A COHOMOLOGICAL APPROACH TO THE MODULAR ISOMORPHISM PROBLEM

INGER CHRISTIN BORGE

ABSTRACT. We consider how cohomological invariants determined by $\mathbb{F}_p G$ can be used to shed some new light on the modular isomorphism problem. In particular, we give a new class \mathcal{C} of finite p-groups which can be distinguished using $\mathbb{F}_p G$.

1. Introduction

In this paper G will always be a finite p-group. The problem whether (the isomorphism class of) G is determined by its group algebra over the field of p elements is usually referred to as the modular isomorphism problem.

There has been a lot of work done on this problem since Deskins first considered it in 1954, see [5]. During this time we have gained a lot of knowledge about \mathbb{F}_pG and some deep results have been obtained. One of the strongest results is the fact that the restricted Lie algebra of G is determined by \mathbb{F}_pG , a result which is due to Quillen and Lazard, see [15] and [10]. However, the restricted Lie algebra does not provide enough information to pin down the group G.

An account of the work on the modular isomorphism problem up to 1984 can be found in Sandling's survey article, see [17]. And Sandling is also one of the people who has recent results on this problem. To summarise, it has been shown that the modular isomorphism problem has a positive solution for

- abelian p-groups (Deskins 1956, see [6]),
- p-groups of order $\leq p^4$ (Passman 1965, see [14]),

Date: 19. August 2002.

Key words and phrases. Massey products, modular isomorphism problem, homological methods in group theory.

D. Phil. work supported by the European Commission under a TMR Marie Curie Research Training Grant, contract no. ERBFMBICT972701.

- groups of class 2 and exponent p (Passi and Sehgal 1972, see [13]),
- groups of order 2⁵ (Makasikis 1976, faults rectified by Sandling 1984, see [17]),
- metacyclic p-groups (completed by Sandling 1994, see [18]),
- groups of order p^5 (completed by Salim and Sandling 1994, see [16]),
- groups of order 2⁶ (Wursthorn 1994, see [20]),
- groups of order 2⁷ (Bleher, Kimmerle, Roggenkamp and Wursthorn 1997, see [3]).

So in order to solve the problem, one searches for classes of p-groups 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. We see that the problem has been successfully answered for p-groups belonging to such classes where the invariants determining the individual groups haven't been too many.

However, if we consider p-groups in general, then the bigger the group, the more invariants we will need. The cohomological invariants we will consider are different from the ones people have used so far, in the sense that we work in terms of a presentation for our group.

Our invariants are given by the Massey product structure on $H^1(G, \mathbb{F}_p)$ and $H^2(G, \mathbb{F}_p)$. We introduce the part of this structure that we will concentrate on in section 2, and we link it to a presentation of G in section 3. In section 4 we explain the Yoneda construction for these products, which in section 5 will help us distinguish a new class \mathcal{C} of p-groups using $\mathbb{F}_p G$.

To quote Sandling, he writes in his survey paper: "The hope has been entertained that for a p-group, $\mathbb{Z}G$ determined via Massey products a certain obstruction morphism in mod p cohomology, and thence G itself." The reference is to Laudal, see [9], my former supervisor. In this paper, we will build on this idea, which in a more general setting comes from deformation theory and a general method for constructing hulls of functors. We will tie this method in with the "classical" theory of Massey products, as found in the works of Massey, Kraines, and May, see [11], [8] and [12] respectively.

Relating our class of p-groups to Quillen and Lazard's result on the restricted Lie algebra, which tells us that we can distinguish p-groups on the level of the commutator- and pth power-structure using \mathbb{F}_pG , our class \mathcal{C} has a generalised such structure, i.e. n-fold commutators, $n \geq 2$, and (powers of p)th power-structure (analogous to calculating more terms in the Taylor series of a function).

2. Preliminary results and definitions

To get a cohomological viewpoint on the modular isomorphism problem, we are lead to studying the ordinary group cohomology of G with values in \mathbb{F}_p .

Lemma 2.1. Let G and H be finite p-groups. If $\mathbb{F}_p G \simeq \mathbb{F}_p H$ then we have $H^n(G, \mathbb{F}_p) = H^n(H, \mathbb{F}_p)$ for all $n \geq 0$.

Proof. We define

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

We can think of an \mathbb{F}_pG -free resolution of \mathbb{F}_p as an \mathbb{F}_pH -free resolution of \mathbb{F}_p and apply the Comparison Theorem.

These cohomology groups are \mathbb{F}_p -vectorspaces, and for the low-dimensional cohomology groups we have some very useful interpretations, namely

Theorem 2.2. Let G be a finite p-group, d the minimal number of generators for G and t the minimal number of relations between these generators in the corresponding free pro-p group. Then

$$(2.1) d = \dim_{\mathbb{F}_n} H^1(G, \mathbb{F}_p);$$

$$(2.2) t = \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p).$$

Proof. See for example Serre, [19].

The next thing to observe about the graded vector space $H^*(G, \mathbb{F}_p)$ is that it carries an algebra structure, usually given by the cup product. However, if we define the product structure using the Yoneda composition (splicing of exact sequences), we get

Theorem 2.3. The cohomology ring $H^*(G, \mathbb{F}_p)$ is determined by \mathbb{F}_pG .

Proof. Whereas the definition of the cup product uses the diagonal map, and therefore G, the Yoneda composition only uses \mathbb{F}_pG . The result follows from the fact that these two products are the same when we work over the trivial module, see [1, page 53].

The algebra structure on the graded vector space $H^*(G, \mathbb{F}_p)$ is induced from the product on the dual resolution (from where we calculate the cohomology). We will use the notation $\langle -, -; 0 \rangle$ (from Laudal, see [9]) to denote both the product between cochains and the induced product between cohomology classes.

The graded algebra $H^*(G, \mathbb{F}_p)$ will be associative and graded-commutative, whereas the dual resolution will only be associative and graded-commutative up to homotopy as a differential graded algebra. 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).

Because of theorem 2.2, we will concentrate on $H^1(G, \mathbb{F}_p)$ and $H^2(G, \mathbb{F}_p)$. 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 $H^1(G, \mathbb{F}_p)$ to $H^2(G, \mathbb{F}_p)$ (\mathcal{P}^0 is the identity operation, see [2, page 138]).

The construction of the Massey products on $H^*(G, \mathbb{F}_p)$ will be the same over any resolution which is used to calculate $H^n(G, \mathbb{F}_p)$ for $n \geq 0$. Since Hochschild cohomology for the group algebra is the same as group cohomology when we work over the trivial module, i.e.

$$H^n(G, \mathbb{F}_p) = HH^n(\mathbb{F}_pG, \mathbb{F}_p), \quad n \ge 0,$$

we have that

Lemma 2.4. The Massey products on $H^*(G, \mathbb{F}_p)$ are determined by \mathbb{F}_pG .

We will give the definitions of Massey products as partially defined functions on tuples of elements in $H^1(G, \mathbb{F}_p)$ into $H^2(G, \mathbb{F}_p)$. For the definitions we will follow Kraines' set-up, see [8], but we will have 1-s on the diagonal in the defining systems, as Dwyer does, see [7]. We also follow Kraines' sign conventions. The ∂ refers to the differential in a dual resolution for \mathbb{F}_p .

Definition 2.5. Let $\xi_1, \ldots, \xi_s \in H^1(G, \mathbb{F}_p)$ and let ϕ_1, \ldots, ϕ_s be cocycle representatives of ξ_1, \ldots, ξ_s respectively. A collection of 1-cochains

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

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

(2.3)
$$m_{i,i+1} = \phi_i$$
 for $i = 1, ..., s$:

(2.4)
$$\partial m_{ij} = \sum_{k=i+1}^{j-1} -\langle m_{ik}, m_{kj}; 0 \rangle \quad \text{for } j \neq i+1.$$

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

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

We say that 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.

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

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

Lemma 2.6. The operation $\langle \phi_1, \ldots, \phi_s; 0 \rangle$ depends only on the cohomology classes of ϕ_1, \ldots, ϕ_s .

Proof. See
$$[8, page 432]$$
.

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

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

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

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 2.7. We say that $\langle \xi_1, \ldots, \xi_s; 0 \rangle$ is strictly defined if each

$$\langle \xi_i, \dots, \xi_j; 0 \rangle$$
 for $1 \le j - i \le s - 2$

is defined and contains only 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 that we have indeterminacy occurring naturally, which we need to deal with.

Definition 2.8. The indeterminacy of the Massey product $\langle \xi_1, \ldots, \xi_s; 0 \rangle$ is defined by

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

We now introduce some canonical groups U(s,r) which will be used in the interpretation of the Massey product. 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.

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

The elements $\{u_i\}_{i=1}^s = \{I_{s+1} + e_{i,i+1}\}_{i=1}^s$ will generate U(s,r).

Let $\Gamma_k(G)$ denote the kth term in the lower central p-series for G defined recursively by

$$\Gamma_0(G) = G,$$

(2.6)
$$\Gamma_i(G) = [\Gamma_{i-1}(G), G] \cdot \Gamma_{i-1}(G)^p.$$

Then for r+s=k+1, $\Gamma_{k+1}(U(s,r))=I_{s+1}$ and $\Gamma_k(U(s,r))/\Gamma_{k+1}(U(s,r))\simeq$ \mathbb{F}_p is generated by the element $[\cdots[u_1,u_2],\ldots,u_s]^{p^r}$.

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 [7, 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). This gives a nice characterisation of a defining system which we will make use of.

Theorem 2.9. Let ξ_1, \ldots, ξ_s be elements in $H^1(G, \mathbb{F}_p)$. There is a one-one correspondence $M \longleftrightarrow \phi_M$ between defining systems M for $\langle \xi_1, \ldots, \xi_s; 0 \rangle$ and group homomorphisms

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

which have ξ_1, \ldots, ξ_s on the superdiagonal (in the order given, i.e. the entry (i, i+1) is ξ_i). Moreover, $\langle \xi_1, \ldots, \xi_s; 0 \rangle_M = 0$ in $H^2(G, \mathbb{F}_p)$ if and only if the dotted arrow exists in the following diagram.

$$U(s,0) \xrightarrow{\longrightarrow} U(s,0)/\Gamma_{s-1}(U(s,0))$$

$$\downarrow^{\phi_M}$$

$$G$$

Proof. See Dwyer, [7, page 185].

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 [8, page 440]. In characteristic p the restricted product $\langle \underbrace{\xi_i, \xi_i, \dots, \xi_i}_{p}; 0 \rangle$ is the first such product that

can be non-zero. Moreover, it is defined as a single class of $H^2(G, \mathbb{F}_p)$, i.e. it has no indeterminacy.

Combining the fact that the Steenrod operations don't do anything for $H^1(G, \mathbb{F}_p)$ and $H^2(G, \mathbb{F}_p)$ with Kraines' theorem 14 in [8] we have that

(2.7)
$$\langle \underbrace{\xi_i, \xi_i, \dots, \xi_i}_{p}; 0 \rangle = -\beta(\xi_i),$$

where β is the Bockstein operation associated to the short exact sequence

$$(2.8) 0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z}/p\mathbb{Z} \longrightarrow 0.$$

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

Now, if $\langle \xi_i; 1 \rangle$ is 0 as an element in $H^2(G, \mathbb{F}_p)$, 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 2.10. 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 [8] tells us that the p^k -fold restricted product

(2.9)
$$\langle -; k \rangle : H^1(G, \mathbb{F}_p) \longrightarrow H^2(G, \mathbb{F}_p)$$

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

$$(2.10) 0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p^{k+1}\mathbb{Z} \stackrel{\cdot p}{\longrightarrow} \mathbb{Z}/p^k\mathbb{Z} \longrightarrow 0.$$

We just need to note that Kraines assumes naturality and works with the first and second cohomology groups for cyclic groups rather than a general p-group G.

If we write the short exact sequences defining the various Bockstein maps using our testgroups, we can formulate an analogous result to theorem 2.9. It says that if $\langle \xi_i; k \rangle$ is defined and is non-zero, 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, and we will use this result in the next section. 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 2.11. Let $\xi_i \in H^1(G, \mathbb{F}_p)$. 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 $H^2(G, \mathbb{F}_p)$ if and only if the dotted arrow exists in the following diagram.

$$U(1,r) \xrightarrow{\longrightarrow} U(1,r)/\Gamma_r(U(1,r))$$

$$\downarrow^{\phi_r}$$

$$G$$

Proof. We observe that $U(1,1)/\Gamma_1(U(1,1)) \simeq \mathbb{F}_p$, $H^1(G,\mathbb{F}_p) \simeq \operatorname{Hom}(G,\mathbb{F}_p^+)$ 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 arising from 2.8:

$$\cdots \longrightarrow \mathrm{H}^1(G,\mathbb{Z}/p\mathbb{Z}) \longrightarrow \mathrm{H}^1(G,\mathbb{Z}/p^2\mathbb{Z}) \xrightarrow{(\cdot p)^*} \mathrm{H}^1(G,\mathbb{Z}/p\mathbb{Z}) \longrightarrow$$

$$\langle -;1 \rangle$$

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

So if $\langle -; 1 \rangle = 0$, then by exactness we have an element $\phi_2 \in H^1(G, \mathbb{Z}/p^2\mathbb{Z})$ 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 sends ϕ_k to 0. If we intertwine the (r-1)st and the rth long-exact sequences, we get the diagram

$$H^{1}(G, \mathbb{Z}/p^{r-1}\mathbb{Z})$$

$$\downarrow \qquad \qquad \downarrow \qquad \qquad \qquad \downarrow \qquad \qquad \qquad \qquad \downarrow \qquad \qquad \downarrow \qquad \qquad \downarrow \qquad \qquad \downarrow \qquad \qquad \qquad \downarrow \qquad \qquad \qquad \qquad \downarrow \qquad \qquad \downarrow \qquad \qquad \qquad \qquad \downarrow \qquad \qquad \qquad \qquad \qquad \qquad \downarrow \qquad \qquad \qquad \qquad \downarrow \qquad \qquad \qquad \qquad \qquad \downarrow \qquad \qquad$$

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 $\phi_{r+1} \in \mathrm{H}^1(G, \mathbb{Z}/p^{r+1}\mathbb{Z}).$

3. Strictly defined Massey products and group relations

We have seen that \mathbb{F}_pG determines the Massey products on $H^*(G,\mathbb{F}_p)$, and in particular the Massey products between $H^1(G, \mathbb{F}_p)$ and $H^2(G, \mathbb{F}_p)$. We will now put together the various results from section 2 and show how we can relate strictly defined Massey products to relations in our group.

Going back to theorem 2.2, this tells us that we are dealing with a minimal pro-p presentation for G, i.e. a presentation of an abstract group where the largest p-quotient is isomorphic to G.

Let $\{\xi_1,\ldots,\xi_d\}$ be a basis for $H^1(G,\mathbb{F}_p)$, let $\{\eta_1,\ldots,\eta_t\}$ be a basis for $H^2(G, \mathbb{F}_p)$ and let T^i be the free pro-p group on a dual basis for $H^i(G, \mathbb{F}_p)$, i =1, 2. This was introduced by Laudal, see [9].

We know that $H^2(G, \mathbb{F}_p)$ classifies group extensions of G by \mathbb{F}_p , and so elements in $H^2(G, \mathbb{F}_p)$ will give us obstructions for lifting group homomorphisms. Using obstruction theory on the lower central p-series of T^1 , $\{\Gamma_i(T^1)\}_{i>0}$, we get a structure theorem for pro-p groups:

Theorem 3.1. The obstructions give rise to a morphism between pro-p groups

$$o_G: T^2 \to T^1$$

 $o_G: \ T^2 \to T^1$ and an isomorphism $G \simeq T^1/\overline{\langle \operatorname{im} o_G \rangle}$, where $\overline{\langle \operatorname{im} o_G \rangle}$ denotes the normal closure of im o_G in T^1 .

Proof. See Laudal,
$$[9, page 10]$$
.

The question we will address here is "How much of the obstruction morphism is determined by \mathbb{F}_pG ?"

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

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

with π_1 being an isomorphism. The obstruction calculus determines the kernels of the π_i -s, starting with i=1 and working upwards in such a way that $\langle \operatorname{im} o_G \rangle$ 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_i^* and consider a basis for $\Gamma_k(T^1)/\Gamma_{k+1}(T^1)$ using leftnormed commutators and pth powers, we have that $o_G(\eta_i^*)$ can be expressed on the form

(3.1)
$$o_G(\eta_j^*) = \prod_{k \ge 1} \left(\prod_{\underline{i},r} [\cdots [\xi_{i_1}^*, \xi_{i_2}^*], \dots, \xi_{i_s}^*]^{p^r c(\underline{i},r,j)} \right)$$

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

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

$$(3.2) r = 0, s \ge 2,$$

$$(3.3) r \ge 1, s = 1.$$

For this, we concentrate on the strictly defined products

$$(3.4)$$
 $\langle -, -, \cdots, -; 0 \rangle$ (definition 2.7),

(3.5)
$$\langle -; r \rangle$$
 (definition 2.10).

We have the following theorem linking (3.2) and (3.4).

Theorem 3.2. Let $\{\xi_1, \ldots, \xi_d\}$ and $\{\eta_1, \ldots, \eta_t\}$ be a basis for $H^1(G, \mathbb{F}_p)$ and $H^2(G, \mathbb{F}_p)$ respectively and let

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

be a strictly defined Massey product. Then, referring to (3.1), $c(\underline{i}, 0, j) = \alpha_j$ 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

$$(3.6) \quad \mathrm{H}^{1}(G, \mathbb{F}_{p}) \otimes_{\mathbb{F}_{p}} U(s, 0) / \Gamma_{1}(U(s, 0)) \simeq \mathrm{Mor}(T^{1}, U(s, 0) / \Gamma_{1}(U(s, 0)).$$

We will proceed by induction on s, so first let s=2 (s=1 comes under (3.3)). Then our product is the Yoneda composition which is always defined. By (3.6), a morphism $T^1 \longrightarrow U(s,0)/\Gamma_1(U(s,0))$ will correspond to elements in $H^1(G, \mathbb{F}_p)$, so pick $\xi_1, \xi_2 \in H^1(G, \mathbb{F}_p)$ and consider the morphism

$$\psi_1: T^1 \longrightarrow U(2,0)/\Gamma_1(U(2.0))$$

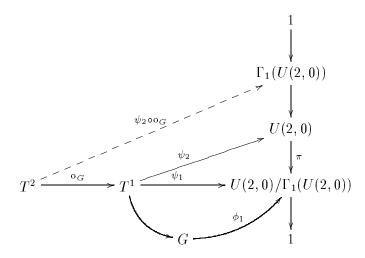
$$\xi_1^* \quad \longmapsto \quad \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xi_2^* \quad \longmapsto \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xi_i^* \quad \longmapsto \quad 1 \quad \text{for } i \neq 1, 2.$$

From (3.1) we see that $\psi_1(o_G(\eta_j^*)) = 0 \ \forall j \in \{1, ..., t\}$, which means that the composition $\psi_1 \circ o_G$ 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 2.9 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 $\psi_1 \circ o_G$ is trivial we get that $\psi_2 \circ o_G: T^2 \longrightarrow \Gamma_1(U(2,0))$. We have the diagram



What happens to $o_G(\eta_j^*)$ under the lifting ψ_2 ? Well, from (3.1) and the diagram above we see that

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

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

(3.7)
$$\psi_2(o_G(\eta_j^*)) = \eta_j^*(\psi_2 \circ o_G).$$

Using (3.6) on T^2 and $U(2,0) \simeq \mathbb{F}_p$, we have that the map $\psi_2 \circ o_G$ gives us an element in $H^2(G,\mathbb{F}_p)$. 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, $o_G(\eta_j^*)$ have no commutators involving $[\cdots [\xi_i^*, \ldots], \xi_k^*]$ occurring.

Using (3.6), we are lead to consider a morphism

$$\psi_1: \quad T^1 \quad \longrightarrow \quad U(s,0)/\Gamma_1(U(s,0))$$

$$\xi_i^* \quad \longmapsto \quad \begin{cases} u_i & \text{for } i=1,\ldots,s \\ 1 & \text{otherwise.} \end{cases}$$

As before, ψ_1 sends $o_G(\eta_i^*)$ 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 $o_G(\eta_j^*)$ 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 $\psi_m(o_G(\eta_j^*)) = 1$ 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

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

where $\underline{i} = \{1, ..., s\}$. The map ϕ_{s-1} will, again by theorem 2.9, give a defining system for $\langle \xi_1, ..., \xi_s; 0 \rangle$, and as for s = 2, the map

$$\psi_s \circ o_G : T^2 \longrightarrow \Gamma_{s-1}(U(s,0))$$

gives us the value of the defining system, so using (3.7) for general s,

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

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

Similarly, we get a theorem linking (3.3) and (3.5):

Theorem 3.3. Let $\{\xi_1, \ldots, \xi_d\}$ and $\{\eta_1, \ldots, \eta_t\}$ be a basis for $H^1(G, \mathbb{F}_p)$ and $H^2(G, \mathbb{F}_p)$ respectively and let

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

for
$$i=1,\ldots,d$$
. Then, referring to (3.1), $c(\underline{i},r,j)=\alpha_{i_j}$, where $\underline{i}=(\underbrace{i,\ldots,i}_{p^r})$

and we consider the restricted product as mentioned in section 2. 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 3.2, using theorem 2.11 and the groups U(1,r).

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 construction of Massey products for $H^1(G, \mathbb{F}_p)$ and $H^2(G, \mathbb{F}_p)$.

We will do this a bit more generally, so let A be an associative 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). We will need to do some calculations and for this we will use the Hochschild cocomplex $C^*(A, \operatorname{Hom}_k(V_i, V_j), \delta)$. We note that $\operatorname{Hom}_k(V_i, V_j)$ is an A-bimodule for $i, j \in \{1, \ldots, n\}$.

Recall that the n-cochains in the Hochschild cocomplex are defined by

$$C^n(A, \operatorname{Hom}_k(V_i, V_j)) = \operatorname{Hom}_k(\underbrace{A \otimes \cdots \otimes A}_n, \operatorname{Hom}_k(V_i, V_j))$$

and that the differential δ is given by the formula

$$\delta^n \phi(a_1 \otimes \cdots \otimes a_{n+1})(v_i)$$

$$=a_1\phi(a_2\otimes\cdots\otimes a_{n+1})(v_i)+\sum_{i=1}^n(-1)^i\phi(a_1\otimes\cdots\otimes a_ia_{i+1}\otimes\cdots\otimes a_{n+1})(v_i)$$

$$+(-1)^{n+1}\phi(a_1\otimes\cdots\otimes a_n)a_{n+1}(v_i)$$

for $\phi \in C^n(A, \operatorname{Hom}_k(V_i, V_i)), a_1, \ldots, a_{n+1} \in A \text{ and } v_i \in V_i.$

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

Now take $\xi_{jk} \in \operatorname{Ext}_A^1(V_j, V_k)$ 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 $\operatorname{Ext}_A^2(V_i, V_k)$. We know that it corresponds to taking the composition of ξ_{ij} and ξ_{jk} , or equivalently, the composition of ψ_{ij} and ψ_{jk} , i.e. $\langle \xi_{ij}, \xi_{jk}; 0 \rangle (a \otimes b) = \psi_{ij}(a) \circ \psi_{jk}(b)$ so $\langle \xi_{ij}, \xi_{jk}; 0 \rangle$ has a representative in

 $C^2(A, \operatorname{Hom}_k(V_i, V_k))$ (we apologise for the two different k-s, but we feel the use should be clear). 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 and Leibniz' rule.

By starting with an extension

$$0 \longrightarrow V_j \longrightarrow E_{ij} \longrightarrow V_i \longrightarrow 0$$

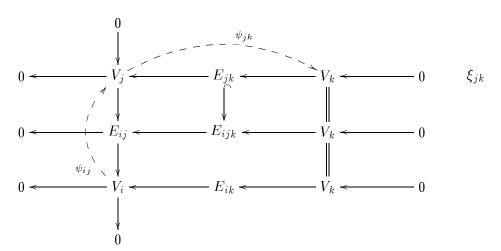
and looking at the A-module structure on E_{ij} , we get a derivation ψ_{ij} . The module structure on E_{ij} will be given by

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

We have seen that by adding an extension E_{jk} and splicing these short-exact sequences we get an element in $\operatorname{Ext}_A^2(V_i, V_k)$ and the formula for the cup product.

Now consider the following diagram.

$$\xi_{ij}$$



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

$$(v_k, v_i, 0)a = (v_k a + \psi_{ik}(a)(v_i), v_i a, 0).$$

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

$$(4.1) (0,0,v_i)(a_1a_2) = ((0,0,v_i)a_1)a_2$$

for $a_1, a_2 \in A$ and $v_i \in V_i$. The left hand side in (4.1) is

$$(\psi_{ijk}(a_1a_2)(v_i), \psi_{ij}(a_1a_2)(v_i), v_i(a_1a_2)),$$

whereas the right hand side is

$$(\psi_{ijk}(a_1)(v_i)a_2 + \psi_{jk}(a_2)(\psi_{ij}(a_1)(v_i)), \psi_{ij}(a_1)(v_i)a_2, 0) + (\psi_{ijk}(a_2)(v_ia_1), \psi_{ij}(a_2)(v_ia_1), (v_ia_1)a_2).$$

We see that the 3rd coordinates are equal since V_i is an A-module, and the 2nd 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. If we consider the 1st coordinates, we get that

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

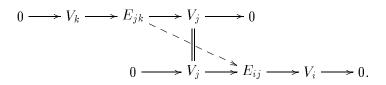
We conclude that an A-module structure on E_{ijk} is given by

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

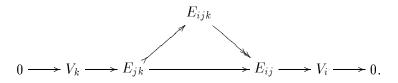
where
$$-\delta^1 \psi_{ijk}(a_1, a_2)(v_i) = \psi_{ij} \circ \psi_{jk}(a_1, a_2)(v_i)$$
.

Next, we draw the 3-dimensional diagram given on the next page. In this diagram we have assumed 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} . Then we add a third extension ξ_{kl} (extending V_k by V_l) and draw a wall of V_l -s, obtaining the diagram.

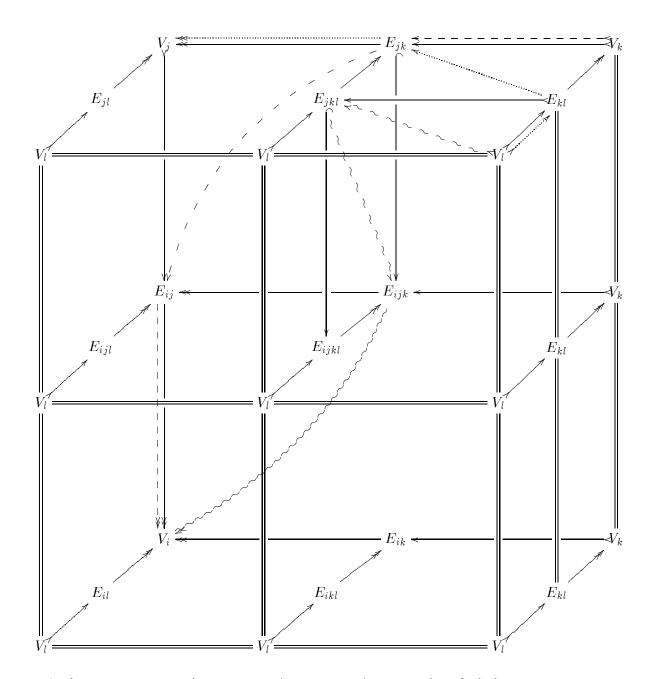
The arrows $-- \rightarrow$ in the diagram draw the splice



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



What conditions have to be satisfied for us to define an A-module structure on E_{ijkl} (the middle entry in the diagram)?



As k-vectorspaces, 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

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

and put $\bullet = \psi_{ijkl}(a)(v_i)$. Similar to E_{ijk} , we now compare $(0,0,0,v_i)(a_1a_2)$ and $((0,0,0,v_i)a_1)a_2$. The 4th coordinates are equal $(V_i$ is an A-module), the 3rd coordinates are equal $(\psi_{ij}$ is a derivation, i.e. E_{ij} is an A-module) and the 2rd 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 1st coordinates to be equal, we need

$$\psi_{ijkl}(a_1 a_2)(v_i)$$

$$= \psi_{ijkl}(a_1)(v_i)a_2 + \psi_{kl}(a_2)(\psi_{ijk}(a_1)(v_i))$$

$$+ \psi_{ikl}(a_2)(\psi_{ij}(a_1)(v_i)) + \psi_{ijkl}(a_2)(v_i a_1)$$

which implies

$$(4.2) \quad \psi_{kl}(a_2)(\psi_{ijk}(a_1)(v_i)) + \psi_{jkl}(a_2)(\psi_{ij}(a_1)(v_i)) = -\delta^1 \psi_{ijkl}(a_1, a_2)(v_i).$$

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 in the 3-dimensional diagram) and we have an element

$$\psi_{ikl} \in \operatorname{Hom}_k(A, \operatorname{Hom}(V_i, V_l))$$

such that $\delta^1 \psi_{jkl} = -\langle \xi_{jk}, \xi_{kl}; 0 \rangle$. 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

$$(v_{l}, v_{k}, v_{j}, v_{i}) a$$

$$=(v_{l}a + \psi_{kl}(a)(v_{k}) + \psi_{jkl}(a)(v_{j}) + \psi_{ijkl}(a)(v_{i}),$$

$$v_{k}a + \psi_{jk}(a)(v_{j}) + \psi_{ijk}(a)(v_{i}),$$

$$v_{j}a + \psi_{ij}(a)(v_{i}),$$

$$v_{i}a)$$

where ψ_{ijkl} satisfies (4.2).

We recognise the formula in (4.2) as a defining system for the 3-fold Massey product $\langle \xi_{ij}, \xi_{jk}, \xi_{kl}; 0 \rangle$. This element in $\operatorname{Ext}_A^2(V_i, V_l)$ is represented by the arrows \longrightarrow in the 3-dimensional diagram.

Remark 4.1. 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 and notations as before we can consider what we need to define an A-module structure on E_{ijklm} . This gives us a defining system for the 4-fold Massey product $\langle \xi_{ij}, \xi_{jk}, \xi_{kl}, \xi_{lm}; 0 \rangle$ as in definition 2.5.

This procedure goes on to give us the formula for a general Massey product as in the formula in definition 2.5. When we are building modules like this we want a module structure on each step, and so the lower order products involved need to be zero. Hence the Massey products we get here are strictly defined.

Remark 4.2. The Yoneda construction can only be used for strictly defined products, since in this situation we 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.

5. The class \mathcal{C}

We now introduce the following class of finite *p*-groups.

Definition 5.1. Let 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.

Using theorems 3.2 and 3.3, we see that the relations in the class \mathcal{C} are exactly those determined by strictly defined Massey products. 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 5.2. The class C is determined by \mathbb{F}_pG , i.e. if $\mathbb{F}_pG \simeq \mathbb{F}_pH$ then G is in C if and only if H is in C.

Proof. 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 $\mathbb{F}_p G$.

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 4.

For the question of distinguishing the individual groups in \mathcal{C} using $\mathbb{F}_p G$, we can introduce a procedure for writing down the strictly defined Massey product structures, see [4]. We intend to come back to this procedure and how to produce and study p-groups using this theory in another paper.

Acknowledgements

I would like to thank Prof. O. A. Laudal for encouraging me and for introducing me to this theory, Prof. R. Sandling for updating me on the modular isomorphism problem, and Prof. D. Segal for his support and for giving me a different viewpoint.

This paper was polished during my stay at the Forschungsinstitut für Mathematik at ETH Zürich and I thank the FIM and Prof. B. Nucinkis for making the stay possible.

REFERENCES

- [1] Benson, D. J., Representations and cohomology I, Cambridge studies in advanced mathematics 30, CUP, 1991.
- [2] ______, Representations and cohomology II, Cambridge studies in advanced mathematics 31, CUP, 1991.
- [3] Bleher, F. M., Kimmerle, W., Roggenkamp, K. W. and Wursthorn, M., Computational aspects of the isomorphism problem, In "Algorithmic algebra and number theory" (Heidelberg 1997), 313-329, Springer 1999.
- [4] Borge, I. C., A cohomological approach to the classification of p-groups, D. Phil. thesis, Oxford University, 2001.
- [5] Deskins, W. E., On finite Abelian groups having isomorphic group algebras, Bull. Amer. Math. Soc. 61 (1955), 125.
- [6] ______, Finite abelian groups with isomorphic group algebras, Duke Math. J. 23 (1956), 35-40.
- [7] Dwyer, W., Homology, Massey products and maps between groups, J. Pure and Appl. Alg. 6 (1975), 177-190.
- [8] Kraines, D., Massey higher products, Trans. Amer. Math. Soc. 124 (1966), 431-449.
- [9] Laudal, O. A., p-groups and Massey products, Aarhus Universitet preprint series no. 30 (1975/76).
- [10] Lazard, M., Sur les groupes nilpotents et les anneaux de Lie, Ann. Ecole Norm. Supér. 71 (1954), 101-190.

- [11] Massey, W. S., Some higher order cohomology operations, Symposium internacional de topologia algebraica, pp. 145-154, Mexico City, 1958.
- [12] May, J. P., Matric Massey products, J. Alg. 12 (1969), 533-568.
- [13] Passi, I. B. S. and Sehgal, S. K., Isomorphism of modular group algebras, Math. Z. 129 (1972), 65-73.
- [14] Passman, D., The group algebra of groups of order p⁴ over a modular field, Michigan Math. Journal 12 (1965), 405-415.
- [15] Quillen, D., On the associated graded ring of a group ring, J. Alg. 10 (1968), 411-418.
- [16] Salim, M. and Sandling, R., The modular group algebra problem for groups of order p⁵, J. Austral. Math. Soc. 61 (1996), 229-237.
- [17] Sandling, R., The isomorphism problem for group rings: A survey, In "Orders and their applications" (Oberwolfach 1984), 256-288, Springer Lecture Notes in Mathematics 1142.
- [18] ______, The modular group algebra problem for metacyclic p-groups, Proc. Amer. Math. Soc. 124 (1996), 1347-1350.
- [19] Serre, J.-P., Galois Cohomology, Springer, 1997.
- [20] Wursthorn, M., Isomorphisms of modular group algebras: An algorithm and its application to groups of order 2⁶, J. Symb. Comput. 15 (1994), 211-227.

MATEMATISK INSTITUTT, UNIVERSITETET I OSLO

 $E ext{-}mail\ address: ingerbo@math.uio.no}$