, two heads] \arrow[ull, dotted] \arrow[ddd, equal] & \\
V_l \arrow[ur, tail] \arrow[rrr, equal] \arrow[ddd, equal] & & & V_l \arrow[ur, tail] \arrow[rrr, equal] \arrow[ddd, equal] & & & V_l \arrow[ur, tail] \arrow[ur, dotted, shift right] \arrow[ull, dashed, squiggly] \arrow[ddd, equal] & & \\
 & & E_{ij} \arrow[ddd, two heads] \arrow[ddd, dashed, two heads, shift right=1.5] & & & E_{ijk} \arrow[lll, two heads] \arrow[dddlll, squiggly, bend left] & & & V_k \arrow[lll, tail] \arrow[ddd, equal] \\
 & E_{ijl} \arrow[ur, two heads] & & & E_{ijkl} \arrow[ur, two heads] & & & E_{kl} \arrow[ur, two heads] \arrow[ddd, equal] & \\
V_l \arrow[ur, tail] \arrow[rrr, equal] \arrow[ddd, equal] & & & V_l \arrow[ur, tail] \arrow[rrr, equal] \arrow[ddd, equal] & & & V_l \arrow[ur, tail] \arrow[ddd, equal] & & \\
 & & V_i & & & E_{ik} \arrow[lll, two heads] & & & V_k \arrow[lll, tail] \\
 & E_{il} \arrow[ur, two heads] & & & E_{ikl} \arrow[ur, two heads] & & & E_{kl} \arrow[ur, two heads] & \\
V_l \arrow[ur, tail] \arrow[rrr, equal] & & & V_l \arrow[ur, tail] \arrow[rrr, equal] & & & V_l \arrow[ur, tail] & &
\end{tikzcd}$$

The arrows $\dashrightarrow$ in the diagram draw the sequence which comes from the splicing of

$$0 \longrightarrow V_j \longrightarrow E_{ij} \longrightarrow V_i \longrightarrow 0 \text{ and } 0 \longrightarrow V_k \longrightarrow E_{jk} \longrightarrow V_j \longrightarrow 0\ .$$

We have assumed that this splice is zero in $\mathrm{Ext}^2_A(V_i, V_k)$, and from the diagram we can now explain what this means, as promised in section 2.7.1. Since we have a module structure on E_{ijk}, the sequence "factors" via E_{ijk}:

$$\begin{tikzcd}
 & & & E_{ijk} \arrow[dr] & & & \\
0 \arrow[r] & V_k \arrow[r] & E_{jk} \arrow[ur] \arrow[rr] & & E_{ij} \arrow[r] & V_i \arrow[r] & 0.
\end{tikzcd}$$

What conditions have to be satisfied for us to define an A-module structure on E_{ijkl} (the middle entry in the diagram)? As vector spaces over k, we have $E_{ijkl} \simeq (V_l \times V_k \times V_j) \times V_i$, and to find the module structure we only need to consider the "new" extensions we get in our diagram, because all the other conditions are included in the previous steps.
We know that

$$(v_l, v_k, v_j, 0)a = (v_l a + \psi_{kl}(a)(v_k) + \psi_{jkl}(a)(v_j), v_k a + \psi_{jk}(a)(v_j), v_j a, 0).$$

Consider

$$(0, 0, 0, v_i)a = (\bullet, \psi_{ijk}(a)(v_i), \psi_{ij}(a)(v_i), v_i a)$$

and put $\bullet = \psi_{ijkl}(a)(v_i)$. By comparing $(0, 0, 0, v_i)(a_1a_2)$ and $((0, 0, 0, v_i)a_1)a_2$ as in the previous step, we get that the 4^{th} coordinates are equal (V_i is an A-module), the 3^{rd} coordinates are equal (ψ_{ij} is a derivation, i.e. E_{ij} is an A-module) and the 2^{nd} coordinates are equal (the cup product $\langle \xi_{ij}, \xi_{jk}; 0\rangle$ is assumed to be zero, i.e. E_{ijk} is an A-module). For the 1^{st} coordinates to be equal, we need

$$\begin{aligned}
&\psi_{ijkl}(a_1a_2)(v_i)\\
=&\psi_{ijkl}(a_1)(v_i)a_2 + \psi_{kl}(a_2)(\psi_{ijk}(a_1)(v_i)) + \psi_{jkl}(a_2)(\psi_{ij}(a_1)(v_i)) + \psi_{ijkl}(a_2)(v_i a_1)
\end{aligned}$$

which implies

$$\psi_{kl}(a_2)(\psi_{ijk}(a_1)(v_i)) + \psi_{jkl}(a_2)(\psi_{ij}(a_1)(v_i)) = -\delta^1\psi_{ijkl}(a_1, a_2)(v_i). \tag{3.9}$$

Conclusion: First of all, we see that we also need an A-module structure on E_{jkl}, i.e. the product between ξ_{jk} and ξ_{kl} must be zero (the arrows $\dashrightarrow$ in the 3-dimensional diagram). So if the products $\langle \xi_{ij}, \xi_{jk}; 0\rangle$ and $\langle \xi_{jk}, \xi_{kl}; 0\rangle$ are both zero, then we can define an A-module structure on E_{ijkl} by

$$\begin{aligned}
&(v_l, v_k, v_j, v_i)a \\
=&(v_l a + \psi_{kl}(a)(v_k) + \psi_{jkl}(a)(v_j) + \psi_{ijkl}(a)(v_i), \\
&v_k a + \psi_{jk}(a)(v_j) + \psi_{ijk}(a)(v_i), \\
&v_j a + \psi_{ij}(a)(v_i), \\
&v_i a)
\end{aligned}$$

where ψ_{ijkl} satisfies (3.9).

We recognise the formula in (3.9) as the 3-fold Massey product. Assume $\langle \xi_{ij}, \xi_{jk}; 0\rangle = 0$ as an element in $\mathrm{Ext}^2_A(V_i, V_k)$ which means that there exists an element $\psi_{ijk} \in \mathrm{Hom}_k(A, \mathrm{Hom}(V_i, V_k))$ such that $\delta^1\psi_{ijk} = -\langle \xi_{ij}, \xi_{jk}; 0\rangle$. And assume $\langle \xi_{jk}, \xi_{kl}; 0\rangle = 0$, so we have an element $\psi_{jkl} \in \mathrm{Hom}_k(A, \mathrm{Hom}(V_j, V_l))$ such that $\delta^1\psi_{jkl} = -\langle \xi_{jk}, \xi_{kl}; 0\rangle$. Then

$$\langle \xi_{ij}, \xi_{jk}, \xi_{kl}; 0\rangle = -\psi_{ij} \circ \psi_{jkl} - \psi_{ijk} \circ \psi_{kl}.$$

This element in $\mathrm{Ext}^2_A(V_i, V_l)$ is represented by the arrows $\rightsquigarrow$ in the 3-dimensional diagram. So the formulas for the Massey products come from considering the elements that need to be zero in cohomology in order to build new extensions.

Remark 3.12 Remember that 1-cocycles correspond to derivations; hence whenever we have a ψ with two subscripts, it is a derivation and therefore a 1-cocycle. The ψ-s with more that two subscripts will be derivations when we assume that the Massey product they correspond to is zero. ■

Now assume that we have an A-module structure on E_{ijkl}, and we want to add an extension ξ_{lm} (extending V_l by V_m). We will make no attempt at drawing a diagram for this situation, but ask the reader to picture a 3-dimensional square spiral (i.e. "we draw a cube of 3^3 V_m-s and draw arrows"). By similar calculations as before, we need

$$\begin{aligned}
&\psi_{ijklm}(a_1a_2)(v_i)\\
=&\psi_{ijklm}(a_1)(v_i)a_2 + \psi_{ijklm}(a_2)(v_ia_1)\\
+&\psi_{lm}(a_2)(\psi_{ijkl}(a_1a_2)(v_i)) + \psi_{klm}(a_2)(\psi_{ijk}(a_1a_2)(v_i))\\
+&\psi_{jklm}(a_2)(\psi_{ij}(a_1a_2)(v_i))
\end{aligned}$$

to define an A-module structure on E_{ijklm}.

From the formula

$$\begin{aligned}
&\psi_{lm}(a_2)(\psi_{ijkl}(a_1a_2)(v_i)) + \psi_{klm}(a_2)(\psi_{ijk}(a_1a_2)(v_i)) + \psi_{jklm}(a_2)(\psi_{ij}(a_1a_2)(v_i))\\
=&-\delta^1\psi_{ijklm}(a_1,a_2)(v_i)
\end{aligned}$$

we recognise the 4-fold Massey product from the formula in definition 3.3. Assume that the products $\langle\xi_{ij},\xi_{jk};0\rangle$, $\langle\xi_{jk},\xi_{kl};0\rangle$ and $\langle\xi_{kl},\xi_{lm};0\rangle$ are all zero. Then we know that we can define the 3-fold Massey products $\langle\xi_{ij},\xi_{jk},\xi_{kl};0\rangle$ and $\langle\xi_{jk},\xi_{kl},\xi_{lm};0\rangle$. Assume that these two Massey products are also zero as elements in $\operatorname{Ext}^2_A(V_i,V_l)$ and $\operatorname{Ext}^2_A(V_j,V_m)$ respectively, i.e. we have a module structure on E_{ijkl} and E_{jklm}. Then there exist $\psi_{ijkl}\in\operatorname{Hom}_k(A,\operatorname{Hom}_k(V_i,V_l))$ such that $\delta^1\psi_{ijkl}=-\langle\xi_{ij},\xi_{jk},\xi_{kl};0\rangle$ and $\psi_{jklm}\in\operatorname{Hom}_k(A,\operatorname{Hom}_k(V_j,V_m))$ such that $\delta^1\psi_{jklm}=-\langle\xi_{jk},\xi_{kl},\xi_{lm};0\rangle$. We have the formula

$$\langle\xi_{ij},\xi_{jk},\xi_{kl},\xi_{lm};0\rangle = -\psi_{ij}\circ\psi_{jklm} - \psi_{ijk}\circ\psi_{klm} - \psi_{ijkl}\circ\psi_{lm}.$$

This procedure goes on to give us the formula for a general Massey product as in the formula in definition 3.3. When we are building modules like this we want a module structure on each step, and so the Massey products we get here are strictly defined.

Remark 3.13 The Yoneda construction can only be used for strictly defined products, since we in this situation know that the product exists because we have cochains to use. In other words, our defining systems are particularly nice for these products.

We have shown that if our product is strictly defined, then we get a certain module structure. However, we don't know whether we have the whole Massey product structure. If we did, we would have been able to build the whole module category. ■

3.5 The Bockstein operation

There is one more thing we need to introduce before we start putting things together. Since we work in characteristic p, we would expect to get some special p-fold products (and (power of p)-fold products), and indeed we do:

Let $\xi_i \in \mathrm{H}^1(G, \mathbb{F}_p)$. If we consider $\langle \xi_i, \xi_i, \dots, \xi_i; 0\rangle$, we may restrict the defining system to get a restricted operation, see [22, page 440]. The defining system M in example 3.9 is such a restricted system for $\langle \xi_1, \xi_1, \xi_1; 0\rangle$.

Theorem 3.14 *In characteristic p the restricted product $\langle \underbrace{\xi_i, \xi_i, \dots, \xi_i}_{p}; 0\rangle$, denoted $\langle \xi_i; 1\rangle$, is the first such product that can be non-zero. Moreover, it is defined as a single class of $\mathrm{H}^2(G, \mathbb{F}_p)$, i.e. it has no indeterminacy.*

Proof: See Kraines, [22, Theorems 15 and 17]. □

We consider the following short-exact sequence of abelian groups

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z}/p\mathbb{Z} \longrightarrow 0. \tag{3.10}$$

To the sequence (3.10) there exist connecting homomorphisms ϕ and β such that we get a long-exact sequence in cohomology, see for example [18]:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^0(G,\mathbb{Z}/p\mathbb{Z}) \arrow[r] & \mathrm{H}^0(G,\mathbb{Z}/p^2\mathbb{Z}) \arrow[r] & \mathrm{H}^0(G,\mathbb{Z}/p\mathbb{Z}) \arrow[dll, rounded corners, "0"] \\
 & \mathrm{H}^1(G,\mathbb{Z}/p\mathbb{Z}) \arrow[r] & \mathrm{H}^1(G,\mathbb{Z}/p^2\mathbb{Z}) \arrow[r] & \mathrm{H}^1(G,\mathbb{Z}/p\mathbb{Z}) \arrow[dll, rounded corners, "\beta"] \\
 & \mathrm{H}^2(G,\mathbb{Z}/p\mathbb{Z}) \arrow[r] & \mathrm{H}^2(G,\mathbb{Z}/p^2\mathbb{Z}) \arrow[r] & \cdots
\end{tikzcd}$$

Definition 3.15 *The map* $\beta: \mathrm{H}^1(G,\mathbb{F}_p) \longrightarrow \mathrm{H}^2(G,\mathbb{F}_p)$ *is called the first order Bockstein operation.*

Theorem 3.16 *The restricted p-fold product and the first order Bockstein operation are the same, i.e.*

$$\langle \xi_i; 1\rangle = -\beta(\xi_i). \tag{3.11}$$

Proof: We note again that the Steenrod operations don't do anything for $\mathrm{H}^1(G,\mathbb{F}_p)$ and $\mathrm{H}^2(G,\mathbb{F}_p)$, i.e. P^0 is the identity operation, see [3, page 138]. Combining this fact with Kraines' theorem 14 in [22] we have the result. □

Putting it the other way around, the Bockstein operation is a Massey product. We will use $\langle -; 1\rangle$ to denote both products. The sign will not make a difference for our purposes.

Now, if $\langle \xi_i; 1\rangle$ is 0 as an element in $\mathrm{H}^2(G,\mathbb{F}_p)$, we can define $\langle \xi_i; 2\rangle$, which is a p^2-fold restricted product etc.. In this way the restricted product is seen to be a strictly defined Massey product:

Definition 3.17 *We say that the product* $\langle \xi_i; k\rangle$ *is defined for* $k \geq 1$ *if* $\langle \xi_i; l\rangle$ *is defined and contains only zero for all* $l < k$.

Kraines' theorem 19 in [22] tells us that the p^k-fold restricted product

$$\langle -; k\rangle : \ \mathrm{H}^1(G, \mathbb{F}_p) \longrightarrow \mathrm{H}^2(G, \mathbb{F}_p) \tag{3.12}$$

has no indeterminacy, and is equal to $-\beta_k$, the Bockstein operation associated to the short exact sequence

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p^{k+1}\mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z}/p^k\mathbb{Z} \longrightarrow 0. \tag{3.13}$$

We note that the Bockstein operation β_k goes from $\mathrm{H}^1(G, \mathbb{F}_p)$ to $\mathrm{H}^2(G, \mathbb{F}_p)$ for all k. We show how this is done in the proof of theorem 4.3. For the statement above we also note that Kraines assumes naturality and works with the first and second cohomology groups for cyclic groups rather than a general p-group G.

To summarise, in characteristic p we have

$$\langle -; r\rangle = \text{ the restricted product } \langle \underbrace{-, -, \ldots, -}_{p^r}; 0\rangle \quad \text{for } r \geq 1. \tag{3.14}$$

In particular, in characteristic 2 we get $\langle -; 1\rangle = \langle -, -; 0\rangle$.

So the Bockstein operations help us keep track of some of the Massey products. In the next chapter we will be interested in these restricted products and the strictly defined Massey products from definition 3.6.

Chapter 4

Cohomological presentations of p-groups

In this chapter we will concentrate on a part of the Massey product structure on $\mathrm{H}^1(G, \mathbb{F}_p)$ and $\mathrm{H}^2(G, \mathbb{F}_p)$, namely the strictly defined products, which include the Bockstein operations.

We will use obstruction theory in the category of pro-p groups to find what relations in a presentation of G the above mentioned products correspond to. Once we have this, we can then study p-groups given by these relations from a cohomological point of view.

4.1 Testgroups and defining systems

Denote by $\{\Gamma_i(G)\}_{i\geq 0}$ the lower central p-series for G, where

$$\begin{aligned}
\Gamma_0(G) &= G; \\
\Gamma_1(G) &= [G, G]G^p; \\
\Gamma_k(G) &= [\Gamma_{k-1}(G), G](\Gamma_{k-1}(G))^p.
\end{aligned}$$

The quotients in this series are elementary abelian p-groups. Moreover, using commutator identities, we can show the following lemma.

Lemma 4.1 *Let G be a group generated by $x_1, \dots, x_n$. Then the elementary abelian p-group $\Gamma_k(G)/\Gamma_{k+1}(G)$ is generated by elements of the form*

$$[[x_{i_1}, x_{i_2}], \dots, x_{i_s}]^{p^r}$$

where $1 \leq i_t \leq n$, $t = 1, \dots, s$ and $s + r = k + 1$.

Proof: See [29, page 295] for the result in the case of the lower central series. □

We now introduce some canonical groups $U(s, r)$, called testgroups, which will be used in the interpretation of the Massey products. Let $U(s, r)$ be the group of upper triangular $(s + 1) \times (s + 1)$-matrices with elements from $\mathbb{Z}/p^{r+1}\mathbb{Z}$ and 1-s on the diagonal, i.e.

$$U(s,r) = \left\{ \left. \begin{pmatrix} 1 & * & * & \cdots & * \\ 0 & 1 & * & \ddots & \vdots \\ 0 & 0 & 1 & \ddots & * \\ \vdots & \ddots & \ddots & \ddots & * \\ 0 & \cdots & 0 & 0 & 1 \end{pmatrix} \right| * \in \mathbb{Z}/p^{r+1} \right\}.$$

We see that the elements $\{u_i\}_{i=1}^{s} = \{I_{s+1} + e_{i,i+1}\}_{i=1}^{s}$ will generate $U(s, r)$. Let us have a look at the lower central p-series for $U(s, r)$:

- For $0 \leq n \leq r$, we have that

$$\Gamma_n(U(s,r)) = \left\{ \left. \begin{pmatrix} 1 & p^n * & p^{n-1} * & \cdots & p^{n-s+1} * \\ 0 & 1 & p^n * & \ddots & \vdots \\ 0 & 0 & 1 & \ddots & p^{n-1} * \\ \vdots & \ddots & \ddots & \ddots & p^n * \\ 0 & \cdots & 0 & 0 & 1 \end{pmatrix} \right| \begin{array}{l} * \in \mathbb{Z}/p^{r+1}\mathbb{Z}; \\ p^j * = * \text{ for } j \leq 0 \end{array} \right\}.$$

Loosely speaking, for $0 \leq n \leq r$, we push the commutators towards the upper right corner, and for $n \geq r + 1$, we start pushing the p^{th} powers as well, till we get the identity matrix.

- For $r+1 \leq n \leq s+r$, we have

$$\Gamma_n(U(s,r)) = \left\{ \begin{pmatrix} 1 & p^n* & p^{n-1}* & \cdots & p^{n-s+1}* \\ 0 & 1 & p^n* & \ddots & \vdots \\ 0 & 0 & 1 & \ddots & p^{n-1}* \\ \vdots & \ddots & \ddots & \ddots & p^n* \\ 0 & \cdots & 0 & 0 & 1 \end{pmatrix} \middle| \begin{array}{l} * \in \mathbb{Z}/p^{r+1}\mathbb{Z}; \\ p^j* = * \text{ for } j \leq 0; \\ p^j* = 0 \text{ for } j \geq r+1 \end{array} \right\}.$$

This holds for $0 \leq n \leq r$ as well, but we want to make clear when the zeros start appearing. We see that we have the identity matrix I_{s+1} when $n-s+1 = r+1$, i.e. $n = r+s$. For $r+s = k+1$ we therefore have $\Gamma_{k+1}(U(s,r)) = I_{s+1}$ and

$$\Gamma_k(U(s,r)) = \left\{ \begin{pmatrix} 1 & 0 & 0 & \cdots & p^r* \\ 0 & 1 & 0 & \ddots & \vdots \\ 0 & 0 & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 0 & 1 \end{pmatrix} \middle| * \in \mathbb{Z}/p^{r+1}\mathbb{Z} \right\},$$

hence $\Gamma_k(U(s,r))/\Gamma_{k+1}(U(s,r)) \simeq \mathbb{F}_p$.

Using lemma 4.1, the quotients $\Gamma_n(U(s,r))/\Gamma_{n+1}(U(s,r))$ are generated by (the images of) the elements

$$u_{i,j,t} = [[u_i, u_{i+1}], \ldots, u_j]^{p^t}$$

where $j-i+t = n$, $1 \leq i \leq \cdots \leq j \leq s$ and $0 \leq t \leq r$. In particular, we see that for $k+1 = s+r$, we have $n-s+1 = r$ in $\Gamma_k/\Gamma_{k+1}(U(s,r))$, i.e. $j-i = s-1$, so $\Gamma_k/\Gamma_{k+1}(U(s,r)) \simeq \mathbb{F}_p$ is generated by the element $u_{1,s,r} = [[u_1, u_2], \ldots, u_s]^{p^r}$.

We will now consider the groups $U(s,0)$. Then $\Gamma_{s-1}(U(s,0))$ consists of matrices which are identically zero except for 1-s on the diagonal and elements from $\mathbb{Z}/p\mathbb{Z}$ in the $(1,s+1)$-entry. We are now in the situation Dwyer considers in his paper, see [13, page 182], with $U(R,n)=U(s,0)$ and $Z(R,n)=\Gamma_{s-1}(U(s,0))$. We give our version of Dwyer's theorem 2.4 (the change of sign appears since we use Kraines' sign convention).

Theorem 4.2 *Let* $\xi_1,\dots,\xi_s$ *be elements in* $\mathrm{H}^1(G,\mathbb{F}_p)$. *There is a one-one correspondence* $M\longleftrightarrow\phi_M$ *between defining systems* M *for* $\langle\xi_1,\dots,\xi_s;0\rangle$ *and group homomorphisms*

$$\phi_M:\ G\longrightarrow U(s,0)/\Gamma_{s-1}(U(s,0))$$

which have $\xi_1,\dots,\xi_s$ *on the superdiagonal (in the order given, i.e. the entry* $(i,i+1)$ *is* ξ_i*). Moreover,* $\langle\xi_1,\dots,\xi_s;0\rangle_M=0$ *in* $\mathrm{H}^2(G,\mathbb{F}_p)$ *if and only if the dotted arrow exists in the following diagram.*

$$\begin{tikzcd}
U(s,0) \arrow[r, two heads] & U(s,0)/\Gamma_{s-1}(U(s,0)) \\
 & G \arrow[u, "\phi_M"'] \arrow[ul, dotted]
\end{tikzcd}$$

Proof: Let M be a defining system for $\langle\xi_1,\dots,\xi_s;0\rangle$, i.e we have a collection of 1-cochains m_{ij} for $1\le i<j\le s+1$ and $(i,j)\neq(1,s+1)$ with

$$m_{i,i+1}=\xi_i \text{ for } i=1,\dots,s; \tag{4.1}$$

$$\partial m_{ij}=\sum_{k=i+1}^{j-1}-m_{ik}\cup m_{kj} \text{ for } j\neq i+1. \tag{4.2}$$

On the other hand, a group homomorphism $\phi:\ G\longrightarrow U(s,0)/\Gamma_{s-1}(U(s,0))$ is given by a component array $\phi_{ij}, 1\le i<j\le s+1$, of set maps $G\longrightarrow\mathbb{Z}/p\mathbb{Z}$

satisfying

$$\phi_{ij}(g_1g_2) = \phi_{ij}(g_1) + \phi_{ij}(g_2) + \sum_{k=i+1}^{j-1} \phi_{ik}(g_1)\phi_{kj}(g_2) \tag{4.3}$$

for $g_1, g_2 \in G$. We see that $\phi_{i,i+1}$ for $i = 1, \dots, s$ are group homomorphisms $G \longrightarrow \mathbb{Z}/p\mathbb{Z}$, and hence cohomology classes in $\mathrm{H}^1(G, \mathbb{F}_p)$.

So if we have a defining system M we can use the collection of 1-cochains to get a group homomorphism ϕ by putting $\phi_{ij} = m_{ij}$ and vice versa. Then $\phi_{i,i+1} = \xi_i$ by 4.1. To go between 4.2 and 4.3 we rewrite 4.3

$$\phi_{ij}(g_1) - \phi_{ij}(g_1g_2) + \phi_{ij}(g_2) = \sum_{k=i+1}^{j-1} -\phi_{ik}(g_1)\phi_{kj}(g_2). \tag{4.4}$$

We recognise the left hand side as $\delta^1\phi_{ij}(g_1, g_2)$. Here we use formula 2.16 from the bar resolution.

The right hand side is recognised as $\sum_{k=i+1}^{j-1} -\langle \phi_{ik}, \phi_{kj}; 0\rangle(g_1, g_2)$ via the Alexander-Whitney map in 3.4. So 4.4 gives 4.2.

For the proof of the second part of the theorem, we note that

$$\Gamma_{s-1}(U(s, 0)) \simeq \mathbb{F}_p,$$

so we are in the situation (2.18) and can apply theorem 2.27 with $v(M) = \mathrm{obs}_G(\phi_M)$. □

If we write the short exact sequences defining the various Bockstein maps, for example 3.10 and 3.13, using our testgroups, we can formulate an analogous result to theorem 4.2. It says that if $\langle \xi_i; k\rangle$ is defined and is nonzero, then we have a group homomorphism from G into $\mathbb{Z}/p^k\mathbb{Z}$ and it cannot be lifted to $\mathbb{Z}/p^{k+1}\mathbb{Z}$. The proof will summarise the various information we have given on the restricted product in section 3.5. Observe that $U(1, r)/\Gamma_r(U(1, r)) \simeq \mathbb{Z}/p^r\mathbb{Z}$ and that $U(1, r) \simeq \mathbb{Z}/p^{r+1}\mathbb{Z}$.

Theorem 4.3 *Let* $\xi_i \in \mathrm{H}^1(G, \mathbb{F}_p)$*. Then* $\langle \xi_i; r\rangle$ *is defined if and only if there is a group homomorphism*

$$\phi_r : \; G \longrightarrow U(1,r)/\Gamma_r(U(1,r))$$

lifting ϕ_{r-1} *for* $r \geq 2$ *with* $\phi_1 = \xi_i$*. In particular,* $\langle \xi_i; r\rangle = 0$ *in* $\mathrm{H}^2(G, \mathbb{F}_p)$ *if and only if the dotted arrow exists in the following diagram.*

$$\begin{tikzcd}
U(1,r) \arrow[r, two heads] & U(1,r)/\Gamma_r(U(1,r)) \\
 & G \arrow[u, "\phi_r"'] \arrow[ul, dotted, "\phi_{r+1}"]
\end{tikzcd}$$

Proof: We observe that $U(1,1)/\Gamma_1(U(1,1)) \simeq \mathbb{F}_p$, $\mathrm{H}^1(G, \mathbb{F}_p) \simeq \mathrm{Hom}(G, \mathbb{F}_p^+)$ and $\langle \xi_i; 1\rangle$ is always defined. By definition, $\langle \xi_i; 2\rangle$ is defined if $\langle \xi_i; 1\rangle$ is 0. The operation $\langle -; 1\rangle$ is the Bockstein operation, which again is the connecting homomorphism in the long-exact sequence from 3.10:

$$\begin{tikzcd}
\cdots \arrow[r] & \mathrm{H}^1(G, \mathbb{Z}/p\mathbb{Z}) \arrow[r] & \mathrm{H}^1(G, \mathbb{Z}/p^2\mathbb{Z}) \arrow[r, "(\cdot p)^*"] & \mathrm{H}^1(G, \mathbb{Z}/p\mathbb{Z}) \arrow[dlll, rounded corners, "\langle -;1\rangle"] \\
 & \mathrm{H}^2(G, \mathbb{Z}/p\mathbb{Z}) \arrow[r] & \mathrm{H}^2(G, \mathbb{Z}/p^2\mathbb{Z}) \arrow[r] & \cdots
\end{tikzcd}$$

So if $\langle -; 1\rangle = 0$, then by exactness we have an element $\phi_2 \in \mathrm{H}^1(G, \mathbb{Z}/p^2\mathbb{Z})$ such that $(\cdot p)^*(\phi_2) = \xi_i$.

Now assume that $\langle \xi_i; k\rangle = 0$ for $k < r$, then the maps

$$\mathrm{H}^1(G, \mathbb{Z}/p^k\mathbb{Z}) \longrightarrow \mathrm{H}^2(G, \mathbb{Z}/p\mathbb{Z})$$

in the long-exact sequences send ϕ_k to 0. If we intertwine the $(r-1)$st and the rth long-exact sequences, we get the diagram

$$\begin{tikzcd}
 & & \mathrm{H}^1(G,\mathbb{Z}/p^{r-1}\mathbb{Z}) \arrow[rd, squiggly, "\phi_{r-1}\mapsto 0"] & & \\
\cdots \arrow[r] & \mathrm{H}^1(G,\mathbb{Z}/p^{r+1}\mathbb{Z})_{\ni\phi_{r+1}} \arrow[r] & \mathrm{H}^1(G,\mathbb{Z}/p^{r}\mathbb{Z})_{\ni\phi_{r}} \arrow[r, "\alpha"] \arrow[u, squiggly] & \mathrm{H}^2(G,\mathbb{Z}/p\mathbb{Z}) \arrow[r] \arrow[d, squiggly] & \cdots \\
 & & \mathrm{H}^1(G,\mathbb{Z}/p\mathbb{Z}) \arrow[u, squiggly] \arrow[ru, "\xi_i\mapsto\langle\xi_i;r\rangle"'] & \mathrm{H}^2(G,\mathbb{Z}/p^{r}\mathbb{Z}) \arrow[d, squiggly] & \\
 & & \vdots \arrow[u, squiggly] & \vdots &
\end{tikzcd}$$

from which we see that ϕ_r exists and lifts ϕ_{r-1} iff $\langle\xi_i;r\rangle$ is defined. In particular, if $\langle\xi_i;r\rangle = 0$ then $\alpha(\phi_r) = 0$ and by exactness there is an element $\phi_{r+1} \in \mathrm{H}^1(G,\mathbb{Z}/p^{r+1}\mathbb{Z})$. ☐

4.2 Strictly defined Massey products and group relations

We have introduced the Massey products on $\mathrm{H}^*(G,\mathbb{F}_p)$, and in particular the Massey products between $\mathrm{H}^1(G,\mathbb{F}_p)$ and $\mathrm{H}^2(G,\mathbb{F}_p)$. We will now use the results in the previous section to show how we can relate strictly defined Massey products to relations in our group.

We now fix the following notation: We let $\{\xi_1,\ldots,\xi_d\}$ be a basis for $\mathrm{H}^1(G,\mathbb{F}_p)$, $\{\eta_1,\ldots,\eta_t\}$ be a basis for $\mathrm{H}^2(G,\mathbb{F}_p)$ and form the free pro-p groups T^1 and T^2 on a dual basis for $\mathrm{H}^1(G,\mathbb{F}_p)$ and $\mathrm{H}^2(G,\mathbb{F}_p)$ respectively. This was introduced by Laudal, see [23]. I.e. if F is the free group generated by $\{\xi_1^*,\ldots,\xi_d^*\}$ we have

$$T^1 = \varprojlim_k (F/\Gamma_k(F))$$

and similarly for T^2, where F is the free group on $\{\eta_1^*,\ldots,\eta_t^*\}$. From the sequence 2.20 and theorem 2.30 we get a short exact sequence of pro-p groups

$$\begin{tikzcd}
1 \arrow[r] & T^2 \arrow[r, "o_G"] & T^1 \arrow[r] & G \arrow[r] & 1.
\end{tikzcd}$$

So we have the existence of the pro-p morphism $\mathrm{o}_G : T^2 \longrightarrow T^1$ and

$$G \simeq T^1/\overline{\langle \mathrm{im}\, \mathrm{o}_G \rangle},$$

where $\overline{\langle \mathrm{im}\, \mathrm{o}_G \rangle}$ denotes the normal closure of $\langle \mathrm{im}\, \mathrm{o}_G \rangle$ in T^1.

We have seen and used, in sections 4.1 and 2.7.4, the fact that elements in $\mathrm{H}^2(G, \mathbb{F}_p)$ are obstructions for lifting group homomorphisms. We want to use obstruction theory to construct o_G, but we can't start lifting if we don't have anywhere to start. However, since

$$T^1/\Gamma_1(T^1) \simeq G/\Gamma_1(G) \tag{4.5}$$

we have a diagram to start us off (this is special for p-groups!), namely

$$\begin{tikzcd}
1 \arrow[r] & \Gamma_1(T^1)/\Gamma_2(T^1) \arrow[r] & T^1/\Gamma_2(T^1) \arrow[r] & T^1/\Gamma_1(T^1) \arrow[r] & 1. \\
 & & & G \arrow[u, two heads] &
\end{tikzcd}$$

And so we can use theorem 2.27 successively to construct o_G as the inverse limit of o_n-s from T^2 into quotients of T^1, see [23]. In this way, using obstruction theory on the lower central p-series of T^1, we get a structure theorem for pro-p groups:

Theorem 4.4 *The obstructions give rise to a morphism between pro-p groups*

$$\mathrm{o}_G : \; T^2 \to T^1$$

and an isomorphism $G \simeq T^1/\overline{\langle \mathrm{im}\, \mathrm{o}_G \rangle}$.

Proof: See Laudal, [23, page 10]. □

The question we will address here is "How much of o_G can we calculate using strictly defined Massey products?"

Note that $\Gamma_0(G) = G$. We have the canonical maps

$$T^1/\Gamma_i(T^1) \xrightarrow{\pi_i} G/\Gamma_i(G) \tag{4.6}$$

with π_1 being an isomorphism. The obstruction calculus determines the kernels of the π_i, starting with $i = 1$ and working upwards in such a way that $\overline{\langle \operatorname{im} \mathrm{o}_G \rangle}$ will include all the obstructions on each level. For finite p-groups, this process will end after finitely many steps

If we pick an η_j^* and consider a basis for $\Gamma_k(T^1)/\Gamma_{k+1}(T^1)$ using left-normed commutators and pth powers as in lemma 4.1, we have that $\mathrm{o}_G(\eta_j^*)$ can be expressed on the form

$$\mathrm{o}_G(\eta_j^*) = \prod_{k \geq 1} \Big(\prod_{\underline{i}, r} [\cdots [\xi_{i_1}^*, \xi_{i_2}^*], \ldots, \xi_{i_s}^*]^{p^r c(\underline{i}, r, j)} \Big) \tag{4.7}$$

where $s + r = k + 1$, $1 \leq i_t \leq d$, $t = 1, \ldots, s$ and $0 \leq c(\underline{i}, r, j) \leq p - 1$.

We will now show how we can determine the $c(\underline{i}, r, j)$-s from the Massey products in the two cases

$$r = 0, s \geq 2, \tag{4.8}$$

$$r \geq 1, s = 1, \tag{4.9}$$

and we will concentrate on the strictly defined products

$$\langle -, -, \cdots, -; 0 \rangle \text{ from definition 3.6,} \tag{4.10}$$

$$\langle -; r \rangle \text{ from definition 3.17.} \tag{4.11}$$

We have the following theorem linking (4.8) and (4.10).

Theorem 4.5 *Let $\{\xi_1, \ldots, \xi_d\}$ and $\{\eta_1, \ldots, \eta_t\}$ be a basis for $\mathrm{H}^1(G, \mathbb{F}_p)$ and $\mathrm{H}^2(G, \mathbb{F}_p)$ respectively and let*

$$\langle \xi_{i_1}, \ldots, \xi_{i_s}; 0 \rangle = \sum_{j=1}^{t} \alpha_j \eta_j$$

be a strictly defined Massey product. Then, referring to (4.7), $c(\underline{i}, 0, j) = \alpha_j$ where $\underline{i} = (i_1, \ldots, i_s)$, $s \geq 2$. Hence we get a correspondence between the *product* $\langle \xi_{i_1}, \ldots, \xi_{i_s}; 0\rangle$ *and the commutator* $[\xi_{i_1}^*, \ldots, \xi_{i_s}^*]$.

Proof: Consider $U(s,0)$ and observe that $U(s,0)/\Gamma_1(U(s,0)) \simeq \mathbb{F}_p^s$. We have

$$\mathrm{H}^1(G,\mathbb{F}_p) \otimes_{\mathbb{F}_p} U(s,0)/\Gamma_1(U(s,0)) \simeq \mathrm{Mor}(T^1, U(s,0)/\Gamma_1(U(s,0)). \tag{4.12}$$

We will proceed by induction on s, so first let $s = 2$ ($s = 1$ comes under (4.9)). Then our product is the Yoneda composition which is always defined. By (4.12), a morphism $T^1 \longrightarrow U(s,0)/\Gamma_1(U(s,0))$ will correspond to elements in $\mathrm{H}^1(G,\mathbb{F}_p)$, so pick $\xi_1, \xi_2 \in \mathrm{H}^1(G,\mathbb{F}_p)$ and consider the morphism

$$\begin{array}{rcl}
\psi_1 : \ T^1 & \longrightarrow & U(2,0)/\Gamma_1(U(2,0)) \\
\xi_1^* & \longmapsto & \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
\xi_2^* & \longmapsto & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \\
\xi_i^* & \longmapsto & 1 \ \text{ for } i \neq 1, 2.
\end{array}$$

From (4.7) we see that $\psi_1(\mathrm{o}_G(\eta_j^*)) = 0 \ \forall \ j \in \{1, \ldots, t\}$, which means that the composition $\psi_1 \circ \mathrm{o}_G$ is trivial, so we get a factorisation of ψ_1 via G, and hence a group homomorphism $\phi_1 : \ G \longrightarrow U(2,0)/\Gamma_1(U(2,0))$.

By theorem 4.2 we have a defining system for $\langle \xi_1, \xi_2; 0\rangle$ since we will have ξ_1 and ξ_2 on the superdiagonal. We note that in the base step, our product is always defined, and the defining system is already uniquely determined. Now, since T^1 is free, we have a lifting of ψ_1 to $\psi_2 : \ T^1 \longrightarrow U(2,0)$, and since $\psi_1 \circ \mathrm{o}_G$ is trivial we get that $\psi_2 \circ \mathrm{o}_G : \ T^2 \longrightarrow \Gamma_1(U(2,0))$. We have the diagram

$$\begin{tikzcd}
 & & & 1 \arrow[d] \\
 & & & \Gamma_1(U(2,0)) \arrow[d] \\
 & & & U(2,0) \arrow[d, "\pi"] \\
T^2 \arrow[r, "\mathrm{o}_G"] \arrow[uurrr, dashed, "\psi_2 \circ \mathrm{o}_G"] & T^1 \arrow[rr, "\psi_1"] \arrow[urr, "\psi_2"] \arrow[dr, bend right] & & U(2,0)/\Gamma_1(U(2,0)) \arrow[d] \\
 & & G \arrow[ur, bend right, "\phi_1"'] & 1
\end{tikzcd}$$

What happens to $\mathrm{o}_G(\eta_j^*)$ under the lifting ψ_2? Well, from (4.7) and the diagram above we see that

$$\psi_2(\mathrm{o}_G(\eta_j^*)) = \begin{pmatrix} 1 & 0 & c(\underline{i}, 0, j) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where $\underline{i} = \{1, 2\}$. Moreover, by properties of the dual operator on finite dimensional vector spaces,

$$\psi_2(\mathrm{o}_G(\eta_j^*)) = \eta_j^*(\psi_2 \circ \mathrm{o}_G). \tag{4.13}$$

Using (4.12) on T^2 and $U(2,0) \simeq \mathbb{F}_p$, we have that the map $\psi_2 \circ \mathrm{o}_G$ gives us an element in $\mathrm{H}^2(G, \mathbb{F}_p)$. This will be the value of our defining system, since it is constructed from ψ_1, so

$$\eta_j^*(\langle \xi_1, \xi_2; 0\rangle = c(\{1, 2\}, 0, j)$$

and therefore if $\langle \xi_1, \xi_2; 0\rangle = \sum_{j=1}^{t} \alpha_j \eta_j$, $(\{1, 2\}, j, 0) = \alpha_j$, which finishes the base step.

Now, let $\langle \xi_1, \ldots, \xi_s; 0\rangle$ be a strictly defined Massey product , $s \geq 3$, which means $\langle \xi_i, \ldots, \xi_k; 0\rangle = 0$ for $1 \leq k - i \leq s - 2$. Then, by induction, $\mathrm{o}_G(\eta_j^*)$ have no commutators involving $[\cdots[\xi_i^*, \ldots], \xi_k^*]$ occurring.

Using (4.12), we are lead to consider a morphism

$$\begin{array}{rccl} \psi_1 : & T^1 & \longrightarrow & U(s,0)/\Gamma_1(U(s,0)) \\ & \xi_i^* & \longmapsto & \begin{cases} u_i & \text{for } i = 1, \ldots, s \\ 1 & \text{otherwise.} \end{cases} \end{array}$$

As before, ψ_1 sends $\mathrm{o}_G(\eta_j^*)$ to 1, and so it factors via G, giving

$$\phi_1 : \; G \longrightarrow U(s,0)/\Gamma_1(U(s,0)) \,.$$

Let ψ_2 be the lifting from T^1, which always exists. By assumption, all the Yoneda compositions $\langle \xi_i, \xi_{i+1}; 0\rangle$ are trivial, and also note that $[u_i, u_k] = 1$ for $k \neq i + 1$. Hence ψ_2 also sends $\mathrm{o}_G(\eta_j^*)$ to 1, and so ψ_2 factors via G to give

$$\phi_2 : \; G \longrightarrow U(s,0)/\Gamma_2(U(s,0)) \,.$$

Again, the lifting $\psi_3 : \; T^1 \longrightarrow U(s,0)/\Gamma_3(U(s,0))$ always exists. In general, we get $\psi_m(\mathrm{o}_G(\eta_j^*)) = 1$ for $m \leq s - 1$. This is because $\langle \xi_i, \ldots, \xi_k; 0\rangle = 0$ for $1 \leq k - i \leq s - 2$ and all k-length commutators with u_i-s for $k \leq s - 1$ with index set of the u_i-s in the commutator $\neq \{i, i+1, \ldots, k\}$ is 0. So for strictly defined products, this set-up singles out the relation we want.

We continue getting ψ_i-2 and ϕ_i-s till we get to $U(s,0)/\Gamma_{s-1}(U(s,0))$. The map ψ_{s-1} factors via G to give ϕ_{s-1}, but for the lifting ψ_s, we now get

$$\psi_s(\mathrm{o}_G(\eta_j^*)) = \begin{pmatrix} 1 & 0 & \cdots & 0 & c(\underline{i}, 0, j) \\ 0 & 1 & \ddots & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

where $\underline{i} = \{1, \ldots, s\}$. The map ϕ_{s-1} will, again by theorem 4.2, give a defining system for the Massey product $\langle \xi_1, \ldots, \xi_s; 0\rangle$, and as for $s = 2$, the map $\psi_s \circ \mathrm{o}_G : T^2 \longrightarrow \Gamma_{s-1}(U(s,0))$ gives us the value of the defining system, so using (4.13) for general s,

$$\eta_j^*(\langle \xi_1, \dots, \xi_s; 0\rangle = c(\{1, \dots, s\}, 0, j)$$

and $c(\{1, \dots, s\}, 0, j) = \alpha_j$, which finishes the induction. □

Similarly we get a theorem linking (4.9) and (4.11):

Theorem 4.6 *Let* $\{\xi_1, \dots, \xi_d\}$ *and* $\{\eta_1, \dots, \eta_t\}$ *be a basis for* $\mathrm{H}^1(G, \mathbb{F}_p)$ *and* $\mathrm{H}^2(G, \mathbb{F}_p)$ *respectively and let*

$$\langle \xi_i; r\rangle = \sum_{j=1}^{t} \alpha_{i_j} \eta_j$$

for i=1,…,d. Then, referring to (4.7)*,* $c(\underline{i}, r, j) = \alpha_{i_j}$*, where* $\underline{i} = (\underbrace{i, \dots, i}_{p^r})$ *and we consider the restricted product as in section* 3.5*. Hence we get a correspondence between the product* $\langle \xi_i; r\rangle$ *and the p-th power* $(\xi_i^*)^{p^r}$*.*

Proof: Similar to the proof of theorem 4.5, using theorem 4.3 and the groups $U(1, r)$. □

Remark 4.7 The products we will consider will be the strictly defined products $\langle \xi_1, \dots, \xi_s; 0\rangle$ where the index-set $\{1, \dots, s\}$ is such that not all entries are the same. If all the ξ_i-s are equal, we can also have strictly defined products, but in this case we can restrict the defining system and recognise it as Bockstein operations which was done in section 3.5.

So the products $\langle \xi_i, \dots, \xi_i; 0\rangle$ are taken care of by the Bockstein operations. By theorems 4.5 and 4.6 we see that this makes sense from a "presenting p-groups point of view". For example, $\langle \xi_1, \xi_1, \xi_1; 0\rangle \neq 0$ would give $[[\xi_1^*, \xi_1^*], \xi_1^*]$ occurring in a relation, but this is always 1, whereas in characteristic 3 (when the Bockstein exists), $\langle \xi_1; 1\rangle \neq 0$ would correspond to ξ_1^3 occurring non-trivially in a relation. It also makes sense from a "Massey product point of view", as the restricted product $\langle \xi_1; 1\rangle$ is contained in the product $\langle \xi_1, \xi_1, \xi_1; 0\rangle$. ■

4.3 Some examples

We now consider what we can do with the results in the previous section, where we obtained a correspondence between certain Massey products and group relations. Let us give a few concrete examples here and then see how we can use the results more generally in the next section.

4.3.1 The Golod-Shafarevich inequality

Let $d = \dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathbb{F}_p)$, $r = \dim_{\mathbb{F}_p} \mathrm{H}^2(G, \mathbb{F}_p)$ and let r_a be the minimal number of relations defining G as an abstract group. We have seen that we are dealing with a minimal pro-p presentation for our group, and that $r_a \geq r$ (section 2.7.5).

The following theorem is due to Golod and Shafarevich.

Theorem 4.8 *For any finite p-group G,*

$$r > \frac{d^2}{4}.$$

Proof: See Roquette's proof, for example [16, page 104]. □

So the Golod-Shafarevich inequality says that to present a finite p-group G with minimal generating set of rank d, we need at least $\lfloor \frac{d^2}{4} \rfloor + 1$ relations where $\lfloor x \rfloor$ denotes the greatest integer $\leq x$. An interesting question is therefore "For how big d has one found p-groups with $\lfloor \frac{d^2}{4} \rfloor + 1$ relations?"

As a first example of writing down Massey products from a group presentation using theorems 4.5 and 4.6, we use a group that relates to this question. In the article [33], Newman, Sauerbier and Wisliceny give the following pro-p presentation on 5 generators and 7 relations.

$G = \{x_1, x_2, x_3, x_4, x_5 | [x_1, x_2] = 1, [x_1, x_3] = x_3^{-p}, [x_5, x_4] = x_4^p, [x_5, x_3] = x_1^{-p},$
$[x_1, x_4] = [x_2, x_3]x_2^p x_3^p, [x_1, x_5] = [x_2, x_4], [x_2, x_5] = [x_3, x_4]x_5^{-p}\}$

which defines a finite group for all $p > 2$. They have found finite pro-p groups with $\lfloor \frac{d^2}{4} \rfloor + 1$ relations for $5 \leq d \leq 8$. For $d \leq 4$ one can find finite p-groups.

Using theorems 4.5 and 4.6 to read off the Massey products requires that the presentation is of a certain form. The interesting observation is that the pro-p presentations Newman et al. have are in such a form. Mike Newman says "Initially we tended to write down the presentations in human intelligible form. With more experience we realised that for computational purposes one should use somewhat different forms".

From the presentation of G we can write down the following Massey products (with $\xi_i^* = x_i$ for $i = 1, \ldots, 5$).

- $\langle \xi_1, \xi_2; 0 \rangle = \eta_1$
- $\langle \xi_1, \xi_3; 0 \rangle = \eta_2$
- $\langle \xi_1, \xi_4; 0 \rangle = -\eta_3$
- $\langle \xi_1, \xi_5; 0 \rangle = \eta_4$
- $\langle \xi_2, \xi_3; 0 \rangle = \eta_3$
- $\langle \xi_2, \xi_4; 0 \rangle = -\eta_4$
- $\langle \xi_2, \xi_5; 0 \rangle = \eta_7$
- $\langle \xi_3, \xi_4; 0 \rangle = -\eta_7$
- $\langle \xi_3, \xi_5; 0 \rangle = -\eta_6$
- $\langle \xi_4, \xi_5; 0 \rangle = \eta_5$
- $\langle \xi_1; 1 \rangle = \eta_6$
- $\langle \xi_2; 1 \rangle = \eta_3$
- $\langle \xi_3; 1 \rangle = \eta_2 + \eta_3$
- $\langle \xi_4; 1 \rangle = \eta_5$
- $\langle \xi_5; 1 \rangle = \eta_7$

This is a strictly defined product structure on $\mathrm{H}^1(G, \mathbb{F}_p)$ and $\mathrm{H}^2(G, \mathbb{F}_p)$ where $\dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathbb{F}_p) = 5$. No higher order products are strictly defined, since all possible products $\langle -, -; 0 \rangle$ and $\langle -; 1 \rangle$ are non-zero.

4.3.2 Groups of a given order

Now consider a group G of a given order, $|G| = p^n$ say. Then we know that there are n possibilities for $\dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathbb{F}_p)$ for $n \neq 0$, as this is the minimal number of generators for G.

For $\dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathbb{F}_p) = 1$, $G \simeq C_{p^n}$ and for $\dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathbb{F}_p) = n$, G is elementary abelian, so we go through the possibilities $\dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathbb{F}_p) \in \{2, \ldots, n-1\}$. For each of these, we choose various Massey product structures. From the products we then write down the relations we get, keeping track of where they end up in the lower central p-series, i.e. we find the kernels of the π_i-s in (4.6). Using the exact sequences

$$1 \longrightarrow \Gamma_i(G)/\Gamma_{i+1}(G) \longrightarrow G/\Gamma_{i+1}(G) \longrightarrow G/\Gamma_i(G) \longrightarrow 1 \tag{4.14}$$

for $i = 0, 1, \ldots$, we make sure $|G|$ doesn't get too big.

Øystein Nordvik, a student of Laudal, considered groups of order p^4 this way, see [34]. We have gone through his calculations and also checked all the presentations using Magma, where we found some interesting groups. Some of them will be used in the examples here.

Let $|G| = p^4$ and consider the case when $\mathrm{H}^1(G, \mathbb{F}_p)$ is 2-dimensional with basis elements ξ_1 and ξ_2. The products $\langle -; 1\rangle$ and $\langle -, -; 0\rangle$ are always defined and have no indeterminacy. The possible products here are $\langle \xi_1; 1\rangle$, $\langle \xi_2; 1\rangle$, $\langle \xi_1, \xi_1; 0\rangle$, $\langle \xi_2, \xi_2; 0\rangle$ and $\langle \xi_1, \xi_2; 0\rangle$. As pointed out in remark 4.7, the products $\langle \xi_1, \xi_1; 0\rangle$ and $\langle \xi_2, \xi_2; 0\rangle$ are taken care of by the Bocksteins, so will be omitted. Hence a choice for a strictly defined Massey product structure is

- $\langle \xi_1; 1\rangle = \eta_1$,
- $\langle \xi_2; 1\rangle = 0$,
- $\langle \xi_1, \xi_2; 0\rangle = \eta_2$.

Then for a strictly defined structure, the only other product that is defined is $\langle \xi_2; 2\rangle$. Suppose

- $\langle \xi_2; 2\rangle = \eta_2$.

By (4.7) and theorems 4.5 and 4.6, this combination of Massey products gives the presentation

$$G = \{\xi_1^*, \xi_2^* | (\xi_1^*)^p = 1, (\xi_2^*)^{p^2}[\xi_1^*, \xi_2^*] = 1\}, \tag{4.15}$$

which we recognise as H from example 2.31 with $p = 3$. Using commutator identities and the sequences (4.14), we find $|G| = p^4$.

Lemma 4.9 *Having chosen a basis,* $\{\xi_1, \xi_2\}$ *say, for* $\mathrm{H}^1(G, \mathbb{F}_p)$*, the following cohomological data completely determine the group* G *in* (4.15).

- $\dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathbb{F}_p) = 2$,
- $\langle -; 1\rangle$ *has rank 1*,
- $\langle -, -; 0\rangle$ *is injective modulo* $\langle -; 1\rangle$,
- $\langle -; 2\rangle$ *has rank 1 and is 0 modulo* $\langle -, -; 0\rangle$.

Proof: We claim that the data given will give us the combinations of products we gave above: From the data we can write down the following.

- $\langle \xi_1; 1\rangle = \alpha_1\eta_1$,
- $\langle \xi_1, \xi_2; 0\rangle = \alpha_2\eta_2$,
- $\langle \xi_2; 2\rangle = \alpha_3\eta_2$,

where $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_p - \{0\}$. Put $\xi_1' = \alpha_3\alpha_2^{-1}\xi_1$ and $\xi_2' = \alpha_2\xi_2$. Using 4) in remark 3.10, we get

- $\langle \xi_1'; 1\rangle = \alpha_3\alpha_2^{-1}\alpha_1\eta_1 := \eta_1'$,
- $\langle \xi_1', \xi_2'; 0\rangle = \alpha_2\alpha_3\eta_2 := \eta_2'$,
- $\langle \xi_2'; 2\rangle = \alpha_2\alpha_3\eta_2 = \eta_2'$,

which is the same as what we had.

Using the relations these products give and commutator identities, we find that $\Gamma_3(G)/\Gamma_4(G) = 1$ and $|G| = p^4$. □

Let us give another example, this time giving a group presentation which is not given by strictly defined Massey products and also showing some calculations using the sequences (4.14). Let

$$G = \{a, b | a^p[a, b] = 1, b^{p^2} = 1, [[a, b], b] = 1\}.$$

Using theorems 4.5 and 4.6 "backwards", we see that the product $\langle a^*, b^*; 0\rangle$ is non-zero, as the commutator $[a, b]$ is involved in one of the relations. This means that the 3-fold product corresponding to the 3-fold commutator is not strictly defined.

We will now show that $|G| = p^4$: Since we have two generators, $G/\Gamma_1(G) \simeq (\mathbb{F}_p)^2$ and since $a^p = [b, a]$, $\Gamma_1(G)/\Gamma_2(G)$ is generated by a^p and b^p, and so $\Gamma_1(G)/\Gamma_2(G) \simeq (\mathbb{F}_p)^2$. By sequence (4.14) for $i = 1$, $|G/\Gamma_2(G)| = p^4$. Now consider $\Gamma_2(G)/\Gamma_3(G)$ which is generated by $a^{p^2}, b^{p^2}, [a, b]^p, [[a, b], a]$ and $[[a, b], b]$. First, observe that $[[a, b], a] = [a^p, a] = 1$, and so we have

$$[a^p, b] = a^{-(p-1)}[a, b]a^{p-1}[a^{p-1}, b] = [a, b][a^{p-1}, b] \tag{4.16}$$

which gives $[a^p, b] = [a, b]^p$ by induction. Hence

$$a^{p^2} = [a, b]^p = [a^p, b] = [[a, b], b] = 1$$

and so $\Gamma_2(G)/\Gamma_3(G) = 1$ and $|G| = p^4$.

4.3.3 Groups of exponent p

An interesting question is “What sort of groups do we get by putting various conditions on the cohomology product structure?” For example, Thomas Weigel asked us “If the (1. order) Bockstein operation is injective, is the group of exponent p?”

A group of exponent p is a group where all non-trivial elements have order p. Let us first consider the case $p = 2$. If we have a group of exponent 2, it is abelian, and

$$B(r, 2) \simeq \bigoplus_{i=1}^{r} C_2,$$

where $B(r, 2)$ is the free Burnside group F/F^2 where F is a free group of rank r.

Again, using theorems 4.5 and 4.6 “backwards’, we see that the Bockstein operations $\langle \xi_i; 1\rangle_{i=1}^{r}$ for $B(r, 2)$ are all non-zero and linearly independent, and so a group of exponent 2 will have injective Bockstein operation. For general p, if G is of exponent p, then the 1. order Bockstein is injective, see [3, sections 4.3 and 5.8] where one finds more details on the Bockstein homomorphism.

Let us consider the reverse statement and give examples to show that the answer to Weigel's question is "no, not in general".

The quaternion group Q of order 8 is an example of a group with injective Bockstein as it is given by the products $\langle \xi_1; 1\rangle = \eta_1$, $\langle \xi_2; 1\rangle = \eta_2$ and $\langle \xi_1, \xi_2; 0\rangle = \eta_1 + \eta_2$, see [23]. The group has exponent 4.

In characteristic p for $p \neq 2$ we can find more groups of exponent $> p$ with injective Bockstein. For example the groups

$$\hat{G}_7 = \{a, b, c | a^p = 1, b^p = 1, c^p[a, b] = 1, [a, c] = 1, [b, c] = 1\}$$

and

$$\hat{G}_9 = \{a, b, c | b^p = 1, c^p = 1, a^p[a, b] = 1, [a, c] = 1, [b, c] = 1\},$$

which both have injective Bockstein operation.

These presentations are pro-p presentations of the groups G_7 and G_9 (hence names) in Burnside's list of groups of order p^4, see [7], both of exponent p^2. For example,

$$G_7 = \{x, y, z | x^{p^2} = 1, y^p = 1, z^p = 1, [y, z] = x^p, [x, y] = 1, [x, z] = 1\},$$

and from $\hat{G}_7$ we deduce $c^{p^2} = 1$ by calculations done in (4.16). We note that Magma gives for $p = 3$, $|\hat{G}_9| = 7 \cdot 3^4$.

Still referring to Burnside's list of groups of order p^4, we would also like to have a look at G_{11}, which is another example of a group of exponent p^2 having injective Bockstein. This also raises an interesting point which we will come back to later. Burnside gives the following presentation of this group.

$$G_{11} = \{a, b, c \mid a^{p^2} = 1, b^p = 1, c^p = 1, b^{-1}ab = a^{1+p}, c^{-1}ac = ab, c^{-1}bc = b\}.$$

This can be reduced to a minimal generating set to give

$$G_{11} = \{a, c \mid a^{p^2} = 1, [a, c]^p = 1, c^p = 1, a^p[[a, c], a] = 1, [[a, c], c] = 1\}.$$

We now use the same argument as in lemma 4.9 with $\xi_1' = \alpha_3\xi_1$ and $\xi_2' =$

$\alpha_3^{-2}\alpha_1\xi_2$. Then the following cohomological data with $\{\xi_1, \xi_2\}$ as a basis for $\mathrm{H}^1(G, \mathbb{F}_p)$ turn out to give this group.

G_{11}
- $\dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathbb{F}_p) = 2$,
- $\dim_{\mathbb{F}_p} \mathrm{H}^2(G, \mathbb{F}_p) = 3$,
- $\langle -; 1\rangle$ is injective,
- $\langle -, -; 0\rangle$ is zero,
- $\langle -, -, -; 0\rangle$ is injective,
- $\langle -, -, -; 0\rangle$ has rank 1 modulo $\langle -; 1\rangle$,
- $\langle \xi_1, \xi_2, \xi_1; 0\rangle \in \langle \xi_1; 1\rangle$.
- Presentation: $\{a, b | a^p[[a, b], a] = 1, b^p = 1, [[a, b], b] = 1\}$.
- Note: For $p = 3$, if we replace $a^3[[a, b], a] = 1$ with $b^3[[a, b], a] = 1$, then, according to Magma, we get a group with largest p-quotient of order 3^8.
- Also note: If we consider the group $\{a, b|b^3[[a, b], a] = 1, a^3 = 1, [[a, b], b] = 1\}$, we get a group of order 81, but it is not isomorphic to G_{11}; it is isomorphic to G_{12}, given by the data

G_{12}
- $\dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathbb{F}_p) = 2$,
- $\dim_{\mathbb{F}_p} \mathrm{H}^2(G, \mathbb{F}_p) = 3$,
- $\langle -; 1\rangle$ is injective,
- $\langle -, -; 0\rangle$ is zero,
- $\langle -, -, -; 0\rangle$ is injective,
- $\langle -, -, -; 0\rangle$ has rank 1 modulo $\langle -; 1\rangle$,
- $\langle \xi_1, \xi_2, \xi_1; 0\rangle \notin \langle \xi_1; 1\rangle$.
- Presentation: $\{a, b|a^p = 1, b^p[[a, b], a] = 1, [[a, b], b] = 1\}$.
- Note: For $p = 5$ we get a group of order $5^4 \cdot 11$, with largest p-quotient isomorphic to Burnside's G_{12} for $p = 5$.

Remark 4.10 We see that what we have in these examples are groups where we start out with the Bockstein being injective and then build a group where some of the other Massey products link (have a linear dependence relation) with the Bockstein. Then the p-power relation ends up in a lower level in the lower central p-series, hence raising the exponent. ■

Using the idea in remark 4.10 we should be able to recognise the cohomological conditions for a group to be of exponent p. So let us give an example of such a group. This group will generate a family of such examples by taking direct products with copies of C_p.

G_{14}
- $\dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathbb{F}_p) = 3$,
- $\dim_{\mathbb{F}_p} \mathrm{H}^2(G, \mathbb{F}_p) = 7$,
- $\langle -; 1\rangle$ is injective,
- $\langle -, -; 0\rangle$ has rank 2, and rank 2 modulo $\langle -; 1\rangle$,
- $\langle -, -, -; 0\rangle$ is injective modulo $\langle -; 1\rangle$ and $\langle -, -; 0\rangle$.
- Presentation: $\{a, b, c | a^p = 1, b^p = 1, c^p = 1, [a, c] = 1, [b, c] = 1, [[a, b], a] = 1, [[a, b], b] = 1\}$.

For this group, the 1. order Bockstein operation $\langle -; 1\rangle$ is injective and the other strictly defined Massey products are linearly independent of the values of $\langle -; 1\rangle$. And the group has exponent p. Also note that since all products are linearly independent, we don't need to worry about the choices we make.

4.4 A procedure and a tree construction

Following up on section 4.3.2, we will now elaborate on the terms used there and try to put the various examples we have seen into a bigger picture.

We are now looking for groups of order p^n for arbitrary n given by strictly defined Massey products, and first we give a procedure for writing down such products. The values of these products are elements in $\mathrm{H}^2(G, \mathbb{F}_p)$, so denote by $\{-\}$ the subspace of $\mathrm{H}^2(G,\mathbb{F}_p)$ spanned by the elements in the bracket.

Procedure:

Level 1:
- Decide the rank of $\langle -;1\rangle$.
- Decide the rank of $\langle -,-;0\rangle$ modulo $\{\langle -;1\rangle\}$.

Level 2:
- Decide the rank of $\langle -;2\rangle$ modulo $\{\langle -;1\rangle,\langle -,-;0\rangle\}$.
- Decide the rank of $\langle -,-,-;0\rangle$ modulo $\{\langle -;1\rangle,\langle -,-;0\rangle,\langle -;2\rangle\}$.

$\vdots$

Level n:
- Decide the rank of $\langle -;n\rangle$ and $\langle \underbrace{-,\cdots,-}_{n+1};0\rangle$ modulo lower order products.

Since we have strictly defined Massey products, this procedure will automatically stop: As long as a product is zero, we have the existence of cochains which we can use to define more products. When a product is non-zero, we don't use this product in a strictly defined situation.

After having decided on the various ranks in the procedure, which we refer to as then having cohomological data, we write down a possible product structure using a chosen basis for $\mathrm{H}^1(G,\mathbb{F}_p)$. If for example $\{\xi_1,\xi_2\}$ is a choice of basis, $\langle -;1\rangle$ is injective and $\langle -,-;0\rangle$ is zero modulo $\langle -;1\rangle$, then a possible product structure is $\langle \xi_1;1\rangle=\eta_1$, $\langle \xi_2;1\rangle=\eta_2$ and $\langle \xi_1,\xi_2;0\rangle=\eta_1$.

Definition 4.11 *As we only write down strictly defined products, the product structure we get is called a strictly defined product structure on* $\mathrm{H}^1(G,\mathbb{F}_p)$ *and* $\mathrm{H}^2(G,\mathbb{F}_p)$*. When we have such a structure, we have a set of elements in* $\mathrm{H}^2(G,\mathbb{F}_p)$ *assigned to the various strictly defined products with linear relations between them telling us how the products relate to each other. Hence telling us how the various group relations corresponding to these products are linked.*

We will come back to how well-defined the procedure is in the next section. For this we will need to consider the choice of basis and the various product structures we can have from the same data. But first we would like to show how we can keep track of this procedure by a tree construction.

We can organise the various possibilities in the procedure and the strictly defined structures in a tree. As soon as our choices make the procedure stop, we work out what the group is using theorems 4.5 and 4.6. In this way, combinations of Massey products give rise to a tree of p-groups.

So via the procedure we use cohomological invariants to group the p-groups into infinite families, which will be branches in our tree. We have investigated some of the branches in the tree for 2-generator groups, as shown in appendix B.

Let us consider the group $G_{1,3}$ appearing in the diagram in appendix B: We follow the path upwards from $G_{1,3}$ to read off the data that give this group as a possibility. Hence for $G_{1,3}$, $\langle -;1\rangle$ has rank 1, $\langle -,-;0\rangle$ is injective modulo $\langle -;1\rangle$, $\langle -;2\rangle$ is 0 modulo $\langle -;1\rangle$ and $\langle -,-;0\rangle$, and it is actually 0, hence $\langle -;3\rangle$ is defined, which is non-zero, but 0 modulo $\langle -;1\rangle$ and $\langle -,-;0\rangle$.

The families of metacyclic p-groups $G_{m,N-2m} := G(m, N-2m)$ will give us branches in the tree. These groups will be studied extensively in the next chapter.

Definition 4.12 *Let $A_{m,n}$ denote the direct product of C_{p^m} and C_{p^n}, i.e. an abelian group of order p^{m+n} on two generators.*

In the tree construction in appendix B, we get out the families $\{A_{m,n}\}_{m\geq 1}$ for each fixed n. Suppose, without loss of generality, that $m \leq n$. These groups are given by the following cohomological data.

$A_{m,n}$

- $\dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathbb{F}_p) = 2$,
- $\dim_{\mathbb{F}_p} \mathrm{H}^2(G, \mathbb{F}_p) = 3$,
- if $m = n$, $\langle -;m\rangle$ is injective,
- if $m < n$, $\langle -;m\rangle$ has rank 1 and $\langle -;n\rangle$ has rank 1 modulo $\langle -;m\rangle$,
- $\langle -,-;0\rangle$ is injective modulo $\langle -;m\rangle$ and $\langle -;n\rangle$.

Another branch will give us groups N_i where the largest p-quotient is of order p^i for $i = 4, 5, \ldots, p+1$. Having $p >$ the class of the group means that we don't mess up the commutator structure.

Definition 4.13 *The family* $\{N_i\}$ *starts out as follows:*

- $N_4 = \{x, y | x^p = 1, y^p = 1, [x, y, y] = 1, [x, y, x, x] = 1, \underline{[x, y, x, y] = 1}\}$
- $N_5 = \{x, y | x^p = 1, y^p = 1, [x, y, y] = 1, \underline{[x, y, x, y] = 1}, [x, y, x, x, y] = 1, [x, y, x, x, x] = 1\}$
- $N_6 = \{x, y | x^p = 1, y^p = 1, [x, y, y] = 1, [x, y, x, y] = 1, \underline{[x, y, x, x, y] = 1}, [x, y, x, x, x, y] = 1, [x, y, x, x, x, x] = 1\}$
- $N_7 = \{x, y | x^p = 1, y^p = 1, [x, y, y] = 1, [x, y, x, y] = 1, [x, y, x, x, y] = 1, \underline{[x, y, x, x, x, y] = 1}, [x, y, x, x, x, x, y] = 1, [x, y, x, x, x, x, x] = 1\}$
- $N_8 = \{x, y | x^p = 1, y^p = 1, [x, y, y] = 1, [x, y, x, y] = 1, [x, y, x, x, y] = 1, [x, y, x, x, x, y] = 1, \underline{[x, y, x, x, x, x, y] = 1}, [x, y, x, x, x, x, x, y] = 1, [x, y, x, x, x, x, x, x] = 1\}$

Studying this family tells us again what a mess presenting p-groups really is. Magma tells us that the underlined relations are in fact redundant, but we have left them in to see the pattern more easily. Some of this can be explained using commutator identities.

We get the family $\{N_i\}$ from the following cohomological data using theorems 4.5 and 4.6: We start with $\mathrm{H}^1(G, \mathbb{F}_p)$ being 2-dimensional with basis ξ_1, ξ_2, where ξ_1^*, ξ_2^* will be x, y respectively. In the procedure we start with $\langle -; 1\rangle$ being injective and $\langle -, -; 0\rangle$ being zero. Since $\langle \xi_1, \xi_2; 0\rangle$ is zero and is antisymmetric, we can define the 3-fold products

$$\langle \xi_1, \xi_2, \xi_1; 0\rangle, \langle \xi_1, \xi_2, \xi_2; 0\rangle, \langle \xi_2, \xi_1, \xi_1; 0\rangle \text{ and } \langle \xi_2, \xi_1, \xi_2; 0\rangle.$$

Now, since the product $\langle -, -; 0\rangle$ is antisymmetric, we will call the products $\langle -, \dots, -; 0\rangle$ going from $\mathrm{H}^1(G, \mathbb{F}_p) \wedge \mathrm{H}^1(G, \mathbb{F}_p) \otimes \mathrm{H}^1(G, \mathbb{F}_p) \otimes \cdots \otimes \mathrm{H}^1(G, \mathbb{F}_p)$ to $\mathrm{H}^2(G, \mathbb{F}_p)$, where $\wedge$ denotes the antisymmetric tensorproduct, the antisymmetric Massey products. So for 2 basis elements we get $\langle \xi_1, \xi_2, \xi_1; 0\rangle$ and $\langle \xi_1, \xi_2, \xi_2; 0\rangle$ as a basis for the 3-fold antisymmetric products etc.

We note that there certainly are more products floating around which will be strictly defined, for example $\langle \xi_2, \xi_1, \xi_1; 0\rangle$. Choosing the antisymmetric products however, will give us the family $\{N_i\}$ (and other groups). Our choice also makes sense from a group theoretic point of view, which we should keep in mind, now that we have theorems 4.5 and 4.6 telling us the correspondence between products and relations. For example, $\Gamma_2(F)/\Gamma_3(F)$ for a 2-generator free group F on x, y can be generated by $x^{p^2}, y^{p^2}, [x,y]^p, [[x,y],x]$ and $[[x,y],y]$. I.e. we don't need elements like $[[y,x],x]$, by commutator calculations.

Building the family $\{N_i\}$, we let $\langle -,-,-;0\rangle$ be of rank 1 and choose $\langle \xi_1,\xi_2,\xi_2;0\rangle \neq 0$, hence no products involving $\langle \xi_1,\xi_2,\xi_2;0\rangle$ will be strictly defined. So we build on the product $\langle \xi_1,\xi_2,\xi_1;0\rangle$. For N_4, the antisymmetric 4-fold product is injective modulo the lower order products, whereas for N_5 it is of rank 1. Choosing $\langle \xi_1,\xi_2,\xi_1,\xi_2;0\rangle \neq 0$ we build on $\langle \xi_1,\xi_2,\xi_1,\xi_1;0\rangle$ and get N_5 when the antisymmetric 5-fold product is injective modulo lower order products.

In general, we get N_i having chosen

$$\langle \xi_1,\xi_2,\underbrace{\xi_1,\ldots,\xi_1}_{i-4},\xi_2;0\rangle \neq 0$$

and the i-fold antisymmetric product being injective modulo lower order products. It is the relation $[x,y,\underbrace{x,\ldots,x}_{i-4},y]=1$ that turns out to be redundant.

Things one can explore further in connection with this family are: Can we spot which relations are redundant from the Massey products? Maybe by considering the defining systems we can have. We have attempted this, but haven't been able to state any nice results.

Also, what happens when we take away the choice of antisymmetric products? For example, for $\langle \xi_1,\xi_2,\xi_1,\xi_2;0\rangle$ to be strictly defined we need $\langle \xi_1,\xi_2,\xi_1;0\rangle = \langle \xi_2,\xi_1,\xi_2;0\rangle = 0$ which we assume here. This relates to the question and problem of how well-defined the procedure is. Because of this, we will need more investigations before we can make any general results. However, we feel that the tree using cohomological data is a nice way of grouping p-groups and, considering certain parts of this tree, we can state small results.

Lemma 4.14 *Let* $\dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathbb{F}_p) = 2$ *and let* ξ_1, ξ_2 *be a basis. If we stop the procedure for writing down strictly defined Massey products on* $\mathrm{H}^1(G, \mathbb{F}_p)$ *and* $\mathrm{H}^2(G, \mathbb{F}_p)$ *after level 1, i.e. having assigned non-zero values to* $\langle \xi_1; 1\rangle, \langle \xi_2; 1\rangle$ *and* $\langle \xi_1, \xi_2; 0\rangle$*, then the finite pro-p groups G we get are either abelian or metacyclic.*

Proof: In order to have a finite pro-p group we must have either that **1)** the products $\langle \xi_1; 1\rangle, \langle \xi_2; 1\rangle$ and $\langle \xi_1, \xi_2; 0\rangle$ are all linearly independent **or** that **2)** $\langle \xi_1; 1\rangle$ and $\langle \xi_2; 1\rangle$ are linearly independent and one or both are linearly dependent on $\langle \xi_1, \xi_2; 0\rangle$.

To see why these are the only possibilities, we use theorems 4.5 and 4.6 to see what kind of presentation we get. By the Golod-Shafarevich inequality, see theorem 4.8, we must have at least 2 relations so the products can't all be linearly dependent. And a group with relations $(\xi_1^*)^p(\xi_2^*)^p = 1$ and $[\xi_1^*, \xi_2^*] = 1$ is not a finite group. 1) is abelian and 2) is metacyclic, as we will see in theorem 5.11. ☐

4.5 Indeterminacy- and well-definedness-considerations

In the previous section we introduced a procedure producing groups via a set of cohomological data. And the tree construction tells us that we can talk about a p-group being in a certain branch and at a certain level according to the cohomological data that determine the group.

On each level of this procedure we made various choices. In this section we consider how well-defined the procedure is. The other problem we need to deal with is the indeterminacy of the Massey products.

Let us first consider the indeterminacy. In order to get useful interpretations from the Massey products, as in [14], [15] and [44] (topological), the first thing we need is to be able to talk about a unique value for these products. This means we want the indeterminacy to be zero.

As we have seen, the Bockstein operations have no indeterminacy, but the products $\langle -, \dots, -; 0\rangle$ do. Recall that

$$\mathrm{In}\langle \xi_1, \dots, \xi_s; 0\rangle = \{x - y | x, y \in \langle \xi_1, \dots, \xi_s; 0\rangle\}.$$

We give an example showing how the indeterminacy come into play.

Example 4.15 Let $\dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathbb{F}_p) = 3$ and let $\{\xi_1, \xi_2, \xi_3\}$ be a set of basis elements. Suppose we have the products

- $\langle \xi_1, \xi_2; 0\rangle = 0$,
- $\langle \xi_2, \xi_3; 0\rangle = 0$,
- $\langle \xi_1, \xi_3; 0\rangle = \eta_1$,
- $\langle \xi_1, \xi_2, \xi_3; 0\rangle = \eta_2$.

The relations corresponding to these products are $[\xi_1^*, \xi_3^*] = 1$ and $[[\xi_1^* \xi_2^*], \xi_3^*] = 1$.

One of these products have non-zero indeterminacy, namely $\langle \xi_1, \xi_2, \xi_3; 0\rangle$. This means that we have several defining systems for the product, giving different values. In example 3.9 we calculated $\mathrm{In}\langle \xi_1, \xi_1, \xi_1; 0\rangle$. Similar calculations will show that

$$\langle \xi_1, \xi_3; 0\rangle \in \mathrm{In}\langle \xi_1, \xi_2, \xi_3; 0\rangle,$$

which means that another value for $\langle \xi_1, \xi_2, \xi_3; 0\rangle$ is $\eta_1 + \eta_2$. So we have a problem since we can't speak of a unique cohomology class as the value for this product.

However, here we see that the relations we get using the other value will not change the group: The relations corresponding to

$$\langle \xi_1, \xi_3; 0\rangle = \eta_1 \text{ and } \langle \xi_1, \xi_2, \xi_3; 0\rangle = \eta_1 + \eta_2$$

are

$$[\xi_1^*, \xi_2^*][[\xi_1^*, \xi_2^*], \xi_3^*] = 1 \text{ and } [[\xi_1^*, \xi_2^*], \xi_3^*] = 1$$

which give the same relations as before! ■

The observation in this example gives us hope: We have indeterminacy, but it looks like we (at least in certain cases) can control it.

The indeterminacy consists of elements in $\mathrm{H}^2(G, \mathbb{F}_p)$ and from the way we build the strictly defined Massey products we see that the indeterminacy must be values of the lower order products. I.e. the indeterminacy will make new linear dependence relations between the different levels in our procedure, hence will link a product to lower order products.

Peter May, see [31], has worked on the indeterminacy for matric Massey products. These products generalise the Massey products, which can be considered as (1×1)-matric Massey products. For example he gives an upper bound for the indeterminacy of strictly defined matric Massey products. However, we feel that the statement he gives, [31, proposition 2.4], is not correct for our purposes, and we give the following result.

Theorem 4.16 *Let* $\dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathbb{F}_p) = 2$ *and let* $p \geq 3$*. Then the strictly defined Massey products on* $\mathrm{H}^1(G, \mathbb{F}_p)$ *and* $\mathrm{H}^2(G, \mathbb{F}_p)$ *have no indeterminacy, i.e. we can uniquely determine the* $c(\underline{i}, r, j)$*-s in* (4.7).

Proof: Let ξ_1, ξ_2 be a basis for $\mathrm{H}^1(G, \mathbb{F}_p)$, i.e. all 1-cocycles are linear combinations $\alpha\xi_1 + \beta\xi_2$ for $\alpha, \beta \in \mathbb{F}_p$. We recall that the Massey products behave well with respect to multiplication by invertible scalars by 4) in remark 3.10, and also with respect to linearity as $\langle -, -; 0\rangle$ is bilinear.

The product $\langle \xi_1, \xi_2; 0\rangle$ has no indeterminacy, so take two defining systems M and M' for a Massey product $\langle \xi_{i_1}, \ldots, \xi_{i_s}; 0\rangle$ with $i_j \in \{1, 2\}$ for $j = 1, \ldots, s$, $s \geq 3$. Since the Massey products don't depend on the representatives of the ξ_i-s, $m_{i,i+1} = m'_{i,i+1}$ for $i = 1, \ldots, s$. The entries $m_{i,j}$ and $m'_{i,j}$ for $1 \leq i < j \leq s + 1; (i, j) \neq (1, s + 1), j \neq i + 1$, will differ by a 1-cocycle.

This means that $v(M) - v(M')$, which is the indeterminacy, will be linear combinations of $\langle \xi_1, \xi_1; 0\rangle$, $\langle \xi_2, \xi_2; 0\rangle$ and $\langle \xi_1, \xi_2; 0\rangle$. Since $p \geq 3$, $\langle \xi_1, \xi_1; 0\rangle = \langle \xi_2, \xi_2; 0\rangle = 0$, and since we have strictly defined products, $\langle \xi_1, \xi_2; 0\rangle = 0$, and so the indeterminacy is zero. □

Remark 4.17 During the viva, the examiners raised doubts about this proof. We therefore would like to add the following: This proof is OK for products only involving ξ_1 and ξ_2. However, for products involving linear combinations of ξ_1 and ξ_2, we need an induction argument to show that a general product is defined. Also, to show that the indeterminacy is zero for such products, we need another induction argument where we make use of May's proposition 2.4 in [31]:

A general triple product will be covered by the case

$$\langle \alpha\xi_1, \beta\xi_1 + \gamma\xi_2, \delta\xi_1 + \epsilon\xi_2; 0\rangle.$$

Assume this product is strictly defined, i.e. all lower order products involved are 0. In particular,

$$0 = \langle \xi_1, \xi_1 + \xi_2; 0\rangle = \langle \xi_1, \xi_1; 0\rangle + \langle \xi_1, \xi_2; 0\rangle,$$

hence $\langle \xi_1, \xi_2; 0\rangle = 0$ since $p \neq 2$. Now, by proposition 2.4 in [31], $\mathrm{In}\langle \alpha\xi_1, \beta\xi_1 + \gamma\xi_2, \delta\xi_1 + \epsilon\xi_2; 0\rangle = 0$, since this will only involve the Yoneda compositions, which are all 0.

For higher products, things are not quite clear. E.g. consider the product $\langle \xi_1, \xi_1 + \xi_2, \xi_1 + \xi_2, \xi_1 + \xi_2; 0\rangle$. If we assume that this is strictly defined, we can write down a system of linear equations from all the lower products which are zero. The question is whether we from these equations can deduce that the indeterminacy is zero. By proposition 2.4 in [31], the product $\langle \xi_1, \xi_2, \xi_1 + \xi_2; 0\rangle$ is an element in the indeterminacy, but we can not see that this should be zero. One thing to do would be to consider the defining systems for all the products involved, but we realise that this will take some time. ■

For more than two generators we will have indeterminacy, as in example 4.15. And so the question is "What does the change of linear dependence relations between the products do to the various groups we get?" To solve this we might need to define an equivalence relation on a strictly defined Massey product structure so that equivalent structures give isomorphic groups. From the point of view of the modular isomorphism problem, which is discussed in the next chapter, we also want the equivalence relation to be determined by

$\mathbb{F}_pG$, i.e. if two structures both come from $\mathbb{F}_pG$, they should be equivalent.

We might also try to push theorem 4.16 further to control the indeterminacy, as it seems to us that only the product $\langle -, -; 0\rangle$ should give a contribution.

However, we feel that the theory of A_∞-algebras, which was suggested to us by Dave Benson, will be a better approach to deal with the problem of indeterminacy in general. This theory seems to put the internal product structure on $\mathrm{H}^*(G, \mathbb{F}_p)$ into a very nice framework, and is something we intend to investigate.

We next consider the well-definedness of the procedure, and concentrate on the case when $\mathrm{H}^1(G, \mathbb{F}_p)$ is 2-dimensional. In this case, theorem 4.16 tells us that our products have unique values, but what if we pick another basis for our products -will the relations we can write down for these various choices give us isomorphic groups?

We saw an example of the sort of argument we need in lemma 4.9. In this lemma we had already chosen a basis, and then showed that if we were given a particular set of cohomological data, we could find a base change such that the cohomological data uniquely determined the group we were considering.

What would it mean for our procedure to be well-defined? Say our choices make the procedure stop at level n and we have a set of cohomological data. If we put in the basis $\{\xi_1, \xi_2\}$ we get out a group G. We need to consider a general base change

$$\xi_1' = \alpha\xi_1 + \beta\xi_2 \quad \text{and} \quad \xi_2' = \gamma\xi_1 + \delta\xi_2 \tag{4.17}$$

with $\alpha, \beta, \gamma, \delta \in \mathbb{F}_p$ and $\alpha\delta - \gamma\beta \neq 0$, and show that the group we get using $\{\xi_1', \xi_2'\}$ is isomorphic to G, as a pro-p group.

To show this it is sufficient that the linear dependence relations between the various products are preserved under the base change, as the linear dependence relations tell us how the relations are linked. For example, the linear dependence relation $\langle \xi_1, \xi_2; 0\rangle = \langle \xi_1; 1\rangle + \langle \xi_2; 1\rangle$ holds for both the structures

$$\begin{array}{lclclcl} \langle \xi_1, \xi_2; 0\rangle & = & \eta_1 & & & = & \eta_1 + \eta_2 \\ \langle \xi_1; 1\rangle & = & -\eta_2 & & \text{and} & = & \eta_2 \\ \langle \xi_2; 1\rangle & = & \eta_1 + \eta_2 & & & = & \eta_1 \end{array}$$

and the two groups we get from these structures are isomorphic.

However, this is not a necessary condition as we are dealing with pro-p presentations, i.e. we can have a finite p-group isomorphic to a finite pro-p group, see lemma 5.29 for an example of this.

Assume the procedure stops after level 1. Then

$$\begin{array}{lcl} \langle \xi_1', \xi_2'; 0\rangle & = & \langle \alpha\xi_1 + \beta\xi_2, \gamma\xi_1 + \delta\xi_2; 0\rangle \\ & = & (\alpha\delta - \beta\gamma)\langle \xi_1, \xi_2; 0\rangle + \alpha\gamma\langle \xi_1, \xi_1; 0\rangle + \beta\delta\langle \xi_2, \xi_2; 0\rangle, \\ \langle \xi_1'; 1\rangle & = & \alpha\langle \xi_1; 1\rangle + \beta\langle \xi_2; 1\rangle, \\ \langle \xi_2'; 1\rangle & = & \gamma\langle \xi_1; 1\rangle + \delta\langle \xi_2; 1\rangle. \end{array}$$

For $p > 2$, $\langle \xi_1, \xi_1; 0\rangle = \langle \xi_2, \xi_2; 0\rangle = 0$, and so since $\alpha\delta - \beta\gamma \neq 0$, the linear dependence relations between $\langle \xi_1, \xi_2; 0\rangle$, $\langle \xi_1, ; 1\rangle$ and $\langle \xi_2; 1\rangle$ are preserved. For $p = 2$, $\langle \xi_i; 1\rangle = \langle \xi_i, \xi_i; 0\rangle$, but we still keep the linear dependence relations.

Now,

$$\begin{array}{lcl} \langle \xi_1', \xi_2', \xi_1'; 0\rangle & = & \langle \alpha\xi_1 + \beta\xi_2, \gamma\xi_1 + \delta\xi_2, \alpha\xi_1 + \beta\xi_2; 0\rangle \\ & = & \quad \alpha\gamma\alpha\langle \xi_1, \xi_1, \xi_1; 0\rangle + \beta\gamma\alpha\langle \xi_2, \xi_1, \xi_1; 0\rangle \\ & & +\alpha\delta\alpha\langle \xi_1, \xi_2, \xi_1; 0\rangle + \beta\delta\alpha\langle \xi_2, \xi_2, \xi_1; 0\rangle \\ & & +\alpha\gamma\beta\langle \xi_1, \xi_1, \xi_2; 0\rangle + \beta\gamma\beta\langle \xi_2, \xi_1, \xi_1; 0\rangle \\ & & +\alpha\delta\beta\langle \xi_1, \xi_2, \xi_2; 0\rangle + \beta\delta\beta\langle \xi_2, \xi_2, \xi_2; 0\rangle. \end{array}$$

So we see that in general a base change will link a product of length s with other products via products of length s.

We state the following conjecture.

Conjecture 4.18 *Let* $\dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathbb{F}_p) = 2$. *Then the procedure in section* 4.4 *is well-defined in the sense described above.*

For the proof, we feel it should be possible to do induction on the level of the procedure. We have seen that the base case (level 1) is OK. For the induction step, consider a base change $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ as in (4.17). We observe that it suffices to solve the conjecture for the base changes $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \delta \end{smallmatrix}\right)$, as these will generate the general case. The second case should follow from the first by symmetry although we might need an extra argument.

However, the induction step needs a bit more work, and we might need to think in terms of an equivalence relation as mentioned earlier. Note that since preserving the linear dependence relations is sufficient but not necessary, we still should be able to solve the conjecture even though this induction should turn out to cause problems.

The procedure and tree construction are an attempt at making the theory we have introduced usable, and although we have identified various problems, this gives a different way of looking at the classification of p-groups.

Chapter 5

Metacyclic p-groups

In this chapter, we study metacyclic p-groups from a cohomological point of view, in particular, we give 0-deficiency presentations for split metacyclic p-groups using strictly defined Massey products.

We start by studying metacyclic p-groups and putting the split metacyclic p-groups of deficiency 0 into families. Using the tree construction in appendix B, it turns out that we can give new 0-deficiency presentations for split metacylic p-groups (another such presentation for metacyclic groups in general is found in [4]).

We find an $\mathbb{F}_pG$-free resolution of $\mathbb{F}_p$ for a metacyclic p-group G, calculate $\mathrm{H}^1(G, \mathbb{F}_p)$ and $\mathrm{H}^2(G, \mathbb{F}_p)$ and then calculate the Massey products using the Yoneda cocomplex. All these calculations are written down in great detail and in the last section we analyse them.

5.1 Basic results on metacyclic p-groups

A finite group G is called metacyclic if G has a cyclic normal subgroup N such that the quotient G/N is cyclic. In this section, we collect some results about metacyclic p-groups. We will **assume throughout this chapter that p is odd**. The reader is referred to Liedahl ([27] and [26]) for the proofs of the results in this section.

Theorem 5.1 *A metacyclic p-group G of order p^N may be given by a presentation*

$$G = \{a, b \mid a^{p^n} = 1, b^{p^m} = a^i, b^{-1}ab = a^q\},$$

where

i) $n + m = N$,

ii) $q^{p^m} \equiv 1 \pmod{p^n}$,

iii) $p^n \mid i(q-1)$,

and each such presentation defines a metacyclic group of order p^N. Moreover, we have the following facts:

iv) We may assume $N \geq 2$ and $n \in \{1, \ldots, N\}$.

v) It suffices to consider those q of the form $(p+1)^{p^t}$ (p is odd), where $t \in \{\max(0, n-m-1), \ldots, n-1\}$.

vi) We may assume $i = p^s$, where s depends on the triple (n, m, t) and $s \in \{n-t-1, \ldots, \min(n, m)\}$.

□

Remark 5.2 The parameters n, m, t and s will refer to the presentation given in 5.1, and we will denote this group by $G(n, m, t, s)$. ■

A metacyclic group is called split if it is expressible as a semidirect product of two cyclic subgroups. We will say K splits G if K is cyclic, normal in G, G/K is cyclic and $G \longrightarrow G/K$ splits.

Theorem 5.3 *If $s = \min(n, m)$ then $\langle a \rangle$ splits G. On the other hand, the element b generates a normal subgroup of G if and only if $s \leq t + 1$. If $s \leq t + 1$ and $s < \min(n, m)$ then $\langle b \rangle$ splits G.* □

Liedahl uses the following result to enumerate split metacyclic p-groups. We will use the result to place the split metacyclic p-groups of deficiency 0 into families, and for each family give presentations given by strictly defined Massey products.

Theorem 5.4 *If $N \geq 3$, then each non-abelian split metacyclic group of order p^N is obtained exactly once by letting the parameters n, m, t and s vary according to*

$$n \in \{2, 3, \ldots, N-1\},$$

$$t \in \{\max(0, 2n-N-1), \ldots, n-2\},$$

$$s = \min(n, N-n).$$

□

5.2 Split metacyclic p-groups of deficiency 0

Because of the relation $b^{-1}ab = a^{(p+1)^{p^t}}$, the following lemma will be very useful to us throughout this chapter (it is also used in the proofs of the results in the previous section):

Lemma 5.5 *Let $t \geq 0$ be an integer. If p is an odd prime, then the highest power of p dividing $(p+1)^{p^t} - 1$ is p^{t+1}.*

Proof: We use induction on t. The base step $t = 0$ is easily checked, so assume $t > 0$. Using Euler's ϕ-function, we get

$$(p+1)^{p^{t-1}} \equiv 1 \pmod{p^t},$$

hence we have $r \in \mathbb{Z}$ so that $(p+1)^{p^{t-1}} = 1 + rp^t$. Our induction hypothesis is $r \not\equiv 0 \pmod{p}$. Raising to the power p, we get the lemma by induction since

$$\begin{aligned}(p+1)^{p^t} = (1+rp^t)^p &= 1 + \binom{p}{1} rp^t + \binom{p}{2} r^2 p^{2t} + \cdots + r^p p^{pt} \\ &= 1 + rp^{t+1} + kp^{t+2}\end{aligned}$$

for $k \in \mathbb{Z}$. Note that the exponent in the last term, pt, will be $\geq t+2$ since p is odd and $t > 0$. □

For finite groups, the difference between the number of generators and the number of relations is an important invariant.

Definition 5.6 *Let the finite group G be given by a presentation $\mathcal{P}$ using d generators and r relations. The number*

$$r - d$$

is called the deficiency of the given presentation of G, denoted $\operatorname{def}_{\mathcal{P}}(G)$. The deficiency of G is defined to be

$$\operatorname{def}(G) = \min\{\operatorname{def}_{\mathcal{P}}(G) \mid \mathcal{P} \textit{ is a finite presentation of } G\}.$$

We quote a theorem by Wamsley, see [45]:

Theorem 5.7 *Let G be a finite group with presentation*

$$G = \{a, b \mid a^{\beta} = 1, b^{\gamma} = a^{\delta}, b^{-1}ab = a^{1+\alpha}\}$$

with α, β, γ and δ nonnegative and such that the order of G is $\gamma\beta$, then the following are equivalent.

i) $\operatorname{def}(G) = 0$,

ii) $\mathrm{H}_2(G, \mathbb{Z}) = 0$*, i.e. the Schur multiplier is trivial,*

iii) $\gcd(\alpha, \beta, \delta, \frac{\alpha\delta}{\beta}, \frac{(1+\alpha)^{\gamma}-1}{\beta}, \frac{(1+\alpha)^{\gamma}-1}{\alpha}) = 1$.

□

From this theorem, we deduce another useful lemma.

Lemma 5.8 *A necessary and sufficient condition for a metacyclic p-group G with parameters n, m, s and t to have deficiency 0 is*

$$t + 1 + s - n = 0.$$

Proof: We use theorem 5.7 and put

$\beta = p^n$,

$\gamma = p^m$,

$\delta = p^s$,

$q = 1 + \alpha = (p+1)^{p^t}$, hence $\alpha = (p+1)^{p^t} - 1$.

We need to find the highest power of p dividing all the expressions from *iii*) in theorem 5.7.

Number	Expression	Highest power of p dividing the expression
1	$(p+1)^{p^t} - 1$	p^{t+1}
2	p^n	p^n
3	p^s	p^s
4	$\frac{((p+1)^{p^t}-1)p^s}{p^n}$	$p^{t+1+s-n}$
5	$\frac{((p+1)^{p^t})^{p^m}-1}{p^n}$	$p^{t+m+1-n}$
6	$\frac{((p+1)^{p^t})^{p^m}-1}{(p+1)^{p^t}-1}$	$p^{t+m+1-t-1} = p^m$

We see that expressions 1, 2, 3 and 6 all have at least one p dividing it. So we need to check when $t+1+s-n$ and $t+m+1-n$ are 0.

From *vi*) in theorem 5.1 we have that $m \geq s$ and $s \geq n-t-1$. Hence both $t+1+s-n$ and $t+m+1-n$ are ≥ 0. If $t+1+s-n > 0$, all expressions are divisible by p, and so gcd $\neq 1$. If $t+1+s-n = 0$, then gcd $= 1$, so our lemma follows from theorem 5.7. □

5.3 Families of split metacyclic p-groups of deficiency 0

We will now find and list the families of split metacyclic p-groups of deficiency 0. In the next section we will give the 0-deficiency presentations for these groups.

We have seen that the metacyclic groups of order p^N have a presentation given by the parameters n, m, s and t where $N = n + m$. Let G be a non-abelian split such group.

First, we let $n = N - 1$. By theorem 5.4 we must have $t = N - 3$ and $s = 1$, and so, by lemma 5.8, all groups with $n = N - 1$ will have deficiency 0. We thus get our first family

$$G(N-1, 1, N-3, 1) = \{a, b \mid a^{p^{N-1}} = 1, b^p = a^p, b^{-1}ab = a^{(p+1)^{p^{N-3}}}\}$$

which is a family of split metacyclic groups of order p^N for $N \geq 3$, of deficiency 0.

Now, assume $n = N - 2$. Theorem 5.4 gives us $N \geq 4$, $s = 2$ and $t \in (\max(0, N-5), \ldots, N-4)$. The condition for 0-deficiency (lemma 5.8) implies $t = N - 5$, so in fact $N \geq 5$ here. We get that

$$G(N-2, 2, N-5, 2) = \{a, b \mid a^{p^{N-2}} = 1, b^{p^2} = a^{p^2}, b^{-1}ab = a^{(p+1)^{p^{N-5}}}\}$$

is a family of split metacyclic groups of order p^N, for $N \geq 5$, of deficiency 0. The groups in this family, up to order p^9, are

Order	n	t	s	Presentation
p^5	3	0	2	$\{a, b \mid a^{p^3} = 1, b^{p^2} = a^{p^2}, b^{-1}ab = a^{p+1}\}$
p^6	4	1	2	$\{a, b \mid a^{p^4} = 1, b^{p^2} = a^{p^2}, b^{-1}ab = a^{(p+1)^p}\}$
p^7	5	2	2	$\{a, b \mid a^{p^5} = 1, b^{p^2} = a^{p^2}, b^{-1}ab = a^{(p+1)^{p^2}}\}$
p^8	6	3	2	$\{a, b \mid a^{p^6} = 1, b^{p^2} = a^{p^2}, b^{-1}ab = a^{(p+1)^{p^3}}\}$
p^9	7	4	2	$\{a, b \mid a^{p^7} = 1, b^{p^2} = a^{p^2}, b^{-1}ab = a^{(p+1)^{p^4}}\}$

We see that, in general, for groups of deficiency 0, $n \neq s$, otherwise we get $t = -1$ (by theorem 5.4), so since $n = N - m$, we must have $s = m$, again by theorem 5.4. Lemma 5.8 then gives $t = N - 2m - 1$, and hence $N \geq 2m + 1$.

This all means that we get the following theorem (which is also found in Beyl's paper, see [4]):

Theorem 5.9 *The groups* $G(N-m, m, N-2m-1, m)$ *for* $m \in \{1, 2, 3, \ldots\}$ *where*

$$\begin{aligned} &G(N-m, m, N-2m-1, m) \\ =&\{a, b \mid a^{p^{N-m}} = 1, b^{p^m} = a^{p^m}, b^{-1}ab = a^{(p+1)^{p^{N-2m-1}}}\}, \end{aligned}$$

will, for each m*, give us a family of isomorphism classes of split metacyclic groups of order* p^N*, for* $N \geq 2m + 1$*, of deficiency 0. Moreover, each split metacyclic p-group of deficiency 0 belongs to one, and only one, of these families.* □

5.4 0-deficiency presentations

From theorem 5.7 we have seen that a metacyclic group can be represented with two generators and two relations if and only if it is a Schur group, i.e. $\mathrm{H}_2(G, \mathbb{Z}) = 0$. This is also a result in Beyl's paper, see [4], and from his proof we deduce the following lemma:

Lemma 5.10 *Let G be a metacyclic p-group of deficiency 0 with generators a and b. Then the group of relations for G is generated by*

$$[a, b] = a^{p^{t+1}} \quad \text{and} \quad b^{p^m} = a^{p^{n-t-1}}.$$

Proof: Since $(p+1)^{p^t} - 1 \equiv p^{t+1} \pmod{p^n}$ by lemma 5.5, we have

$$[a, b] = a^{-1}b^{-1}ab = a^{(p+1)^{p^t}-1} = a^{p^{t+1}},$$

hence the relation $[a, b] = a^{p^{t+1}}$ clearly holds for all metacyclic p-groups.

For metacyclic p-groups of deficiency 0, we know that $s = n - t - 1$, so $b^{p^m} = a^{p^s}$ becomes $b^{p^m} = a^{p^{n-t-1}}$.

Let us check that we get $a^{p^n} = 1$ from these relations:

$$\begin{aligned} a^{p^{n-t-1}} &= b^{-1}a^{p^{n-t-1}}b \\ &= (b^{-1}ab)^{p^{n-t-1}} \\ &= (aa^{-1}b^{-1}ab)^{p^{n-t-1}} \\ &= a^{p^{n-t-1}}[a, b]^{p^{n-t-1}}, \end{aligned}$$

hence $[a, b]^{p^{n-t-1}} = 1$, and so $(a^{p^{t+1}})^{p^{n-t-1}} = 1$. □

We will now give another 0-deficiency presentations for the *split* metacyclic groups of order p^N, and we will do this using the families we have introduced in the previous section. There will be a few exceptions in the presentations we give (for small N), but we know exactly how many there will be.

These presentations will be nice from a cohomological point of view, in the sense that they involve the "right" combination of commutators and p^{th} powers. "Right" means that the product structure on $\mathrm{H}^1(G, \mathbb{F}_p)$ and $\mathrm{H}^2(G, \mathbb{F}_p)$ for these groups will be given by strictly defined Massey products, applying theorems 4.5 and 4.6. The presentations came out after considering various possibilities in the tree construction in appendix B and we will come back to them in example 5.28.

We have seen in theorem 5.9 that for metacyclic groups of order p^N of deficiency 0, we only need two parameters, m and N, and these will be used in our presentations as well.

Theorem 5.11 *$G(N-m, m, N-2m-1, m)$ has a minimal presentation given by*

$$G(m, N-2m) = \{a, b \mid a^{p^m}[a,b] = 1, b^{p^{N-2m}}[a,b] = 1\} \quad \textit{for } N \geq 3m.$$

Moreover, this presentation is symmetric in a and b, in the sense that

$$G(N-2m, m) \simeq G(m, N-2m).$$

Proof: First of all, note that these presentations are symmetric because we can change the names of the generators. Because of this symmetry, we require $N-2m \geq m$, hence we get $N \geq 3m$. It is because of this we get exceptions to these presentations (see more on this after the proof).

Next, we want to show that the presentations

i) $\{a, b \mid a^{p^{N-m}} = 1, b^{p^m} = a^{p^m}, b^{-1}ab = a^{(p+1)^{p^{N-2m-1}}}\}$

ii) $\{a, b \mid a^{p^m}[a,b] = 1, b^{p^{N-2m}}[a,b] = 1\}$

iii) $\{a, b \mid a^{p^{N-2m}}[b,a] = 1, b^{p^m}[b,a] = 1\}$

give isomorphic groups. ii) and iii) are the symmetric presentations, and so we will show that i) and iii) are isomorphic.

By the proof of lemma 5.5, we see that

$$(p+1)^{p^{N-2m-1}} - 1 \equiv p^{N-2m} \pmod{p^{N-m}}$$

and so the relations $b^{-1}ab = a^{(p+1)^{p^{N-2m-1}}}$ and $a^{p^{N-m}} = 1$ give us

$$a^{p^{N-2m}}[b,a] = 1. \tag{5.1}$$

If we multiply through (5.1) by a^{p^m}, we get $[b,a] = a^{p^m}$, and since $b^{p^m} = a^{p^m}$, we have $[b,a] = b^{p^m}$.

On the other hand, if we start with $b^{p^m}[a,b] = 1$ and $a^{p^{N-2m}}[b,a] = 1$ (so $b^{-p^m} = a^{p^{N-2m}}$), we get

$$\begin{aligned} b^{-p^m} &= a^{-1}b^{-p^m}a \\ &= (a^{-1}b^{-1}abb^{-1})^{p^m} \\ &= [a,b]^{p^m}b^{-p^m}. \end{aligned}$$

Hence $[a,b]^{p^m} = 1$, so $(a^{p^{N-2m}})^{p^m} = 1$, and we have $a^{p^{N-m}} = 1$. From this we also get $a^{p^m} = b^{p^m}$. □

Remark 5.12 So $G(N-2m, m)$ and $G(m, N-2m)$ will end up in the same family from theorem 5.9, but the families remain unique. ■

Example 5.13 $G(N-2, 2, N-5, 2)$ has a minimal presentation given by

$$\{a, b \mid a^{p^2}[a,b] = 1, b^{p^{N-4}}[a,b] = 1\} \quad \text{for } N \geq 6.$$

The exception is

Order	n	t	s	Presentation
p^5	3	0	2	$\{a, b \mid a^{p^3} = 1, b^{p^2} = a^{p^2}, b^{-1}ab = a^{p+1}\}$.

■

As mentioned in the beginning of the proof of theorem 5.11, the reason why we get exceptions is that the presentations in theorem 5.11 are symmetric in a and b, so these families will give isomorphic groups for small N. Now, we always want unique families, in the sense that a group should belong to one, and only one, family.

Definition 5.14 *We shall call $G(N-m, m, N-2m-1, m)$ an exception-group if, by including this group in a family $G(m, N)$, the family is no longer unique.*

Since for each m, $G(N-m, m, N-2m-1, m)$ give us unique families of groups of order p^N for $N \geq 2m+1$, whereas $G(m, N)$ give us unique families of groups of order p^N for $N \geq 3m$, there will be $m-1$ exception-groups of order p^N for each m.

We will now consider metacyclic groups from a cohomological point of view.

5.5 Resolution for metacyclic groups

In this section we write down a $\mathbb{Z}G$-free resolution of $\mathbb{Z}$ for metacyclic groups using Beyl's paper, see [4] (correcting a couple of misprints that occur), which we will use to find the cohomology groups $\mathrm{H}^1(G, \mathbb{F}_p)$ and $\mathrm{H}^2(G, \mathbb{F}_p)$ for metacyclic p-groups G, and to calculate the product structure on these cohomology groups.

Theorem 5.15 *Let G be given by the presentation*

$$G = \{a, b | a^\beta = 1, b^\gamma = a^\delta, b^{-1}ab = a^\alpha\}.$$

Then the following complex starts off a $\mathbb{Z}G$-free resolution of $\mathbb{Z}$.

$$\begin{tikzcd} 0 & \mathbb{Z} \arrow[l] & \mathbb{Z}G \arrow[l, "d_0"'] & (\mathbb{Z}G)^2 \arrow[l, "d_1"'] & (\mathbb{Z}G)^3 \arrow[l, "d_2"'] & (\mathbb{Z}G)^4 \arrow[l, "d_3"'] & \cdots \arrow[l] \end{tikzcd}$$

where d_0 is the augmentation map, $d_1 = \begin{pmatrix} a-1 \\ b-1 \end{pmatrix}$, $d_2 = \begin{pmatrix} N & 0 \\ 1-bL_1 & a-1 \\ M & \sum_{j=0}^{\gamma-1} b^j \end{pmatrix}$

and $d_3 = \begin{pmatrix} a-1 & 0 & 0 \\ bL_1 - 1 & N & 0 \\ -\frac{1}{\beta}(\alpha^\gamma - 1) & -\sum_{j=0}^{\gamma-1} b^j L_j & a-1 \\ -b(\frac{\delta\alpha-\delta}{\beta}) & M & b-1 \end{pmatrix}$, *and where*

$N = 1 + a + a^2 + \cdots + a^{\beta-1}$, $L_j = \sum a^i, \quad 0 \leq i < \alpha^j$ *and*

$$M = \begin{cases} -1 - a - a^2 - \cdots - a^{\delta-1} & ,\delta \neq 0 \\ 0 & ,\delta = 0. \end{cases}$$

Proof: To check that this gives us a resolution, we note that we need to have written the matrices the way we have, and not using the transpose, which is more usual. This is because of the relation $b^{-1}ab = a^\alpha$. We give a couple of examples of the calculations needed. As part of showing $d_2 d_1 = 0$, we show that $\begin{pmatrix} 1 - bL_1 & a-1 \end{pmatrix}$ lies in $\ker d_1$:

$$\begin{aligned} &\begin{pmatrix} 1 - bL_1 & a-1 \end{pmatrix} \begin{pmatrix} a-1 \\ b-1 \end{pmatrix} \\ =&(1 - bL_1)(a-1) + (a-1)(b-1) \\ =&(1 - b(1 + a + a^2 + \cdots + a^{\alpha-1}))(a-1) + (ab - b - a + 1) \\ =&-b(a^\alpha - 1) + ab - b \\ =&-ab + b + ab - b \\ =&0 \end{aligned}$$

As another example, we show that $\begin{pmatrix} -b(\frac{\delta\alpha-\delta}{\beta}) & M & b-1 \end{pmatrix}$ lies in $\ker d_2$. Here we get two columns, and we only write down the calculations for the first column. We have the expression

$$-b(\frac{\delta\alpha-\delta}{\beta})(1+a+a^2+\cdots+a^{\beta-1})+M(1-b(1+a+a^2+\cdots+a^{\alpha-1}))+(b-1)M.$$

If $\delta = 0$, this is 0, so assume $\delta \neq 0$:

$$= -b(\frac{\delta\alpha - \delta}{\beta})(1 + a + a^2 + \cdots + a^{\beta-1})$$
$$+(-1-a-\cdots-a^{\delta-1})(1-b(1+a+a^2+\cdots+a^{\alpha-1}))+(b-1)(-1-a-\cdots-a^{\delta-1})$$

$$\begin{aligned}
=& -b(\frac{\delta\alpha - \delta}{\beta})(1 + a + a^2 + \cdots + a^{\beta-1})\\
&-1 - a - a^2 - \cdots - a^{\delta-1}\\
&+(1 + a + a^2 + \cdots + a^{\delta-1})b\\
&+(1 + a + a^2 + \cdots + a^{\delta-1})ba\\
&\vdots\\
&+(1 + a + a^2 + \cdots + a^{\delta-1})ba^{\alpha-1}\\
&-b - ba - \cdots - ba^{\delta-1} + 1 + a + \cdots + a^{\delta-1}\\
=& -b(\frac{\delta\alpha - \delta}{\beta})(1 + a + a^2 + \cdots + a^{\beta-1})\\
&-1 - a - a^2 - \cdots - a^{\delta-1}\\
&+b(1 + a^{\alpha} + a^{2\alpha} + \cdots + a^{(\delta-1)\alpha})\\
&+b(a + a^{\alpha+1} + a^{2\alpha+1} + \cdots + a^{(\delta-1)\alpha+1})\\
&\vdots\\
&+b(a^{\alpha-1} + a^{\alpha+(\alpha-1)} + a^{2\alpha+(\alpha-1)} + \cdots + a^{(\delta-1)\alpha+(\alpha-1)})\\
&-b - ba - \cdots - ba^{\delta-1} + 1 + a + \cdots + a^{\delta-1}\\
=& -b(\frac{\delta\alpha - \delta}{\beta})(1 + a + a^2 + \cdots + a^{\beta-1})\\
&+b(1 + a + a^2 + \cdots + a^{\delta\alpha-1}) \quad \delta\alpha \text{ terms}\\
&-b(1 + a + a^2 + \cdots + a^{\delta-1}) \quad \delta \text{ terms}\\
=&0 \quad \text{since } a^{\beta} = 1.
\end{aligned}$$

□

5.6 Calculating $\mathrm{H}^{\mathbf{1}}(\mathbf{G},\mathbb{F}_{\mathbf{p}})$ and $\mathrm{H}^{\mathbf{2}}(\mathbf{G},\mathbb{F}_{\mathbf{p}})$ for metacyclic p-groups

To calculate $\mathrm{H}^1(G,\mathbb{F}_p)$ and $\mathrm{H}^2(G,\mathbb{F}_p)$, we need an $\mathbb{F}_pG$-free resolution of $\mathbb{F}_p$. To get this, we use the resolution in theorem 5.15, and reduce the matrix-entries mod p. First of all, we introduce the parameters n, m, t and s again, by putting

$$\alpha = q = (p+1)^{p^t},\ \ \beta = p^n,\ \ \gamma = p^m \ \text{ and } \ \delta = p^s.$$

This gives us the, by now, familiar presentation

$$G = \{a, b | a^{p^n} = 1, b^{p^m} = a^{p^s}, b^{-1}ab = a^{(p+1)^{p^t}}\}.$$

Theorem 5.1 told us that

$$((p+1)^{p^t})^{p^m} \equiv 1 \pmod{p^n} \ \text{ and } \ p^s((p+1)^{p^t} - 1) \equiv 0 \pmod{p^n},$$

hence there exist $\sigma, \tau \in \mathbb{Z}$ so that

$$((p+1)^{p^t})^{p^m} - 1 = \sigma p^n \ \text{ and } \ p^s((p+1)^{p^t} - 1) = \tau p^n. \tag{5.2}$$

We get an $\mathbb{F}_pG$-free resolution of $\mathbb{F}_p$,

$$\begin{tikzcd}
0 & \mathbb{F}_p \arrow[l] & \mathbb{F}_pG \arrow[l, "d_0"'] & (\mathbb{F}_pG)^2 \arrow[l, "d_1"'] & (\mathbb{F}_pG)^3 \arrow[l, "d_2"'] & (\mathbb{F}_pG)^4 \arrow[l, "d_3"'] & \cdots \arrow[l]
\end{tikzcd}$$

where d_0, d_1 and d_2 are the same as in the $\mathbb{Z}G$-free resolution using parameters n, m, s and t instead of α, β, γ and δ. So

$$d_2 = \begin{pmatrix} 1 + a + a^2 + \cdots + a^{p^n - 1} & 0 \\ 1 - b(1 + a + a^2 + \cdots + a^{(p+1)^{p^t}}) & a - 1 \\ -1 - a - a^{-} \cdots - a^{p^s - 1} & 1 + b + b^2 + \cdots + b^{p^m - 1} \end{pmatrix} \tag{5.3}$$

whereas d_3 will change in two of its entries, namely

$$-\frac{1}{\beta}(\alpha^\gamma - 1) = -\frac{1}{p^n}(((p+1)^{p^t})^{p^m} - 1) = -\sigma$$

and

$$\frac{\delta\alpha - \delta}{\beta} = \frac{1}{p^n}(p^s((p+1)^{p^t} - 1)) = \tau.$$

To find the cohomology groups, we use $\mathrm{Hom}_{\mathbb{F}_pG}(-,\mathbb{F}_p)$ to get

$$\begin{tikzcd} 0 \arrow[r, "d^0"] & \mathbb{F}_p \arrow[r, "d^1"] & (\mathbb{F}_p)^2 \arrow[r, "d^2"] & (\mathbb{F}_p)^3 \arrow[r, "d^3"] & (\mathbb{F}_p)^4 \arrow[r] & \cdots \end{tikzcd}$$

where the differentials d^i, for $i \geq 1$, will be the transpose of the d_i-s, with entries induced by the augmentation map. Hence, d^1 will be the 0-map, and we also see that all the entries in d^2, induced from (5.3), are either 0 or divisible by p, so d^2 is also the 0-map. This means that

$$\mathrm{H}^1(G,\mathbb{F}_p) = \frac{\ker d^2}{\operatorname{im} d^1} \simeq (\mathbb{F}_p)^2$$

and

$$\mathrm{H}^2(G,\mathbb{F}_p) = \frac{\ker d^3}{\operatorname{im} d^2} = \ker d^3.$$

We see that

$$d^3 = \begin{pmatrix} 0 & 0 & \sigma & \tau \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

and so $\dim_{\mathbb{F}_p} \mathrm{H}^2(G,\mathbb{F}_p)$ is either 2 or 3.

Lemma 5.16 *Let G be a metacyclic p-group with parameters n, m, s and t. Then $\dim_{\mathbb{F}_p} \mathrm{H}^2(G,\mathbb{F}_p) = 2$ if, and only if, $t + s + 1 - n = 0$.*

Proof: We use the following: We know that $m \geq s$ and $t + s + 1 - n \geq 0$ by theorem 5.1, hence we have (recall (5.2) and lemma 5.5):

$$\begin{aligned}
&\text{If } t+m+1>n, \text{ then } \sigma = 0 \text{ in } \mathbb{F}_p.\\
&\text{If } t+m+1=n, \text{ then } \sigma \neq 0 \text{ in } \mathbb{F}_p.\\
&\text{If } t+s+1>n, \text{ then } \tau = 0 \text{ in } \mathbb{F}_p.\\
&\text{If } t+s+1=n, \text{ then } \tau \neq 0 \text{ in } \mathbb{F}_p.
\end{aligned}$$

So suppose $\dim \mathrm{H}^2(G, \mathbb{F}_p) = 2$, then $\dim \ker d^3 = 1$, hence either σ or $\tau \neq 0$. If $\sigma \neq 0, t+m+1-n = 0$, and therefore $t+s+1-n = 0$ since $t+s+1-n \geq 0$ and $m \geq s$. If $\tau \neq 0, t+s+1-n = 0$.

Conversely, if $t+s+1-n=0$, then $\tau \neq 0$, and $\dim \mathrm{H}^2(G,\mathbb{F}_p) = 2$. □

Remark 5.17 Using theorem 2.30 and lemma 5.8, this means that metacyclic p-groups have deficiency 0, both as an abstract group and as a finite pro-p group, iff $t+s+1-n=0$.

During the viva it was pointed out that for a finite p-group G, the Schur multiplier is trivial iff G has deficiency 0 as a pro-p group. This follows from the Universal Coefficient Theorem. ■

5.7 Massey products for metacyclic p-groups

We will now use the Yoneda cocomplex introduced in section 2.5 to calculate Massey products of metacyclic p-groups. So let G be a metacyclic p-group, and let $\{\xi_1, \xi_2\}$ be a basis for $\mathrm{H}^1(G, \mathbb{F}_p)$. We go back to denoting differentials by δ.

We will need the first three differentials of the $\mathbb{F}_pG$-free resolution $F_\bullet$, so recall

$$\begin{tikzcd}
0 & \mathbb{F}_p \arrow[l] & \mathbb{F}_pG \arrow[l, "\delta_0"'] & (\mathbb{F}_pG)^2 \arrow[l, "\delta_1"'] & (\mathbb{F}_pG)^3 \arrow[l, "\delta_2"'] & \cdots \arrow[l]
\end{tikzcd}$$

where δ_0 is the augmentation map, $\delta_1 = \begin{pmatrix} a-1 \\ b-1 \end{pmatrix}$ and

$$\delta_2 = \begin{pmatrix} 1+a+a^2+\cdots+a^{p^n-1} & 0 \\ 1-b(1+a+a^2+\cdots+a^{(p+1)^{p^t}}) & a-1 \\ -1-a-a^{-}\cdots-a^{p^s-1} & 1+b+b^2+\cdots+b^{p^m-1} \end{pmatrix}.$$

We use the notation from section 3.3 for the different maps in the Yoneda cocomplex. Also, recall the various diagrams we introduced in that section. First, we calculate $(\psi_1)_1, (\psi_1)_2, (\psi_2)_1$ and $(\psi_2)_2$ in diagram (3.7). We see that

$$\delta_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rho = 0,$$

and

$$\delta_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \rho = 0,$$

hence $(\psi_1)_1 = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ and $(\psi_2)_1 = \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$ are cocycles and so we can use the standard basis here (recall remark 3.11). We now lift $(\psi_1)_1$ and $(\psi_2)_1$ to get $(\psi_1)_2$ and $(\psi_2)_2$, so put $(\psi_1)_2 = \left(\begin{smallmatrix} c & d \\ e & f \\ g & h \end{smallmatrix}\right)$. We need to have

$$\delta_2 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} c & d \\ e & f \\ g & h \end{pmatrix} \delta_1,$$

and so we need to solve the equations

$$c(a-1)+d(b-1) = 1+a+a^2+\cdots+a^{p^n-1} \tag{5.4}$$

$$e(a-1)+f(b-1) = 1-b(1+a+a^2+\cdots+a^{(p+1)^{p^t}}) \tag{5.5}$$

$$g(a-1)+h(b-1) = -1-a-a^2-\cdots-a^{p^s-1} \tag{5.6}$$

where a, b are the generators for G and c, d, e, f, g and h are elements of $\mathbb{F}_pG$.

Remark 5.18 We will now make use of the fact that we are in characteristic p, and add and subtract terms that are divisible by p. ■

Consider (5.4):

and so we choose

$$\begin{aligned} c =&(1+(a+1)+(a^2+a+1)+\cdots+(a^{p^n-2}+a^{p^n-3}+\cdots+a+1))\\ d =&0. \end{aligned}$$

For (5.5) we note that $(p+1)^{p^t}-1$ is divisible by p by lemma 5.5. Hence we add and subtract to get

$$\begin{aligned} &1-b(1+a+a^2+\cdots+a^{(p+1)^{p^t}-1})\\ =&-(b-1)\\ &-b((1-1)+(a-1)+(a^2-1)+\cdots+(a^{(p+1)^{p^t}-1}-1))-b((p+1)^{p^t}-1)\\ =&-(b-1)\\ &-B(1+(a+1)+(a^2+a+1)+\cdots+(a^{(p+1)^{p^t}-2}+\cdots+a+1))(a-1), \end{aligned}$$

and so we put

$$\begin{aligned} e =&-b(1+(a+1)+(a^2+a+1)+\cdots+(a^{(p+1)^{p^t}-2}+\cdots+a+1))\\ f =&-1. \end{aligned}$$

Similarly, we find

$$\begin{aligned} g =&-(1+(a+1)+(a^2+a+1)+\cdots+(a^{p^s-2}+a^{p^s-3}+\cdots+a+1))\\ h =&0. \end{aligned}$$

Hence,

$$\begin{aligned} &\begin{pmatrix} c & d\\ e & f\\ g & h \end{pmatrix}\\ =&\begin{pmatrix} (1+(a+1)+(a^2+a+1)+\cdots+(a^{p^n-2}+\cdots+a+1)) & 0\\ -b(1+(a+1)+(a^2+a+1)+\cdots+(a^{(p+1)^{p^t}-2}+\cdots+a+1)) & -1\\ -(1+(a+1)+(a^2+a+1)+\cdots+(a^{p^s-2}+\cdots+a+1)) & 0 \end{pmatrix}. \end{aligned}$$

Next, we find the lifting of $\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$, so put $(\psi_2)_2 = \left(\begin{smallmatrix}c' & d'\\ e' & f'\\ g' & h'\end{smallmatrix}\right)$. Then we need to have

$$\delta_2 \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}c' & d'\\ e' & f'\\ g' & h'\end{pmatrix} \delta_1,$$

and so we get the equations

$$c'(a-1) + d'(b-1) = 0 \tag{5.7}$$

$$e'(a-1) + f'(b-1) = a-1 \tag{5.8}$$

$$g'(a-1) + h'(b-1) = 1 + b + b^2 + \cdots + b^{p^m-1}, \tag{5.9}$$

where a, b are the generators for G and c', d', e', f', g' and h' are elements of $\mathbb{F}_pG$. Equation (5.9) is solved similarly to (5.4), and we find

$$\begin{pmatrix}c' & d'\\ e' & f'\\ g' & h'\end{pmatrix} = \begin{pmatrix}0 & 0\\ 1 & 0\\ 0 & 1 + (b+1) + (b^2+b+1) + \cdots + (b^{p^m-2} + \cdots + b + 1)\end{pmatrix}.$$

We can now calculate the product $\langle \xi_1, \xi_2; 0\rangle$ using the following diagram:

$$\begin{tikzcd}
\mathbb{F}_p & \mathbb{F}_pG \arrow[l, two heads] & (\mathbb{F}_pG)^2 \arrow[l] & (\mathbb{F}_pG)^3 \arrow[l] \arrow[dl, shift right, "\left(\begin{smallmatrix}c & d\\ e & f\\ g & h\end{smallmatrix}\right)"'] \arrow[dl, shift left, "\left(\begin{smallmatrix}c' & d'\\ e' & f'\\ g' & h'\end{smallmatrix}\right)"] & \cdots \arrow[l] \\
\mathbb{F}_p & \mathbb{F}_pG \arrow[l, two heads] & (\mathbb{F}_pG)^2 \arrow[l] \arrow[dl, shift right, "\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)"'] \arrow[dl, shift left, "\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)"] & (\mathbb{F}_pG)^3 \arrow[l] & \cdots \arrow[l] \\
\mathbb{F}_p & \mathbb{F}_pG \arrow[l, two heads, "\rho"'] & (\mathbb{F}_pG)^2 \arrow[l] & (\mathbb{F}_pG)^3 \arrow[l] & \cdots \arrow[l]
\end{tikzcd}$$

The product is an element in $\mathrm{Ext}^2_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$, and so we need to compose our maps with ρ, hence we get the products

$$\langle \xi_1, \xi_1; 0\rangle = \begin{pmatrix} c & d \\ e & f \\ g & h \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rho$$

$$= \begin{pmatrix} (1 + (a+1) + (a^2+a+1) + \cdots + (a^{p^n-2} + \cdots + a + 1)) \\ -b(1 + (a+1) + (a^2+a+1) + \cdots + (a^{(p+1)^{p^t}-2} + \cdots + a + 1))) \\ -(1 + (a+1) + (a^2+a+1) + \cdots + (a^{p^s-2} + \cdots + a + 1)) \end{pmatrix} \rho$$

$$= \begin{pmatrix} 1 + 2 + 3 + \cdots + (p^n - 1) \\ -(1 + 2 + 3 + \cdots + ((p+1)^{p^t} - 1)) \\ -(1 + 2 + 3 + \cdots + (p^s - 1)) \end{pmatrix}$$

$$= \begin{pmatrix} \frac{(p^n-1)p^n}{2} \\ -\frac{((p+1)^{p^t}-1)(p+1)^{p^t}}{2} \\ -\frac{(p^s-1)p^s}{2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

since we are in $\mathbb{F}_p$, p is odd and $(p+1)^{p^t}-1$ is divisible by p by lemma 5.5,

$$\langle \xi_1, \xi_2; 0\rangle = \begin{pmatrix} c & d \\ e & f \\ g & h \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \rho = \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix},$$

$$\langle \xi_2, \xi_1; 0\rangle = \begin{pmatrix} c' & d' \\ e' & f' \\ g' & h' \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rho = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},$$

which gives us the antisymmetry for the cup product and

$$\langle \xi_2, \xi_2; 0\rangle = \begin{pmatrix} 0 \\ 0 \\ \frac{(p^m-1)p^m}{2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

again since we are in $\mathbb{F}_p$ and p is odd.

This means that two cup products are zero (as elements in $\mathrm{Ext}^2_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$), and so we know that we will get 3-fold Massey products. We will now consider $\langle \xi_1, \xi_1; 0\rangle$, and the calculations will be very similar for $\langle \xi_2, \xi_2; 0\rangle$.

Since $\langle \xi_1, \xi_1; 0\rangle = 0$, there exists $\phi = \{\phi_i\}_{i\geq 1} \in \mathrm{Hom}^{(1)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet)$ such that $\partial\phi = (\psi_1)_2(\psi_1)_1 = \left(\begin{smallmatrix} c & d \\ e & f \\ g & h \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) := AB$, so consider

$$\begin{tikzcd}
\mathbb{F}_p & \mathbb{F}_pG \arrow[l, two heads] & (\mathbb{F}_pG)^2 \arrow[l] \arrow[ddl, dashed, "\phi_1"'] & (\mathbb{F}_pG)^3 \arrow[l, "\delta_1"'] \arrow[dl, "A"'] \arrow[ddll, squiggly, "AB"] \arrow[ddl, dashed, "\phi_2"] & \cdots \arrow[l] \\
\mathbb{F}_p & \mathbb{F}_pG \arrow[l, two heads] & (\mathbb{F}_pG)^2 \arrow[l] \arrow[dl, "B"'] & (\mathbb{F}_pG)^3 \arrow[l] & \cdots \arrow[l] \\
\mathbb{F}_p & \mathbb{F}_pG \arrow[l, two heads] & (\mathbb{F}_pG)^2 \arrow[l, "\delta_0"] & (\mathbb{F}_pG)^3 \arrow[l] & \cdots \arrow[l]
\end{tikzcd}$$

We need to calculate ϕ_1 and ϕ_2 using the formula

$$\delta_1\phi_1 - \phi_2\delta_0 = AB,$$

i.e. if we put $\phi_1 = \left(\begin{smallmatrix} i \\ j \end{smallmatrix}\right)$ and $\phi_2 = \left(\begin{smallmatrix} k & l \\ m & n \\ o & p \end{smallmatrix}\right)$, we get

$$\delta_1 \begin{pmatrix} i \\ j \end{pmatrix} - \begin{pmatrix} k & l \\ m & n \\ o & p \end{pmatrix} \begin{pmatrix} a-1 \\ b-1 \end{pmatrix} = AB.$$

This means we get the equations

$$\begin{aligned}(1+a+a^2+\cdots+a^{p^n-1})i &- (k(a-1)+l(b-1)) \\ &= (1+(a+1)+(a^2+a+1)+\cdots+(a^{p^n-2}+\cdots+a+1)),\end{aligned} \quad (5.10)$$

$$\begin{aligned}(1-b(1+a+a^2+\cdots+a^{(p+1)^{p^t}-1}))i &+ (a-1)j - (m(a-1)+n(b-1)) \\ &= -b(1+(a+1)+(a^2+a+1)+\cdots+(a^{(p+1)^{p^t}-2}+\cdots+a+1)),\end{aligned} \quad (5.11)$$

$$\begin{aligned}(-1-a-a^2-\cdots-a^{p^s-1})i&+(1+b+b^2+\cdots+b^{p^m-1})j-(o(a-1)+p(b-1)) \\ &= -(1+(a+1)+(a^2+a+1)+\cdots+(a^{p^s-2}+\cdots+a+1)).\end{aligned} \quad (5.12)$$

where a, b are the generators for G and i, j, k, l, m, n, o and p are elements of $\mathbb{F}_pG$.

Remark 5.19 We now observe something important, which will apply to all the liftings of the Massey products that are zero: The expressions on the right hand side in (5.10), (5.11) and (5.12) all lie in the augmentation ideal, so we can choose $i = j = 0$, hence ϕ_1 is the 0-map. ■

To find ϕ_2, we use remark 5.18. This gives us

$$\begin{aligned}
k &= -(1 + [1 + (a + 1)] + [1 + (a + 1) + (a^2 + a + 1)] + \cdots \\
&\qquad\qquad \cdots + [1 + (a + 1) + \cdots + (a^{p^n-3} + \cdots + a + 1)]), \\
l &= 0, \\
m &= b(1 + [1 + (a + 1)] + [1 + (a + 1) + (a^2 + a + 1)] + \cdots \\
&\qquad\qquad \cdots + [1 + (a + 1) + \cdots + (a^{(p+1)^{p^t}-3} + \cdots + a + 1)]), \\
n &= 0, \\
o &= 1 + [1 + (a + 1)] + [1 + (a + 1) + (a^2 + a + 1)] + \cdots \\
&\qquad\qquad \cdots + [1 + (a + 1) + \cdots + (a^{p^s-3} + \cdots + a + 1)], \\
p &= 0,
\end{aligned}$$

and so we calculate the 3-fold Massey product $\langle \xi_1, \xi_1, \xi_1; 0\rangle$ from the formula

$$\langle \xi_1, \xi_1, \xi_1; 0\rangle = ((\psi_1)_2\phi_1 + \phi_2(\psi_1)_1)\rho.$$

This gives us (remember ϕ_1 is zero and $(\psi_1)_1 = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$, and also note that in the middle entry we can (but don't need to) cancel the last term, because of lemma 5.5)

$$\begin{aligned}
&\langle \xi_1, \xi_1, \xi_1; 0\rangle \\
&= \begin{pmatrix} -(1 + (1 + 2) + (1 + 2 + 3) + \cdots + (1 + 2 + 3 + \cdots + (p^n - 2))) \\ 1 + (1 + 2) + (1 + 2 + 3) + \cdots + (1 + 2 + 3 + \cdots + ((p + 1)^{p^t} - 2)) \\ 1 + (1 + 2) + (1 + 2 + 3) + \cdots + (1 + 2 + 3 + \cdots + (p^s - 2)) \end{pmatrix} \\
&= \begin{pmatrix} -(\frac{1\cdot 2}{2} + \frac{2\cdot 3}{2} + \frac{3\cdot 4}{2} + \cdots + \frac{(p^n-2)(p^n-1)}{2}) \\ \frac{1\cdot 2}{2} + \frac{2\cdot 3}{2} + \frac{3\cdot 4}{2} + \cdots + \frac{((p+1)^{p^t}-2)((p+1)^{p^t}-1)}{2} \\ \frac{1\cdot 2}{2} + \frac{2\cdot 3}{2} + \frac{3\cdot 4}{2} + \cdots + \frac{(p^s-2)(p^s-1)}{2} \end{pmatrix}
\end{aligned}$$

$$= \begin{pmatrix} -\frac{1}{2}\sum_{i=1}^{p^n-2} i(i+1) \\ \\ \frac{1}{2}\sum_{i=1}^{(p+1)^{p^t}-2} i(i+1) \\ \\ \frac{1}{2}\sum_{i=1}^{p^s-2} i(i+1) \end{pmatrix}$$

$$= \begin{pmatrix} -\frac{p^n(p^n-1)(p^n-2)}{2\cdot 3} \\ \\ \frac{(p+1)^{p^t}((p+1)^{p^t}-1)((p+1)^{p^t}-2)}{2\cdot 3} \\ \\ \frac{p^s(p^s-1)(p^s-2)}{2\cdot 3} \end{pmatrix}.$$

The last equality is a special case of the following theorem, which is a nice formula from number theory. We prove the result now, because the expressions will appear as we calculate higher order Massey products. The proof was suggested by Roger Heath-Brown.

Theorem 5.20 *Let $n \in \mathbb{N}$. Then*

$$\sum_{i=1}^{p^n-k} i(i+1)\cdots(i+(k-1)) = \frac{p^n(p^n-1)\cdots(p^n-k)}{k+1}$$

for $k \in \{1, 2, \ldots, p^n-1\}$.

Proof: We observe that we can reformulate the result, so that what we want to prove is

$$\sum_{i=1}^{p^n-k} k!\binom{i+(k-1)}{k} = k!\binom{p^n}{k+1}$$

where we define $\binom{n}{k} = 0$ if $k < 0$ or $k > n$. The result holds more generally, not only for prime powers, so let us put $n := p^n$ and change variables in the sum. Then what we get is

$$\sum_{m=1}^{n-1} \binom{m}{k} = \binom{n}{k+1}, \tag{5.13}$$

which is proved by fixing k and doing induction on n. The base step follows as the left hand side is 0 (empty sum) and $\binom{1}{k+1} = 0$. For the induction step we observe that

$$\binom{n}{k+1} + \binom{n}{k} = \binom{n+1}{k+1},$$

and so we are done. Just note that we have fixed k, and that this is OK for $n \geq k+1$. For $n < k+1$, both sides in (5.13) is zero due to the fact that $\binom{n}{k} = 0$ if $k < 0$ or $k > n$, and so everything is fine. $\square$

We will analyse the formulas for the Massey products for different values of n, t and s once we have found a general formula for the Massey products that are defined. I.e. for $\langle \xi_1, \xi_1, \xi_1; 0\rangle$ we see that some values for n, t and s will give that this Massey product is non-zero, and so for these values of n, t and s, we can't find $\langle \xi_1, \xi_1, \xi_1, \xi_1; 0\rangle$.

However, in order to get the general formula for $\langle \underbrace{\xi_1, \xi_1, \ldots, \xi_1}_{i}; 0\rangle$, we will assume that we are working with the values of the parameters n, t and s such that $\langle \underbrace{\xi_1, \xi_1, \ldots, \xi_1}_{i-1}; 0\rangle = 0$. Under this assumption, we will now hunt for the general formula for $\langle \underbrace{\xi_1, \xi_1, \ldots, \xi_1}_{i}; 0\rangle$.

Let us first calculate the 4-fold Massey product, i.e. assume $\langle \xi_1, \xi_1, \xi_1; 0\rangle$ is 0 (as an element in $\mathrm{Ext}^2_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$). Then there exists $\mu = \{\mu_i\}_{i\geq 1} \in \mathrm{Hom}^{(1)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet)$ such that $\partial\mu = (\psi_1)_2\phi_1 + \phi_2(\psi_1)_1$. As before, this gives us the diagram

$$\begin{tikzcd}
\mathbb{F}_p & \mathbb{F}_pG \arrow[l, two heads] & (\mathbb{F}_pG)^2 \arrow[l] \arrow[dddl, dashed, "\mu_1"'] & (\mathbb{F}_pG)^3 \arrow[l, "\delta_1"'] \arrow[dddll, squiggly, "(\psi_1)_2\phi_1+\phi_2(\psi_1)_1"'] \arrow[dddl, dashed, "\mu_2"] & \cdots \arrow[l] \\
\mathbb{F}_p & \mathbb{F}_pG \arrow[l, two heads] & (\mathbb{F}_pG)^2 \arrow[l] & (\mathbb{F}_pG)^3 \arrow[l] & \cdots \arrow[l] \\
\mathbb{F}_p & \mathbb{F}_pG \arrow[l, two heads] & (\mathbb{F}_pG)^2 \arrow[l] & (\mathbb{F}_pG)^3 \arrow[l] & \cdots \arrow[l] \\
\mathbb{F}_p & \mathbb{F}_pG \arrow[l, two heads] & (\mathbb{F}_pG)^2 \arrow[l, "\delta_0"] & (\mathbb{F}_pG)^3 \arrow[l] & \cdots \arrow[l]
\end{tikzcd}$$

and we can immediately deduce that μ_1 is the zero map, by the observation in remark 5.19. Put $\mu_2 = \begin{pmatrix} q & r \\ s & t \\ u & v \end{pmatrix}$, then this gives the following equations.

$$\begin{aligned}
&-(q(a-1)+r(b-1)) \\
&\qquad = -(1+[1+(a+1)]+[1+(a+1)+(a^2+a+1)]+\cdots \\
&\qquad\qquad \cdots+[1+(a+1)+\cdots+(a^{p^n-3}+\cdots+a+1)]), \quad (5.14)
\end{aligned}$$

$$\begin{aligned}
&-(s(a-1)+t(b-1)) \\
&\qquad = b(1+[1+(a+1)]+[1+(a+1)+(a^2+a+1)]+\cdots \\
&\qquad\qquad \cdots+[1+(a+1)+\cdots+(a^{(p+1)p^t-3}+\cdots+a+1)]) \quad (5.15)
\end{aligned}$$

$$\begin{aligned}
&-(u(a-1)+v(b-1)) \\
&\qquad = 1+[1+(a+1)]+[1+(a+1)+(a^2+a+1)]+\cdots \\
&\qquad\qquad \cdots+[1+(a+1)+\cdots+(a^{p^s-3}+\cdots+a+1)] \quad (5.16)
\end{aligned}$$

where a, b are the generators for G and q, r, s, t, u and v are elements of $\mathbb{F}_pG$. As we solve equation (5.14), we see a pattern developing. We still apply the trick in remark 5.18:

$$\begin{aligned}&-(1+[1+(a+1)]+[1+(a+1)+(a^2+a+1)]+\cdots\\&\qquad\cdots+[1+(a+1)+\cdots+(a^{p^n-3}+\cdots+a+1)])\\=&-((a-1)+[(a-1)+((a^2-1)+(a-1))]\\&+[(a-1)+((a^2-1)+(a-1))+((a^3-1)+(a^2-1)+(a-1))]+\cdots\\&\cdots+[(a-1)+((a^2-1)+(a-1))+((a^3-1)+(a^2-1)+(a-1))+\cdots\\&\cdots+((a^{p^n-3}-1)+\cdots+(a-1))]+\frac{1\cdot 2+2\cdot 3+\cdots+(p^n-2)(p^n-1)}{2})\end{aligned}$$

Remark 5.21 We note that the number of 1-s we subtract (and hence we add at the end) will always be 0 in characteristic p, because it is the number that we get in the formula for the previous Massey products, and we assume we are working with the values of n, t and s that makes this 0 (otherwise the next Massey product wouldn't be defined). ■

Let us finish the calculation of equation (5.14):

$$\begin{aligned}=&-(1+[1+(1+(a+1))]+\\&\qquad+[1+(1+(a+1))+(1+(a+1)+(a^2+a+1))]+\cdots\\&\qquad\cdots+[1+(1+(a+1))+(1+(a+1)+(a^2+a+1))+\cdots\\&\qquad\quad\cdots+(1+(a+1)+\cdots+(a^{p^n-4}+\cdots+a+1))])(a-1),\end{aligned}$$

and so we choose

$$\begin{aligned}q=&1+[1+(1+(a+1))]+\\&\qquad+[1+(1+(a+1))+(1+(a+1)+(a^2+a+1))]+\cdots\\&\qquad\cdots+[1+(1+(a+1))+(1+(a+1)+(a^2+a+1))+\cdots\\&\qquad\quad\cdots+(1+(a+1)+\cdots+(a^{p^n-4}+\cdots+a+1))],\\r=&0.\end{aligned}$$

Remark 5.22 We have calculated the liftings $\phi_2 = \begin{pmatrix} k & l \\ m & n \\ o & p \end{pmatrix}$ and $\mu_2 = \begin{pmatrix} q & r \\ s & t \\ u & v \end{pmatrix}$. Let us at this stage just note that we get the terms for q (terms are in [ ]-brackets) by using k. We get the n-th term for q by adding the n-th term of k to the $(n-1)$-st term of q. We will make this more precise soon. ■

Similarly, we choose

$$\begin{aligned} s =& - b(1 + [1 + (1 + (a+1))]+ \\ & \qquad + [1 + (1 + (a+1)) + (1 + (a+1) + (a^2+a+1))] + \cdots \\ & \qquad \cdots + [1 + (1 + (a+1)) + (1 + (a+1) + (a^2+a+1)) + \cdots \\ & \qquad\quad \cdots + (1 + (a+1) + \cdots + (a^{(p+1)p^t-4} + \cdots + a + 1))]), \\ t =& 0, \end{aligned}$$

$$\begin{aligned} u =& - (1 + [1 + (1 + (a+1))]+ \\ & \qquad + [1 + (1 + (a+1)) + (1 + (a+1) + (a^2+a+1))] + \cdots \\ & \qquad \cdots + [1 + (1 + (a+1)) + (1 + (a+1) + (a^2+a+1)) + \cdots \\ & \qquad\quad \cdots + (1 + (a+1) + \cdots + (a^{p^s-4} + \cdots + a + 1))]), \end{aligned}$$

$$v = 0,$$

and so we have the entries in the matrix for μ_2.

To calculate $\langle \xi_1, \xi_1, \xi_1, \xi_1; 0 \rangle$, we have the formula

$$\langle \xi_1, \xi_1, \xi_1, \xi_1; 0 \rangle = ((\psi_1)_2\mu_1 + \phi_2\phi_1 + \mu_2(\psi_1)_1)\rho$$

and the following diagram.

$$\begin{tikzcd}
\mathbb{F}_p & \mathbb{F}_pG \arrow[l, two heads] & (\mathbb{F}_pG)^2 \arrow[l] & (\mathbb{F}_pG)^3 \arrow[l] \arrow[dl, "(\psi_1)_2"'] \arrow[ddll, dashed] & \cdots \arrow[l] \\
\mathbb{F}_p & \mathbb{F}_pG \arrow[l, two heads] & (\mathbb{F}_pG)^2 \arrow[l] \arrow[dl, "\mu_1"'] & (\mathbb{F}_pG)^3 \arrow[l] & \cdots \arrow[l] \\
\mathbb{F}_p & \mathbb{F}_pG \arrow[l, two heads] & (\mathbb{F}_pG)^2 \arrow[l] & (\mathbb{F}_pG)^3 \arrow[l] \arrow[dl, "\phi_2"'] \arrow[ddll, dashed] & \cdots \arrow[l] \\
\mathbb{F}_p & \mathbb{F}_pG \arrow[l, two heads] & (\mathbb{F}_pG)^2 \arrow[l] \arrow[dl, "\phi_1"'] & (\mathbb{F}_pG)^3 \arrow[l] & \cdots \arrow[l] \\
\mathbb{F}_p & \mathbb{F}_pG \arrow[l, two heads] & (\mathbb{F}_pG)^2 \arrow[l] & (\mathbb{F}_pG)^3 \arrow[l] \arrow[dl, "\mu_2"'] \arrow[ddll, dashed] & \cdots \arrow[l] \\
\mathbb{F}_p & \mathbb{F}_pG \arrow[l, two heads] & (\mathbb{F}_pG)^2 \arrow[l] \arrow[dl, "(\psi_1)_1"'] & (\mathbb{F}_pG)^3 \arrow[l] & \cdots \arrow[l] \\
\mathbb{F}_p & \mathbb{F}_pG \arrow[l, two heads, "\rho"'] & (\mathbb{F}_pG)^2 \arrow[l] & (\mathbb{F}_pG)^3 \arrow[l] & \cdots \arrow[l]
\end{tikzcd}$$

We have seen that ϕ_1 and μ_1 can both be chosen to be the 0-maps by remark 5.19. Moreover, we have $(\psi_1)_1 = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$, hence

$$\langle \xi_1, \xi_1, \xi_1, \xi_1; 0\rangle = \mu_2(\psi_1)_1\rho = \begin{pmatrix} q \\ s \\ u \end{pmatrix} \rho.$$

ρ is the augmentation map, and we get that $\langle \xi_1, \xi_1, \xi_1, \xi_1; 0\rangle$, as an element of $\mathrm{Ext}^2_{\mathbb{F}_pG}(\mathbb{F}_p,\mathbb{F}_p)$, is

$$\begin{pmatrix} \begin{pmatrix} \begin{array}{c} 1+[1+(1+(a+1))]+ \\ +[1+(1+(a+1))+(1+(a+1)+(a^2+a+1))]+\cdots \\ \cdots+[1+(1+(a+1))+(1+(a+1)+(a^2+a+1))+\cdots \\ \cdots+(1+(a+1)+\cdots+(a^{p^n-4}+\cdots+a+1))] \end{array} \end{pmatrix} \\ \\ \begin{pmatrix} \begin{array}{c} (-b(1+[1+(1+(a+1))]+ \\ +[1+(1+(a+1))+(1+(a+1)+(a^2+a+1))]+\cdots \\ \cdots+[1+(1+(a+1))+(1+(a+1)+(a^2+a+1))+\cdots \\ \cdots+(1+(a+1)+\cdots+(a^{(p+1)^{p^t}-4}+\cdots+a+1))]) \end{array} \end{pmatrix} \\ \\ \begin{pmatrix} \begin{array}{c} -(1+[1+(1+(a+1))]+ \\ +[1+(1+(a+1))+(1+(a+1)+(a^2+a+1))]+\cdots \\ \cdots+[1+(1+(a+1))+(1+(a+1)+(a^2+a+1))+\cdots \\ \cdots+(1+(a+1)+\cdots+(a^{p^s-4}+\cdots+a+1))]) \end{array} \end{pmatrix} \end{pmatrix} \rho$$

$$= \begin{pmatrix} \begin{pmatrix} \begin{array}{c} 1+[1+(1+2)]+[1+(1+2)+(1+2+3)]+\cdots \\ \cdots+[1+(1+2)+(1+2+3)+\cdots+(1+2+\cdots+(p^n-3))] \end{array} \end{pmatrix} \\ \\ \begin{pmatrix} \begin{array}{c} -(1+[1+(1+2)]+[1+(1+2)+(1+2+3)]+\cdots \\ \cdots+[1+(1+2)+(1+2+3)+\cdots+(1+2+\cdots+((p+1)^{p^t}-3))]) \end{array} \end{pmatrix} \\ \\ \begin{pmatrix} \begin{array}{c} -(1+[1+(1+2)]+[1+(1+2)+(1+2+3)]+\cdots \\ \cdots+[1+(1+2)+(1+2+3)+\cdots+(1+2+\cdots+(p^s-3))]) \end{array} \end{pmatrix} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{1\cdot 2}{2} + [\frac{1\cdot 2+2\cdot 3}{2}] + [\frac{1\cdot 2+2\cdot 3+3\cdot 4}{2}] + \cdots + [\frac{1\cdot 2+2\cdot 3+3\cdot 4+\cdots+(p^n-3)(p^n-2)}{2}] \\ \\ -(\frac{1\cdot 2}{2} + [\frac{1\cdot 2+2\cdot 3}{2}] + [\frac{1\cdot 2+2\cdot 3+3\cdot 4}{2}] + \cdots + [\frac{1\cdot 2+2\cdot 3+3\cdot 4+\cdots+((p+1)^{p^t}-3)((p+1)^{p^t}-2)}{2}]) \\ \\ -(\frac{1\cdot 2}{2} + [\frac{1\cdot 2+2\cdot 3}{2}] + [\frac{1\cdot 2+2\cdot 3+3\cdot 4}{2}] + \cdots + [\frac{1\cdot 2+2\cdot 3+3\cdot 4+\cdots+(p^s-3)(p^s-2)}{2}]) \end{pmatrix}$$

$$= \begin{pmatrix} \frac{1}{2}\sum_{k=1}^{p^n-3}\sum_{i=1}^{k} i(i+1) \\ \\ -\frac{1}{2}\sum_{k=1}^{(p+1)^{p^t}-3}\sum_{i=1}^{k} i(i+1) \\ \\ -\frac{1}{2}\sum_{k=1}^{p^s-3}\sum_{i=1}^{k} i(i+1) \end{pmatrix}$$

$$= \begin{pmatrix} \frac{1}{2}\sum_{k=1}^{p^n-3}\frac{k(k+1)(k+2)}{3} \\ \\ -\frac{1}{2}\sum_{k=1}^{(p+1)^{p^t}-3}\frac{k(k+1)(k+2)}{3} \\ \\ -\frac{1}{2}\sum_{k=1}^{p^s-3}\frac{k(k+1)(k+2)}{3} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{p^n(p^n-1)(p^n-2)(p^n-3)}{2\cdot 3\cdot 4} \\ \\ -\frac{(p+1)^{p^t}((p+1)^{p^t}-1)((p+1)^{p^t}-2)((p+1)^{p^t}-3)}{2\cdot 3\cdot 4} \\ \\ -\frac{p^s(p^s-1)(p^s-2)(p^s-3)}{2\cdot 3\cdot 4} \end{pmatrix}$$

where we have used theorem 5.20.

We have now seen in detail what happens for the 4-fold Massey product, which we needed, as this is where all the liftings come in to play in the formula. From this we can now state a theorem, and then use our remarks to prove it by induction.

Theorem 5.23 *Let G be a metacyclic p-group given by the parameters n, m, t and s, and generators a and b, as in theorem 5.1. Put $a := \xi_1^*$. If the x-th Massey product $\langle \underbrace{\xi_1, \dots, \xi_1}_{x}; 0\rangle$ is defined, it is given by the formula*

$$\langle \underbrace{\xi_1, \dots, \xi_1}_{x}; 0\rangle = \begin{pmatrix} \frac{(-1)^x}{2} \underbrace{\sum_{k_{x-3}=1}^{p^n-(x-1)} \sum_{k_{x-4}=1}^{k_{x-3}} \cdots \sum_{i=1}^{k_1}}_{x-2} i(i+1) \\ \\ \frac{(-1)^{x+1}}{2} \underbrace{\sum_{k_{x-3}=1}^{(p+1)^{p^t}-(x-1)} \sum_{k_{x-4}=1}^{k_{x-3}} \cdots \sum_{i=1}^{k_1}}_{x-2} i(i+1) \\ \\ \frac{(-1)^{x+1}}{2} \underbrace{\sum_{k_{x-3}=1}^{p^s-(x-1)} \sum_{k_{x-4}=1}^{k_{x-3}} \cdots \sum_{i=1}^{k_1}}_{x-2} i(i+1) \end{pmatrix}$$

$$= \begin{pmatrix} (-1)^x \left(\frac{p^n(p^n-1)(p^n-2)\cdots(p^n-(x-1))}{x!}\right) \\ \\ (-1)^{x+1} \left(\frac{(p+1)^{p^t}((p+1)^{p^t}-1)((p+1)^{p^t}-2)\cdots((p+1)^{p^t}-(x-1))}{x!}\right) \\ \\ (-1)^{x+1} \left(\frac{p^s(p^s-1)(p^s-2)\cdots(p^s-(x-1))}{x!}\right) \end{pmatrix}$$

as an element in $\mathrm{Ext}^2_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$, for $x \in \{3, 4, 5, \dots\}$ and $k_0 := i$. The last equality also holds for $x = 2$. Note that we have expressions in p which depend on x.

Proof: The last equality follows by applying theorem 5.20 sufficiently many times, and so it remains to show the first equality. We have seen that

$$\langle \xi_1, \xi_1; 0\rangle = \begin{pmatrix} \frac{p^n(p^n-1)}{2} \\ \\ -\frac{(p+1)^{p^t}((p+1)^{p^t}-1)}{2} \\ \\ -\frac{p^s(p^s-1)}{2} \end{pmatrix},$$

$$\langle \xi_1, \xi_1, \xi_1; 0\rangle = \begin{pmatrix} -\frac{1}{2}\sum_{i=1}^{p^n-2} i(i+1) \\ \\ \frac{1}{2}\sum_{i=1}^{(p+1)^{p^t}-2} i(i+1) \\ \\ \frac{1}{2}\sum_{i=1}^{p^s-2} i(i+1) \end{pmatrix} = \begin{pmatrix} -\frac{p^n(p^n-1)(p^n-2)}{2\cdot 3} \\ \\ \frac{(p+1)^{p^t}((p+1)^{p^t}-1)((p+1)^{p^t}-2)}{2\cdot 3} \\ \\ \frac{p^s(p^s-1)(p^s-2)}{2\cdot 3} \end{pmatrix},$$

$$\langle \xi_1, \xi_1, \xi_1, \xi_1; 0\rangle = \begin{pmatrix} \frac{1}{2}\sum_{k=1}^{p^n-3}\sum_{i=1}^{k} i(i+1) \\ \\ -\frac{1}{2}\sum_{k=1}^{(p+1)^{p^t}-3}\sum_{i=1}^{k} i(i+1) \\ \\ -\frac{1}{2}\sum_{k=1}^{p^s-3}\sum_{i=1}^{k} i(i+1) \end{pmatrix}$$

$$= \begin{pmatrix} \frac{p^n(p^n-1)(p^n-2)(p^n-3)}{2\cdot 3\cdot 4} \\ \\ -\frac{(p+1)^{p^t}((p+1)^{p^t}-1)((p+1)^{p^t}-2)((p+1)^{p^t}-3)}{2\cdot 3\cdot 4} \\ \\ -\frac{p^s(p^s-1)(p^s-2)(p^s-3)}{2\cdot 3\cdot 4} \end{pmatrix},$$

so suppose $x \geq 5$. We will proceed by induction, and we will only consider the first row, since the second and third row are done similarly.

We have seen that when a Massey product is zero, we find an element $\phi \in \mathrm{Hom}^{(1)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet)$ such that $\partial\phi$ is this Massey product (without composing with ρ). We then find the first two components ϕ_1 and ϕ_2 of ϕ which we use in the next Massey product together with the ϕ-s from lower order Massey products. In this procedure the ϕ_1-s can always be chosen to be the 0-map (as we observed in remark 5.19). Hence the formula for the Massey product is always $\phi_2(\psi_1)_1\rho$, where ϕ_2 is as above.

So assume the first row in the Massey product $\langle\underbrace{\xi_1, \xi_1, \ldots, \xi_1}_{x-1}; 0\rangle$ is given by

$$\frac{(-1)^{x-1}}{2}\underbrace{\sum_{k_{x-4}=1}^{p^n-(x-2)}\sum_{k_{x-5}=1}^{k_{x-4}}\cdots\sum_{i=1}^{k_1}}_{x-3} i(i+1),$$

and that we work with n such that this expression is 0 in $\mathbb{F}_p$. To introduce some names, put $\langle\underbrace{\xi_1, \xi_1, \ldots, \xi_1}_{x-1}; 0\rangle = \phi_2(\psi_1)_1\rho$, and let $\mu \in \mathrm{Hom}^{(1)}_{\mathbb{F}_pG}(F_\bullet, F_\bullet)$ such that $\partial\mu = \phi_2(\psi_1)_1$, i.e. $\langle\underbrace{\xi_1, \xi_1, \ldots, \xi_1}_{x}; 0\rangle = \mu_2(\psi_1)_1\rho$.

Since $(\psi_1)_1 = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$, we are only interested in the first column of ϕ_2 and μ_2 (also, the second column will be $\left(\begin{smallmatrix}0\\0\\0\end{smallmatrix}\right)$), and since we only consider the first row, we only look at the top left entry. Let k be the top left entry in ϕ_2 and q the top left entry in μ_2. Hence $\langle\underbrace{\xi_1, \xi_1, \ldots, \xi_1}_{x-1}; 0\rangle = \rho(k)$ and $\langle\underbrace{\xi_1, \xi_1, \ldots, \xi_1}_{x}; 0\rangle = \rho(q)$.

To proceed, recall remark 5.22, where we noted that we get the n-th term of q by adding the n-th term of k to the $(n-1)$-st term of q. If we denote $[k]_n$ by the n-th term of k, this says

$$[q]_n = [k]_n + [q]_{n-1} \text{ for } n \geq 1 \text{ with } [q]_0 = 0.$$

Let us see why: The expression for $k \in \mathbb{F}_pG$ involves 1-s and powers of the generator a. Using remarks 5.18 and 5.21, we see that when we go from k to q, the 1-s vanish, a becomes 1, a^2 becomes $a+1$ (since $a^2-1 = (a+1)(a-1)$) etc. In general, a^{p^n-i} becomes $a^{p^n-(i+1)} + \cdots + a + 1$. Our starting point is the resolution, and the top left entry in δ_2 is

$$[1] + [a] + [a^2] + \cdots + [a^{p^n-1}]$$

([ ]-notation to denote terms). And so the next lifting will be

$$[1]+[a+1]+[a^2+a+1]+\cdots+[a^{p^n-2}+\cdots a+1],$$

etc. In this way, we find $[q]_n$ by adding $[k]_n$ (the previous lifting) to $[q]_{n-1}$.

Now, ρ is the augmentation map sending all group elements to 1, and we have

$$[\rho(q)]_n=[\rho(k)]_n+[\rho(q)]_{n-1} \quad \text{for } n\geq 1 \text{ with } [\rho(q)]_0=0,$$

which means

$$\begin{aligned}[\rho(q)]_n=&[\rho(k)]_n+[\rho(k)]_{n-1}+[\rho(q)]_{n-2}\\ &\vdots\\ =&[\rho(k)]_n+\cdots+[\rho(k)]_1+[\rho(q)]_0.\end{aligned}$$

We observe that there will be one less term each time we lift (since the first term is 1, which vanishes). Moreover, $\rho(k)=\langle\underbrace{\xi_1,\xi_1,\ldots,\xi_1}_{x-1};0\rangle$ has $p^n-(x-2)$ terms, and by the inductive hypothesis it is given by

$$\frac{(-1)^{x-1}}{2}\underbrace{\sum_{k_{x-4}=1}^{p^n-(x-2)}\sum_{k_{x-5}=1}^{k_{x-4}}\cdots\sum_{i=1}^{k_1}}_{x-3}i(i+1).$$

E.g. $[\rho(k)]_2=\underbrace{\sum_{k_{x-5}=1}^{2}\cdots\sum_{i=1}^{k_1}}_{x-4}i(i+1)$ and $[\rho(k)]_1=\underbrace{\sum_{k_{x-5}=1}^{1}\cdots\sum_{i=1}^{k_1}}_{x-4}i(i+1)$, and so we get that $[\rho(q)]_2=\underbrace{\sum_{k_{x-4}=1}^{2}\sum_{k_{x-5}=1}^{k_{x-4}}\cdots\sum_{i=1}^{k_1}}_{x-3}i(i+1)$. From this we see that

$$[\rho(q)]_n=\underbrace{\sum_{k_{x-4}=1}^{n}\sum_{k_{x-5}=1}^{k_{x-4}}\cdots\sum_{i=1}^{k_1}}_{x-3}i(i+1).$$

Finally, $\rho(q)$ has $p^n - (x-1)$ terms, hence

$$\rho(q) = \frac{(-1)^x}{2} \underbrace{\sum_{k_{x-3}=1}^{p^n-(x-1)} \sum_{k_{x-4}=1}^{k_{x-3}} \cdots \sum_{i=1}^{k_1}}_{x-2} i(i+1),$$

which is what we wanted (the sign is obvious). $\square$

Using the calculations we have done for $\langle \xi_1, \xi_1, \ldots, \xi_1; 0\rangle$, we can easily find $\langle \xi_2, \xi_2, \ldots, \xi_2; 0\rangle$.

Theorem 5.24 *Let G be a metacyclic p-group given by the parameters n, m, t and s, and generators a and b, as in theorem 5.1. Put $b := \xi_2^*$. If the x-th Massey product $\langle\underbrace{\xi_2, \ldots, \xi_2}_{x}; 0\rangle$ is defined, it is given by the formula*

$$\langle\underbrace{\xi_2, \ldots, \xi_2}_{x}; 0\rangle = \begin{pmatrix} 0 \\ 0 \\ \frac{(-1)^x}{2} \underbrace{\sum_{k_{x-3}=1}^{p^m-(x-1)} \sum_{k_{x-4}=1}^{k_{x-3}} \cdots \sum_{i=1}^{k_1}}_{x-2} i(i+1) \end{pmatrix}$$

$$= \begin{pmatrix} 0 \\ 0 \\ (-1)^x \left(\frac{p^m(p^m-1)(p^m-2)\cdots(p^m-(x-1))}{x!}\right) \end{pmatrix}$$

as an element in $\mathrm{Ext}^2_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$, for $x \in \{3, 4, 5, \ldots\}$ and $k_0 := i$. The last equality also holds for $x = 2$.

Proof: We do the same calculations as in the proof of theorem 5.23 with $(\psi_1)_2 = \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$ instead of $(\psi_1)_1 = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$. $\square$

To summarise this section, we have calculated and found the strictly defined Massey products of a metacyclic p-group G,

$$G = \{a, b | a^{p^n} = 1, b^{p^m} = a^{p^s}, b^{-1}ab = a^{(p+1)^{p^t}}\},$$

namely

$$\langle \xi_1, \xi_2; 0\rangle = \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix},$$

$$\langle \xi_2, \xi_1; 0\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},$$

$$\langle \underbrace{\xi_1, \xi_1, \dots, \xi_1}_{x}; 0\rangle = \begin{pmatrix} (-1)^x \left(\frac{p^n(p^n-1)(p^n-2)\cdots(p^n-(x-1))}{x!}\right) \\ (-1)^{x+1} \left(\frac{(p+1)^{p^t}((p+1)^{p^t}-1)((p+1)^{p^t}-2)\cdots((p+1)^{p^t}-(x-1))}{x!}\right) \\ (-1)^{x+1} \left(\frac{p^s(p^s-1)(p^s-2)\cdots(p^s-(x-1))}{x!}\right) \end{pmatrix},$$

$$\langle \underbrace{\xi_2, \xi_2, \dots, \xi_2}_{x}; 0\rangle = \begin{pmatrix} 0 \\ 0 \\ (-1)^x \left(\frac{p^m(p^m-1)(p^m-2)\cdots(p^m-(x-1))}{x!}\right) \end{pmatrix}.$$

Example 5.25 The group $G = C_3 \times C_3$ is given by the parameters $n = 1, m = 1, t = 0$ and $s = 1$, and so we have the following Massey products:

$$\langle \xi_1, \xi_2; 0\rangle = \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix}, \qquad \langle \xi_2, \xi_1; 0\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},$$

$$\langle \xi_1, \xi_1; 0\rangle = \begin{pmatrix} \frac{3\cdot 2}{2} \\ -\frac{4\cdot 3}{2} \\ -\frac{3\cdot 2}{2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \quad \langle \xi_1, \xi_1, \xi_1; 0\rangle = \begin{pmatrix} -\frac{3\cdot 2\cdot 1}{2\cdot 3} \\ \frac{4\cdot 3\cdot 2}{2\cdot 3} \\ \frac{3\cdot 2\cdot 1}{2\cdot 3} \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix},$$

$$\langle \xi_2, \xi_2; 0\rangle = \begin{pmatrix} 0 \\ 0 \\ \frac{3\cdot 2}{2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \quad \langle \xi_2, \xi_2, \xi_2; 0\rangle = \begin{pmatrix} 0 \\ 0 \\ -\frac{3\cdot 2\cdot 1}{2\cdot 3} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}.$$

■

Example 5.26 Consider the groups $G(N-m, m, N-2m-1, m)$ from theorem 5.9. Let us calculate the Massey products for different values of m, and recall that $N \geq 3$. The cup products between ξ_1 and ξ_2 are $\langle \xi_1, \xi_2; 0\rangle = \left(\begin{smallmatrix} 0 \\ -1 \\ 0 \end{smallmatrix}\right)$ and $\langle \xi_2, \xi_1; 0\rangle = \left(\begin{smallmatrix} 0 \\ 1 \\ 0 \end{smallmatrix}\right)$ for all m.

Let $m = 1$, hence we consider $G(N-1, 1, N-3, 1)$. Then

$$\langle \xi_1, \xi_1; 0\rangle = \begin{pmatrix} \frac{p^{N-1}(p^{N-1}-1)}{2} \\ -\frac{(p+1)^{p^{N-3}}((p+1)^{p^{N-3}}-1)}{2} \\ -\frac{p(p-1)}{2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad \text{for all } p$$

$$\langle \xi_2, \xi_2; 0\rangle = \begin{pmatrix} 0 \\ 0 \\ \frac{p(p-1)}{2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad \text{for all } p$$

$$\langle \xi_1, \xi_1, \xi_1; 0\rangle = \begin{pmatrix} -\frac{p^{N-1}(p^{N-1}-1)(p^{N-1}-2)}{2\cdot 3} \\ \\ \frac{(p+1)^{p^{N-3}}((p+1)^{p^{N-3}}-1)((p+1)^{p^{N-3}}-2)}{2\cdot 3} \\ \\ \frac{p(p-1)(p-2)}{2\cdot 3} \end{pmatrix} = \begin{cases} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} & \text{for } p = 3, \\ & N = 3 \\ \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} & \text{for } p = 3, \\ & N > 3 \\ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} & \text{for } p \geq 5 \end{cases}$$

$$\langle \xi_2, \xi_2, \xi_2; 0\rangle = \begin{pmatrix} 0 \\ 0 \\ -\frac{p(p-1)(p-2)}{2\cdot 3} \end{pmatrix} = \begin{cases} \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix} & \text{for } p = 3 \\ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} & \text{for } p \geq 5 \end{cases}$$

So for $p = 3$, we have found all strictly defined Massey products.

We see that $\langle \xi_1, \xi_1, \xi_1, \xi_1; 0\rangle = \left(\begin{smallmatrix} 0 \\ 0 \\ 0 \end{smallmatrix}\right)$ and also $\langle \xi_2, \xi_2, \xi_2, \xi_2; 0\rangle = \left(\begin{smallmatrix} 0 \\ 0 \\ 0 \end{smallmatrix}\right)$ for all $p \geq 5$, whereas when we come to the 5-fold Massey products, we get the same as for the 3-fold ones, i.e.

$$\langle \xi_1, \xi_1, \xi_1, \xi_1, \xi_1; 0\rangle = \begin{cases} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} & \text{for } p = 5, \\ & N = 3 \\ \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} & \text{for } p = 5, \\ & N > 3 \\ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} & \text{for } p \geq 7, \end{cases}$$

$$\langle \xi_2,\xi_2,\xi_2,\xi_2,\xi_2;0\rangle = \begin{cases} \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix} & \text{for } p=5 \\ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} & \text{for } p \geq 7 \end{cases}$$

so for $p=5$, we have found all strictly defined Massey products.

We claim that this generalises, i.e. assume we are in characteristic p. Then $\langle \underbrace{\xi_1,\ldots,\xi_1}_{i};0\rangle = \left(\begin{smallmatrix} 0 \\ 0 \\ 0 \end{smallmatrix}\right)$ and $\langle \underbrace{\xi_2,\ldots,\xi_2}_{i};0\rangle = \left(\begin{smallmatrix} 0 \\ 0 \\ 0 \end{smallmatrix}\right)$ for $2 \leq i \leq p-1$. Moreover,

$$\langle \underbrace{\xi_1,\ldots,\xi_1}_{p};0\rangle = \begin{cases} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} & \text{for } N=3 \\ \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} & \text{for } N>3 \end{cases}$$

$$\langle \underbrace{\xi_2,\ldots,\xi_2}_{p};0\rangle = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}.$$

To see this, we observe that in order for an entry in the matrix of the p-fold Massey product to be 0 in characteristic p, we need at least one more p in the numerator than in the denominator. So the top entry is always 0, because $N \geq 3$, which means we always have a p^2 in the numerator, whereas only one p in the denominator ($p!$). For the middle entry, we get $\frac{(p+1)!}{p!}$ for $N=3$, and hence we get 1. For $N>3$, $(p+1)^{p^{N-3}}-1$ will be divisible by at least p^2 by lemma 5.5, and so we get 0 (since we have only one p in the denominator). The bottom entry is always $\frac{p!}{p!}=1$.

For the i-fold Massey product, $i \leq p-1$, we have a p in the numerator and no p in the denominator, so in characteristic p this is 0. This fits in well with the theory of the Bockstein operation in section 3.5.

All this generalises to $m \geq 2, N \geq 3m$. ■

5.8 Analysing the results

We will now have a look at examples 5.25 and 5.26 to see if we can find the groups we started with. By (2.13), ξ_1^* and ξ_2^* will be the generators for our groups. We let $\eta_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \eta_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ and $\eta_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ be basis-elements for $\mathrm{H}^2(G, \mathbb{F}_p)$.

Example 5.27 Consider example 5.25. We have the products

$$\langle \xi_1, \xi_2; 0\rangle = -\eta_2,$$

$$\langle \xi_2, \xi_1; 0\rangle = \eta_2,$$

$$\langle \xi_1, \xi_1, \xi_1; 0\rangle = -\eta_1 + \eta_2 + \eta_3,$$

$$\langle \xi_2, \xi_2, \xi_2; 0\rangle = -\eta_3.$$

Using (3.14) and theorems 4.5 and 4.6 we get that

$$\mathrm{o}_G(\eta_1^*) = (\xi_1^*)^{-3},$$

$$\mathrm{o}_G(\eta_2^*) = [\xi_1^*, \xi_2^*](\xi_1^*)^3,$$

$$\mathrm{o}_G(\eta_3^*) = (\xi_1^*)^3(\xi_2^*)^{-3}.$$

So we have a group with presentation

$$\{\xi_1^*, \xi_2^* | (\xi_1^*)^{-3} = 1, [\xi_1^*, \xi_2^*](\xi_1^*)^3 = 1, (\xi_1^*)^3(\xi_2^*)^{-3} = 1\},$$

which is isomorphic to $C_3 \times C_3$. ■

Example 5.28 Let us continue example 5.26. Using (3.14) and theorems 4.5 and 4.6 the other way, we see that the presentation we gave in theorem 5.11 corresponds to the Massey products

$$\langle \xi_1; m\rangle = \eta_1,$$

$$\langle \xi_2; N - 2m\rangle = \eta_2,$$

$$\langle \xi_1, \xi_2; 0\rangle = \eta_1 + \eta_2,$$

which tell us that the groups $G(m, N)$ for $N \geq 3m$ from theorem 5.11 is given by strictly defined Massey products. And we see that it comes out in the tree construction in appendix B.

We have actually calculated the strictly defined Massey products for the split metacyclic p-groups in example 5.26. When we analyse these calculations, we will see that the Massey products reflect the explicit resolution we had as a basis for our calculations.

To explain further, let us analyse the Massey products in example 5.26: We assume $N = 3, m = 1$, so we have $G(2, 1, 0, 1)$ (as this will easily generalise to $m \geq 2, N \geq 3m$). We have the Massey products

$$\langle \xi_1, \xi_2; 0\rangle = -\eta_2,$$

$$\langle \xi_2, \xi_1; 0\rangle = \eta_2,$$

$$\langle \underbrace{\xi_1, \dots, \xi_1}_{p}; 0\rangle = \eta_2 + \eta_3,$$

$$\langle \underbrace{\xi_2, \dots, \xi_2}_{p}; 0\rangle = -\eta_3,$$

and this will give us the group presentation (again using (3.14) and theorems 4.5 and 4.6)

$$\{\xi_1^*, \xi_2^* | (\xi_1^*)^p[\xi_1^*, \xi_2^*] = 1, (\xi_1^*)^p(\xi_2^*)^{-p} = 1\},$$

which is isomorphic to $G(2, 1, 0, 1)$, by theorem 5.11.

However, when $N > 3$, we get the products

$$\langle \xi_1, \xi_2; 0\rangle = -\eta_2,$$

$$\langle \xi_2, \xi_1; 0\rangle = \eta_2,$$

$$\langle \underbrace{\xi_1, \dots, \xi_1}_{p}; 0\rangle = \eta_3,$$

$$\langle \underbrace{\xi_2, \dots, \xi_2}_{p}; 0\rangle = -\eta_3,$$

and the group presentation

$$\{\xi_1^*, \xi_2^* | (\xi_1^*)^p = (\xi_2^*)^p, [\xi_1^*, \xi_2^*] = 1\}.$$

Hence we see that η_2 is the link between the commutator and the p-th power relations.

We would like for $\langle\underbrace{\xi_1, \ldots, \xi_1}_{p}; 0\rangle$ to be 0 for $N > 3$, because then higher order Massey products would be strictly defined. In this situation, we would actually get out that the next product that is non-zero for $N = 4$ and 0 for $N > 4$ is $\langle\underbrace{\xi_1, \ldots, \xi_1}_{p^2}; 0\rangle$, because this is when we have exactly 3 powers of p in the numerator, which cancels p^3 in the denominator $(p^2)!$. And then we would get the products

$$\langle\xi_1, \xi_2; 0\rangle = -\eta_2,$$

$$\langle\xi_2, \xi_1; 0\rangle = \eta_2,$$

$$\langle\underbrace{\xi_1, \ldots, \xi_1}_{p^2}; 0\rangle = \eta_2 + \eta_3,$$

$$\langle\underbrace{\xi_2, \ldots, \xi_2}_{p}; 0\rangle = -\eta_3,$$

and the group

$$G = \{\xi_1^*, \xi_2^* | (\xi_1^*)^{p^2}[\xi_1^*, \xi_2^*] = 1, (\xi_2^*)^p[\xi_1^*, \xi_2^*] = 1\},$$

and hence this would generalise to the groups in theorem 5.11.

But the bottom entry in $\langle\underbrace{\xi_1, \ldots, \xi_1}_{p}; 0\rangle$ will always be non-zero due to the relation $a^p = b^p$ for these groups. This is why we use the Bockstein operations independent of the Massey products, as to get the Bockstein operations we restrict the defining system for this Massey product and this gives the (powers of p)-th power relations in general. ■

We end this chapter by the following. Recall that the Massey product structure we read off from the presentation in theorem 5.11 is $\langle\xi_1; m\rangle = \eta_1$,

$\langle \xi_2; N-2m\rangle = \eta_2$ and $\langle \xi_1, \xi_2; 0\rangle = \eta_1 + \eta_2$. This gives a group $G(m, N-2m)$ of order p^N.

Lemma 5.29 *The products* $\langle \xi_1; m\rangle = \eta_1$, $\langle \xi_2; N-2m\rangle = \eta_2$ *and* $\langle \xi_1, \xi_2; 0\rangle = \eta_2$ *give a pro-p presentation of* $G(m, N-2m)$.

Proof: To see this we need to show that the largest p-quotient of the presentation we get has order p^N. The presentation is

$$\hat{G}(m, N-2m) = \{a, b | a^{p^m} = 1, [a, b]b^{p^{N-2m}} = 1\}.$$

By writing out $[a, b]$, we find that b has order $(p^{N-2m}+1)^{p^m} - 1$, and expanding this gives that the largest power of p dividing $|\hat{G}(m, N-2m)|$ is $p^m p^{N-2m} p^m = p^N$. □

And so we have seen a lot of interesting points occurring by studying the metacyclic p-groups from a cohomological point of view.

Chapter 6

The modular isomorphism problem

The problem whether (the isomorphism class of) a finite p-group G is determined by its group algebra over the field of p elements is usually referred to as the **modular isomorphism problem**. Deskins seems to be the first to consider this problem in print (in a paper presented at the 61. Annual Meeting of the American Mathematical Society at the University of Pittsburgh, December 1954, see [12]).

Since then there has been a lot of work on this problem. We will consider some of it here, to see why the problem hasn't been solved in general yet. We will then see how we can approach the modular isomorphism problem using the cohomological machinery we have developed and give reasons for why this is a "better" approach. Our aim will be to exhibit "new" groups for which the modular isomorphism problem has a positive answer. This is done by defining a class $\mathcal{C}$ of p-groups given by strictly defined Massey products.

If we know $\mathbb{F}_pG$ what can we say about G? Well, before we answer this we need to have a look at what it means to know $\mathbb{F}_pG$.

6.1 Getting to know $\mathbb{F}_pG$

Definition 6.1 *Let $\mathcal{C}$ be a conjugacy class of G. Then*

$$\sum_{c\in\mathcal{C}} c := \hat{\mathcal{C}}$$

is called a class sum for G.

Lemma 6.2 *The centre $\zeta(\mathbb{F}_pG)$ is the linear space spanned by all class sums of G.*

Proof: Take $a \in \mathbb{F}_pG$ and let $a = \sum_{g\in G} \alpha_g g$ where $\alpha_g \in \mathbb{F}_p$. Then $a \in \zeta(\mathbb{F}_pG)$ iff $ha - ah = 0\ \forall\ h \in G$, i.e. iff $h^{-1}ah = a$. But

$$h^{-1}ah = \sum_{g\in G} \alpha_g h^{-1}gh = \sum_{k\in G} \alpha_{hkh^{-1}} k,$$

and so $a \in \zeta(\mathbb{F}_pG)$ iff the coefficients of a are constant on each conjugacy class of G. The class sums are linearly independent, and the lemma follows. □

Lemma 6.3 *The commutator subspace $[\mathbb{F}_pG, \mathbb{F}_pG]$ consists of all elements $a = \sum_{g\in G} \alpha_g g$ with*

$$\sum_{g\in\mathcal{C}} \alpha_g = 0$$

for every conjugacy class $\mathcal{C}$ in G.

Proof: First note that $[\mathbb{F}_pG, \mathbb{F}_pG]$ is the vector space spanned by all Lie products $[g, h] = gh - hg$ where $g, h \in G$. Let X be the set consisting of all elements of the form $a = \sum_{g\in G} \alpha_g g$ with $\sum_{g\in\mathcal{C}} \alpha_g = 0$ for every conjugacy class $\mathcal{C}$ in G. We see that X has the structure of a subspace, so we need to check that $X = [\mathbb{F}_pG, \mathbb{F}_pG]$.

For one inclusion, pick $[g, h] \in [\mathbb{F}_pG, \mathbb{F}_pG]$. Then $[g, h] \in X$ since

$$gh - hg = gh - g^{-1}(gh)g.$$

Conversely, let $a = \sum_{i=1}^{n} \alpha_i g^{h_i}$ with $\sum_{i=1}^{n} \alpha_i = 0$ where $\{g^{h_1}, g^{h_2}, \ldots, g^{h_n}\}$ is a conjugacy class in G. Then $a \in [\mathbb{F}_pG, \mathbb{F}_pG]$ because

$$a = \sum_{i=1}^{n} \alpha_i (g^{h_i} - g) = \sum_{i=1}^{n} \alpha_i ((h_i^{-1} g) h_i - h_i (h_i^{-1} g)).$$

□

Note that the commutator subspace is not an ideal, and that this is easily seen once we have the characterisation of $[\mathbb{F}_pG, \mathbb{F}_pG]$ in the lemma above:

Corollary 6.4 *Let G be a non-abelian p-group. Then the commutator subspace $[\mathbb{F}_pG, \mathbb{F}_pG]$ is not an ideal.*

Proof: If G is abelian, $[\mathbb{F}_pG, \mathbb{F}_pG] = (0)$, so let g be an element in $\zeta(G)$ where G is a non-abelian finite p-group. Find non-central elements h and k in G such that $g = hk$. Consider k's conjugacy class and make an element a in the commutator subspace using the proof of lemma 6.3. We can assume the coefficient of k is non-zero. Now, when we multiply a by h, we will get a central element in the sum, and so ha is not in the commutator subspace, by lemma 6.3. □

Another useful result, which is often used to simplify calculations is the following (the proof is slightly different from what you usually find in the literature):

Lemma 6.5 *Let $a_1, a_2, \ldots, a_n \in \mathbb{F}_pG$. Then*

$$(a_1 + \cdots + a_n)^p \equiv a_1^p + \cdots + a_n^p \mod [\mathbb{F}_pG, \mathbb{F}_pG]. \tag{6.1}$$

Proof: Let A be the set of all words $a_{i_1} a_{i_2} \cdots a_{i_p}$ with at least two distinct subscripts. We expand out the left side of (6.1) to get

$$(a_1 + \cdots + a_n)^p = a_1^p + \cdots a_n^p + a$$

where a is the sum of all words in A. Let C_p act on A by cyclic permutation.

Observe that if we have words

$$\omega_1 = a_{i_1}a_{i_2}\cdots a_{i_p}$$
$$\omega_2 = a_{i_j}a_{i_{j+1}}\cdots a_{i_p}a_{i_1}\cdots a_{i_{j-1}}$$

then $\omega_1 - \omega_2 \in [\mathbb{F}_pG, \mathbb{F}_pG]$. Hence, modulo $[\mathbb{F}_pG, \mathbb{F}_pG]$, the elements in A in an orbit under the action of C_p are the same. Furthermore, the orbit size is divisible by p, and so we are done since we are in characteristic p. ☐

Recall that $\mathbb{F}_pG$ is an augmented algebra via (2.4).

Lemma 6.6 *Let G and H be finite p-groups and let α be an isomorphism between their modular group algebras. Then there exists an isomorphism $\overline{\alpha}: \mathbb{F}_pG \xrightarrow{\simeq} \mathbb{F}_pH$ preserving the augmentation.*

Proof: We have the diagram

$$\begin{tikzcd}
\mathbb{F}_pG \arrow[rr, "\simeq", "\alpha"'] \arrow[dr, "\epsilon_G"'] & & \mathbb{F}_pH \arrow[dl, "\epsilon_H"] \\
& \mathbb{F}_p &
\end{tikzcd}$$

where ϵ_G and ϵ_H are the augmentation maps. Since $\alpha(g)$ is not necessarily in IH, this diagram is not necessarily commutative (except for $p = 2$), and so we need to show that there is an isomorphism $\overline{\alpha}$ replacing α such that we get a commutative diagram.

Consider the ring homomorphism $\beta = \epsilon_H \circ \alpha$:

$$\begin{tikzcd}
\mathbb{F}_pG \arrow[r, "\simeq", "\alpha"'] \arrow[dr, "\beta"'] & \mathbb{F}_pH \arrow[d, "\epsilon_H"] \\
& \mathbb{F}_p.
\end{tikzcd}$$

For $g \in G$, $\beta(g) \in \mathbb{F}_p\backslash\{0\}$ (a unit). If $p = 2$, $\beta = \epsilon_G$, and so the diagram commutes with $\overline{\alpha} = \alpha$. For $p \neq 2$, define a map $\mathbb{F}_pG \xrightarrow{\gamma} \mathbb{F}_pG$ by

$$\gamma(g) = \beta(g)^{p-2}g$$

and extend linearly to elements $\sum_{g\in G}\alpha_g g$. Then γ is a ring automorphism, and what's more,

$$\beta(\gamma(g)) = \beta(\beta(g)^{p-2}g) = \beta(g)^{p-1}$$

and so $\beta\circ\gamma$ is the augmentation ϵ_G by Fermat's little theorem. If we put $\overline{\alpha} = \alpha\circ\gamma$ the diagram commutes, which is what we wanted. □

Note that this result is not special for characteristic p, and holds when $\mathbb{F}_p$ is replaced by any commutative ring with 1 and G and H are groups. In this case the proof uses $\gamma(g) = \beta(g)^{-1}g$.

Also note that this means that the modular isomorphism problem really asks whether $\mathbb{F}_pG$ as an augmented algebra determines a finite p-group G.

Using the identities

$$\begin{aligned} gh-1 &= g(h-1)+(g-1) && (6.2)\\ g^{-1}-1 &= -g^{-1}(g-1) && (6.3)\end{aligned}$$

we see that IG is generated as a G-module by elements $g-1$ where g is an element in the generating set for G. We also have

Lemma 6.7 *The augmentation ideal IG is determined by $\mathbb{F}_pG$.*

Proof: This follows since IG is the Jacobson radical of $\mathbb{F}_pG$. □

The group algebra will be finite dimensional since we consider finite groups, and so when we form a filtration of IG, this will eventually stop. In particular, the IG-adic filtration stops, i.e. there is an $N\in\mathbb{N}$ such that

$$IG \supset (IG)^2 \supset \cdots \supset (IG)^N \supset (IG)^{N+1} = \{0\}. \qquad (6.4)$$

Now, $(IG)^n$ is the ideal consisting of sums of products of n elements of IG and by associativity of ideals, $(IG)^n(IG)^m = (IG)^{n+m}$.

Corollary 6.8 *Powers of the augmentation ideal are determined by $\mathbb{F}_pG$. In particular, $\mathbb{F}_pG$ determines the filtration* (6.4). □

The filtration (6.4) gives rise to a sequence of characteristic subgroups

$$\mathcal{D}_n(G) = \{g \in G | g - 1 \in (IG)^n\} \tag{6.5}$$

called the modular dimension subgroups.

Lemma 6.9 *The $\mathcal{D}$-series satisfies the properties*

$$\begin{aligned} [\mathcal{D}_n(G), \mathcal{D}_m(G)] &\leq \mathcal{D}_{n+m}(G), && (6.6)\\ \mathcal{D}_n(G)^p &\leq \mathcal{D}_{np}(G). && (6.7) \end{aligned}$$

Property (6.6) *is called the strong centrality property.*

Proof: To prove (6.6), pick elements g_n, g_m in $\mathcal{D}_n(G), \mathcal{D}_m(G)$ respectively. Then

$$\begin{aligned} &[g_n, g_m] - 1\\ =&g_n^{-1} g_m^{-1} (g_n g_m - g_m g_n)\\ =&g_n^{-1} g_m^{-1} (\underbrace{(g_n - 1)(g_m - 1) - (g_m - 1)(g_n - 1)}_{\in (IG)^{n+m}}) \end{aligned}$$

and $[g_n, g_m] \in \mathcal{D}_{n+m}(G)$.

For (6.7) we use that $g_n^p - 1 = (g_n - 1)^p$ in characteristic p. □

It can be shown that the $\mathcal{D}$-series is the fastest descending series satisfying properties (6.6) and (6.7), see [37, page 90]. Also, we know what this series looks like:

Definition 6.10 *We define the $\mathcal{M}$-series inductively by*

$$\begin{aligned} \mathcal{M}_1(G) &= G && (6.8)\\ \mathcal{M}_i(G) &= \langle [\mathcal{M}_{i-1}(G), G], \mathcal{M}_{(i/p)}(G)^{(p)} \rangle && (6.9) \end{aligned}$$

where (i/p) is the least integer $\geq i/p$ and $\mathcal{M}_i(G)^{(p)}$ denotes the set of p-th powers in $\mathcal{M}_i(G)$.

This series is usually called the Jennings series. However, Jennings called it the $\mathcal{M}$-series, and so that is the name we will use. The following deep theorem tells us what we need.

Theorem 6.11 (Jennings) *The $\mathcal{D}$-series and the $\mathcal{M}$-series of G are identical, i.e. $g \in \mathcal{M}_i(G)$ if and only if $(g-1) \in (IG)^i$.*

Proof: See [21]. $\square$

We will soon see an important application of this theorem.

The group algebra has many structures, and among these we also find the structure of a Hopf algebra. The comultiplication $\Delta : \mathbb{F}_pG \longrightarrow \mathbb{F}_pG \otimes_{\mathbb{F}_p} \mathbb{F}_pG$ is given by

$$\Delta(\sum_{g\in G} \alpha_g g) = \sum_{g \in G} \alpha_g g \otimes g. \tag{6.10}$$

6.2 Understanding the problem

When we say we know $\mathbb{F}_pG$, we mean that we know all features that are preserved under an isomorphism of algebras. And to solve the modular isomorphism problem means to find G from these features, without using information about G.

We can not use the comultiplication (6.10) since it uses G: The group algebra as a Hopf algebra determines the group, because we know exactly how the group sits inside the group algebra then, namely embedded diagonally. Hence we can recover G from the Hopf algebra $\mathbb{F}_pG$ as the set of non-zero elements $a \in \mathbb{F}_pG$ such that $\Delta(a) = a \otimes a$.

The Zassenhaus conjecture in the p-group case said that for F a field of characteristic p, G is determined up to conjugacy within the unit group of FG, i.e. an isomorphism from FH to FG must map H to a conjugate of G in the unit group of FG. Roggenkamp and Scott, [39], solved this conjecture by proving that in the normalised units of $\mathbb{Z}_pG$ there is only one conjugacy class of groups of order $|G|$. Consequently, $\mathbb{Z}_pG$ determines G, and in a very strong sense, namely we can pick out the group elements of G from $\mathbb{Z}_pG$. Here $\mathbb{Z}_p$ denotes the p-adic integers.

To say that G is determined by $\mathbb{F}_pG$ means we know how G sits inside $\mathbb{F}_pG$. But we don't necessarily know how each element of G sits in $\mathbb{F}_pG$: For example, let $C_3 = \{1, g, g^2\}$ and consider $\mathbb{F}_3C_3$. Then any element in $\mathbb{F}_3C_3$ with augmentation 1 will generate a copy of C_3 in $\mathbb{F}_3C_3$ ($\{1, 1+g+2g^2, 2+2g^2\}$ is another C_3). So what Roggenkamp and Scott proved for $\mathbb{Z}_pG$ cannot be done for $\mathbb{F}_pG$, but the modular isomorphism problem may still have a positive answer. The cohomological approach doesn't engage this way of thinking, but rather works in terms of a presentation for G.

Another reason why we feel the cohomological methods are promising, is the article by Al Weiss, see [47], where he uses representation theory to generalise and prove results introduced by Roggenkamp and Scott.

6.3 Known results

First of all, $\dim_{\mathbb{F}_p} \mathbb{F}_pG = |G|$, so we know the order of the group. From theorem 6.11, we also have

Proposition 6.12 *If $\mathbb{F}_pG \simeq \mathbb{F}_pH$ then for all i*

$$\mathcal{M}_i(G)/\mathcal{M}_{i+1}(G) \simeq \mathcal{M}_i(H)/\mathcal{M}_{i+1}(H).$$

Proof: The quotients in the $\mathcal{M}$-series (or the $\mathcal{D}$-series) are elementary abelian p-groups, and so are completely determined by their orders. Let $|\mathcal{D}_n(G)/\mathcal{D}_{n+1}(G)| = p^{b_n}$. If $a_n(G) = \dim(IG)^n/(IG)^{n+1}$ then our result follows since we have the following formula for the generating function for $a_n(G)$ ($|G| = p^d$):

$$\sum_{n=0}^{\infty} a_n(G)t^n = \left(\frac{t^p-1}{t-1}\right)^{b_1} \left(\frac{t^{2p}-1}{t-1}\right)^{b_2} \cdots \left(\frac{t^{dp}-1}{t-1}\right)^{b_d}.$$

The formula can be deduced by finding a basis for $(IG)^n/(IG)^{n+1}$, which is done by refining the $\mathcal{D}$-series to a composition series for G and using the notion of weight, see e.g. Passman [37]. □

This means that the "class" of G with respect to the $\mathcal{M}$-series is determined by $\mathbb{F}_pG$, i.e. the property $\mathcal{M}_i(G) = 1$ for some i is determined. As a consequence, if the nilpotency class of G is less than p, then the exponent of G is determined, see [41, theorem 6.17] and the bibliography there.

In [35], Passi and Sehgal investigate the $\mathcal{M}$-series and show for example that $\mathbb{F}_pG$ determines G in the case G is of class 2 and exponent p.

The following theorem, attributed to Deskins, has been proved in many ways, and for $\mathbb{F}_p$ it will follow from proposition 6.12. However, we give Coleman's proof, see [10] , which does not make use of the $\mathcal{M}$-series.

Theorem 6.13 (Deskins) *If G and H are finite abelian p-groups, and if $\mathbf{F}G \simeq \mathbf{F}H$ for some field $\mathbf{F}$ of characteristic p, then $G \simeq H$.*

Proof: Let $G^p = \{g^p | g \in G\}$ and let G and H be abelian p-groups. If $|G| = |H|$ and $G^p \simeq H^p$ then $G \simeq H$. Using this fact, the result follows by induction on $n = |G|$ since any isomorphism $\mathbf{F}G \simeq \mathbf{F}H$ maps $(\mathbf{F}G)^p$ onto $(\mathbf{F}H)^p$, and since G is abelian, $(\mathbf{F}G)^p = \mathbf{F}^pG^p$, see lemma 6.5. $\square$

More results follow from theorem 6.13:

Corollary 6.14 *Let G and H be p-groups with $\mathbb{F}_pG \simeq \mathbb{F}_pH$. Then*

$$G/G' \simeq H/H' \quad \text{and} \tag{6.11}$$

$$\zeta(G) \simeq \zeta(H). \tag{6.12}$$

Proof: See for example Passman's article [36]. $\square$

Another important result is due to Quillen and Lazard, see [24], namely

Theorem 6.15 *Let G and H be p-groups with $\mathbb{F}_pG \simeq \mathbb{F}_pH$. Then their restricted graded Lie algebras are isomorphic, i.e.*

$$\mathcal{L} := \bigoplus_{i \geq 1} \mathcal{D}_i(G)/\mathcal{D}_{i+1}(G) \simeq \bigoplus_{i \geq 1} \mathcal{D}_i(H)/\mathcal{D}_{i+1}(H).$$

Proof: The associated graded ring of $\mathbb{F}_pG$ for the IG-adic filtration

$$\mathcal{U} = \bigoplus_{n\geq 0} (IG)^n/(IG)^{n+1}$$

is determined by $\mathbb{F}_pG$ by corollary 6.8.

It turns out that $\mathcal{U}$ is the universal enveloping algebra of $\mathcal{L}$, see [38, page 417]. And so the Lie algebra $\mathcal{L}$ is sitting as a sub-p-Lie algebra in $\mathcal{U}$ generated by the elements of dimension 1, and the result follows. □

Note that proposition 6.12 follows from this, and also that this is a stronger result, because it tells us that the commutator structure between the quotients is also preserved under an isomorphism of modular group algebras.

The results above have helped people in solving the problem for p-groups of small order and certain classes of p-groups. An account of the work on the modular isomorphism problem up to 1984 can be found in Bob Sandling's survey article, see [41]. And Sandling is also one of the people who has recent results on this problem. For example, it has been shown that the modular isomorphism problem has a positive solution for

- abelian p-groups (Deskins 1956),
- p-groups of order $\leq p^4$ (Passman 1965),
- groups of class 2 and exponent p (Passi and Sehgal 1972),
- groups of order 2^5 (Makasikis 1976, faults rectified by Sandling 1984),
- metacyclic p-groups (completed by Sandling 1994, see [42]),
- groups of order p^5, p odd (completed by Salim and Sandling 1994, see [40]),
- groups of order 2^6 (Wursthorn 1994, see [49]),
- groups of order 2^7 (Bleher, Kimmerle, Roggenkamp and Wursthorn 1997, see [5]).

In [20] there are lists of the groups of order p^5 and p^6, which were used as a reference, but not a necessity, in the work on groups of order p^5. However, continuing working with these methods does not have a lot to recommend it. Sandling, who supervised Mohamed Salim's work on p^5 says "Order p^6 looks much too difficult and tedious, and would mainly be instructive concerning presentations of p-groups."

Of other results, we should mention Czesław Bagiński and Jon F. Carlson's work on 2-groups of maximal class (dihedral, semidihedral and quaternion groups), see [8]. During "Groups St. Andrews" in Oxford , August 2001, Alexander B. Konovalov reported on joint work with Bagiński on the 2-groups of almost maximal class. It remains to distinguish 2 disjoint pairs of groups (of order 2^8) and 2 families before these groups can be added to the list.

We see that the problem has been successfully answered for p-groups belonging to classes which are recognisable from the information provided by the modular group algebra, and where the individual groups are given by invariants also determined by the modular group algebra. Moreover, the invariants people have needed haven't been too many (the order, the isomorphism types of the centre and the commutator factor group etc.). If we consider the classification of p-groups in general, then for bigger groups one needs more and more invariants. The cohomological invariants we will use are different in the sense that we work in terms of a presentation for our group.

Salim and Sandling write in their article [40] "One can chart a progression in recent papers on the modular isomorphism problem. Each sets out to deduce as much as possible from a quotient algebra of FG. The ideals which are divided out have become smaller and smaller, resulting in larger and larger sections of FG susceptible to purposeful analysis. At each stage a more complicated group basis becomes embeddable in the quotient algebra and thence its structure made accessible."

However, there has been a paucity of results on the modular isomorphism problem, and asking Sandling about his thoughts on the problem today, he replied "I think that majority opinion on the subject leans now to the negative side – really there is little evidence one way or the other. Perhaps, if the answer is positive, the likeliest way to establish it is to reconstruct $\mathbb{Z}G$ from FG somehow and apply the positive result of Roggenkamp and Scott for p-groups in the case of integral coefficients (if not $\mathbb{Z}G$, which does not seem at all likely, at least that information about it used in their argument)."

He also suggests some themes that could be pursued: 1) analogues of the results proven only for $\mathbb{F}_p$ for other fields of characteristic p; 2) deductions about G from its cohomology ring.

In his survey paper from 1984, Sandling refers to Laudal and says "The hope has been entertained that, for G a p-group, $\mathbb{Z}G$ determines via Massey products a certain obstruction morphism in mod p cohomology, and thence G itself." This is the morphism o_G introduced in theorem 4.4. So let us see what our work can say about this.

6.4 A cohomological viewpoint

We will now see the benefit of having various definitions of the cohomology groups, because some of them will not use information about G. Also the various constructions from earlier chapters will help us now. The following result starts us off.

Theorem 6.16 *Let G and H be finite p-groups. If $\mathbb{F}_pG \simeq \mathbb{F}_pH$ then we have $\mathrm{H}^n(G,\mathbb{F}_p) = \mathrm{H}^n(H,\mathbb{F}_p)$ for all $n \geq 0$.*

Proof: When we have $\mathbb{F}_pG \simeq \mathbb{F}_pH$, we can think of $F_\bullet$ as being an $\mathbb{F}_pH$-free resolution of $\mathbb{F}_p$, and apply lemma 2.10. □

We note that we can let our $F_\bullet$ start with the augmentation map, i.e. $F_0 = \mathbb{F}_pG$, and then let the F_i-s be free $\mathbb{F}_pG$-modules on the kernel of the previous differential (so F_1 is free on IG etc.). This resolution is very big (the more canonical a resolution is, the bigger it is), but at least it only uses the algebra structure, so we can find resolutions which do not use any information about G.

Theorems 2.30 and 6.16 tell us that the minimal number of generators and pro-p relations for G are determined by $\mathbb{F}_pG$. And using the Golod-Shafarevich inequality in theorem 4.8, we see that also a lower bound on the minimal number of relations is determined. Recall that we are dealing with a minimal pro-p presentation of G, so by a presentation we always mean a pro-p presentation.

We would like to make use of the Massey products and theorems 4.5 and 4.6.

Lemma 6.17 *The Yoneda composition* (3.3) *is determined by* $\mathbb{F}_pG$.

Proof: This product is defined by splicing sequences, which only uses information about $\mathbb{F}_pG$. $\square$

And also:

Lemma 6.18 *The cohomology ring* $\mathrm{H}^*(G, \mathbb{F}_p)$ *is determined by* $\mathbb{F}_pG$. $\square$

We only work with $\mathrm{H}^1(G, \mathbb{F}_p)$ and $\mathrm{H}^2(G, \mathbb{F}_p)$, but we mention this lemma since Ian Leary has given an example of two non-isomorphic p-groups with isomorphic cohomology rings, see [25]. This means that the algebra structure on $\mathrm{H}^*(G, \mathbb{F}_p)$ is not enough to determine G, and we therefore need to study generalised cup products, i.e. Massey products. This is analogous to determining a function by calculating more and more terms of its Taylor series.

Theorem 6.19 *Let G be a p-group. The Massey products on* $\mathrm{H}^1(G, \mathbb{F}_p)$ *and* $\mathrm{H}^2(G, \mathbb{F}_p)$ *are determined by* $\mathbb{F}_pG$.

Proof: The Massey products can for example be defined using the Hochschild cocomplex which only depends on $\mathbb{F}_pG$. By theorem 2.13 we are done. $\square$

Note that the procedure introduced in section 4.4 is determined by $\mathbb{F}_pG$ since the strictly defined Massey products come from extensions of extending $\mathbb{F}_p$ in the module category, as in section 3.4. And so the fact whether a strictly defined Massey products is zero or not tells us whether we have a certain module structure on an extension or not.

We now introduce the following class of finite p-groups.

Definition 6.20 *Let $\mathcal{C}$ be the class of finite p-groups having a pro-p presentation with relations on the form*

i) a generator to some (power of p)th power,
ii) left-normed n-fold commutators for $n \geq 2$,
and/or iii) products of i) and ii)

where if a certain $(n-1)$-fold commutator y for $n \geq 3$ occurs, then we don't have a k-fold commutator, $k \geq n$, involving y occurring.

By "involving" we mean if $y = [[a, b], c]$ say, then we don't have commutators $[\cdots[\ldots, [[a, b], c], \ldots], \ldots]$ occurring. Note that this is a class of groups, i.e. we don't say anything about parameters for example.

Using theorems 4.5 and 4.6, we see that the relations in the class $\mathcal{C}$ are exactly those determined by strictly defined Massey products. I.e. the groups in $\mathcal{C}$ have a presentation given by strictly defined Massey products, meaning you can write down the Massey products and they will all be strictly defined. Conversely, p-groups given by strictly defined Massey products are in $\mathcal{C}$.

So all the groups coming out of the procedure and tree construction in section 4.4 are in this class. In fact, the 2-generator groups in the class $\mathcal{C}$ are those coming from the tree construction in appendix B.

Also note that the class intersects non-trivially with all the classes for which it is known that the modular isomorphism problem has a positive answer.

Theorem 6.21 *The class $\mathcal{C}$ is determined by $\mathbb{F}_pG$, i.e. if $\mathbb{F}_pG \simeq \mathbb{F}_pH$ then G is in $\mathcal{C}$ if and only if H is in $\mathcal{C}$.*

Proof: To summarise, the class $\mathcal{C}$ gives us exactly the p-groups having a pro-p presentation coming from strictly defined Massey products. The Massey products, as we have seen, live on the Hochschild cocomplex, which is determined by $\mathbb{F}_pG$.

Moreover, the fact whether a Massey product is strictly defined or not is also determined by $\mathbb{F}_pG$ as this can be detected by considering the existence of certain module-structures as we saw in section 3.4. $\square$

We would like to distinguish the groups in the class $\mathcal{C}$. To do this we would need to sort out the problems we considered in section 4.5. However, we got some results on the 2-generator groups, so let us see what this tells us. First we state

Corollary 6.22 *Let $\mathcal{C}_2$ be the 2-generator groups in $\mathcal{C}$. Then $\mathcal{C}_2$ is determined by $\mathbb{F}_pG$, i.e. if $\mathbb{F}_pG \simeq \mathbb{F}_pH$ then G is in $\mathcal{C}_2$ if and only if H is in $\mathcal{C}_2$.*

Proof: In $\mathcal{C}_2$, $\dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathbb{F}_p) = 2$, which is determined by $\mathbb{F}_pG$, and so the result follows from theorem 6.21. $\square$

In the class $\mathcal{C}_2$ we have dealt with the indeterminacy for $p \geq 3$ in theorem 4.16. Moreover, the class $\mathcal{C}_2$ consists of the groups in the tree in appendix B. We see that this tree has three main branches.

Theorem 6.23 *Let $G \in \mathcal{C}_2$, $p \geq 3$. Then, referring to the procedure in section 4.4 and the tree in appendix B, $\mathbb{F}_pG$ determines what main branch G is in and at what level G is. Moreover, if conjecture 4.18 is true, then $\mathbb{F}_pG$ determines exactly where in the tree we can find G, hence determining G, i.e. if H is any group with $\mathbb{F}_pH \simeq \mathbb{F}_pG$ then $H \simeq G$.*

Proof: We first note that building extensions as we did in section 3.4 detects how the various products are related, hence $\mathbb{F}_pG$ distinguishes between groups like G_{11} and G_{12} in section 4.3.3. And so the choices of the various ranks in the procedure in section 4.4 are determined by $\mathbb{F}_pG$. These ranks will define the branches in the tree. Since the base step in the proof of conjecture 4.18 is OK, $\mathbb{F}_pG$ determines in which of the main branches G sits.

For each level in the procedure we form new branches, and so if we get the induction step in the proof of conjecture 4.18 to work, we have dealt with the well-definedness problems, and the result follows. $\square$

Appendix A

A Magma-session on G_6

The following Magma-session was run in example 2.31.

```
> G<x,y> := Group<x,y|x^27=1,y^3=1,(x,y)=x^9>;
> print Order(G);
81
> print pQuotient(G,3,0);
GrpPC of order 81 = 3^4
PC-Relations:
    $.1^3 = $.3,
    $.3^3 = $.4,
    $.2^$.1 = $.2 * $.4^2
> H<x,y> := Group<x,y|x^3=1,y^9*(x,y)=1>;
> print Order(H);
2997
> print pQuotient(H,3,0);
GrpPC of order 81 = 3^4
PC-Relations:
    $.2^3 = $.3,
    $.3^3 = $.4,
    $.2^$.1 = $.2 * $.4
> IsIsomorphic(pQuotient(G,3,0),pQuotient(H,3,0));
true
> K<x,y> := Group<x,y|x^27=y^3,(x,y)=x^9>;
> print Order(K);
81
> IsIsomorphic(pQuotient(K,3,0),pQuotient(H,3,0));
true
```

Appendix B

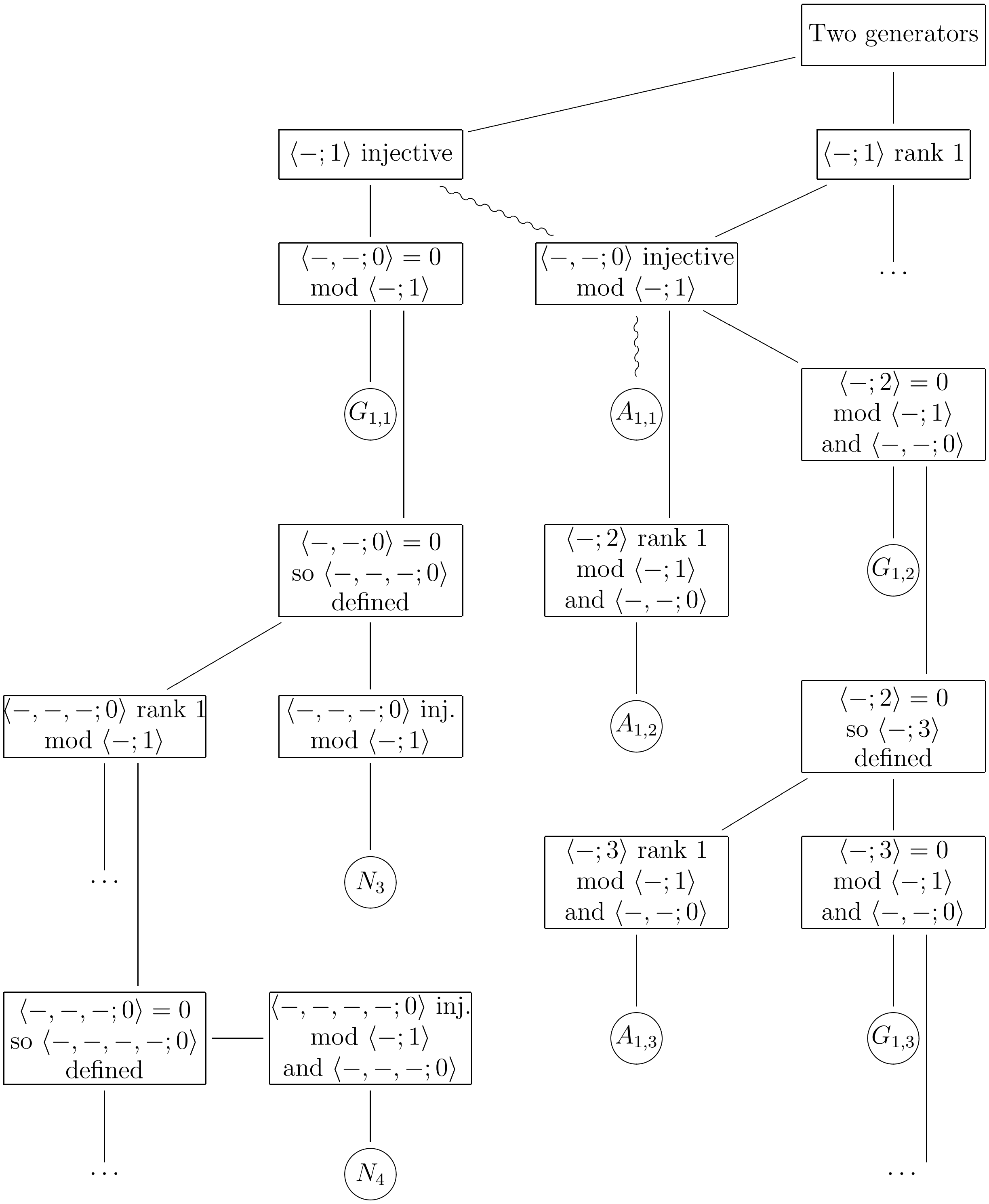
A tree of 2-generator p-groups

In chapters 4 and 5 we introduced the families

- $\{A_{m,n}\}_{n\geq 1}$ for fixed m (**Definition 4.12**);
- $\{N_i\}_{i\geq 3}$ (**Definition 4.13**);
- $G(m, N-2m)$, which we will denote $G_{m,N-2m}$ here to save space (**Theorem 5.11**).

The following groups appear in the tree-construction on the next page:

- $A_{1,n} = C_p \times C_{p^n}$ for $n = 1, 2, 3$;
- $A_{2,n} = C_{p^2} \times C_{p^n}$ for $n = 2, 3, 4$;
- $G_{1,N-2} \simeq \{x, y | x^p[x, y] = 1, y^{p^{N-2}}[x, y] = 1\}$ for $N = 3, 4, 5$;
- $G_{2,N-4} \simeq \{x, y | x^{p^2}[x, y] = 1, y^{p^{N-4}}[x, y] = 1\}$ for $N = 6, 7, 8$;
- $N_3 = \{x, y | x^p = 1, y^p = 1, [x, y, y] = 1, [x, y, x] = 1\}$;
- $N_4 = \{x, y | x^p = 1, y^p = 1, [x, y, y] = 1, [x, y, x, x] = 1, [x, y, x, y] = 1\}$ where the last relation can be omitted.


Two generators
$\langle -;1\rangle$ injective
$\langle -;1\rangle$ rank 1
$\langle -,-;0\rangle = 0$ mod $\langle -;1\rangle$
$\langle -,-;0\rangle$ injective mod $\langle -;1\rangle$
$\dots$
$G_{1,1}$
$A_{1,1}$
$\langle -;2\rangle = 0$ mod $\langle -;1\rangle$ and $\langle -,-;0\rangle$
$\langle -,-;0\rangle = 0$ so $\langle -,-,-;0\rangle$ defined
$\langle -;2\rangle$ rank 1 mod $\langle -;1\rangle$ and $\langle -,-;0\rangle$
$G_{1,2}$
$\langle -,-,-;0\rangle$ rank 1 mod $\langle -;1\rangle$
$\langle -,-,-;0\rangle$ inj. mod $\langle -;1\rangle$
$A_{1,2}$
$\langle -;2\rangle = 0$ so $\langle -;3\rangle$ defined
$\dots$
N_3
$\langle -;3\rangle$ rank 1 mod $\langle -;1\rangle$ and $\langle -,-;0\rangle$
$\langle -;3\rangle = 0$ mod $\langle -;1\rangle$ and $\langle -,-;0\rangle$
$\langle -,-,-;0\rangle = 0$ so $\langle -,-,-,-;0\rangle$ defined
$\langle -,-,-,-;0\rangle$ inj. mod $\langle -;1\rangle$ and $\langle -,-,-;0\rangle$
$A_{1,3}$
$G_{1,3}$
$\dots$
N_4
$\dots$

Bibliography

[1] A. Babakhanian. *Cohomological Methods in Group Theory.* Marcel Dekker, 1972.

[2] D. J. Benson. *Representations and cohomology I.* Cambridge studies in advanced mathematics 30, CUP, 1991.

[3] D. J. Benson. *Representations and cohomology II.* Cambridge studies in advanced mathematics 31, CUP, 1991.

[4] F. R. Beyl. The Schur multiplicator of metacyclic groups. *Proc. Amer. Math. Soc.* 40 (1973), 413 − 418.

[5] F. M. Bleher, W. Kimmerle, K. W. Roggenkamp, and M. Wursthorn. Computational aspects of the isomorphism problem. In *"Algorithmic algebra and number theory" (Heidelberg* 1997*),* 313 − 329*, Springer* 1999.

[6] R. Brauer. Representations of finite groups. In T. L. Saaty, editor, *Lectures on modern mathematics 1*, pages 135–175. Wiley, 1963.

[7] W. Burnside. *Theory of groups of finite order.* Cambridge University Press, 1911.

[8] J. F. Carlson. Periodic modules over modular group algebras. *J. London Math. Soc.* 15 (1977), 431 − 436.

[9] J. F. Carlson. *Modules and group algebras.* Lectures in Mathematics, ETH Zürich, Birkhäuser, 1996.

[10] D. B. Coleman. On the modular group ring of a p-group. *Proc. Amer. Math. Soc.* 15 (1964), 511 − 514.

[11] E.C. Dade. Deux groupes finis distincts ayant la même algèbre de groupe sur tout corps. *Math. Z.* 119 (1971), 345 – 348.

[12] W. E. Deskins. On finite abelian groups having isomorphic group algebras. *Bull. Amer. Math. Soc.* 61 (1955), 125.

[13] W. Dwyer. Homology, Massey products and maps between groups. *J. Pure and Appl. Alg.* 6 (1975), 177 – 190.

[14] R. Fenn and D. Sjerve. Basic commutators and minimal Massey products. *Can. J. Math.* 36 (1984), 1119 – 1146.

[15] R. Fenn and D. Sjerve. Massey products and lower central series of free groups. *Can. J. Math.* 39 (1987), 322 – 337.

[16] K. W. Gruenberg. *Some cohomological topics in group theory.* Queen Mary College Mathematics Notes, 1967.

[17] M. Hertweck. A counterexample to the isomorphism problem for integral group rings. *Annals of Math.* 154 (2001), 115 – 138.

[18] P. J. Hilton and U. Stammbach. *A course in homological algebra.* Springer GTM 4, 1971.

[19] G. Hochschild. On the cohomology groups of an associative algebra. *Annals of Math.,* 46 (1945), 58 – 67.

[20] R. James. The groups of order p^6. *Mathematics of computation, volume* 34, *number* 150 (1980), 613 – 637.

[21] S. A. Jennings. The structure of the group ring of a p-group over a modular field. *Trans. Amer. Math. Soc.* 50 (1941), 175 – 185.

[22] D. Kraines. Massey higher products. *Trans. Amer. Math. Soc.* 124 (1966), 431 – 449.

[23] O. A. Laudal. p-groups and Massey products. *Preprint series* 1975/76*, No.* 30*, Matematisk Institut, Aarhus Universitet,* 1976.

[24] M. Lazard. Sur les groupes nilpotents et les anneaux de Lie. *Ann. Ecole Norm. Supér.* 71 (1954), $101 - 190$.

[25] I. J. Leary. The mod-p cohomology rings of some p-groups. *Math. Proc. Camb. Phil. Soc.* 112 (1992), $63 - 75$.

[26] S. Liedahl. Enumeration of metacyclic p-groups. *J. Alg.* 186 (1996), $436 - 446$.

[27] S. Liedahl. Presentations of metacyclic p-groups with applications to k-admissibility questions. *J. Alg.* 169 (1994), $965 - 983$.

[28] J.-L. Loday. *Cyclic homology.* Springer, 1992.

[29] W. Magnus, A. Karrass, and D. Solitar. *Combinatorial group theory.* Wiley, 1966.

[30] W. S. Massey. Some higher order cohomology operations. *Symposium internacional de topologia algebraica, pp.* $145 - 154$*, Mexico City,* 1958.

[31] J. P. May. Matric Massey products. *J. Alg.* 12 (1969), $533 - 568$.

[32] J. McCleary. *A user's guide to spectral sequences.* Cambridge studies in advanced mathematics 58, 2. edition, CUP, 2001.

[33] M. F. Newman, G. Sauerbier, and J. Wisliceny. Groups of prime-power order with a small number of relations. *Rostock Math. Kolloq.* 49 (1995), $141 - 154$.

[34] Ø. Nordvik. A cohomological classification of p-groups of small orders. Master's thesis, University of Oslo, 1983.

[35] I. B. S. Passi and S. K. Sehgal. Isomorphism of modular group algebras. *Math. Z.* 129 (1972), $65 - 73$.

[36] D. Passman. The group algebra of groups of order p^4 over a modular field. *Michigan Math. Journal* 12 (1965), $405 - 415$.

[37] D. Passman. *The algebraic structure of group rings.* Wiley, 1965.

[38] D. Quillen. On the associated graded ring of a group ring. *J. Alg.* 10 (1968), $411-418$.

[39] K. W. Roggenkamp and L. Scott. Isomorphisms of p-adic group rings. *Annals of Math.* 126 (1987), $593-647$.

[40] M. Salim and R. Sandling. The modular group algebra problem for groups of order p^5. *J. Austral. Math. Soc.* 61 (1996), $229-237$.

[41] R. Sandling. The isomorphism problem for group rings: A survey. In *"Orders and their applications" (Oberwolfach* 1984*),* $256-288$*, Springer Lecture Notes in Mathematics* 1142.

[42] R. Sandling. The modular group algebra problem for metacyclic p-groups. *Proc. Amer. Math. Soc.* 124 (1996), $1347-1350$.

[43] J.-P. Serre. *Galois cohomology.* Springer, 1997.

[44] D. Stein. Massey products in the cohomology of groups with applications to link theory. *Trans. Amer. Math. Soc.* 318 (1990), $301-325$.

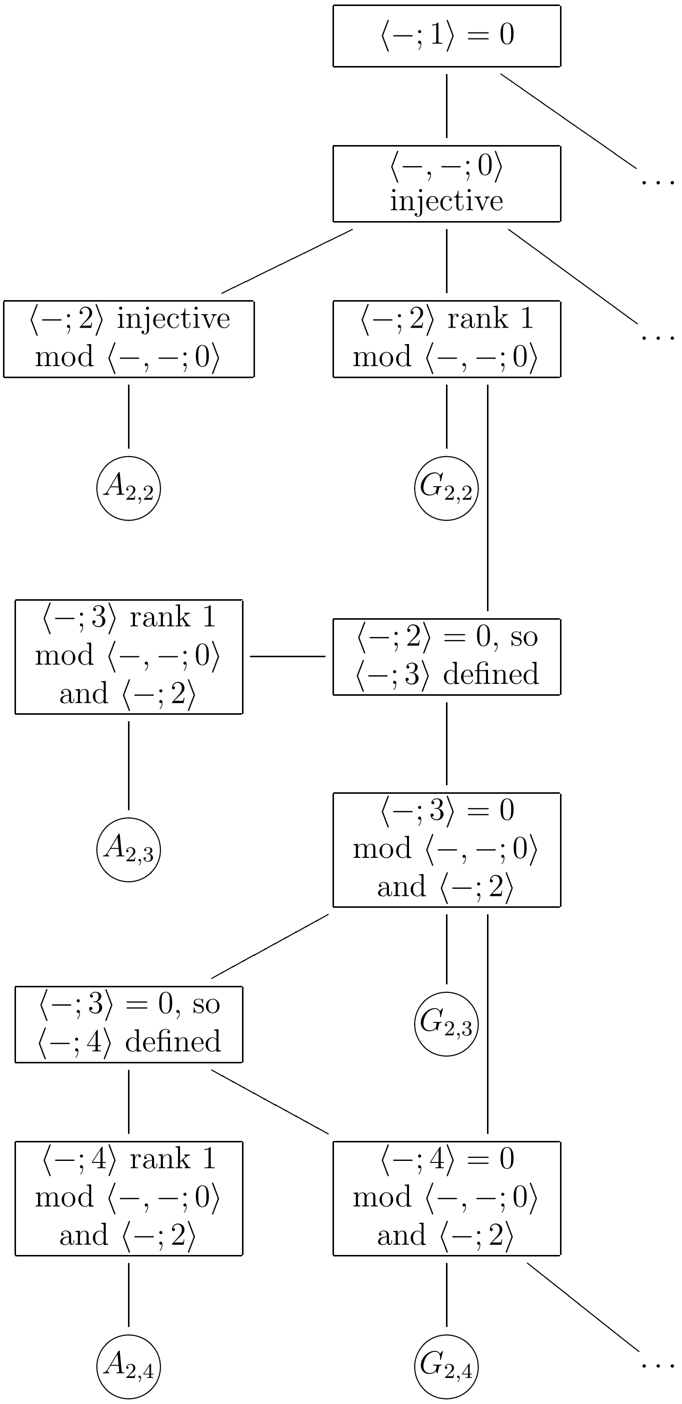
[45] J. W Wamsley. The deficiency of metacyclic groups. *Proc. Amer. Math. Soc.* 24 (1970), $724-726$.

[46] C. Weibel. *An introduction to homological algebra.* Cambridge studies in advanced mathematics 38, CUP, 1994.

[47] A. Weiss. Rigidity of p-adic p-torsion. *Annals of Math.,* 127 (1988), $317-332$.

[48] J. Wilson. *Profinite groups.* LMS monographs, Oxford University Press, 1998.

[49] M. Wursthorn. Isomorphisms of modular group algebras: An algorithm and its application to groups of order 2^6. *J. Symb. Comput.* 15 (1994), $211-227$.


$\langle -;1\rangle = 0$
$\langle -,-;0\rangle$ injective
. . .
$\langle -;2\rangle$ injective mod $\langle -,-;0\rangle$
$\langle -;2\rangle$ rank 1 mod $\langle -,-;0\rangle$
. . .
$A_{2,2}$
$G_{2,2}$
$\langle -;3\rangle$ rank 1 mod $\langle -,-;0\rangle$ and $\langle -;2\rangle$
$\langle -;2\rangle = 0$, so $\langle -;3\rangle$ defined
$A_{2,3}$
$\langle -;3\rangle = 0$ mod $\langle -,-;0\rangle$ and $\langle -;2\rangle$
$\langle -;3\rangle = 0$, so $\langle -;4\rangle$ defined
$G_{2,3}$
$\langle -;4\rangle$ rank 1 mod $\langle -,-;0\rangle$ and $\langle -;2\rangle$
$\langle -;4\rangle = 0$ mod $\langle -,-;0\rangle$ and $\langle -;2\rangle$
$A_{2,4}$
$G_{2,4}$
. . .

A cohomological approach to the classification of p-groups

Inger Christin Borge, Wadham College

Thesis submitted to the Faculty of Mathematical Sciences as partial
fulfilment for the degree of Doctor of Philosophy, Trinity term 2001

Abstract

In this thesis we apply methods from homological algebra to the study of finite p-groups.

Let G be a finite p-group and let $\mathbb{F}_p$ be the field of p elements. We consider the cohomology groups $\mathrm{H}^1(G, \mathbb{F}_p)$ and $\mathrm{H}^2(G, \mathbb{F}_p)$ and the Massey product structure on these cohomology groups, which we use to deduce properties about G.

We tie the classical theory of Massey products in with a general method from deformation theory for constructing hulls of functors and see how far the strictly defined Massey products can take us in this setting.

We show how these Massey products relate to extensions of modules and to relations, giving us cohomological presentations of p-groups. These presentations will be minimal pro-p presentations and will often be different from the presentations we are used to.

This enables us to shed some new light on the classification of p-groups, in particular we give a "tree construction" illustrating how we can "produce" p-groups using cohomological methods. We investigate groups of exponent p and some of the families of groups appearing in the tree. We also investigate the limits of these methods.

As an explicit example illustrating the theory we have introduced, we calculate Massey products using the Yoneda cocomplex and give 0-deficiency presentations for split metacyclic p-groups using strictly defined Massey products.

We also apply these methods to the modular isomorphism problem, i.e. the problem whether (the isomorphism class of) G is determined by $\mathbb{F}_pG$. We give a new class $\mathcal{C}$ of finite p-groups which can be distinguished using $\mathbb{F}_pG$.