FACULTY OF SCIENCE
UNIVERSITY OF COPENHAGEN, DENMARK

Master thesis

Morten Poulsen

Depth, detection and associated primes in the cohomology of finite groups

An introduction to Carlson's depth conjecture

Academic advisor: Jesper Michael Møller

Submitted: 06/08/2007

Corrected: 04/11/2007

Abstract

For a fixed prime p, let $H^*(G)$ denote the mod p cohomology ring of a finite group G, that is, $\mathrm{Ext}^*_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$ interpreted algebraically and $H^*(K(G,1);\mathbb{F}_p)$ interpreted topologically. The cohomology ring is a graded commutative Noetherian ring, or equivalently, a finitely generated graded commutative $\mathbb{F}_p$-algebra. Although the ring is not strictly commutative, the usual concepts from commutative ring theory apply, e.g., Krull dimension and depth. The prime ideal spectrum is well understood due to the work by Quillen. The depth and associated primes appear to be more mysterious. It is well known that the depth of $H^*(G)$ is bounded above by the minimum of the Krull dimensions of $H^*(G)/\mathfrak{p}$ of all associated primes $\mathfrak{p}$ of $H^*(G)$. For general finitely generated (graded) commutative $\mathbb{F}_p$-algebras the bound is not tight. In 1995 J. F. Carlson asked if the cohomology rings of finite groups are special in the sense that the bound is always tight. The question is related to a question about detection on certain collections of subgroups. This thesis is an introduction to these fairly unknown questions for which affirmative answers are known as Carlson's depth conjecture.

Abstrakt

For et fast primtal p lad $H^*(G)$ betegne mod p kohomologiringen af en endelig gruppe G, dvs. $\mathrm{Ext}^*_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$ fortolket algebraisk og $H^*(K(G,1);\mathbb{F}_p)$ fortolket topologisk. Kohomologiringen er en gradueret kommutativ Noethersk ring, eller ækvivalent, en endeligt frembragt gradueret kommutativ $\mathbb{F}_p$-algebra. Selvom ringen ikke er strengt kommutativ, er det muligt at anvende de sædvanlige begreber fra kommutativ ringteori, f.eks. Krull dimension og dybde. Primidealerne er velbeskrevet af Quillen. Dybden og de associerede primidealer forekommer mere mystiske. Det er velkendt, at minimummet af Krull dimensionerne af $H^*(G)/\mathfrak{p}$ af alle associerede primidealer $\mathfrak{p}$ i $H^*(G)$ er en øvre grænse for dybden af $H^*(G)$. Der findes endeligt frembragte (graduerede) kommutative $\mathbb{F}_p$-algebraer, hvor dybden er strengt mindre end minimummet. I 1995 stillede J. F. Carlson spørgsmålet, om kohomologiringe af endelig grupper er specielle i den forstand, at dybden altid er lig minimummet. Spørgsmålet er relateret til et spørgsmål om detektion på en bestemt samling af undergrupper. Dette speciale er en introduktion til disse forholdsvis ukendte spørgsmål, for hvilke bekræftende svar er kendt som Carlsons dybde-formodning.

Contents

Preface

This constitutes my Master thesis for the Cand.Scient. degree in Mathematics at the University of Copenhagen, Denmark. The field is cohomology of finite groups (Mathematics Subject Classification (2000): 20J06). The purpose is to study a conjecture by J. F. Carlson about depth, detection and associated primes in the cohomology rings of finite groups. Another goal is to investigate the conjecture for some concrete groups.

My interest in this particular conjecture began one afternoon in the office of my advisor, Jesper M. Møller. Some formulas involving depth and group cohomology on the blackboard in his office caught my attention. Knowing some group cohomology and commutative algebra through graduate courses in algebraic topology and homological algebra – two of my primary fields of interest – I curiously inquired about the formulas. After a brief introduction I was immediately fascinated by the question: How is the group structure related to the structure of the cohomology ring? In particular, I found the speculations about possible characterizations of the depth interesting. At the time I was searching for a subject for my thesis. Intrigued by these fairly unknown questions about the depth, known to some as Carlson's depth conjecture, my search came to an end.

A few words on prerequisites: Beside basic knowledge of group theory such as permutation groups and group actions, we require some knowledge of commutative ring theory and homological algebra. I will not give references to elementary definitions and theorems. A few references on group theory are Robinson [41] and Rotman [42]. Good textbooks on commutative algebra are Matsumura [34], Atiyah & MacDonald [3] and Eisenbud [22]. Cartan & Eilenberg [19], Mac Lane [32] and Weibel [49] are good books on homological algebra. Familiarity with group cohomology is also necessary, either the algebraic or topological approach. Nevertheless, section 1 provides a brief review of some elementary facts from group cohomology. For a thorough introduction to group cohomology, recommended references are the classic textbooks by Brown [12] and Evens [24]. Other recommended references are Adem & Milgram [2], Benson [6, 7] and Carlson et al. [18]. Note that the books [2] and [7] are more topological in their approach while [18] and [24] are purely algebraic. The books on homological algebra also contain some group cohomology. Knowledge of spectral sequences especially the Lyndon-Hochschild-Serre spectral sequence of a group extension is required to understand the computations in appendix B. Information about spectral sequences may be found in all of the references on homological algebra and group cohomology. Cohomology of finite groups draws heavily on topological methods. Beside the possible topological definition of group cohomology, the topological presence in this thesis is mainly felt in the use of Steenrod operations. The basic facts about Steenrod operations are given when needed. See e.g. Hatcher [28], a modern classic on algebraic topology, for more information.

Concerning the content of this thesis, I have used a mix of many different sources. Some results are classic as well as the proofs, some proofs are developed by the author and a few results are original. With this in mind, I continuously account for the used source. In general, a reference to the original source is (if possible) provided with the exceptions of section 1 and appendix A.

First and foremost, I would like to thank Jesper M. Møller for being a good advisor, for the countlessly many rewarding discussions and for enthusiastically teaching a course in algebraic topology which sparked my interest for algebraic topology. I also thank Jesper Grodal for introducing me to the beautiful computation of the mod 2 cohomology ring of the dihedral group of order 8. Hans-Werner Henn helped me with the proof of theorem 3.47 for which I am grateful.

Next is an overview of the content of this thesis.

Copenhagen, August 2007

Morten Poulsen

Introduction

Fix a prime p and let $H^*(G)$ denote the mod p cohomology ring $H^*(G;\mathbb{F}_p)$ of a finite group G, that is, $H^*(K(G,1);\mathbb{F}_p)$ interpreted topologically, where $K(G,1)$ is an Eilenberg-Mac Lane space of G, and $\operatorname{Ext}^*_{\mathbb{F}_pG}(\mathbb{F}_p,\mathbb{F}_p)$ interpreted algebraically, where $\mathbb{F}_pG$ is the group algebra over $\mathbb{F}_p$. The cohomology ring is a graded commutative $\mathbb{F}_p$-algebra.

A fundamental result in group cohomology is the Evens-Venkov theorem which states that $H^*(G)$ is a graded commutative Noetherian ring, or equivalently, a finitely generated graded commutative $\mathbb{F}_p$-algebra. In 1959 Golod [25] proved the theorem for finite p-groups using the Lyndon-Hochschild-Serre spectral sequence. Also in 1959 Venkov [48] proved it for all finite groups (or more generally for compact Lie groups) using topological methods. A few years later, in 1961, Evens [23] gave a purely algebraic proof for all finite groups. In any event, this provides the Noetherian hypothesis ubiquitous in commutative algebra.

Although graded commutative rings are not entirely the same as strictly commutative rings, the usual concepts from commutative ring theory apply, e.g., prime ideals, Krull dimension and depth. As a rule of thumb, graded commutative Noetherian rings with a field in degree zero behave like local rings, and all the well known results hold.

In 1971 in his landmark paper Quillen [38] described the cohomology ring in terms of the elementary abelian p-subgroups up to nilpotent phenomena. An elementary abelian p-group of rank n is a group isomorphic to $(\mathbb{Z}/p)^n$. As a consequence he settled an earlier conjecture by Atiyah and Swan that the Krull dimension is equal to the p-rank, denoted $\operatorname{rk}_p(G)$, of G, that is, the maximal rank of an elementary abelian p-subgroup of G. A truly satisfying result in that it relates the cohomological structure directly to the group structure. Quillen also proved that the minimal prime ideals of $H^*(G)$ correspond to the conjugacy classes of maximal elementary abelian p-subgroups of G, i.e., the maximal elements in the partial ordered set of elementary abelian p-subgroups of G ordered under inclusion. The minimal rank of these maximal elements is denoted $\operatorname{mrk}_p(G)$.

The depth is more difficult to compute and so far the best group theoretical characterizations only provide bounds on the depth. Duflot [20] proved in 1981 that the p-rank of the center of a Sylow p-subgroup is a lower bound. An upper bound is given by the Krull dimension.

The depth of $H^*(G)$ is also bounded above by the minimum

$$\omega_a = \omega_a(G) = \min\{\, \dim H^*(G)/\mathfrak{p} \mid \mathfrak{p} \text{ associated prime of } H^*(G)\,\}.$$

Remember that an associated prime is a prime ideal in $H^*(G)$ which is the annihilator of an element in $H^*(G)$, and that there are only finitely many since $H^*(G)$ is Noetherian. Every associated prime $\mathfrak{p}$ correspond to some elementary abelian p-subgroup E of G, and the Krull dimension of $H^*(G)/\mathfrak{p}$ is the rank of E, a result first proved by Duflot [21] in 1981 for odd primes. Unfortunately, very little is known about which subgroups actually correspond to the associated primes. However, the minimal primes are always among the associated primes, i.e., $\operatorname{mrk}_p(G) \leq \operatorname{rk}_p(G)$ is an improved upper bound of the depth.

There are examples of finitely generated (graded) commutative $\mathbb{F}_p$-algebras such that the depth is strictly less than ω_a. In 1995 Carlson [15] raised several questions about the depth. One is if the cohomology rings are special in the sense of the question:

Question. *Suppose $H^*(G)$ has depth d. Is there an associated prime $\mathfrak{p}$ in $H^*(G)$ such that $\dim H^*(G)/\mathfrak{p} = d$?*

Other bounds are determined by the depth of the cohomology ring of a subgroup, e.g., a Sylow p-subgroup provides a lower bound. Finally, in 2006 Notbohm [36] proved an equality. Specifically, the depth is equal to the minimum

$$\min\{\operatorname{depth} H^*(C_G(E)) \mid E \text{ elementary abelian } p\text{-subgroup of } G\}.$$

We offer an improvement in the sense that the depth is equal to the depth of $H^*(C_G(E))$ for any E elementary p-subgroup contained in the center of a Sylow p-subgroup of G.

Summarizing, let P be a Sylow p-subgroup of G and E a central elementary abelian p-subgroup of P. Then

$$\begin{gathered}\operatorname{rk}_p(Z(P)) \leq \operatorname{depth} H^*(P) \leq \operatorname{depth} H^*(C_G(E)) = \\ \operatorname{depth} H^*(G) \leq \operatorname{mrk}_p(G) \leq \operatorname{rk}_p(G) = \dim H^*(G).\end{gathered}$$

A collection $\mathcal{H}$ of subgroups of G is said to detect the cohomology of G if the intersection of the kernels of the restriction maps, the maps induced by the inclusion maps, to the subgroups in $\mathcal{H}$ is trivial.

Returning to Carlson's questions about the depth, he related the depth and associated primes of the cohomology ring to detection on the collection, denoted $\mathcal{H}_s(G)$, of centralizers of elementary abelian p-subgroups of G of rank s via the following theorem.

Theorem. *If $H^*(G)$ is not detected on $\mathcal{H}_s(G)$, then $H^*(G)$ has an associated prime $\mathfrak{p}$ such that the dimension of $H^*(G)/\mathfrak{p}$ is strictly less than s. In particular, the depth of $H^*(G)$ is strictly less than s.*

In other words, the maximum

$$\omega_d = \omega_d(G) = \max\{\, s \mid H^*(G) \text{ is detected by } \mathcal{H}_s(G)\,\}$$

is an upper bound of ω_a. In particular, if $\operatorname{depth} H^*(G) \geq s$, then $H^*(G)$ is detected by the centralizers of the elementary abelian subgroups of rank s. Carlson raised the question about the converse:

Question. *Suppose $H^*(G)$ is detected by $\mathcal{H}_s(G)$. Is* $\operatorname{depth} H^*(G) \geq s$*?*

The affirmative answers to the above questions are known to some as Carlson's depth conjecture which is the subject of this thesis. For emphasis we state the conjecture:

Carlson's depth conjecture. *Let G be a finite group. Suppose the depth of $H^*(G)$ is d. Then*

(1) $H^*(G)$ has an associated prime $\mathfrak{p}$ such that $\dim H^*(G)/\mathfrak{p} = d$, and

(2) if $H^*(G)$ is detected by $\mathcal{H}_s(G)$, then $d \geq s$.

In other words, $d = \omega_a = \omega_d$.

Carlson raised another intriguing question for which an affirmative answer in fact implies the conjecture:

Question. *Let H be a subgroup of G. Is* $\operatorname{depth} \operatorname{res}_{G,H} H^*(G) \geq \operatorname{depth} H^*(H)$*?*

Carlson & Henn [16] computed the depths of the cohomology rings of the symmetric groups and verified the conjecture for these groups. An obvious question is: What about the alternating groups? For odd primes, the situation is completely determined by the symmetric groups. The case $p = 2$ seems more difficult. Using properties of the Sylow 2-subgroups and of the ranks of the elementary 2-subgroups of the alternating groups we establish the conjecture for the alternating groups A_n for $n \equiv 2, 3 \pmod 4$. As an application of our improved version of the theorem by Notbohm we use the structure of centralizers of the symmetric groups to establish the conjecture for the wreath products $\mathbb{Z}/p \wr S_n$ for all n at the prime p. In addition, we offer a delightful result on p-fusion in the alternating groups.

For other aspects of commutative algebra in the cohomology of groups, the interested reader is referred to the survey [8] by Benson.

The outline of this thesis is as follows: Section 1 contains a cursory survey, without any proofs, of some elements of the theory of cohomology rings of finite groups.

In section 2 we go through some of Quillen's classic results on the prime ideal spectrum of a cohomology ring. The main purpose is to establish the results necessary in the investigation of the associated primes. The results are naturally also interesting in themselves.

The next two sections constitutes the primary parts of the thesis: Section 3 is devoted to the depth of cohomology rings, in particular the conjecture and an alternative proof of the above theorem by Carlson using results from the theory of unstable modules over the Steenrod algebra. Section 4 is dedicated to the symmetric and alternating groups.

Appendix A provides the necessary background theory from commutative ring theory in the realm of graded commutative rings. Since every book on commutative ring theory only studies strictly commutative rings, another purpose of the appendix is also to address the issue that our rings of interest are not strictly commutative. The reader unfamiliar with commutative algebra and/or concerned with the issue that our rings are graded commutative may jump to appendix A after reading section 1 and afterwards continue with section 2. Since we in general refer to the appendix when needed, the reader acquainted with the concepts mentioned above in case of a commutative local ring may be better off accepting that the usual concepts hold and simply lookup up the references if needed and thus keeping focus on the rings of interest, the cohomology rings of finite groups. For readability, some essential definitions are also included in the main text.

A few words on the notation: The tensor product $\otimes$ always denotes the graded tensor product $\otimes_{\mathbb{F}_p}$. For the convenience of the reader a list of some of the notation used in this thesis is available on page 107. Note that $\subset$ denotes subset with the possibility of equality and proper inclusion is denoted by $\subsetneq$.

1 Cohomology rings of finite groups

Let G be a finite group and k a field. In later sections we restrict our attention to the case where k is the Galois field $\mathbb{F}_p$ with p elements. Let kG denote the group algebra over k, that is, the free k-module with basis the elements of G and a k-bilinear product $kG \times kG \to kG$ given by extending the product in G. The augmentation map $kG \to k$, $\sum \lambda_g g \mapsto \sum \lambda_g$ allows us to view k as a module over kG.

The nth cohomology group of G with coefficients in k is defined to be the abelian group

$$H^n(G;k) = \operatorname{Ext}^n_{kG}(k,k) \cong \operatorname{Ext}^n_{\mathbb{Z}G}(\mathbb{Z},k).$$

The cohomology of G is the graded group

$$H^*(G;k) = \operatorname{Ext}^*_{kG}(k,k) = \bigoplus_{n\geq 0} \operatorname{Ext}^n_{kG}(k,k).$$

More generally, for a (left) kG-module M the cohomology of G with coefficients in M is

$$H^*(G;M) = \operatorname{Ext}^*_{kG}(k,M) = \bigoplus_{n\geq 0} \operatorname{Ext}^n_{kG}(k,M).$$

Group cohomology $H^*(-;-)$ is a bifunctor, contravariant in the first variable and covariant in the second. The main references for this review of group cohomology are [12], [24] and [28]. The diligent reader should have no problem looking up wanted details.

Let $X = K(G,1)$ be an Eilenberg-Mac Lane space of type $(G,1)$, that is, a based connected CW complex X such that $\pi_1(X) \cong G$ and $\pi_n(X)$ is trivial for $n > 1$, or equivalently, such that $\pi_1(X) \cong G$ and the universal cover $\widetilde{X}$ is contractible. An Eilenberg-Mac Lane space is unique up to homotopy equivalence. For example, the real projective plane $\mathbb{R}\mathrm{P}^\infty$ is a $K(\mathbb{Z}/2,1)$. The singular chain complex $C_*(\widetilde{X})$ is a complex of $\mathbb{Z}G$-modules via the action of $\pi_1(X) \cong G$ on $\widetilde{X}$ by deck transformations. The cohomology $H^*(X;M)$ of X with (local) coefficients in M is the homology of the chain complex $\operatorname{Hom}_{\mathbb{Z}G}(C_*(\widetilde{X}),M)$. Since $\widetilde{X}$ is contractible, $C_*(\widetilde{X})$ is a free resolution of $\mathbb{Z}$ considered a module over $\mathbb{Z}G$ via the augmentation map $C_0(\widetilde{X}) \to \mathbb{Z} \to 0$. In other words, $H^*(X;M) = H^*(G;M)$ and we may study the cohomology of G from a topological viewpoint. In particular, the mod p cohomology $H^*(G;\mathbb{F}_p)$ of G has Steenrod operations.

For kG-modules M and N, G acts on $\operatorname{Hom}_k(N,M)$ by $(gf)(n) = gf(g^{-1}n)$ for $n \in N$. Let M^G denote the G-invariant subgroup of M, i.e., the elements $m \in M$ such that $gm = m$ for all $g \in G$.

Cohomology in low degrees has nice interpretations,

$$H^0(G;M) = \operatorname{Hom}_{kG}(k,M) = \operatorname{Hom}_k(k,M)^G \cong M^G.$$

Furthermore, if M is a trivial kG-module, that is, $gm = g$ for all g in G, then

$$H^1(G; M) = \mathrm{Hom}(G, M) = \mathrm{Hom}(G/[G, G], M).$$

For nontrivial modules $H^1(G; M)$ is described by derivations.

Another definition of group cohomology is as the right derived functors $R^*(-^G)(M)$ of the invariant subgroup functor $(-)^G$ from the category of kG-modules to the category of abelian groups. The functors $H^*(G; -)$ are universal δ-functors in the sense of Grothendieck, see e.g. [49] ch. 2 and 6.

The cohomology of G may be endowed with a graded ring structure in several ways such as Yoneda splices, composition products, and via cross products. Fortunately, they all produce the same ring structure on $H^*(G; k)$, see e.g. [18] ch. 4, known as the cup product. For example, consider the cohomology cross product

$$\times\colon H^*(G; k) \otimes_k H^*(G; k) \to H^*(G \times G; k),$$

and the diagonal map $\Delta\colon G \to G \times G$, $\Delta(g) = (g, g)$ which induces a homomorphism $\Delta^*\colon H^*(G; k) \to H^*(G \times G; k)$. The cup product is the composite

$$\cup\colon\ H^*(G; k) \otimes_k H^*(G; k) \xrightarrow{\times} H^*(G \times G) \xrightarrow{\Delta^*} H^*(G; k),$$

and $x \cup y \in H^{m+n}(G; k)$, or simply xy, for $x \in H^m(G; k)$ and $y \in H^n(G; k)$. The cup product is graded commutative,

$$xy = (-1)^{mn} yx.$$

Since $H^0(G; k) = k$, $H^*(G; k)$ is a graded commutative k-algebra. More generally, there is a cup product $\cup\colon H^*(G; k) \otimes_k H^*(G; M) \to H^*(G; M)$, i.e., $H^*(G; M)$ is a module over $H^*(G; k)$.

Our objects of interest are the cohomology rings, henceforth we restrict our attention to these.

A group homomorphism $\varphi\colon H \to G$ induces a homogeneous homomorphism of graded rings

$$\varphi^*\colon H^*(G; k) \to H^*(H; k).$$

In the particular case of φ being an inclusion the induced map is called the restriction of G to H and is denoted $\mathrm{res}_{G,H}$.

Suppose H is a subgroup of G and g is an element of G. Then conjugation $c_{g^{-1}}\colon gHg^{-1} \to H$, $h \mapsto g^{-1}hg$, induces an isomorphism

$$\cdot g\colon H^*(H; k) \to H^*(gHg^{-1}; k), gx = c^*_{g^{-1}}(x)$$

for $x \in H^*(H; k)$. It is well known that $\cdot g$ is the identity map on $H^*(G; k)$ for any g in G. In particular, if H is a normal subgroup of G, then G/H acts on $H^*(H; k)$.

The transfer map and the Evens norm map are useful maps in the other direction which are not induced by group homomorphisms. Let H be a subgroup of G.

The transfer map,

$$\operatorname{tr}_{H,G}\colon H^*(H;k) \to H^*(G;k),$$

is a homomorphism of groups but not a ring homomorphism. The following proposition gives a few elementary properties of the transfer map.

Proposition 1.1. *Consider groups $K \subset H \subset G$. If $x \in H^*(G;k)$ and $y \in H^*(H;k)$, then*

(1) $\operatorname{tr}_{K,G} = \operatorname{tr}_{H,G}\operatorname{tr}_{K,H}$,

(2) $\operatorname{tr}_{H,G}(y \operatorname{res}_{G,H}(x)) = \operatorname{tr}_{H,G}(y)x$,

(3) $\operatorname{tr}_{H,G}(\operatorname{res}_{G,H}(x)y) = x \operatorname{tr}_{H,G}(y)$, *and*

(4) $\operatorname{tr}_{H,G}\operatorname{res}_{G,H}(x) = [G:H]x$.

In particular, the transfer map is $H^*(G;k)$-linear when $H^*(H;k)$ is viewed as a module over $H^*(G;k)$ via the restriction map. Furthermore, the image of the transfer map is an ideal in $H^*(G;k)$. Another immediate consequence is that $|G|H^n(G;k) = 0$ for all $n > 0$ since $H^n(\{1\};k) = 0$ for $n > 0$.

The Evens norm map,

$$\operatorname{norm}_{H,G}\colon H^{2n}(H;k) \to H^{2n[G:H]}(G;k),$$

is multiplicative but not additive. It may be defined for elements of arbitrary degree using other coefficients, see e.g. [7] or [18]. We only need the following property, known as the Mackey formula, of the norm map.

Proposition 1.2. *Suppose $G = \bigcup_{g\in D} HgK$ is a double coset decomposition of G. Then for $x \in H^{2n}(K;k)$,*

$$\operatorname{res}_{G,H}\operatorname{norm}_{K,G}(x) = \prod_{g\in D}\operatorname{norm}_{H\cap gKg^{-1},H}\operatorname{res}_{gKg^{-1},H\cap gKg^{-1}}(gx) \in H^*(H;k).$$

Suppose k has characteristic zero or characteristic not dividing the order of G. Then multiplication by $|G|$ is an isomorphism on the k-vector space $H^n(G;k)$, i.e., $H^n(G;k) = 0$ for $n > 0$. Consequently, the interesting cases are when the characteristic of k divides the order of G.

Any field k of characteristic $p > 0$ may be viewed as an algebra over $\mathbb{F}_p$ and there is an isomorphism of k-algebras $H^*(G;k) \cong k \otimes_{\mathbb{F}_p} H^*(G;\mathbb{F}_p)$, see [24] section 3.4. In other words, only the characteristic of the field is really important.

The computation of the cohomology rings of the cyclic groups is classic, see [19] section XII.7 for a algebraic computation or [28] example 3.41 for a topological computation.

Theorem 1.3. *Let G be a cyclic group of prime power order p^n. Then*

$$H^*(G;\mathbb{F}_p) = \begin{cases} \mathbb{F}_p[x], & |G| = 2 \\ \wedge_{\mathbb{F}_p}(x) \otimes_{\mathbb{F}_p} \mathbb{F}_p[y], & |G| > 2, \end{cases}$$

where $|x| = 1$ and $|y| = 2$.

The Künneth formula (the cross product is an isomorphism) determines the cohomology ring of any finitely generated abelian group.

The elementary abelian p-groups play an important role in the cohomology of groups. Recall that an elementary abelian p-group of rank n is a finite group E isomorphic to the direct product of n cyclic groups of order p, i.e., $E \cong (\mathbb{Z}/p)^n$. In other words, an elementary abelian p-group E is a finite dimensional vector space over $\mathbb{F}_p$ with the obvious scalar multiplication, that is, $cx = x + \cdots + x$ (c times) for $0 \leq c \leq p-1$ and $x \in E$. Furthermore, any group homomorphism $E \to \mathbb{Z}/p$ is $\mathbb{F}_p$-linear, i.e., $\mathrm{Hom}(E, \mathbb{Z}/P) = \mathrm{Hom}_{\mathbb{F}_p}(E, \mathbb{F}_p)$. The p-rank of a finite group G, denoted $\mathrm{rk}_p(G)$, is the maximal rank of an elementary abelian p-subgroup of G.

The Bockstein operation $\beta\colon H^n(\mathbb{Z}/p;\mathbb{F}_p) \to H^{n+1}(\mathbb{Z}/p;\mathbb{F}_p)$ of the sequence $0 \to \mathbb{Z}/p \to \mathbb{Z}/p^2 \to \mathbb{Z}/p \to 0$ is an isomorphism in odd degrees and zero in even degrees, see e.g. [24] section 3.5 or [28] section 3.E. This gives the following description of the cohomology rings of elementary abelian p-groups.

Corollary 1.4. *Let E be an elementary abelian p-group of rank n. Then*

$$H^*(E;\mathbb{F}_p) = \begin{cases} \mathbb{F}_p[x_1, \ldots, x_n], & p = 2 \\ \wedge_{\mathbb{F}_p}(x_1, \ldots, x_n) \otimes_{\mathbb{F}_p} \mathbb{F}_p[\beta(x_1), \ldots, \beta(x_n)], & p > 2, \end{cases}$$

where $|x_i| = 1$.

For nonabelian groups the computations are in general more difficult. In the calculation of cohomology one often ends up with applying spectral sequences. Appendix B contains computations of the mod 2 cohomology of the dihedral group of order 8 and the quaternion group using the Lyndon-Hochschild-Serre spectral sequence. These groups will be used as examples throughout the text. The computations illustrate nicely how complicated it usually is to compute the cohomology ring by hand even for very small groups. Rusin [43] computed by hand the mod 2 cohomology of the groups of order 32 using the Eilenberg-Moore spectral sequence. Carlson [14] has computed the mod 2 cohomology of all groups of order dividing 64 by computer calculations, see also [18] for more information on these computer computations. Green [26] has computed the mod p cohomology of some small p-groups also using computer calculations. These computer computations are great sources of examples and as tools in testing ideas. Note that they also provide a lot of other information beside the actual ring structure, e.g., restriction maps to certain subgroups et cetera.

Example 1.5. The mod 2 cohomology of D_8, the dihedral group of order 8, is

$$H^*(D_8; \mathbb{F}_2) = \mathbb{F}_2[x, y, v]/(x(x+y))$$

with x and y in degree 1 and v in degree 2, see appendix B.

Example 1.6. The mod 2 cohomology ring of Q_8 is

$$H^*(Q_8; \mathbb{F}_2) = \mathbb{F}_2[x, y, v]/(x^2 + xy + y^2, x^2y + xy^2)$$

with x and y in degree 1 and v in degree 4, see appendix B.

We finish this overview with the Evens-Venkov theorem, see e.g. [24] section 7.4 for more information, which provides the Noetherian property essential to applying the concepts from commutative ring theory.

Theorem 1.7. *Let M be a kG-module. If M is Noetherian as a k-module, then $H^*(G; M)$ is Noetherian as a module over $H^*(G; k)$. In particular, $H^*(G; k)$ is a graded commutative Noetherian ring.*

In other words, $H^*(G; k)$ is a finitely generated graded commutative k-algebra by proposition A.5. The following consequence is used extensively throughout the text and follows by an application of the Eckmann-Shapiro lemma. It says that the restriction map is always close to being surjective.

Corollary 1.8. *Suppose H is a subgroup of G. Then $H^*(H; k)$ is finitely generated as a module over $H^*(G; k)$ via the restriction map.*

2 The prime ideal spectrum of a cohomology ring

In this section we study the prime ideal spectrum of the mod p cohomology ring of a finite group. A part from introducing Quillen's description of the prime ideal spectrum in group theoretic terms we give a characterization of the ideals that are closed under Steenrod operations.

Let G denote a finite group and p be a prime divisor of G. Since we shall apply Steenrod operations, and in later sections use results from the theory of unstable modules over the Steenrod algebra, we restrict our attention to mod p cohomology and abbreviate $H^*(G;\mathbb{F}_p)$ to $H^*(G)$.

2.1 Quillen's theorem

Let $\mathcal{A}(G)$ be the category with objects the elementary abelian p-subgroups of G and morphisms inclusions and the homomorphisms of elementary abelian p-subgroups induced by conjugation by an element in G. This category is called the Quillen category. Associating $H^*(E)$ to an elementary abelian p-subgroup E of G gives a contravariant functor from the Quillen category to the category of rings.

Consider the product of the restriction maps

$$\mathrm{res}\colon H^*(G) \to \prod_{E\in\mathcal{A}(G)} H^*(E), x \mapsto (\mathrm{res}_{G,E}(x))_{E\in\mathcal{A}(G)}.$$

An element in the image clearly has to satisfy relations given by conjugation and inclusion.

Recall that the limit $\lim_{E\in\mathcal{A}(G)} H^*(E)$ is the subring of the direct product of the rings $H^*(E)$, $E \in \mathcal{A}(G)$, consisting of the sequences $(x_E)_{E\in\mathcal{A}(G)}$ such that

$$\mathrm{res}_{E,E'}(x_E) = x_{E'} \text{ if } E' \subset E$$

and

$$gx_E = x_{E'} \text{ if } E' = gEg^{-1} \text{ for some } g \in G.$$

The map res induces a map

$$H^*(G) \to \lim_{E\in\mathcal{A}(G)} H^*(E).$$

The following theorem is due to Quillen [38] and is also known as Quillen's theorem.

Theorem 2.1. *The map*

$$H^*(G) \to \lim_{E\in\mathcal{A}(G)} H^*(E)$$

induced by the product of the restriction maps is an F-isomorphism, that is, the kernel consists of nilpotent elements and every element $x \in \lim_{E\in\mathcal{A}(G)} H^*(E)$ satisfies that x^{p^n} is in the image for some n.

An F-isomorphism induces a bijection on prime ideal spectra, see proposition A.16.

Example 2.2. Consider the cyclic group $\mathbb{Z}/p^n$. The restriction map to the cyclic subgroup of order p is zero in odd degrees and an isomorphism in even degrees, see e.g. [2] corollary II.5.7. In particular, the homomorphism from Quillen's theorem is in general neither injective nor surjective.

Example 2.3. The quaternion group Q_8 has only one elementary abelian 2-subgroup, namely the center which is cyclic of order 2. The homomorphism from Quillen's theorem

$$H^*(Q_8;\mathbb{F}_2) = \mathbb{F}_2[x,y,v]/(x^2+xy+y^2, x^2y+xy^2) \to \mathbb{F}_2[w] = H^*(Z(Q_8);\mathbb{F}_2),$$

where $|x| = |y| = |w| = 1$ and $|v| = 4$, maps x and y to zero and v to w^4, see appendix B.

Quillen's original proof uses equivariant cohomology. However, Quillen & Venkov [40] proved the following part of Quillen's theorem using only the cohomology of finite groups.

Theorem 2.4. *Let $x \in H^*(G)$. If x restricts to zero on all elementary abelian p-subgroups of G, then x is nilpotent.*

With the previous theorem as a starting point we shall derive a series of consequences about the prime ideals of the cohomology ring. The primary references are [24] ch. 8 & 9, [37], [38] and [7] ch. 5. Our view on the prime ideal spectrum is basic, we simply view it as the set of prime ideals contrary to most other expositions which employ tools from classic algebraic geometry. Readers interested in more information such as the proofs of the above theorems are referred to the above sources. The notation is standard. For example, the radical of an ideal I of a ring R is denoted $\sqrt{I}$, e.g., the nilradical $\operatorname{Nil}(R) = \sqrt{0}$, and $V(I)$ is the set of prime ideals $\mathfrak{p} \supset I$. See appendix A for more information. We begin with a basic description of the prime ideal spectrum.

The cohomology of an elementary abelian p-group E modulo its nilradical is a polynomial ring, particularly an integral domain. Thus, the nilradical is a prime ideal of $H^*(E)$. Furthermore, the pullback of the nilradical,

$$\mathfrak{p}_E = \operatorname{res}_{G,E}^{-1}(\operatorname{Nil}(H^*(E))) = \sqrt{\operatorname{Ker}\operatorname{res}_{G,E}},$$

is a homogeneous prime ideal in $H^*(G)$. The latter equality follows since if $\operatorname{res}_{G,E}(x) \in \operatorname{Nil}(H^*(E))$, then $\operatorname{res}_{G,E}(x)^n = 0$ for some n, i.e., $x^n \in \operatorname{Ker}\operatorname{res}_{G,E}$. Conversely, if $x^n \in \operatorname{Ker}\operatorname{res}_{G,E}$, then $\operatorname{res}_{G,E}(x)^n = \operatorname{res}_{G,E}(x^n) = 0$. Homogeneity follows by proposition A.6 since $\operatorname{Ker}\operatorname{res}_{G,E}$ is clearly homogeneous.

In other words, $\mathfrak{p}_E$ is the kernel of the homomorphism

$$\begin{tikzcd} H^*(G) \arrow[r, "\operatorname{res}_{G,E}"] & H^*(E) \arrow[r] & H^*(E)/\operatorname{Nil}(H^*(E)). \end{tikzcd}$$

Remember that $H^*(E)$ is finitely generated as a module over $H^*(G)$ via the restriction map, i.e., as a module over $\operatorname{Im}\operatorname{res}_{G,E}$ which is isomorphic to $H^*(G)/\operatorname{Ker}\operatorname{res}_{G,E}$. By the going-up theorem, see theorem A.14, the map

$$i^{-1}\colon \operatorname{Spec} H^*(E) \to \operatorname{Spec}\operatorname{Im}\operatorname{res}_{G,E}$$

of prime ideal spectra induced by the inclusion map $i\colon \operatorname{Im}\operatorname{res}_{G,E} \to H^*(E)$ is surjective. It follows that

$$\operatorname{res}_{G,E}^{-1}(\operatorname{Spec} H^*(E)) = V(\operatorname{Ker}\operatorname{res}_{G,E}) = V(\sqrt{\operatorname{Ker}\operatorname{res}_{G,E}}).$$

Corollary 2.5. $\operatorname{Spec} H^*(G) = \bigcup_{E\in\mathcal{A}(G)} V(\sqrt{\operatorname{Ker}\operatorname{res}_{G,E}})$.

Proof. Theorem 2.4 gives that the product of the restriction maps,

$$\operatorname{res}\colon H^*(G) \to \prod_{E\in\mathcal{A}(G)} H^*(E),$$

has nilpotent kernel. In particular, $\operatorname{Spec} H^*(G) = V(\operatorname{Ker}\operatorname{res})$.

The product $\prod_{E\in\mathcal{A}(G)} H^*(E)$ is finitely generated as a module over $H^*(G)$ via res and the going-up theorem implies that

$$\operatorname{res}^{-1}\colon \operatorname{Spec} \prod_{E\in\mathcal{A}(G)} H^*(E) \to V(\operatorname{Ker}\operatorname{res}) = \operatorname{Spec} H^*(G)$$

is surjective. Furthermore,

$$\operatorname{Spec} \prod_{E\in\mathcal{A}(G)} H^*(E) = \bigcup_{E\in\mathcal{A}(G)} \pi_E^{-1}(\operatorname{Spec} H^*(E)),$$

where $\pi_{E'}\colon \prod_{E\in\mathcal{A}(G)} H^*(E) \to H^*(E')$ is the projection map. Here we used the fact that the prime ideals in a product ring are precisely the pullbacks under the projection maps: Suppose $R = R_1 \times \cdots \times R_n$. Let $e_i = (0,\dots,0,1,0,\dots,0)$ with 1 in the ith place. Since $e_ie_j = 0$ for $i \neq j$, any prime ideal of R contains all but one e_i.

For a prime ideal $\mathfrak{p}$ in $H^*(E)$,

$$\operatorname{res}^{-1}(\pi_E^{-1}(\mathfrak{p})) = (\pi_E \operatorname{res})^{-1}(\mathfrak{p}) = \operatorname{res}_{G,E}^{-1}(\mathfrak{p}).$$

This finishes the proof. □

We shall work with the standard definition of Krull dimension.

Definition 2.6. *The Krull dimension, or simply the dimension, of a graded commutative Noetherian ring R, $R^0 = \mathbb{F}_p$, is denoted* $\dim R$ *and is defined to be the supremum of lengths n of strictly increasing chains of prime ideals*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

in R. For an R-module M the dimension of M is defined to be the dimension of $R/\operatorname{Ann}_R M$ and is denoted $\dim_R M$.

Example 2.7. The cohomology of an elementary abelian p-group E modulo its nilradical is a polynomial ring in $\mathrm{rk}_p(E)$ variables. In particular, $\dim H^*(E) = \mathrm{rk}_p(E)$.

Lemma 2.8. *Suppose E is an elementary abelian p-subgroup of G. Then the dimension of $H^*(G)/\sqrt{\operatorname{Ker}\operatorname{res}_{G,E}}$ is $\mathrm{rk}_p(E)$.*

Proof. Recall that $H^*(E)$ is finitely generated as a module over $H^*(G)$ via the restriction map. Corollary A.15 gives that $\operatorname{Im}\operatorname{res}_{G,E} \cong H^*(G)/\operatorname{Ker}\operatorname{res}_{G,E}$ and $H^*(E)$ has the same dimension, which is $\mathrm{rk}_p(E)$. Noting that $V(\operatorname{Ker}\operatorname{res}_{G,E}) = V(\sqrt{\operatorname{Ker}\operatorname{res}_{G,E}})$ finishes the proof. □

An important consequence of Quillen's theorem is that it determines the dimension of a cohomology ring:

Corollary 2.9. *The dimension of $H^*(G)$ is the p-rank of G.*

Proof. Corollary 2.5 and lemma 2.8 gives that

$$\begin{aligned}\dim H^*(G) &= \max\{\, \dim H^*(G)/\sqrt{\operatorname{Ker}\operatorname{res}_{G,E}} \mid E \in \mathcal{A}(G)\,\} \\ &= \max\{\, \mathrm{rk}_p(E) \mid E \in \mathcal{A}(G)\,\} \\ &= \mathrm{rk}_p(G).\end{aligned}$$

□

Our next objective is a group theoretic characterization of the minimal prime ideals. First some results due to Quillen [37].

Lemma 2.10. *Let E and E' be elementary abelian p-subgroups of G. Then there exists $\tau_E \in H^*(G)$ such that $\tau_E \notin \mathfrak{p}_E$ and $\tau_E \in \mathfrak{p}_{E'}$ if E is not conjugate to a subgroup of E'.*

Proof. Consider the element

$$\rho_E = \prod_{0 \neq x \in H^1(E)} \beta(x) \in H^*(E),$$

where β is the Bockstein homomorphism. Note that ρ_E is not nilpotent.

For $0 \neq x \in H^1(E) = \operatorname{Hom}(E, \mathbb{Z}/p)$, the restriction of x to the kernel of x is zero. On the other hand, any maximal proper subgroup of E correspond to a homomorphism $x\colon E \to \mathbb{Z}/p$. Consequently, the restriction of ρ_E to any proper subgroup E' of E is zero since

$$\operatorname{res}_{E,E'}(\beta(x)) = \beta \operatorname{res}_{E,E'}(x) = \beta \operatorname{res}_{E,E'} \operatorname{res}_{E,\operatorname{Ker} x}(x) = 0$$

for some $x\colon E \to \mathbb{Z}/p$ with $E' \subset \operatorname{Ker} x$.

Also consider the element

$$\sigma_E = \operatorname{norm}_{E,G}(1 + \rho_E) \in H^*(G).$$

Write $[N_G(E) : E] = p^k q$ with $(p, q) = 1$. Let $G = \bigcup_{g\in D} EgE$ be a double coset decomposition of G.

Let $g \in G$. Observe that if $g \notin N_G(E)$, then $E \cap gEg^{-1}$ is a proper subgroup of gEg^{-1}. Since multiplication by g is an isomorphism $H^*(E) \to H^*(gEg^{-1})$,

$$g\rho_E = \rho_{gEg^{-1}}.$$

It follows that

$$\mathrm{res}_{gEg^{-1},E\cap gEg^{-1}}(g\rho_E) = \begin{cases} \rho_E & \text{if } g \in N_G(E) \\ 0 & \text{if } g \notin N_G(E). \end{cases}$$

Note that $D \cap N_G(E)$ contains exactly $[N_G(E) : E]$ double coset representatives. The Mackey formula, see proposition 1.2, gives that

$$\begin{aligned}
\mathrm{res}_{G,E}(\sigma_E) &= \mathrm{res}_{G,E}\,\mathrm{norm}_{E,G}(1+\rho_E) \\
&= \prod_{g\in D} \mathrm{norm}_{E\cap gEg^{-1},E}\,\mathrm{res}_{gEg^{-1},E\cap gEg^{-1}}(1+g\rho_E) \\
&= \prod_{g\in D\cap N_G(E)} \mathrm{norm}_{E\cap gEg^{-1},E}\,\mathrm{res}_{gEg^{-1},E\cap gEg^{-1}}(1+g\rho_E) \\
&= \prod_{g\in D\cap N_G(E)} \mathrm{norm}_{E,E}(1+\rho_E) \\
&= (1+\rho_E)^{[N_G(E):E]}.
\end{aligned}$$

By an application of the binomial formula,

$$\mathrm{res}_{G,E}(\sigma_E) = (1+\rho_E^{p^k})^q = 1 + q\rho_E^{p^k} + \text{ terms of higher degree.}$$

Define τ_E in $H^*(G)$ to be $1/q$ times the homogeneous part of σ_E of degree the degree of $\rho_E^{p^k}$. By the above calculation, $\mathrm{res}_{G,E}(\tau_E) = \rho_E^{p^k}$ which is not nilpotent, that is, $\tau_E \notin \mathfrak{p}_E$.

Suppose E' be an elementary abelian p-subgroup of G such that E is not conjugate to a subgroup of E'. Then $E' \cap gEg^{-1}$ is a proper subgroup of gEg^{-1} and

$$\mathrm{res}_{gEg^{-1},E'\cap gEg^{-1}}(g\rho_E) = \mathrm{res}_{gEg^{-1},E'\cap gEg^{-1}}(\rho_{gEg^{-1}}) = 0.$$

Let $G = \bigcup_{g\in D'} E'gE$ be double coset decomposition of G. Again, the Mackey formula gives that

$$\begin{aligned}
\mathrm{res}_{G,E'}(\sigma_E) &= \mathrm{res}_{G,E'}\,\mathrm{norm}_{E,G}(1+\rho_E) \\
&= \prod_{g\in D'} \mathrm{norm}_{E'\cap gEg^{-1},E'}\,\mathrm{res}_{gEg^{-1},E'\cap gEg^{-1}}(1+g\rho_E) \\
&= 1.
\end{aligned}$$

In particular, $\mathrm{res}_{G,E'}(\tau_E) = 0$, that is, $\tau_E \in \mathfrak{p}_{E'}$ if E is not conjugate to a subgroup of E'. □

In other words, the cohomology ring $H^*(G)$ distinguishes between the elementary abelian p-subgroups of G. In the sense that given two elementary abelian p-subgroups of G which are not conjugated there exists an element in $H^*(G)$ which is nilpotent on restriction to one subgroup but not on the other.

Theorem 2.11. *Suppose E and E' are elementary abelian p-subgroups of G. Then $\mathfrak{p}_E \supset \mathfrak{p}_{E'}$ if and only if E is conjugate to a subgroup of E'. In particular, $\mathfrak{p}_E = \mathfrak{p}_{E'}$ if and only if E and E' are conjugate in G.*

Proof. Suppose E is not conjugate to a subgroup of E'. By lemma 2.10 there exists $\tau_E \in \mathfrak{p}_{E'}$ such that $\tau_E \notin \mathfrak{p}_E$.

Conversely, suppose that E is conjugate to a subgroup of E', i.e., $gEg^{-1} \subset E'$ for some $g \in G$. To prove that $\mathfrak{p}_E \supset \mathfrak{p}_{E'}$ it suffices to prove that $\operatorname{res}_{G,E}(x)$ is nilpotent for all x in $\mathfrak{p}_{E'}$. To see this consider the commutative diagram

$$\begin{tikzcd}
E \arrow[rr] \arrow[d, "c_g"] & & G \arrow[d, "c_g"] \\
gEg^{-1} \arrow[r] & E' \arrow[r] & G
\end{tikzcd}$$

where the unlabeled arrows denote inclusion. Since conjugation induces the identity on G, see e.g. [24] proposition 4.1.1, commutativity of the diagram gives that

$$\operatorname{res}_{G,E} = c_g^* \operatorname{res}_{E',gEg^{-1}} \operatorname{res}_{G,E'} .$$

Suppose $x \in \mathfrak{p}_{E'}$, i.e., $\operatorname{res}_{G,E'}(x)$ is nilpotent, say of degree n. Then

$$\operatorname{res}_{G,E}(x)^n = c_g^* \operatorname{res}_{E',gEg^{-1}}(\operatorname{res}_{G,E'}(x))^n = 0,$$

that is, $\operatorname{res}_{G,E}(x)$ is nilpotent. □

Remark 2.12. A consequence of theorem 2.11 is that in

$$\operatorname{Spec} H^*(G) = \bigcup_{E \in \mathcal{A}(G)} V(\sqrt{\operatorname{Ker} \operatorname{res}_{G,E}})$$

it suffices to take the union over a set of representatives of the conjugacy classes in G of the elementary abelian p-subgroups of G.

Corollary 2.13. *Suppose E and E' are elementary abelian p-subgroups of G. Then*

$$\tau_E \notin \mathfrak{p}_{E'} \Leftrightarrow E \textit{ conjugate in } G \textit{ to a subgroup of } E' \Leftrightarrow \mathfrak{p}_E \supset \mathfrak{p}_{E'}.$$

Proof. By lemma 2.10, if $\tau_E \notin \mathfrak{p}_{E'}$, then E is conjugate in G to a subgroup of E'. Theorem 2.11 gives that $\mathfrak{p}_E \supset \mathfrak{p}_{E'}$ if E is conjugate in G to a subgroup of E'. Clearly, if $\mathfrak{p}_E \supset \mathfrak{p}_{E'}$, then $\tau_E \notin \mathfrak{p}_{E'}$. □

Now, we are able to prove Quillen's characterization of the minimal prime ideals. By a maximal elementary abelian p-subgroup we always mean a maximal element in the partial ordered set $\mathcal{A}(G)$ ordered under inclusion.

Theorem 2.14. *There is a one-to-one correspondence between the conjugacy classes of maximal elementary abelian p-subgroups of G and the minimal primes in $H^*(G)$. For a maximal elementary abelian p-subgroup E of G the corresponding minimal prime is $\mathfrak{p}_E = \sqrt{\operatorname{Ker}\operatorname{res}_{G,E}}$. In addition, the dimension of $H^*(G)/\mathfrak{p}_E$ is $\operatorname{rk}_p(E)$.*

Proof. Let E_i, $1 \leq i \leq n$, be representatives for the conjugacy classes in G of maximal elementary abelian p-subgroups.

The nilradical is the intersection of all prime ideals, see proposition A.6. By corollary 2.5 and theorem 2.11,

$$\operatorname{Nil}(H^*(G)) = \bigcap_{E \in \mathcal{A}(G)} \mathfrak{p}_E = \mathfrak{p}_{E_1} \cap \cdots \cap \mathfrak{p}_{E_n},$$

and the prime ideals $\mathfrak{p}_{E_1}, \ldots, \mathfrak{p}_{E_n}$ are distinct.

Let $\mathfrak{p}$ be a prime ideal of $H^*(G)$. Note that $\operatorname{Nil}(H^*(G)) \subset \mathfrak{p}$. We claim that $\mathfrak{p}$ contains $\mathfrak{p}_{E_i}$ for some i: Suppose $\mathfrak{p}_{E_i} - \mathfrak{p}$ contains an element x_i for all i. Then

$$x_1 \cdots x_n \in \mathfrak{p}_{E_1} \cap \cdots \cap \mathfrak{p}_{E_n} \subset \mathfrak{p},$$

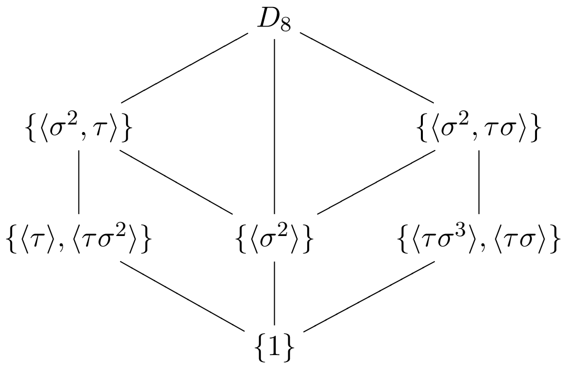
i.e., $x_i \in \mathfrak{p}$ for some i which is a contradiction.

The statement about the dimension follows from lemma 2.8. □

Example 2.15. Recall that the mod 2 cohomology ring of the dihedral group $D_8 = \langle\, \sigma, \tau \,|\, \sigma^4 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \,\rangle$ of order 8 is

$$H^*(D_8; \mathbb{F}_2) = \mathbb{F}_2[x, y, v]/(x(x + y))$$

with $|x| = |y| = 1$ and $|v| = 2$. The conjugacy classes of elementary abelian 2-subgroups are


D_8
$\{\langle \sigma^2, \tau \rangle\}$
$\{\langle \sigma^2, \tau\sigma \rangle\}$
$\{\langle \tau \rangle, \langle \tau\sigma^2 \rangle\}$
$\{\langle \sigma^2 \rangle\}$
$\{\langle \tau\sigma^3 \rangle, \langle \tau\sigma \rangle\}$
$\{1\}$

This also illustrates the Quillen category $\mathcal{A}(D_8)$. The corresponding prime ideals are

$$\begin{tikzcd}
 & 0 \arrow[dl, dash] \arrow[dd, dash] \arrow[dr, dash] & \\
\mathfrak{p}_{\langle\sigma^2,\tau\rangle} = (x) \arrow[d, dash] \arrow[dr, dash] & & \mathfrak{p}_{\langle\sigma^2,\tau\sigma\rangle} = (x+y) \arrow[dl, dash] \arrow[d, dash] \\
\mathfrak{p}_{\langle\tau\rangle} = (x,v) \arrow[dr, dash] & \mathfrak{p}_{\langle\sigma^2\rangle} = (x,y) \arrow[d, dash] & \mathfrak{p}_{\langle\tau\sigma\rangle} = (x+y,v) \arrow[dl, dash] \\
 & H^*(D_8;\mathbb{F}_2) &
\end{tikzcd}$$

See appendix B for the computational details.

For an elementary abelian p-group E of G set

$$V^+_{G,E} = V(\sqrt{\operatorname{Ker}\operatorname{res}_{G,E}}) - \bigcup_{E'<E} V(\sqrt{\operatorname{Ker}\operatorname{res}_{G,E'}})$$

and

$$V^+_E = \operatorname{Spec} H^*(E) - \bigcup_{E'<E} V(\sqrt{\operatorname{Ker}\operatorname{res}_{E,E'}}),$$

where $E' < E$ denotes that E' is a proper subgroup of E.

Notice that $V^+_{G,E}$ only depends on the conjugacy class in G of E. The following is an improvement of corollary 2.5. The proof given here is adapted from the proof of [24] theorem 9.1.3.

Theorem 2.16. *The prime ideal spectrum* $\operatorname{Spec} H^*(G)$ *is the disjoint union* $\coprod_{1\le i\le n} V^+_{G,E_i}$ *where* $\{E_1,\dots,E_n\}$ *is a set of representatives of the conjugacy classes of elementary abelian p-subgroups of G.*

We begin with a few of technical lemmas.

Lemma 2.17. *Suppose* $0 \neq x \in H^1(E) = \operatorname{Hom}(E,\mathbb{Z}/p)$*. Then*

(1) if $p = 2$*, then* $\operatorname{Ker}\operatorname{res}_{E,\operatorname{Ker} x} = (x)$*, and*

(2) if p odd, then $\operatorname{Ker}\operatorname{res}_{E,\operatorname{Ker} x} \cap H^*(E)^{ev} = \beta(x)H^*(E)^{ev}$*, where* $H^*(E)^{ev}$ *denotes* $\bigoplus_{n\ge 0} H^{2n}(E)$*.*

Proof. Note that every subgroup of E is a direct factor of E. In particular, $E = \operatorname{Ker} x \times \mathbb{Z}/p$. Let $e_1,\dots,e_{n-1}$ be generators of $\operatorname{Ker} x$ and e a generator of $\mathbb{Z}/p$ such that $x(e) = 1$. In other words, we have chosen generators of E such that x is the projection onto the last factor.

Let $x_1,\dots,x_{n-1},x$ be the dual basis of $e_1,\dots,e_{n-1},e$, i.e., an $\mathbb{F}_p$-basis of $\operatorname{Hom}(E,\mathbb{Z}/p) = H^1(E)$. Similarly, let $x'_1,\dots,x'_{n-1}$ be the dual basis of

$e_1, \ldots, e_{n-1}$, i.e., an $\mathbb{F}_p$-basis of $\operatorname{Hom}(\operatorname{Ker} x, \mathbb{Z}/p) = H^1(\operatorname{Ker} x)$. Observe that $\operatorname{res}_{E,\operatorname{Ker} x}(x_i) = x_i'$ for $1 \leq i \leq n-1$, and $\operatorname{res}_{E,\operatorname{Ker} x}(x) = 0$. In particular, $\operatorname{res}_{E,\operatorname{Ker} x}(\beta(x_i)) = \beta(x_i')$ and $\operatorname{res}_{E,\operatorname{Ker} x}(\beta(x)) = 0$.

As a consequence, for $p = 2$, $\operatorname{res}_{E,\operatorname{Ker} x}$ maps the unique factorization domain $\mathbb{F}_2[x_1, \ldots, x_{n-1}] \subset H^*(E)$ isomorphically onto $\mathbb{F}_2[x_1', \ldots, x_{n-1}'] = H^*(\operatorname{Ker} x)$. In case of p odd, $\operatorname{res}_{E,\operatorname{Ker} x}$ maps the UFD $\mathbb{F}_p[\beta(x_1), \ldots, \beta(x_{n-1})] \subset H^*(E)$ isomorphically onto $\mathbb{F}_p[\beta(x_1'), \ldots, \beta(x_{n-1}')] \subset H^*(\operatorname{Ker} x)$.

(1) Let $y \in \operatorname{Ker} \operatorname{res}_{E,\operatorname{Ker} x}$, $|y| > 0$. Suppose $y \notin (x)$. Note that $H^{|y|}(E)$ is the $\mathbb{F}_2$-vector space generated by the homogeneous polynomials of degree $|y|$. Since $y \notin (x)$, $y = f + gx$, where $f \neq 0$ is a polynomial in $x_1, \ldots, x_{n-1}$ and g is a polynomial in $x_1, \ldots, x_{n-1}, x$. Since $\operatorname{res}_{E,\operatorname{Ker} x}$ is an isomorphism on the subring $\mathbb{F}_2[x_1, \ldots, x_{n-1}]$, it follows that

$$\operatorname{res}_{E,\operatorname{Ker} x}(y) = \operatorname{res}_{E,\operatorname{Ker} x}(f) + \operatorname{res}_{E,\operatorname{Ker} x}(gx) = \operatorname{res}_{E,\operatorname{Ker} x}(f) \neq 0,$$

which is a contradiction. We conclude that $y \in (x)$.

Conversely, since $\operatorname{res}_{E,\operatorname{Ker} x}(x) = 0$, $(x) \subset \operatorname{Ker} \operatorname{res}_{E,\operatorname{Ker} x}(x)$.

(2) Similar to the case $p = 2$, simply replace x_i with $\beta(x_i)$, $1 \leq i \leq m-1$, and x by $\beta(x)$. □

Remember the element

$$\rho_E = \prod_{0 \neq x \in H^1(E)} \beta(x) \in H^*(E)$$

from the proof of lemma 2.10.

Lemma 2.18. *Suppose E is an elementary abelian p-group. Then $V(\rho_E) = \bigcup_{E' < E} V(\sqrt{\operatorname{Ker} \operatorname{res}_{E,E'}})$.*

Proof. Note that

$$V(\rho_E) = V(\prod_{0 \neq x \in H^1(E)} \beta(x)) = \bigcup_{0 \neq x \in H^1(E)} V(\beta(x)),$$

see proposition A.7. Next, we investigate $V(\beta(x))$. As usual, we may view x as a homomorphism $E \to \mathbb{Z}/p$.

$V(\beta(x)) = V(\sqrt{\operatorname{Ker} \operatorname{res}_{E,\operatorname{Ker} x}})$: Suppose $(\beta(x)) \subset \mathfrak{p} \in \operatorname{Spec} H^*(E)$. If $p = 2$, then $\beta(x) = x^2$. It follows that $x \in \mathfrak{p}$, and lemma 2.17 gives that

$$(x) = \operatorname{Ker} \operatorname{res}_{E,\operatorname{Ker} x} \subset \mathfrak{p}.$$

If p odd, then

$$\beta(x) H^*(E)^{ev} = \operatorname{Ker} \operatorname{res}_{E,\operatorname{Ker} x} \cap H^*(E)^{ev} \subset \mathfrak{p}.$$

Since elements of odd degree are nilpotent, $\operatorname{Ker} \operatorname{res}_{E,\operatorname{Ker} x} \subset \mathfrak{p}$. Consequently, $\mathfrak{p} \in V(\sqrt{\operatorname{Ker} \operatorname{res}_{E,\operatorname{Ker} x}})$. Conversely, if $\sqrt{\operatorname{Ker} \operatorname{res}_{E,\operatorname{Ker} x}} \subset \mathfrak{p}$, then $\beta(x) \in \mathfrak{p}$ since $x \in \operatorname{Ker} \operatorname{res}_{E,\operatorname{Ker} x}$.

Suppose E' is a subgroup of $\operatorname{Ker} x$, then

$$\operatorname{res}_{E,E'}(\beta(x)) = \operatorname{res}_{\operatorname{Ker} x,E'} \operatorname{res}_{E,\operatorname{Ker} x}(\beta(x)) = 0.$$

It follows that

$$V(\sqrt{\operatorname{Ker} \operatorname{res}_{E,E'}}) \subset V(\sqrt{\operatorname{Ker} \operatorname{res}_{E,\operatorname{Ker} x}}) = V(\beta(x)).$$

Noting that every proper subgroup of E is contained in $\operatorname{Ker} x$ for some $0 \neq x \in H^1(E)$ finishes the proof. □

Corollary 2.19. *Suppose E is an elementary abelian p-group. Then V_E^+ are the prime ideals of $H^*(E)$ not containing ρ_E, that is, $V_E^+ = \operatorname{Spec} H^*(E) - V(\rho_E)$.*

We are now able to proof theorem 2.16.

Proof of theorem 2.16. Recall that

$$\begin{aligned} V_{G,E}^+ &= V(\mathfrak{p}_E) - \bigcup_{E'<E} V(\mathfrak{p}_{E'}) \\ &= \operatorname{res}_{G,E}^{-1}(\operatorname{Spec} H^*(E)) - \bigcup_{E'<E} \operatorname{res}_{G,E'}^{-1}(\operatorname{Spec} H^*(E')). \end{aligned}$$

By corollary 2.13, there exists $\tau_E \in H^*(G)$ such that $\tau_E \notin \mathfrak{p}_E$, and $\tau_E \notin \mathfrak{p}_{E'}$ if and only if E is conjugate to a subgroup of E' if and only if $\mathfrak{p}_E \supset \mathfrak{p}_{E'}$.

Define U_E to be the subset of $\operatorname{res}_{G,E}^{-1}(\operatorname{Spec} H^*(E))$ of prime ideals not containing τ_E, that is,

$$U_E = V(\sqrt{\operatorname{Ker} \operatorname{res}_{G,E}}) - V(\tau_E).$$

We claim that the theorem follows if $V_{G,E}^+ = U_E$:

The sets $V_{G,E}^+$ are disjoint: Suppose $\mathfrak{p} \in V_{G,E}^+ \cap V_{G,E'}^+$. Since $\tau_E \notin \mathfrak{p}$ and $\mathfrak{p}_{E'} \subset \mathfrak{p}$, $\tau_E \notin \mathfrak{p}_{E'}$ hence E is conjugate to a subgroup of E'. Similarly, E' is conjugate to a subgroup of E. So E and E' are conjugate, i.e., $V_{G,E}^+ = V_{G,E'}^+$.

$\operatorname{Spec} H^*(G) = \bigcup_{E \in \mathcal{A}(G)} V_{G,E}^+$: Consider a prime ideal $\mathfrak{p}$ of $H^*(G)$. Let E be the smallest elementary abelian p-subgroup of G such that $\mathfrak{p}_E \subset \mathfrak{p}$, i.e., $\mathfrak{p}_E$ is the largest prime ideal of the form $\mathfrak{p}_{E'}$ for $E' \in \mathcal{A}(G)$ contained in $\mathfrak{p}$. Consequently, $\mathfrak{p} \in V_{G,E}^+$ due to corollary 2.5.

Since $V_{G,E}^+$ only depend on the conjugacy class of E, it follows that

$$\operatorname{Spec} H^*(G) = \coprod_{1 \le i \le n} V_{G,E_i}^+.$$

It remains to prove that $V_{G,E}^+ = U_E$:

By construction, U_E is disjoint from the set $\bigcup_{E'<E} V(\mathfrak{p}_{E'})$. In particular, $U_E \subset V_{G,E}^+$. To prove that $U_E = V_{G,E}^+$ it suffices to show that

$$V_{G,E}^+ \subset \operatorname{res}_{G,E}^{-1}(V_E^+) \text{ and } \operatorname{res}_{G,E}^{-1}(V_E^+) \subset U_E.$$

Note that this also implies that $V^+_{G,E} = \operatorname{res}^{-1}_{G,E}(V^+_E)$.

$V^+_{G,E} \subset \operatorname{res}^{-1}_{G,E}(V^+_E)$: Consider $\mathfrak{p} = \operatorname{res}^{-1}_{G,E}(\mathfrak{q}) \in V^+_{G,E}$, $\mathfrak{q} \in \operatorname{Spec} H^*(E)$. Since $\mathfrak{p} \in V^+_{G,E}$, $\mathfrak{p}_{E'}$ is not contained in $\mathfrak{p}$ for all $E' < E$. Suppose $\mathfrak{q} \notin V^+_E$, i.e., $\sqrt{\operatorname{Ker} \operatorname{res}_{E,E'}} \subset \mathfrak{q}$ for some $E' < E$. Then

$$\mathfrak{p}_{E'} = \sqrt{\operatorname{Ker} \operatorname{res}_{G,E'}} \subset \operatorname{res}^{-1}_{G,E}(\sqrt{\operatorname{Ker} \operatorname{res}_{E,E'}}) \subset \mathfrak{p},$$

contradicting that $\mathfrak{p} \in V^+_{G,E}$. We conclude that $\mathfrak{q} \in V^+_E$.

$\operatorname{res}^{-1}_{G,E}(V^+_E) \subset U_E$: Let $\mathfrak{q} \in V^+_E$. By corollary 2.19,

$$V^+_E = \operatorname{Spec} H^*(E) - V(\rho_E) = \operatorname{Spec} H^*(E) - V(\sqrt{\rho_E}).$$

Recall from the proof of 2.10 that $\operatorname{res}_{G,E}(\tau_E) = \rho_E^{p^k}$ for some k. In other words, $\operatorname{res}_{G,E}(\tau_E) \in \sqrt{\rho_E}$ which implies that $\operatorname{res}_{G,E}(\tau_E) \notin \mathfrak{q}$, i.e., $\operatorname{res}^{-1}_{G,E}(\mathfrak{q}) \in U_E$.

This finishes the proof. □

During the previous proof we observed:

Corollary 2.20. *Let E be an elementary abelian p-subgroup of G. Then $V^+_{G,E} = \operatorname{res}^{-1}_{G,E}(V^+_E)$.*

2.2 Steenrod operations

For the reader's convenience we recall a few basic facts about Steenrod operations. The mod p cohomology of a group G has Steenrod squares

$$Sq^i\colon H^n(G;\mathbb{F}_2) \to H^{n+i}(G;\mathbb{F}_2)$$

for $p = 2$, and reduced Steenrod powers

$$P^i\colon H^n(G;\mathbb{F}_p) \to H^{n+2i(p-1)}(G;\mathbb{F}_p)$$

for p odd. The square Sq^1 is the Bockstein operation. For p odd the Bockstein operation is a separate Steenrod operation. Classically, the Steenrod operations are cohomology operations of the mod p cohomology of a space, see e.g. [28] section 4.L. These cohomology operations have many nice properties such as Sq^0 and P^0 are both the identity map, additivity, and naturality with respect to group homomorphisms. The multiplicative structure is given by the Cartan formula,

$$Sq^n(xy) = \sum_{i+j=n} Sq^i(x)Sq^j(y)$$

and

$$P^n(xy) = \sum_{i+j=n} P^i(x)P^j(y).$$

The Steenrod operations also satisfy the instability property,

$$Sq^{|x|}(x) = x^2 \text{ and, } Sq^i(x) = 0 \text{ for } i > |x|$$

and

$$P^{|x|/2}(x) = x^p \text{ for } |x| \text{ even, and } P^i(x) = 0 \text{ for } 2i > |x|.$$

The total Steenrod operations

$$Sq = \bigoplus_{i \geq 0} Sq^i \text{ and } P = \bigoplus_{i \geq 0} P^i$$

are (by the Cartan formula) ring homomorphisms.

Under composition the Steenrod operations satisfy certain, somewhat complicated, relations known as the Adem relations. The mod 2 Steenrod algebra is the graded algebra over $\mathbb{F}_2$ generated by Sq^i subject to the Adem relations. For p odd the mod p Steenrod algebra is the graded algebra over $\mathbb{F}_p$ generated by P^i and the Bockstein β subject to the Adem relations and $\beta^2 = 0$. Consequently, the mod p cohomology of a group is a module over the Steenrod algebra. These concepts are the starting point of the theory of unstable modules over the Steenrod algebra, see [44].

We now investigate the so called invariant ideals.

Definition 2.21. *A homogeneous ideal I in $H^*(G)$ is called invariant if it is closed under the reduced Steenrod operations, that is, $Sq^i(I) \subset I$ if $p = 2$, and $P^i(I) \subset I$ if p odd.*

Remark 2.22. The Cartan formula gives that the radical of an invariant ideal is also invariant. A reason for not including the Bockstein for odd primes is that the radical of the zero ideal in $H^*(\mathbb{Z}/p) = \wedge_{\mathbb{F}_p}[x] \otimes \mathbb{F}_p[\beta(x)]$, $|x| = 1$, is not invariant under the Bockstein.

The following theorem by Quillen, see [38] theorem 12.1, shows that the invariant prime ideals are special. It relies on the corresponding result for elementary abelian p-groups which is due to Serre, see [45] proposition 1. Note that Serre's proof is purely geometric. The proof of the case of an elementary abelian p-group given here is a modified version of the proof of [46] proposition 11.4.1 and uses techniques from Adams & Wilkerson [1].

Theorem 2.23. *A prime ideal $\mathfrak{p}$ of $H^*(G)$ is of the form $\mathfrak{p} = \sqrt{\operatorname{Ker} \operatorname{res}_{G,E}}$ for some E elementary abelian p-subgroup of G if and only if it is invariant.*

Proposition 2.24. *Let E be an elementary abelian p-group. If $\mathfrak{p}$ is an invariant prime ideal of $H^*(E)$, then $\mathfrak{p} = \sqrt{\operatorname{Ker} \operatorname{res}_{E,E'}}$ for some subgroup E' of E.*

Proof of theorem 2.23. We treat the cases $p = 2$ and p odd simultaneously. Let $\mathcal{P}^i$ denote Sq^i if $p = 2$ and P^i if p odd, and $\mathcal{P}$ denote the total Steenrod operation.

Consider the homogeneous prime ideal $\mathfrak{p}_E = \sqrt{\operatorname{Ker} \operatorname{res}_{G,E}}$ and a homogeneous element x in $\mathfrak{p}_E$, i.e., $\operatorname{res}_{G,E}(x^n) = 0$ for some n. Note that

$$0 = \mathcal{P} \operatorname{res}_{G,E}(x^n) = \operatorname{res}_{G,E}(\mathcal{P}(x)^n).$$

that is, $\mathcal{P}(x) \in \mathfrak{p}_E$. Since $\mathfrak{p}_E$ is homogeneous, it follows that each homogeneous term of $\mathcal{P}(x)$ is in $\mathfrak{p}_E$, i.e., $\mathcal{P}^i(x) \in \mathfrak{p}_E$ for all i. In other words, it is invariant.

Conversely, suppose $\mathfrak{p}$ is an invariant prime ideal of $H^*(G)$. Recall that $\mathfrak{p} \in V^+_{G,E}$ for some elementary abelian p-subgroup of G and $\mathfrak{p}_E$ is the largest prime ideal of the form $\mathfrak{p}_{E'}$, $E' \in \mathcal{A}(G)$, contained in $\mathfrak{p}$.

We claim that $\mathfrak{p} = \mathfrak{p}_E$: Since $\mathfrak{p} \in V^+_{G,E} \subset V(\mathfrak{p}_E)$, corollary 2.20 gives that $\mathfrak{p}$ is equal to $\operatorname{res}^{-1}_{G,E}(\mathfrak{q})$ for some prime ideal $\mathfrak{q}$ in V^+_E.

Remember that $H^*(E)$ is finitely generated as a module over $H^*(G)$ via restriction. Furthermore, $V(\mathfrak{p}_E)$ and $\operatorname{Spec} H^*(G)/\operatorname{Ker}\operatorname{res}_{G,E}$ coincide and is via restriction identified with $\operatorname{Spec}\operatorname{Im}\operatorname{res}_{G,E}$, that is, if $\mathfrak{p}_E \subset \mathfrak{p}'$, then the corresponding prime ideal of $\operatorname{Im}\operatorname{res}_{G,E}$ is the image $\operatorname{res}_{G,E}(\mathfrak{p}')$.

$\mathfrak{q}$ is homogeneous: Let $\mathfrak{q}^*$ be the ideal generated by the homogeneous elements in $\mathfrak{q}$, i.e., the largest homogeneous ideal contained in $\mathfrak{q}$. Note that $\mathfrak{q}^*$ is a prime ideal of $H^*(E)$, see proposition A.9. Since $\mathfrak{p}$ is homogeneous, $\mathfrak{p} = \operatorname{res}^{-1}_{G,E}(\mathfrak{q}^*)$. Thus, $\mathfrak{q}$ and $\mathfrak{q}^*$ are two prime ideals lying over $\operatorname{res}_{G,E}(\mathfrak{p})$. By the going-up theorem, see theorem A.14, there are no strict inclusions between prime ideals lying over a prime ideal, which implies that $\mathfrak{q} = \mathfrak{q}^*$. In other words, $\mathfrak{q}$ is homogeneous.

$\mathfrak{q}$ is invariant: Note that if $\mathcal{P}(x) = x + \sum_{i>0} \mathcal{P}^i(x) \in \mathfrak{p}$ for x homogeneous, then $x \in \mathfrak{p}$ since $\mathfrak{p}$ homogeneous. In particular, $\mathcal{P}^{-1}(\mathfrak{p}) = \mathfrak{p}$.

Since $\operatorname{res}_{G,E} \mathcal{P} = \mathcal{P} \operatorname{res}_{G,E}$, it follows that

$$\operatorname{res}^{-1}_{G,E} \mathcal{P}^{-1}(\mathfrak{q}) = \mathcal{P}^{-1} \operatorname{res}^{-1}_{G,E}(\mathfrak{q}) = \mathcal{P}^{-1}(\mathfrak{p}) = \mathfrak{p}.$$

Hence, $\mathcal{P}^{-1}(\mathfrak{q}) \subset \mathfrak{q}$ is a prime ideal lying over $\operatorname{res}_{G,E}(\mathfrak{p})$. As above, it follows that $\mathfrak{q} = \mathcal{P}^{-1}(\mathfrak{q})$. Consequently, $\mathfrak{q}$ is invariant.

Since $\mathfrak{q} \in V^+_E$ and invariant, proposition 2.24 gives that $\mathfrak{q} = \operatorname{Nil}(H^*(E))$. Hence,

$$\mathfrak{p} = \operatorname{res}^{-1}_{G,E}(\operatorname{Nil}(H^*(E))) = \mathfrak{p}_E.$$

□

We proceed with proposition 2.24. Recall that a derivation ∂ of an $\mathbb{F}_p$-algebra R is a $\mathbb{F}_p$-homomorphism $\partial\colon R \to R$ such that $\partial(x+y) = \partial(x) + \partial(y)$ and $\partial(xy) = \partial(x)y + x\partial(y)$ (Leibniz rule) for all $x, y \in R$. See e.g. [34] ch. 9 or [10] III §10 for background on derivations.

A classic example of a derivation is the partial derivative $\partial/\partial x_i$, $1 \le i \le n$, on the polynomial algebra $\mathbb{F}_p[x_1, \dots, x_n]$.

A more complicated example is the derivations $Q^i\colon H^*(G;\mathbb{F}_2) \to H^*(G;\mathbb{F}_2)$ defined inductively by $Q^1 = Sq^1$ and $Q^{i+1} = Sq^{2^i} Q^i - Q^i Sq^{2^i}$. Similarly for p odd. See [1] section 2 for more information.

To prove proposition 2.24 we need the following technical lemmas, see [1] lemmas 3.1 and 5.9.

Lemma 2.25. *Suppose $\partial_1, \dots, \partial_n \colon R \to R$ are derivations and $x_1, \dots, x_n \in R$. If the matrix $\partial_i(x_j)$, $1 \le i, j \le n$, has nonzero determinant. Then $x_1, \dots, x_n$ are algebraically independent over $\mathbb{F}_p$.*

Lemma 2.26. *The determinant of the matrix*

$$A = \begin{pmatrix} x_1 & x_1^p & \cdots & x_1^{p^{n-1}} \\ x_2 & x_2^p & \cdots & x_2^{p^{n-1}} \\ \vdots & \vdots & \cdots & \vdots \\ x_n & x_n^p & \cdots & x_n^{p^{n-1}} \end{pmatrix}$$

is the polynomial in $\mathbb{F}_p[x_1, \dots, x_n]$ given by the product

$$\det(A) = \prod (c_1 x_1 + \cdots c_n x_n),$$

where $(c_1, \dots, c_n) \in \mathbb{F}_p^n$ are nonzero and the last nonzero c_i is 1.

Proof of proposition 2.24. Let $\mathfrak{p}$ be an invariant prime ideal of $H^*(E)$. Consider the quotient map $\pi \colon H^*(E) \to H^*(E)/\mathfrak{p}$. Since $\mathfrak{p}$ is invariant, the Steenrod operations also act on the quotient algebra. In particular, Q^i is a derivation on $H^*(E)/\mathfrak{p}$ for all i.

Let $y_1, \dots, y_n$ be an $\mathbb{F}_p$-basis of $\pi(H^1(E))$ for $p = 2$ or $\pi(H^2(E))$ for p odd. Note that $y_1, \dots, y_n$ generate $H^*(E)/\mathfrak{p}$ as an algebra over $\mathbb{F}_p$.

Let A be the matrix with entries $A_{i,j} = Q^i(y_j)$ for $1 \le i, j \le n$.

$Q^i(y_j) = y_j^{p^i}$: Suppose $p = 2$. Then $Q^1(y_j) = Sq^1(y_j) = y_j^2$ for $1 \le j \le n$. Assume inductively that $Q^i(y_j) = y_j^{2^i}$. Then, using that $|y_j| = 1$,

$$Q^{i+1}(y_j) = Sq^{2^i} Q^i(y_j) - Q^i Sq^{2^i}(y_j) = Sq^{2^i} Q^i(y_j) = Sq^{2^i}(y_j^{2^i}) = y_j^{2^{i+1}}.$$

The case of p odd is similar.

The transpose of A is the matrix

$$\begin{pmatrix} y_1^p & y_1^{p^2} & \cdots & y_1^{p^n} \\ y_2^p & y_2^{p^2} & \cdots & y_2^{p^n} \\ \vdots & \vdots & \cdots & \vdots \\ y_n^p & y_n^{p^2} & \cdots & y_n^{p^n} \end{pmatrix}$$

Substituting $x_i = y_i^p$ and using lemma 2.26 gives that

$$\det(A) = \prod (c_1 y_1^p + \cdots c_n y_n^p) = \prod (c_1 y_1 + \cdots c_n y_n)^p,$$

where we used that the Frobenius map, $x \mapsto x^p$, is a homomorphism. Since $H^*(E)/\mathfrak{p}$ is an integral domain generated by $y_1, \dots, y_n$, it follows that $\det(A) \neq 0$. By lemma 2.25, $y_1, \dots, y_n$ are algebraically independent over $\mathbb{F}_p$, i.e., $H^*(E)/\mathfrak{p}$ is a polynomial algebra.

For $p = 2$ it follows that $\mathfrak{p}$ is generated by the elements of $H^1(E)$ it contains. The proposition follows from the fact that subspaces of $H^1(E) = \operatorname{Hom}(E, \mathbb{Z}/p)$ correspond to subgroups of E. More specifically, choose an $\mathbb{F}_2$-basis $x_1, \dots, x_{m+n}$ of $H^1(E)$ such that $x_1, \dots, x_m$ constitute an $\mathbb{F}_2$-basis of the subspace $H^1(E) \cap \mathfrak{p}$. Furthermore, choose an $\mathbb{F}_2$-basis $e_1, \dots, e_{m+n}$ of E with dual basis $x_1, \dots, x_{m+n}$. Let $E' = \langle e_{m+1}, \dots, e_{m+n} \rangle \subset E$ and $x'_{m+1}, \dots, x'_{m+n}$ be the dual basis, i.e., $H^*(E') = \mathbb{F}_2[x'_{m+1}, \dots, x'_{m+n}] \cong H^*(G)/\mathfrak{p}$. Then

$$\operatorname{res}_{G,E'}(x_i) = \begin{cases} 0, & 1 \le i \le m \\ x'_i, & m+1 \le i \le m+n, \end{cases}$$

and $\mathfrak{p} = \operatorname{res}^{-1}_{E,E'}(\{0\}) = \operatorname{res}^{-1}_{E,E'}(\operatorname{Nil}(H^*(E'))) = \sqrt{\operatorname{Ker} \operatorname{res}_{E,E'}}$.

Similarly for p odd using that $\mathfrak{p}$ (modulo the nilradical) is generated by the elements of $H^2(E)$ it contains and that the Bockstein homomorphism $\beta \colon H^1(E) \to H^2(E)$ is an isomorphism. The gory details are left to the reader. □

3 Depth, detection and associated primes

The Krull dimension is completely determined by the group structure. The depth seems to be more mysterious. This section is all about the depth of the cohomology ring of a finite group especially Carlson's depth conjecture.

As usual, let G be a finite group, p a prime divisor of the order of G and let $H^*(G)$ denote the mod p cohomology of G.

3.1 Depth and associated primes

We begin with the definitions of regular elements and sequences, depth and associated primes.

Definition 3.1. *Let R be a graded commutative Noetherian ring with $R^0 = \mathbb{F}_p$ and M a finitely generated graded R-module. A homogeneous element x of positive degree is called an M-regular element in R if x is not a zero divisor of M, or equivalently, if multiplication by x is injective.*

A sequence $x_1, \dots, x_n$ of homogeneous elements of positive degree R is called an M-regular sequence in R if x_i is $M/(x_1, \dots, x_{i-1})M$-regular for $1 \leq i \leq n$ $((\emptyset) = 0)$.

The depth of a finitely generated R-module M is the maximal length of an M-regular sequence and is denoted $\operatorname{depth}_R M$. The depth of R is simply denoted $\operatorname{depth} R$.

Definition 3.2. *Let R be a graded commutative Noetherian ring with $R^0 = \mathbb{F}_p$. An ideal in R is said to be associated to an R-module M if it is the annihilator of some nonzero element in M. An associated prime ideal, or simply associated prime, of M is a prime ideal associated to M. The set of prime ideals associated to M is denoted $\operatorname{Ass}_R M$, that is,*

$$\operatorname{Ass}_R M = \{\, \mathfrak{p} \in \operatorname{Spec} R \,|\, \mathfrak{p} = \operatorname{Ann}_R(m) \text{ for some } m \in M \,\}.$$

The associated primes of R is simply denoted $\operatorname{Ass} R$.

In fact, any associated prime is homogeneous and the annihilator of a homogeneous element. Furthermore, the associated primes are among the minimal primes of $H^*(G)$ and there are only finitely many since $H^*(G)$ is Noetherian, see proposition A.8. See appendix A for more information. However, keep the following fundamental result in mind, see propositions A.11 and A.33.

Proposition 3.3.

$$\operatorname{depth} H^*(G) \leq \min\{\, \dim H^*(G)/\mathfrak{p} \,|\, \mathfrak{p} \in \operatorname{Ass} H^*(G) \,\} \leq \dim H^*(G).$$

In the case where the depth and dimension coincide we say that the ring is Cohen-Macaulay.

Suppose E is a maximal elementary abelian p-subgroup of G. Then the ideal $\sqrt{\operatorname{Ker}\operatorname{res}_{G,E}}$ is a minimal prime ideal, and an associated prime, of $H^*(G)$ such that the dimension of $H^*(G)/\sqrt{\operatorname{Ker}\operatorname{res}_{G,E}}$ is $\operatorname{rk}_p(E)$, see theorem 2.14. Let $\operatorname{mrk}_p(G)$ denote the minimal rank amongst the maximal elementary abelian p-subgroups of G. Summarizing, we have proved the following result.

Proposition 3.4. $\operatorname{depth} H^*(G) \leq \operatorname{mrk}_p(G)$.

Example 3.5. The cohomology of an elementary abelian p-group is

$$H^*(E) = \begin{cases} \mathbb{F}_p[x_1, \ldots, x_n], & p = 2 \\ \wedge_{\mathbb{F}_p}(x_1, \ldots, x_n) \otimes \mathbb{F}_p[\beta(x_1), \ldots, \beta(x_n)], & p > 2, \end{cases}$$

where $|x_i| = 1$ and $n = \operatorname{rk}_p(E)$. The sequence $x_1, \ldots, x_n$ is a maximal regular sequence in the case $p = 2$, and $\beta(x_1), \ldots, \beta(x_n)$ is a maximal regular sequence for odd primes. So $\operatorname{depth} H^*(E) = \operatorname{rk}_p(E) = \dim H^*(E)$, that is, the cohomology of an elementary abelian p-group is Cohen-Macaulay.

Example 3.6. Remember that the mod 2 cohomology ring of the dihedral group D_8 of order 8 is

$$H^*(D_8; \mathbb{F}_2) = \mathbb{F}_2[x, y, v]/(x(x + y))$$

with $|x| = |y| = 1$ and $|v| = 2$. Clearly, v is a regular element and

$$H^*(D_8; \mathbb{F}_2)/(v) = \mathbb{F}_2[x, y]/(x(x + y)).$$

Evidently, y is a regular element of $H^*(D_8; \mathbb{F}_2)/(v)$ and

$$H^*(D_8; \mathbb{F}_2)/(v, y) = \mathbb{F}_2[x]/(x^2),$$

that is, an exterior algebra. So $\operatorname{depth} H^*(D_8; \mathbb{F}_2) = 2$.

Example 3.7. The mod 2 cohomology ring of Q_8 is

$$H^*(Q_8; \mathbb{F}_2) = \mathbb{F}_2[x, y, v]/(x^2 + xy + y^2, x^2y + xy^2)$$

with x and y in degree 1 and v in degree 4. Clearly, v is a regular element. The dimension of $H^*(Q_8; \mathbb{F}_2)$ is 1 hence $\operatorname{depth} H^*(Q_8; \mathbb{F}_2) = 1$.

Lemma 3.8. *Suppose H is a subgroup of G such that $[G : H]$ is coprime to p. Then $\operatorname{res}_{G,H}$ is injective, $\operatorname{tr}_{H,G}$ is surjective and*

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Ker}\operatorname{tr}_{H,G} \arrow[r] & H^*(H) \arrow[r, "\operatorname{res}_{G,H}\operatorname{tr}_{H,G}"] & \operatorname{Im}\operatorname{res}_{G,H} \arrow[r] & 0 \end{tikzcd}$$

is a split-exact sequence of $H^*(G)$-modules via restriction.

Proof. Remember that the transfer map and the restriction map are $H^*(G)$-linear via the restriction map, and that $\operatorname{tr}_{H,G} \operatorname{res}_{G,H} \colon H^*(G) \to H^*(G)$ is multiplication by $[G : H]$, see proposition 1.1. It follows that the composite is an isomorphism and has an inverse $\varphi\colon H^*(G) \to H^*(G)$. In particular, $\operatorname{res}_{G,H}$ is injective and $\operatorname{tr}_{H,G}$ is surjective.

Consequently, the sequence

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Ker} \operatorname{tr}_{H,G} \arrow[r] & H^*(H) \arrow[r, "\operatorname{tr}_{H,G}"] & H^*(G) \arrow[r] & 0 \end{tikzcd}$$

is an exact sequence of $H^*(G)$-modules. Since $\operatorname{tr}_{H,G}(\operatorname{res}_{G,H} \varphi)$ is the identity on $H^*(G)$, the sequence splits. Noting that $\operatorname{res}_{G,H}$ is injective finishes the proof. □

An immediate consequence is that the restriction to any Sylow p-subgroup is injective.

The following theorem is traditionally stated for a Sylow p-subgroup of G, see e.g. [18] proposition 12.3.1. However, we need the slightly more general version later, and the usual proof goes through in this case.

Theorem 3.9. *Suppose H is a subgroup of G with $[G : H]$ coprime to p. Then*

$$\operatorname{depth} H^*(H) \leq \operatorname{depth} H^*(G).$$

In addition, if $x_1, \dots, x_n$ is a sequence of homogeneous elements in $H^*(G)$ such that $\operatorname{res}_{G,H}(x_1), \dots, \operatorname{res}_{G,H}(x_n)$ is a regular sequence in $H^*(H)$, then $x_1, \dots, x_n$ is a regular sequence in $H^*(G)$.

Proof. Lemma 3.8 gives that

$$H^*(H) = \operatorname{Ker} \operatorname{tr}_{H,G} \oplus \operatorname{Im} \operatorname{res}_{G,H} = \operatorname{Ker} \operatorname{tr}_{H,G} \oplus H^*(G)$$

as $H^*(G)$-modules. Proposition A.37 gives that

$$\operatorname{depth}_{H^*(G)} H^*(H) \leq \operatorname{depth} H^*(G).$$

Since $H^*(H)$ is finitely generated as a module over $H^*(G)$ via restriction, proposition A.38 gives that

$$\operatorname{depth}_{H^*(G)} H^*(H) = \operatorname{depth} H^*(H),$$

which proves the first statement.

Suppose $\operatorname{res}_{G,H}(x_1), \dots, \operatorname{res}_{G,H}(x_n)$ is a regular sequence in $H^*(H)$. By theorem A.22, $H^*(H)$ is a free module over $\mathbb{F}_p[x_1, \dots, x_n]$. Since $H^*(G)$ is a direct summand of $H^*(H)$, $H^*(G)$ is also a free module over $\mathbb{F}_p[x_1, \dots, x_n]$. Again by theorem A.22, $x_1, \dots, x_n$ is a regular sequence in $H^*(G)$. □

A Sylow p-subgroup P of G is a canonical example of a subgroup of G satisfying that $[G : P]$ is coprime to p. However, as the following example shows, the depth of $H^*(G)$ may be strictly greater than the depth of $H^*(P)$.

Example 3.10. The Mathieu group M_{11} is a sporadic simple group of order 7920. The mod 2 cohomology ring is

$$H^*(M_{11}; \mathbb{F}_2) = \mathbb{F}_2[x, y, z]/(x^2y + z^2)$$

with $|x| = 3$, $|y| = 4$ and $|z| = 5$. The calculation is due to Benson & Carlson [9], see also [2]. It is straightforward to verify that the depth of $H^*(M_{11}; \mathbb{F}_2)$ is 2 and that y, x is a maximal regular sequence in $H^*(M_{11}; \mathbb{F}_2)$. The Sylow 2-subgroup P of M_{11} is a semidihedral (or quasidihedral) group of order 16. The cohomology ring is

$$H^*(P; \mathbb{F}_2) = \mathbb{F}_2[a, b, c, d]/(ab, b^3, bc, a^2d + c^2)$$

with $|a| = |b| = 1$, $|c| = 3$ and $|d| = 4$, see [14]; the Hall-Senior number is 16 and the Magma small group library number is 8. Note that the annihilator of b^2 is the ideal (a, b, c), which is a prime ideal since $H^*(P; \mathbb{F}_2)/(a, b, c) = \mathbb{F}_2[d]$ is an integral domain. Thus, $\mathrm{Ann}_{H^*(P;\mathbb{F}_2)}(b^2)$ is an associated prime with $\dim H^*(P; \mathbb{F}_2)/\mathrm{Ann}_{H^*(P;\mathbb{F}_2)}(b^2) = 1$. Since d is a regular element, the depth of $H^*(P; \mathbb{F}_2)$ is 1. That the depth is positive also follows by Duflot's theorem, see theorem 3.11. Summarizing,

$$\operatorname{depth} H^*(P; \mathbb{F}_2) = 1 < 2 = \operatorname{depth} H^*(M_{11}; \mathbb{F}_2).$$

A classic result that relates properties of the group to the depth of the cohomology ring is the following theorem which was first proved Duflot [20] and is known as Duflot's theorem.

Theorem 3.11. *The depth of $H^*(G)$ is greater than or equal to the p-rank of the center of a Sylow p-subgroup of G. More specifically, if P is a Sylow p-subgroup of G, then $\mathrm{rk}_p(Z(P)) \leq \operatorname{depth} H^*(G)$.*

A few immediate consequences:

Corollary 3.12. *The depth of $H^*(G)$ is positive.*

Proof. The center of any p-group contains an element of order p. □

Of course, here we used the assumption that p is a prime divisor of G.

Corollary 3.13. *Suppose G has abelian Sylow p-subgroups. Then $H^*(G)$ is Cohen-Macaulay. In particular, if G abelian, then $H^*(G)$ is Cohen-Macaulay.*

Duflot's proof uses equivariant cohomology. Broto & Henn [11] gave a conceptually easier proof of Duflot's theorem. The idea is to construct a sequence $x_1, \dots, x_n$ of elements in $H^*(G)$ whose restriction to a central elementary abelian p-subgroup C of P, i.e., $C \subset Z(P)$, is a regular sequence in $H^*(C)$ and prove that $x_1, \dots, x_n$ is a regular sequence in $H^*(G)$. Carlson et al. [18], see proposition 12.3.3, generalized this idea slightly and proved that any sequence $x_1, \dots, x_n$ in $H^*(G)$ whose restriction to C is a regular sequence in $H^*(C)$ is indeed a regular sequence in $H^*(G)$. We shall follow the latter approach. The basic ingredient is the following construction.

For a central subgroup C of a group G, the multiplication in G gives a group homomorphism

$$\mu \colon C \times G \to G, (c, g) \mapsto cg,$$

which induces a map $\mu^* \colon H^*(G) \to H^*(C \times G)$. Using the cross product we get a map

$$\Delta \colon H^*(G) \to H^*(C) \otimes H^*(G),$$

that is, Δ is defined by commutativity of the diagram

$$\begin{tikzcd}
H^*(G) \arrow[r, "\mu^*"] \arrow[dr, "\Delta"] & H^*(C \times G) \\
& H^*(C) \otimes H^*(G) \arrow[u, "\times", "\cong"']
\end{tikzcd}$$

where the tensor product is the graded tensor product with the usual sign convention.

An important property of Δ is that for any $x \in H^n(G)$, $n > 0$, we have

$$\Delta(x) = \mathrm{res}_{G,C}(x) \otimes 1 + 1 \otimes x + \sum_i x_i' \otimes x_i'',$$

where $|x_i'|, |x_i''| > 0$: Let $i_C \colon C \to C \times G$, $c \mapsto (c, 1)$ and $i_G \colon G \to C \times G$, $g \mapsto (1, g)$ be the canonical inclusion maps, and consider the commutative diagram

$$\begin{tikzcd}
H^*(G) \arrow[r, "\mu^*"] \arrow[dr, "\Delta"] & H^*(C \times G) \arrow[r, "\mathrm{res}_{C\times G,C}"] & H^*(C) \\
& H^*(C) \otimes H^*(G) \arrow[u, "\times", "\cong"'] \arrow[ur, "\pi"] \arrow[r, "\mathrm{id} \otimes \mathrm{res}_{G,\{1\}}"] & H^*(C) \otimes H^*(\{1\}) \arrow[u, "\times", "\cong"']
\end{tikzcd}$$

where π is defined by commutativity. Note that $\pi(x \otimes 1) = x$, and $\pi(x \otimes y) = 0$ if $|y| > 0$. Since μi_C is the inclusion $C \subset G$, we have that $\pi\Delta = \mathrm{res}_{G,C}$. Hence, the component of $\Delta(x)$ in $H^n(C) \otimes H^0(G)$ is $\mathrm{res}_{G,C}(x) \otimes 1$. A similar argument, using that μi_G is the identity map, gives that the component of $\Delta(x)$ in $H^0(C) \otimes H^n(G)$ is $1 \otimes x$.

Consider $H^*(C \times G)$ as a module over $H^*(G)$ via the homomorphism μ^*. The fact that μi_G is the identity on G gives that $\mathrm{res}_{C\times G,G}\, \mu^*$ is the identity on $H^*(G)$. Therefore, the restriction map $\operatorname{res}_{C\times G,G}\colon H^*(C\times G)\to H^*(G)$ is a map of $H^*(G)$-modules. More specifically, if $x\in H^*(G)$ and $y\in H^*(C\times G)$, then

$$\operatorname{res}_{C\times G,G}(\mu^*(x)y)=\operatorname{res}_{C\times G,G}(\mu^*(x))\operatorname{res}_{C\times G,G}(y)=x\operatorname{res}_{C\times G,G}(y).$$

Furthermore, since $\operatorname{res}_{C\times G,G}\mu^*$ is the identity, the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Ker}\operatorname{res}_{C\times G,G} \arrow[r] & H^*(C\times G) \arrow[r, "\operatorname{res}_{C\times G,G}"] & H^*(G) \arrow[r] & 0 \end{tikzcd}$$

of $H^*(G)$-modules splits. Thus, $H^*(G)$ is a direct summand in $H^*(C\times G)$ as a module over $H^*(G)$. Of course, the same results hold if we consider $H^*(C)\otimes H^*(G)$ as a module over $H^*(G)$ via Δ.

Now, we are ready to prove the result about regular sequences and restriction to central subgroups.

Theorem 3.14. *Suppose C is a central subgroup of G. If $x_1,\dots,x_n$ is a sequence of homogeneous elements in $H^*(G)$ such that $\operatorname{res}_{G,C}(x_1),\dots,\operatorname{res}_{G,C}(x_n)$ is a regular sequence in $H^*(C)$, then $x_1,\dots,x_n$ is a regular sequence in $H^*(G)$.*

Proof. Remember that $H^*(C)\otimes H^*(G)$ is a module over $H^*(G)$ via the homomorphism Δ and for $x\in H^m(G)$,

$$\Delta(x)=\operatorname{res}_{G,C}(x)\otimes 1+1\otimes x+\sum_j x'_j\otimes x''_j,$$

where $|x'_j|,|x''_j|>0$.

The idea is to use theorem A.22 and prove that $H^*(C)\otimes H^*(G)$ is free as a module over $\mathbb{F}_p[x_1,\dots,x_n]$ and use that $H^*(G)$ is a direct summand in $H^*(C)\otimes H^*(G)$ as a $H^*(G)$-module.

For $i\geq 0$, let $H^{\geq i}(G)=\bigoplus_{j\geq i}H^j(G)$ be the ideal generated by the homogeneous elements of degree at least i. In particular, $H^*(C)\otimes H^{\geq i}(G)$ is a $H^*(G)$-submodule of $H^*(C)\otimes H^*(G)$ for all $i\geq 0$. Furthermore, the quotient

$$(H^*(C)\otimes H^{\geq i}(G))/(H^*(C)\otimes H^{\geq i+1}(G))$$

is a module over $H^*(G)$. Let $a\in H^k(C)$ and $b\in H^{\geq i}(G)$ of degree s. If $s>i$, then $[a\otimes b]=0$ in the quotient module. Henceforth, we assume b has degree i. The $H^*(G)$-module structure on the quotient module is given by

$$\begin{aligned} x[a\otimes b]&=[\Delta(x)(a\otimes b)]\\ &=[(\operatorname{res}_{G,C}(x)\otimes 1+1\otimes x+\sum_j x'_j\otimes x''_j)(a\otimes b)]\\ &=[(\operatorname{res}_{G,C}(x)a)\otimes b], \end{aligned}$$

in the latter equality we used that $|xb|,|x''_jb|>i$.

The map

$$\varphi\colon (H^*(C)\otimes H^{\geq i}(G))/(H^*(C)\otimes H^{\geq i+1}(G)) \to H^*(C)\otimes H^i(G),$$

defined by $\varphi([a\otimes b]) = a\otimes b$ is clearly an isomorphism of vector spaces over $\mathbb{F}_p$.

Consider $H^*(C)\otimes H^i(G)$ as a module over $H^*(G)$ in the natural way, i.e., with multiplication given by $x(a\otimes b) = (\mathrm{res}_{G,C}(x)a)\otimes b$. So φ is an isomorphism of $H^*(G)$-modules.

Recall that $H^i(G)$ is a finite dimensional vector space over $H^0(G) = \mathbb{F}_p$. Therefore, $H^i(G) = \mathbb{F}_p\{e_1,\dots,e_d\} \cong H^0(G)^d$ for some $e_1,\dots,e_d \in H^i(G)$ and $d = \dim_{\mathbb{F}_p} H^i(G)$.

Consider the canonical isomorphism of $\mathbb{F}_p$-vector spaces,

$$\psi\colon H^*(C)\otimes H^i(G) \to (H^*(C)\otimes H^0(G))^d \to H^*(C)^d,$$

where $\psi(a\otimes b) = ar_1 + \cdots + ar_d$ for $b = r_1e_1 + \cdots r_de_d \in H^i(G)$, $r_1,\dots,r_d \in \mathbb{F}_p$.

Consider $H^*(C)^d$ as a module over $H^*(G)$ in the obvious way, that is, $H^*(G)$ acts on each factor via restriction. Note that

$$\begin{aligned}\psi(x(a\otimes b)) &= \psi((\mathrm{res}_{G,C}(x)a)\otimes(r_1e_1+\cdots+r_de_d))\\ &= \mathrm{res}_{G,C}(x)ar_1 + \cdots + \mathrm{res}_{G,C}(x)ar_d.\end{aligned}$$

So ψ is also an isomorphism of $H^*(G)$-modules.

Summarizing, the composite

$$\psi\varphi\colon H^*(C)\otimes H^{\geq i}(G))/(H^*(C)\otimes H^{\geq i+1}(G)) \to H^*(C)^d$$

is an isomorphism of $H^*(G)$-modules.

Since $\mathrm{res}_{G,C}(x_1),\dots,\mathrm{res}_{G,C}(x_n)$ is a regular sequence in $H^*(C)$, it is also a regular sequence in $H^*(C)$ of the $H^*(C)$-module $H^*(C)^d$. In other words, $x_1,\dots,x_n$ is a regular sequence of the $H^*(G)$-module $H^*(C)^d$. By theorem A.22, $H^*(C)^d$ is a free module over $\mathbb{F}_p[x_1,\dots,x_n]$. It follows that the quotient module $(H^*(C)\otimes H^{\geq i}(G))/(H^*(C)\otimes H^{\geq i+1}(G))$ is a free module over $\mathbb{F}_p[x_1,\dots,x_n]$ for all $i \geq 0$.

Consequently,

$$\begin{aligned}H^*(C)\otimes H^*(G) &= \bigoplus_{i\geq 0} H^*(C)\otimes H^i(G)\\ &\cong \bigoplus_{i\geq 0}(H^*(C)\otimes H^{\geq i}(G))/(H^*(C)\otimes H^{\geq i+1}(G))\end{aligned}$$

is a free module over $\mathbb{F}_p[x_1,\dots,x_n]$. Since $H^*(G)$ is a direct summand of $H^*(C)\otimes H^*(G)$ as an $H^*(G)$-module, it follows that $H^*(G)$ is a free module over $\mathbb{F}_p[x_1,\dots,x_n]$. Finally, by theorem A.22, $x_1,\dots,x_n$ is a regular sequence in $H^*(G)$. □

Corollary 3.15. *Suppose C is a central subgroup of a Sylow p-subgroup P of G. If $x_1, \dots, x_n \in H^*(G)$ is a sequence of homogeneous elements in $H^*(G)$ such that $\operatorname{res}_{G,C}(x_1), \dots, \operatorname{res}_{G,C}(x_n)$ is a regular sequence in $H^*(C)$, then $x_1, \dots, x_n$ is a regular sequence in $H^*(G)$.*

Proof. By assumption, $\operatorname{res}_{P,C}(\operatorname{res}_{G,P}(x_1)), \dots, \operatorname{res}_{P,C}(\operatorname{res}_{G,P}(x_n))$ is a regular sequence in $H^*(C)$. Theorem 3.14 gives that $\operatorname{res}_{G,P}(x_1), \dots, \operatorname{res}_{G,P}(x_n)$ is a regular sequence in $H^*(P)$, and theorem 3.9 implies that $x_1, \dots, x_n$ is a regular sequence in $H^*(G)$. □

Duflot's theorem is an easy application of this result.

Proof of theorem 3.11. Let E be a maximal elementary abelian p-subgroup contained in the center $Z(P)$ of a Sylow p-subgroup P of G. The cohomology ring $H^*(E)$ is Cohen-Macaulay and has depth $n = \operatorname{rk}_p(E) = \operatorname{rk}_p(Z(P))$, see example 3.5. Since $H^*(E)$ is finitely generated as a module over $H^*(G)$ via restriction, proposition A.38 gives that $\operatorname{depth}_{H^*(G)} H^*(E) = \operatorname{depth} H^*(E)$. In particular, there exists $x_1, \dots, x_n$ in $H^*(G)$ such that $\operatorname{res}_{G,E}(x_1), \dots, \operatorname{res}_{G,E}(x_n)$ is a regular sequence of maximal length. Corollary 3.15 gives that $x_1, \dots, x_n$ is a regular sequence in $H^*(G)$. This finishes the proof of Duflot's theorem. □

So far, the bounds provided by the minimal associated primes, see proposition 3.4, and Duflot's theorem are the best known results linking the depth of the cohomology ring directly to the group structure.

Theorem 3.9 gives a lower bound on the depth by the depths given by certain subgroups, e.g., the Sylow p-subgroups. Recently, Notbohm [36] proved that the depth is determined by the depths of the cohomology rings of the centralizers of the elementary abelian p-subgroups. More concisely:

Theorem 3.16. $\operatorname{depth} H^*(G) = \min\{ \operatorname{depth} H^*(C_G(E)) \mid E \in \mathcal{A}(G) \}$.

One of Notbohm's main results is the succeeding theorem which gives part of the previous theorem.

Theorem 3.17. *Suppose E is an elementary abelian p-subgroup of G. Then*

$$\operatorname{depth} H^*(G) \leq \operatorname{depth} H^*(C_G(E)).$$

The proofs of these results use the theory of unstable modules over the Steenrod algebra and rely heavily on the properties of Lannes' T-functor. In fact, Notbohm proves that an application of Lannes' T-functor only increases depth.

As noted by Notbohm, it suffices to take the minimum over the cyclic subgroups of order p. To see this suppose $E = \langle g \rangle \times E'$. Then $E \subset C_G(g)$ and $C_G(E) = C_{C_G(g)}(E)$. Using theorem 3.17 with $G = C_G(g)$ gives that

$$\operatorname{depth} H^*(C_G(g)) \leq \operatorname{depth} H^*(C_{C_G(g)}(E)) = \operatorname{depth} H^*(C_G(E)).$$

The theorem possibly reduces the problem of computing the depth to the computation of the depths of a collection of smaller subgroups. The reduction being in the size of the involved groups. Of course, if G is a p-group, then one of the centralizers is G itself so no reduction in this case.

A simple observation and theorem 3.9 allow us to point out subgroups on which the minimum in Notbohm's theorem is attained:

Theorem 3.18. *Let P be a Sylow p-subgroup of G. Suppose E is a central elementary abelian p-subgroup of P. Then*

$$\operatorname{depth} H^*(G) = \operatorname{depth} H^*(C_G(E)).$$

Proof. Note that $E \subset Z(P) \subset P \subset C_G(E) \subset G$, i.e., $[G : C_G(E)]$ is coprime to p. By theorem 3.9,

$$\operatorname{depth} H^*(C_G(E)) \leq \operatorname{depth} H^*(G).$$

Theorem 3.17 gives the reverse inequality. □

Suppose E is a central elementary abelian p-subgroup of a Sylow p-subgroup P of G such that $P = C_G(E)$, then the depth of $H^*(G)$ is equal to the depth of $H^*(P)$. This gives a sufficient group theoretic condition on when these depths are equal.

Let us summarize what we so far know about the relation between the group structure, the depth and dimension of the cohomology ring of a finite group.

Corollary 3.19. *Let P be a Sylow p-subgroup of G, and E a central elementary abelian p-subgroup of P. Then*

$$\begin{aligned} 0 < \operatorname{rk}_p(Z(P)) &\leq \operatorname{depth} H^*(P) \leq \operatorname{depth} H^*(C_G(E)) \\ &= \operatorname{depth} H^*(G) \leq \operatorname{mrk}_p(G) \leq \operatorname{rk}_p(G) = \dim H^*(G). \end{aligned}$$

Remark 3.20. For the cohomology ring to be Cohen-Macaulay it is necessary that all maximal elementary abelian p-subgroups have the same rank. However, the next example shows that it is not sufficient.

Example 3.21. The semidihedral group G of order 16 has depth 1, see example 3.10. A presentation of G is

$$G = \langle\, \sigma, \tau \,|\, \sigma^8 = \tau^2 = 1, \tau\sigma\tau = \sigma^3 \,\rangle.$$

The two maximal elementary abelian 2-subgroups $\langle \sigma^4, \tau \rangle$ and $\langle \sigma^4, \sigma^2\tau \rangle$ both have rank 2. So in this case the depth is strictly less than the minimal rank of a maximal elementary abelian 2-subgroup.

Remember that the minimum

$$\omega_a = \omega_a(G) = \min\{\, \dim H^*(G)/\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Ass} H^*(G)\,\}$$

is an upper bound on the depth. As the following example shows there exists finitely generated graded commutative $\mathbb{F}_p$-algebras such that the depth is strictly less than this minimum.

Example 3.22. Consider the graded polynomial $\mathbb{F}_p$-algebra $\mathbb{F}_p[x, y]$ on two generators x and y of positive even degree. The subring R generated by x^2, x^3, xy, y consists of polynomials in x and y such that the coefficient of the x term is zero. Since R is an integral domain, every element is regular, e.g., the element y. Since $xy \notin (y) \subset R$ and every element in $R/(y)$ of positive degree annihilate xy, it follows that $\operatorname{depth} R = 1$. Since $\mathbb{F}_p[x, y]$ is finitely generated, by x and 1, as a module over R, corollary A.15 gives that $\dim R = \dim \mathbb{F}_p[x, y] = 2$. On the other hand, the only associated prime of R is 0 since R is an integral domain.

However, there is no known example of a cohomology ring where the upper bound ω_a is strict. In [15] Carlson asks if the cohomology ring of a finite group is special in the sense of the following question.

Question 3.23. *Suppose $H^*(G)$ has depth d. Is there an associated prime $\mathfrak{p}$ in $H^*(G)$ such that $\dim H^*(G)/\mathfrak{p} = d$?*

Beside the difficult problem of the actual computation of the depth of the cohomology ring, the question also raises the question of determining the minimum ω_a as well as the associated primes.

We already know that the minimal primes are associated primes and they are of the form $\sqrt{\operatorname{Ker} \operatorname{res}_{G,E}}$ for some maximal elementary abelian p-subgroup of G. It turns out that all the associated primes are of this form. The first step is to prove that the radical of an annihilator ideal is an invariant ideal. We give a slightly modified version of a proof in [18], see proposition 12.7.3. Benson [8] notes that it is a theorem by C. Wilkerson in private correspondence with F. Adams.

Proposition 3.24. *The radical of an annihilator of a homogeneous element x in $H^*(G)$ is invariant, that is, if $I = \operatorname{Ann}_{H^*(G)}(x)$, then $\sqrt{I}$ is an invariant ideal.*

Proof. Clearly, the annihilator of a homogeneous element is a homogeneous ideal. By proposition A.6, $\sqrt{I}$ is also a homogeneous ideal. It remains to prove that $\sqrt{I}$ is closed under the reduced Steenrod operations.

We treat the cases $p = 2$ and p odd simultaneously. Let $\mathcal{P}^i$ denote Sq^i if $p = 2$ and P^i if p odd, and $\mathcal{P}$ denote the total Steenrod operation.

Let y be a homogeneous element in $\sqrt{I}$. Choose n such that $|x| < 2p^n$ and $y^{p^n}x = 0$. Then $\mathcal{P}^{p^n m}(y^{p^n}x) = 0$ for all $m > 0$. By the Cartan formula,

$$\mathcal{P}^{p^n m}(y^{p^n}x) = \sum_{i=0}^{p^n m} \mathcal{P}^{p^n m - i}(y^{p^n})\mathcal{P}^i(x) = 0.$$

Using the Frobenius map,

$$\sum_{i\geq 0} \mathcal{P}^i(y^{p^n}) = \mathcal{P}(y^{p^n}) = \mathcal{P}(y)^{p^n} = (\sum_{i\geq 0}\mathcal{P}^i(y))^{p^n} = \sum_{i\geq 0}\mathcal{P}^i(y)^{p^n}.$$

In particular, the nonzero terms of $\mathcal{P}(y^{p^n})$ occur in degrees divisible by p^n. Note that, if $i = p^n j$, then $|\mathcal{P}^i(y^{p^n})| = |(\mathcal{P}^j(y))^{p^n}| = p^n(|y| + j)$. Comparing degrees gives that

$$\mathcal{P}^i(y^{p^n}) = \begin{cases} 0, & p^n \nmid i \\ \mathcal{P}^j(y)^{p^n}, & i = p^n j. \end{cases}$$

Thus, the equation above becomes

$$\sum_{j=0}^{m} (\mathcal{P}^{m-j}(y))^{p^n}\mathcal{P}^{p^n j}(x) = 0.$$

Since $|x| < 2p^n$, instability gives that $\mathcal{P}^{p^n j}(x) = 0$ unless $j = 0$. Hence,

$$(\mathcal{P}^m(y))^{p^n}(x) = 0$$

for all $m > 0$. In other words, $\sqrt{I}$ is invariant. □

The following characterization of the associated primes was first proved by Duflot [21] for equivariant cohomology and odd primes.

Proposition 3.25. *Any associated prime in $H^*(G)$ is of the form $\sqrt{\operatorname{Ker}\operatorname{res}_{G,E}}$ for some elementary abelian p-subgroup E of G.*

Proof. Suppose $\mathfrak{p}$ is an associated prime of $H^*(G)$. Propositions 3.24 and A.6 gives that $\sqrt{\mathfrak{p}} = \mathfrak{p}$ is invariant. By theorem 2.23, any invariant ideal is of the desired form. This finishes the proof. □

The obvious question is: Which elementary abelian p-subgroups correspond to the associated prime ideals? This is still an open and very interesting question. A more specific question:

Question 3.26. *Is there a group theoretic characterization of the elementary abelian p-subgroups corresponding to the associated primes?*

Remember that $\dim H^*(G)/\sqrt{\operatorname{Ker}\operatorname{res}_{G,E}} = \operatorname{rk}_p(E)$. Positive answers to the previous question and the question about the minimum of the dimensions of quotients by the associated primes would provide a description of the depth solely in terms of the group structure.

A partial answer to the previous question excludes certain elementary abelian p-subgroups and is due to Carlson & Henn [17].

Proposition 3.27. *Let E be an elementary abelian p-subgroup of G. If $\mathfrak{p}_E = \sqrt{\operatorname{Ker}\operatorname{res}_{G,E}}$ is an associated prime, then E contains all central elements of G of order p.*

Proof. Suppose $\mathfrak{p}_E$ is an associated prime and x is a central element of G of order p not contained in E. Clearly, $\langle x\rangle$ is an elementary abelian p-subgroup of G and $\langle x\rangle$ is not conjugate to a subgroup of E since x is central.

Remember that, by lemma 2.10, there exists $\tau_{\langle x\rangle} \in H^*(G)$ such that $\tau_{\langle x\rangle} \notin \mathfrak{p}_{\langle x\rangle}$ and $\tau_{\langle x\rangle} \in \mathfrak{p}_E$. However, since $\operatorname{res}_{G,\langle x\rangle}(\tau_{\langle x\rangle})$ is not nilpotent and $H^*(\langle x\rangle)$ modulo its nilradical is an integral domain, $\operatorname{res}_{G,\langle x\rangle}(\tau_{\langle x\rangle})$ is not a zero divisor. Theorem 3.14 gives that $\tau_{\langle x\rangle}$ is not a zero divisor. In particular, $\tau_{\langle x\rangle}$ is not in any annihilator, that is, $\tau_{\langle x\rangle} \notin \mathfrak{p}_E$, a contradiction. □

Example 3.28. The associated primes of

$$H^*(Q_8;\mathbb{F}_2) = \mathbb{F}_2[x,y,v]/(x^2+xy+y^2, x^2y+xy^2),$$

$|x| = |y| = 1$ and $|v| = 4$: The center of the quaternion group is the only elementary abelian 2-subgroup. The corresponding minimal prime ideal, and associated prime, is $\sqrt{\operatorname{Ker}\operatorname{res}_{Q_8,Z(Q_8)}} = (x,y)$. So (x,y) is the annihilator of a homogeneous element. Actually, $(x,y) = \operatorname{Ann}_{H^*(Q_8;\mathbb{F}_2)}(x^2y)$. See appendix B for some computational details.

The next example shows that even though an elementary abelian p-subgroup contains all elements of order p it need not correspond to an associated prime.

Example 3.29. The associated primes of

$$H^*(D_8;\mathbb{F}_2) = \mathbb{F}_2[x,y,v]/(x(x+y)),$$

$|x| = |y| = 1$ and $|v| = 2$: The dihedral group D_8 has five conjugacy classes of elementary abelian 2-subgroups, see example 2.15. The depth of $H^*(D_8;\mathbb{F}_2)$ is 2, see example 3.6. So none of the cyclic elementary abelian 2-subgroups correspond to associated primes, in particular the center. The kernels of the restriction maps to the two maximal elementary abelian 2-subgroups are the prime ideals (x) and $(x+y)$ and they are equal to their radicals, see proposition A.6. Evidently, $(x) = \operatorname{Ann}_{H^*(D_8;\mathbb{F}_2)}(x+y)$ and $(x+y) = \operatorname{Ann}_{H^*(D_8;\mathbb{F}_2)}(x)$. Thus, both the two maximal elementary abelian 2-subgroups correspond to associated primes.

3.2 Depth and detection

We begin with the concept of detection:

Definition 3.30. *The cohomology $H^*(G)$ of G is said to be detected by a collection $\mathcal{H}$ of subgroups of G if*

$$\bigcap_{H\in\mathcal{H}} \operatorname{Ker}(\operatorname{res}_{G,H}\colon H^*(G) \to H^*(H)) = 0.$$

Remark 3.31. If the collection $\mathcal{H}$ detects the cohomology, the cohomology ring can be studied using the restriction maps. The important property is that the ideal of relations between generators is the intersection of the kernels of the restrictions to the subgroups in the detecting family. In other words, it reduces the computation to finding generators of the cohomology ring and determine their restriction to the subgroups in the detecting collection.

Remark 3.32. Any family of subgroups containing a Sylow p-subgroup or more generally a subgroup with index coprime to p is a detecting collection since the restriction to this subgroup is injective.

Example 3.33. The cohomology $H^*(D_8;\mathbb{F}_2)$ is detected by the two maximal elementary abelian 2-subgroups: The kernels of the restriction maps to the maximal elementary 2-subgroups of D_8 are (x) and $(x+y)$, see example 3.29. The intersection of the kernels is $(x)\cap(x+y)=(x(x+y))$ which is zero in the cohomology ring.

Example 3.34. The quaternion group Q_8 is an example of a group that have no detecting collection consisting of proper subgroups: Recall that

$$H^*(Q_8;\mathbb{F}_2)=\mathbb{F}_2[x,y,v]/(x^2+xy+y^2,x^2y+xy^2)$$

with $|x|=|y|=1$ and $|v|=4$, and that Q_8 has four nontrivial proper subgroups, three are cyclic of order 4 and one cyclic of order 2. Let $\mathbb{Z}/4$ be one of the three cyclic subgroups of order 4. Remember that

$$H^*(\mathbb{Z}/4;\mathbb{F}_2)=\wedge_{\mathbb{F}_2}(x_1)\otimes\mathbb{F}_2[x_2]$$

with $|x_i|=i$. The restriction of x^2 and y^2 is zero. To see this note that $\mathrm{res}_{G,\mathbb{Z}/4}(x)$ and $\mathrm{res}_{G,\mathbb{Z}/4}(y)$ is both either 0 or x_1. In any event, the square of the restrictions of x and y is zero. It follows that the restriction of every element in $H^2(Q_8;\mathbb{F}_2)$ and $H^3(Q_8;\mathbb{F}_2)$ to any of these three subgroups is zero. The restriction of x and y to the sole elementary abelian 2-subgroup of Q_8 is also zero. Summarizing, the restriction of all elements in $H^2(Q_8;\mathbb{F}_2)$ and $H^3(Q_8;\mathbb{F}_2)$ to any proper subgroup of Q_8 is zero.

For a group G set

$$\mathcal{A}_s(G)=\{\,E\in\mathcal{A}(G)\mid \mathrm{rk}_p(E)=s\,\}$$

and

$$\mathcal{H}_s(G)=\{\,C_G(E)\,|\,E\in\mathcal{A}_s(G)\,\}.$$

Example 3.35. The collection $\mathcal{H}_1(G)$ always detects the cohomology of G: Let g be a central element of a Sylow p-subgroup of G. Then $C_G(g)$ contains a Sylow p-subgroup of G. Hence, the restriction to $C_G(g)$ is injective.

Our interest in detection is due to the following theorem by Carlson [15] which, using the transfer map, relates depth, detection on centralizers of elementary abelian p-subgroups and associated primes. From now on this theorem is also referred to as Carlson's theorem.

Theorem 3.36. *Suppose a nonzero element x in $H^*(G)$ restricts to zero on every subgroup in $\mathcal{H}_s(G)$. Then $\dim H^*(G)/\operatorname{Ann}_{H^*(G)}(x) < s$. In particular, there exists an associated prime $\mathfrak{p}$ of $H^*(G)$ such that $\dim H^*(G)/\mathfrak{p} < s$, and $\operatorname{depth} H^*(G) < s$.*

The proof uses a rather technical theorem by Benson [4]:

Theorem 3.37. *Suppose $\mathcal{H}$ is a non empty collection of subgroups of G. Let $\mathcal{K}$ be the collection of all subgroups K of G such that the Sylow p-subgroups of the centralizer $C_G(K)$ are not conjugate to a subgroup of the subgroups in $\mathcal{H}$.*

Let

$$J = \bigoplus_{H\in\mathcal{H}} \operatorname{Im}\operatorname{tr}_{H,G} \text{ and } J' = \bigcap_{K\in\mathcal{K}} \operatorname{Ker}\operatorname{res}_{G,K}.$$

In case $\mathcal{K}$ is empty, the intersection is taken to be the ideal generated by all elements of positive degree in $H^*(G)$. Then $\sqrt{J} = \sqrt{J'}$. In particular, $V(J) = V(J')$.

Remark 3.38. A few notes on the case where $\mathcal{K}$ is empty. If $\mathcal{H}$ contains a subgroup H such that $p \nmid [G : H]$, then $\operatorname{tr}_{H,G}$ is surjective since $\operatorname{tr}_{H,G}\operatorname{res}_{G,H}$ is multiplication by $[G : H]$. Thus, $J = H^*(G)$. On the other hand, suppose $\mathcal{K}$ is empty. In particular, any Sylow p-subgroup of $C_G(\{1\}) = G$ is conjugate to a subgroup of a subgroup in $\mathcal{H}$, i.e., there exists a subgroup of G in $\mathcal{H}$ with index not divisible by p.

Proof of theorem 3.36. Abbreviate $\mathcal{H}_s(G)$ to $\mathcal{H}_s$. Let $J_s = \bigoplus_{H\in\mathcal{H}_s} \operatorname{Im}\operatorname{tr}_{H,G}$ and z be the p-rank of the center of a Sylow p-subgroup of G.

Let $y = \sum_{H\in\mathcal{H}_s} \operatorname{tr}_{H,G}(y_H) \in J_s$, y_H in $H^*(H)$. Since the transfer map is $H^*(G)$-linear via restriction, see proposition 1.1, and $\operatorname{res}_{G,H}(x) = 0$ for all $H \in \mathcal{H}_s$, it follows that

$$\begin{aligned} yx &= \sum_{H\in\mathcal{H}_s} \operatorname{tr}_{H,G}(y_H)x \\ &= \sum_{H\in\mathcal{H}_s} \operatorname{tr}_{H,G}(y_H \operatorname{res}_{G,H}(x)) \\ &= 0. \end{aligned}$$

In other words, $J_s \subset \operatorname{Ann}_{H^*(G)}(x)$. Hence,

$$\dim H^*(G)/\operatorname{Ann}_{H^*(G)}(x) \leq \dim H^*(G)/J_s.$$

To prove the first statement, it remains to show that the dimension of $H^*(G)/J_s$ is less than s.

Let $\mathcal{K}_s$ be the collection of subgroups corresponding to $\mathcal{H}_s$ in theorem 3.37.

Suppose $s \leq z$. Then there exists $E \in \mathcal{A}_s(G)$ such that E is contained in the center of a Sylow p-subgroup of G. It follows that $C_G(E)$ contains a Sylow p-subgroup of G, that is, $[G : C_G(E)]$ is not divisible by p. Hence, J_s is the ideal generated by elements of positive degree, i.e., $\dim H^*(G)/J_s = 0 < s$.

Suppose $s > z$. Then for $E \in \mathcal{A}_s(G)$, the centralizer $C_G(E)$ do not contain a Sylow p-subgroup of G, that is, $[G : C_G(E)]$ is divisible by p.

Let $K \in \mathcal{K}_s$. Suppose $E \subset K$ for some $E \in \mathcal{A}_s(G)$. Then $C_G(E) \supset C_G(K)$, i.e., $C_G(K)$ contains the Sylow p-subgroups of $C_G(K)$ which is a contradiction. Thus, K contains no elementary abelian p-subgroups of rank s. In other words, $\operatorname{rk}_p(K) < s$.

Consider the finite intersection $J'_s = \bigcap_{K \in \mathcal{K}_s} \operatorname{Ker} \operatorname{res}_{G,K}$. Theorem 3.37 implies that $\dim H^*(G)/J_s = \dim H^*(G)/J'_s$. Thus, it suffices to prove that the dimension of $H^*(G)/J'_s$ is less than s.

As always, $H^*(K)$ is finitely generated as a module over $H^*(G)$ via restriction, and corollary A.15 implies that

$$\dim H^*(G)/\operatorname{Ker} \operatorname{res}_{G,K} = \dim H^*(K).$$

An application of proposition A.12 gives that

$$\dim H^*(G)/J'_s = \max_{K \in \mathcal{K}_s} \{ \dim H^*(K) \} = \max_{K \in \mathcal{K}_s} \{ \operatorname{rk}_p(K) \} < s.$$

This proves the first statement of the theorem.

By proposition A.8, maximal annihilators are associated primes. Thus, there exists an associated prime $\mathfrak{p}$ containing $\operatorname{Ann}_{H^*(G)}(x)$, i.e., $\dim H^*(G)/\mathfrak{p} < s$ and $\operatorname{depth} H^*(G) < s$. □

The next corollary is just another formulation of Carlson's theorem but is included for emphasis.

Corollary 3.39. *Suppose $\omega_a \geq s$. Then $H^*(G)$ is detected by $\mathcal{H}_s(G)$. In particular, if* $\operatorname{depth} H^*(G) \geq s$, *then $H^*(G)$ is detected by $\mathcal{H}_s(G)$.*

The following corollary, also due to Carlson, explains in some cases using group theoretic terms why the cohomology rings are not Cohen-Macaulay.

Corollary 3.40. *Suppose G is a p-group and G has a proper subgroup H such that $C_G(E) \subset H$ for all $E \in \mathcal{A}_s(G)$. Then* $\operatorname{depth} H^*(G) < s$.

Proof. We may assume H is a maximal subgroup. Any maximal subgroup of a p-group is normal and has index p, see e.g. [42] theorem 4.4.6. Thus, H is the kernel of a homomorphism $x \in \operatorname{Hom}(G, \mathbb{Z}/p) = H^1(G)$. In particular, $\operatorname{res}_{G,H}(x) = 0$, i.e., $\operatorname{res}_{G,C_G(E)}(x) = 0$ for all $E \in \mathcal{A}_s(G)$. Applying theorem 3.36 finishes the proof. □

Example 3.41. Consider the semidihedral group G of order 16 discussed in examples 3.10 and 3.21. Recall that $H^*(G)$ has depth 1 and dimension 2. A presentation of G is $\langle\, \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \tau\sigma\tau = \sigma^3 \,\rangle$. The two maximal elementary abelian 2-subgroups $\langle \sigma^4, \tau\rangle$ and $\langle \sigma^4, \sigma^2\tau\rangle$ are conjugated ($\sigma^3\langle\sigma^4, \tau\rangle\sigma^5 = \langle\sigma^4, \sigma^2\tau\rangle$), both have rank 2 and are self centralizing. Moreover, they are contained in the proper subgroup $\langle\sigma^2, \tau\rangle$. So corollary 3.40 explains (using only the group structure) why in this case the depth is strictly less than the dimension.

The following lemma is straightforward but is stated for emphasis.

Lemma 3.42. *Suppose $H^*(G)$ is not detected by $\mathcal{H}_s(G)$. Then $H^*(G)$ is not detected by $\mathcal{H}_t(G)$ for all $t \geq s$.*

Proof. Let E be an elementary abelian p-subgroup of G with $\mathrm{rk}_p(E) = t > s$, and E' an elementary abelian p-subgroup of rank s of G contained in E. Since $C_G(E) \subset C_G(E') \subset G$, the kernel of $\mathrm{res}_{G,C_G(E')}$ is contained in the kernel of $\mathrm{res}_{G,C_G(E)}$. Thus,

$$0 \neq \bigcap_{E' \in \mathcal{A}_s(G)} \mathrm{Ker}\,\mathrm{res}_{G,C_G(E')} \subset \bigcap_{E \in \mathcal{A}_t(G)} \mathrm{Ker}\,\mathrm{res}_{G,C_G(E)},$$

that is, $H^*(G)$ is not detected by $\mathcal{H}_t(G)$ for all $t \geq s$. □

In example 3.35 we saw that $H^*(G)$ is always detected by the collection $\mathcal{H}_1(G)$. So the maximum

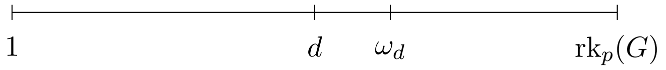
$$\omega_d = \omega_d(G) = \max\{\, s \mid H^*(G) \text{ is detected by } \mathcal{H}_s(G) \,\}$$

is a well defined integer between 1 and $\mathrm{rk}_p(G)$. By the previous lemma, $H^*(G)$ is detected by $\mathcal{H}_t(G)$ for all t less than or equal to the maximum. A consequence of corollary 3.39 is that $\omega_d \geq \omega_a$ and in particular ω_d is an upper bound of the depth of $H^*(G)$.

Perhaps more illustratively, if d denotes the depth of $H^*(G)$, then in the figure below we have that the product of the restriction maps,

$$H^*(G) \to \prod_{E \in \mathcal{A}_s(G)} H^*(C_G(E)),$$

is injective for $1 \leq s \leq \omega_d$ and not injective for $\omega_d < s \leq \mathrm{rk}_p(G)$.



Observe that if $H^*(G)$ is Cohen-Macaulay, then ω_d is equal to both the depth and dimension. More generally, there are no known examples where ω_d is strictly greater that the depth. In [15] Carlson raises the question:

Question 3.43. *Suppose $H^*(G)$ is detected by the centralizers of the elementary abelian subgroups of rank s. Is* depth $H^*(G) \geq s$*?*

In other words, is ω_d always equal to the depth of $H^*(G)$? Or equivalently, if the depth of $H^*(G)$ is d and $H^*(G)$ is not Cohen-Macaulay, is $H^*(G)$ not detected by $\mathcal{H}_{d+1}(G)$? As noted above, $\omega_d \geq \omega_a$ so an affirmative answer to the previous question implies an affirmative answer to question 3.23. We return to the relationship between these questions in the next section.

We end this section with an alternative proof of Carlson's theorem. Carlson [15] states that Henn has pointed out that theorem 3.36 may be proved using methods from the theory of unstable modules over the Steenrod algebra. More specifically, by using results from [29]. Since such a proof has never been published we provide one here.

For $n > 0$, let $(H^*(G))^{<n}$ denote the quotient of $H^*(G)$ by the ideal $H^{\geq n}(G) = \bigoplus_{m \geq n} H^m(G)$ generated by the homogeneous elements of degree greater than or equal to n.

The alternative proof uses the following technical lemma by the author.

Lemma 3.44. *Let C be a central subgroup of G. For any positive integer n, $H^*(C) \otimes (H^*(G))^{<n}$ is integral over $H^*(G)$ via the map induced by $\Delta\colon H^*(G) \to H^*(C) \otimes H^*(G)$.*

Proof. The elements in $H^*(C) \otimes (H^*(G))^{<n}$ which are integral over $H^*(G)$ constitute a subring, see theorem A.13, i.e., it suffices to prove that any homogeneous element $x \otimes y$ is integral.

Suppose $|y| > 0$. Since

$$(x \otimes y)^n = \pm x^n \otimes y^n = \pm x^n \otimes 0 = 0,$$

$x \otimes y$ is integral.

Suppose $|y| = 0$. Then we may assume $y = 1$. Recall that $H^*(C)$ is finitely generated as a $H^*(G)$-module via restriction. In particular, $H^*(C)$ is integral over $H^*(G)$. Thus, x is a root of a monic polynomial f with coefficients in $H^*(G)$, i.e., there exists $c_1, \ldots, c_m \in H^*(G)$ such that

$$f(x) = x^m + \operatorname{res}_{G,C}(c_1)x^{m-1} + \cdots \operatorname{res}_{G,C}(c_{m-1})x + \operatorname{res}_{G,C}(c_m) = 0.$$

Suppose $|c_i| > 0$ for all $1 \leq i \leq m$. Recall that

$$\Delta(c_i) = \operatorname{res}_{G,C}(c_i) \otimes 1 + r_i,$$

where $r_i = 1 \otimes c_i + \sum_j c'_{i,j} \otimes c''_{i,j}$, $|c'_{i,j}|, |c''_{i,j}| > 0$. Notice that r_i is nilpotent, being a sum of nilpotent elements.

Now,

$$\begin{aligned}(x\otimes 1)^m+\sum_{1\le i\le m}\Delta(c_i)(x\otimes 1)^{m-i} &= (x^m\otimes 1)+\sum_{1\le i\le m}\Delta(c_i)(x^{m-i}\otimes 1)\\ &= (x^m\otimes 1)+\sum_{1\le i\le m}(\operatorname{res}_{G,C}(c_i)\otimes 1+r_i)(x^{m-i}\otimes 1)\\ &= f(x)\otimes 1+\sum_{1\le i\le m} r_i(x^{m-i}\otimes 1)\\ &= \sum_{1\le i\le m} r_i(x^{m-i}\otimes 1).\end{aligned}$$

Since r_i is nilpotent, this is an element in the nilradical of $H^*(C)\otimes(H^*(G))^{<n}$, that is,

$$((x\otimes 1)^m+\sum_{1\le i\le m}\Delta(c_i)(x\otimes 1)^{m-i})^l=0$$

for l sufficiently large. In other words, $x\otimes 1$ is integral.

The case where $|c_i|=0$ for at least one i is straightforward, use that Δ and $\operatorname{res}_{G,C}$ both are the identity on $\mathbb{F}_p=H^0(G)=H^0(C)\otimes H^0(G)=H^0(C\times G)$. The details are left to the reader. □

Remark 3.45. An obvious question is, does a more general result hold, for example is $H^*(C)\otimes H^*(G)$ finitely generated as a module over $H^*(G)$ via Δ? However, this is not true in general. Consider the cyclic group $\mathbb{Z}/2$ of order two. The kernel of the group multiplication map $\mu\colon \mathbb{Z}/2\times\mathbb{Z}/2\to\mathbb{Z}/2$ has order two. By [38] corollary 2.4, $H^*(\mathbb{Z}/2)\otimes H^*(\mathbb{Z}/2)$ is not finitely generated as a module over $H^*(\mathbb{Z}/2)$ via Δ. It is unknown to the author whether or not $H^*(C)\otimes(H^*(G))^{<n}$ is finitely generated as a module over $H^*(G)$ via Δ.

The main tool in the alternative proof of Carlson's theorem is the following theorem by Henn, Lannes & Schwartz [29], see corollary 5.6.

Theorem 3.46. *For n sufficiently large, the map*

$$\lambda_n\colon H^*(G)\to\prod_{E\in\mathcal{A}(G)}H^*(E)\otimes(H^*(C_G(E)))^{<n}$$

induced by the maps $E\times C_G(E)\to G$, $(e,g)\mapsto eg$, is injective.

Now, we are ready to reprove Carlson's theorem. For convenience, we restate the essential part of the theorem.

Theorem 3.47. *Suppose a nonzero element x in $H^*(G)$ restricts to zero on every subgroup in $\mathcal{H}_s(G)$. Then $\dim H^*(G)/\operatorname{Ann}_{H^*(G)}(x)<s$.*

Proof. Choose n sufficiently large such that the map

$$\lambda_n \colon H^*(G) \to \prod_{E \in \mathcal{A}(G)} H^*(E) \otimes (H^*(C_G(E)))^{<n}$$

from theorem 3.46 is injective. Notice that λ_n is induced by the product of the composites

$$\Delta \operatorname{res}_{G, C_G(E)} \colon H^*(G) \to H^*(C_G(E)) \to H^*(E) \otimes H^*(C_G(E))$$

for $E \in \mathcal{A}(G)$. In particular, λ_n factors through the product of the restriction maps

$$H^*(G) \to \prod_{E \in \mathcal{A}(G)} H^*(C_G(E)).$$

Consider the maps

$$\lambda'_n \colon H^*(G) \to \prod_{E \in \mathcal{A}_t(G),\, t<s} H^*(E) \otimes (H^*(C_G(E)))^{<n}$$

and

$$\lambda''_n \colon H^*(G) \to \prod_{E \in \mathcal{A}_t(G),\, t \geq s} H^*(E) \otimes (H^*(C_G(E)))^{<n}$$

both given by λ_n, that is, λ_n is the product of λ'_n and λ''_n.

Recall that if x restricts to zero on every subgroup in $\mathcal{H}_s(G)$, then x restricts to zero on every subgroup in $\mathcal{H}_t(G)$, $t \geq s$, see lemma 3.42.

Consequently, the principal ideal (x) is contained in the kernel of λ''_n. Furthermore, since any nonzero element in $(x) \cap \operatorname{Ker} \lambda'_n$ is in the kernel of λ_n, it follows that λ'_n is injective on (x).

Multiplication by x is a homomorphism $H^*(G) \to H^*(G)$ with image (x) and kernel $\operatorname{Ann}_{H^*(G)}(x)$. The reader concerned with the sign issues involved in multiplication by an element being a homomorphism is referred to remark A.21. In any event, $H^*(G)/\operatorname{Ann}_{H^*(G)}(x)$ and (x) are isomorphic as $H^*(G)$-modules.

Consider

$$\prod_{E \in \mathcal{A}_t(G),\, t<s} H^*(E) \otimes (H^*(C_G(E)))^{<n}$$

as a $H^*(G)$-module via λ'_n.

Now,

$$\begin{aligned} \dim H^*(G)/\operatorname{Ann}_{H^*(G)}(x) &= \dim_{H^*(G)} H^*(G)/\operatorname{Ann}_{H^*(G)}(x) \\ &= \dim_{H^*(G)} (x) \\ &\leq \dim_{H^*(G)} \prod_{E \in \mathcal{A}_t(G),\, t<s} H^*(E) \otimes (H^*(C_G(E)))^{<n} \\ &\leq \dim \operatorname{Im} \lambda'_n. \end{aligned}$$

The first equality follows from proposition A.12. The second equality above follows from the fact that the $H^*(G)$-modules are isomorphic. The first inequality follows since the restriction of λ'_n to (x) is injective. More specifically, injectivity of λ'_n implies that

$$I = \operatorname{Ann}_{H^*(G)} \prod_{E\in\mathcal{A}_t(G),\, t<s} H^*(E) \otimes (H^*(C_G(E)))^{<n} \subset \operatorname{Ann}_{H^*(G)}(x),$$

i.e., $\dim H^*(G)/\operatorname{Ann}_{H^*(G)}(x) \leq \dim H^*(G)/I$. The second inequality follows from the fact that $\dim \operatorname{Im} \lambda'_n$ is an upper bound of the dimension of any module over $\operatorname{Im} \lambda'_n$, see proposition A.12.

Combining that $H^*(C_G(E))$ is finitely generated as a module over $H^*(G)$ via restriction with lemma 3.44 gives that

$$\operatorname{Im} \lambda'_n \subset \prod_{E\in\mathcal{A}_t(G),\, t<s} H^*(E) \otimes (H^*(C_G(E)))^{<n}$$

is an integral extension. Thus,

$$\begin{aligned}\dim \operatorname{Im} \lambda'_n &= \dim \prod_{E\in\mathcal{A}_t(G),\, t<s} H^*(E) \otimes (H^*(C_G(E)))^{<n} \\ &= \max\{ \dim H^*(E) \otimes (H^*(C_G(E)))^{<n} \mid E \in \mathcal{A}_t(G), t < s \} \\ &= \max\{ \dim H^*(E) \mid E \in \mathcal{A}_t(G),\, t < s \} < s.\end{aligned}$$

The first equality is corollary A.15. The second follows from the structure of prime ideals in a product of rings, see the proof of corollary 2.5. The third follows from the fact that $H^*(E) \otimes (H^+(G)/H^{\geq n}(G))$ is a nilpotent ideal in $H^*(E) \otimes (H^*(C_G(E)))^{<n}$ and proposition A.12.

This finishes the proof of the theorem. □

3.3 Carlson's depth conjecture

Carlson's depth conjecture is affirmative answers to the questions 3.23 and 3.43:

Carlson's depth conjecture. *Let G be a finite group. Suppose the depth of $H^*(G)$ is d. Then*

(1) there exists $\mathfrak{p} \in \operatorname{Ass} H^*(G)$ such that $\dim H^*(G)/\mathfrak{p} = d$, and

(2) if $H^*(G)$ is detected $\mathcal{H}_s(G)$, then $d \geq s$.

In other words, the numbers

$$\omega_a = \min\{ \dim H^*(G)/\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Ass} H^*(G) \}$$

and

$$\omega_d = \max\{ s \mid H^*(G) \text{ is detected by } \mathcal{H}_s(G) \}$$

are both equal to d.

In fact, the two statements of the conjecture are equivalent, a fact that the author has not been able to find explicitly stated in the literature. However, it is an immediate consequence of the following result due to Carlson [15]. There are a few small misleading errors/typos in the proof which have been corrected in the given proof.

Proposition 3.48. *Suppose* $\dim H^*(G)/\operatorname{Ann}_{H^*(G)}(x) = d$ *for* $x \in H^*(G)$. *Then* x *restricts to zero on every subgroup in* $\mathcal{H}_s(G)$, $s > d$.

Proof. Suppose $\operatorname{res}_{G,C_G(E)}(x) \neq 0$ and $\operatorname{rk}(E) > d$. Let $I = \operatorname{Ann}_{H^*(G)}(x)$, and $J = \operatorname{Ann}_{H^*(C_G(E))}(\operatorname{res}_{G,C_G(E)}(x))$. Note that $I \subset \operatorname{res}^{-1}_{G,C_G(E)}(J)$.

The restriction map $\operatorname{res}_{G,C_G(E)} \colon H^*(G) \to H^*(C_G(E))$ induces an isomorphism

$$\varphi\colon H^*(G)/\operatorname{res}^{-1}_{G,C_G(E)}(J) \to \operatorname{res}_{G,C_G(E)} H^*(G)/(J \cap \operatorname{res}_{G,C_G(E)} H^*(G)),$$

where $\varphi([y]) = [\operatorname{res}_{G,C_G(E)}(y)]$. As usual, $H^*(C_G(E))$ is finitely generated as a module over $H^*(G)$ via restriction. Corollary A.15 gives that

$$\begin{aligned}\dim H^*(G)/\operatorname{res}^{-1}_{G,C_G(E)}(J) &= \dim \operatorname{res}_{G,C_G(E)} H^*(G)/(J \cap \operatorname{res}_{G,C_G(E)} H^*(G)) \\ &= \dim H^*(C_G(E))/J.\end{aligned}$$

Consequently,

$$d = \dim H^*(G)/I \geq \dim H^*(G)/\operatorname{res}^{-1}_{G,C_G(E)}(J) = \dim H^*(C_G(E))/J.$$

Since maximal annihilators are associated primes, it follows that $H^*(C_G(E))$ has an associated prime $\mathfrak{p}$ such that $\dim H^*(C_G(E))/\mathfrak{p} \leq d$. In particular, $\operatorname{depth} H^*(C_G(E)) \leq d$. But, by Duflot's theorem,

$$\operatorname{depth} H^*(C_G(E)) \geq \operatorname{rk}_p(E) > d,$$

which is a contradiction. This finishes the proof. □

Corollary 3.49. *The numbers* ω_a *and* ω_d *are equal.*

Proof. Recall that $\omega_a \leq \omega_d$ by Carlson's theorem. The previous proposition implies the reverse inequality. □

Thus, to prove Carlson's depth conjecture it suffices to prove either statement.

The trivial case is when the cohomology ring is Cohen-Macaulay, e.g., all abelian groups or more generally groups with abelian Sylow p-subgroups. A classic family of finite groups is the general linear groups $\mathrm{GL}_n(\mathbb{F}_q)$, where $\mathbb{F}_q$ is a finite field with q elements. The calculation of $H^*(\mathrm{GL}_n(\mathbb{F}_q); \mathbb{F}_p)$, where p does not divide q, is due to Quillen [39], see also [2] section VII.4. The cohomology ring is the tensor product of a polynomial algebra and an exterior algebra. In particular, it is Cohen-Macaulay.

The next theorem, see [15] proposition 3.2, establishes the conjecture for all groups of p-rank at most 2.

Theorem 3.50. *Suppose G has p-rank 2. Then the depth of $H^*(G)$ is 2 if and only if the dimension of $H^*(G)/\mathfrak{p}$ is 2 for all $\mathfrak{p} \in \operatorname{Ass} H^*(G)$.*

Green [27] settled the conjecture in the special case where G is a p-group and $\operatorname{depth} H^*(G) = \operatorname{rk}_p(Z(G))$. Using computer calculations, Carlson [14] has verified the conjecture for all the 340 2-groups of order dividing 64. These examples are what led Carlson to ask the questions about depth, detection and associated primes. Green [26] has also computed the cohomology rings of some small p-groups. It is not explicitly stated in the computations by Green that the conjecture has been verified for these groups. However, using the results above and the computer computations, the author has checked that this is indeed the case.

Due to the computational issues in determining the cohomology ring of a finite group, it is in general not easy for a specific group to check the conjecture hence the evidence of interesting (not Cohen-Macaulay) cases is not overwhelming. However, given a group it is sometimes possible to use information about subgroups and their cohomology rings, e.g., Sylow p-subgroups or normal subgroups of index coprime to p, to get information about the cohomology ring of the group. For example, if the depth of a Sylow p-subgroup P of G is d and is equal to $\operatorname{mrk}_p(G)$, then the depth of $H^*(G)$ is equal to d, and G satisfies the conjecture.

Appendix C describes a program written in Magma with functions that given a group try to determine the depth of the cohomology ring and/or if the group satisfies the conjecture using information about the subgroups. The program uses theoretical results and the calculations by Carlson and Green. If the reader is interested in investigating some small groups, the appendix also contains a table of the 69 groups out of the 3775 nonabelian groups of order strictly less that 256 and not a power of 2 for which the program can not determine whether or not they satisfy the conjecture for $p = 2$.

In the next section we add more groups to the list of examples of groups without Cohen-Macaulay cohomology rings. We end this section with another intriguing question, also asked by Carlson [15]:

Question 3.51. *Suppose H is a subgroup of G. Is*

$$\operatorname{depth} \operatorname{res}_{G,H} H^*(G) \geq \operatorname{depth} H^*(H)?$$

The mod 2 cohomology of Mathieu group M_{11} and its Sylow 2-subgroup is an example where the inequality is strict since the restriction to any Sylow p-subgroup is injective, see example 3.10. The next theorem also due to Carlson shows that an affirmative answer to the previous question implies Carlson's depth conjecture.

Theorem 3.52. *Let s, $1 \leq s \leq \operatorname{rk}_p(G)$, be a fixed integer. Suppose*

$$\operatorname{depth} \operatorname{res}_{G,C_G(E)} H^*(G) \geq \operatorname{depth} H^*(C_G(E))$$

for all $E \in \mathcal{A}_s(G)$ and $H^*(G)$ is detected by the collection $\mathcal{H}_s(G)$. Then $\operatorname{depth} H^*(G) \geq s$.

Proof. By Duflot's theorem,

$$\operatorname{depth} \operatorname{res}_{G,C_G(E)} H^*(G) \geq \operatorname{depth} H^*(C_G(E)) \geq s.$$

By theorem A.24, any regular sequence can be extended to a regular sequence of maximal length. Therefore it suffices to prove that for any regular sequence $x_1, \dots, x_r$, $0 \leq r < s$, in $H^*(G)$ there exists an $H^*(G)/(x_1, \dots, x_r)$-regular element x_{r+1} in $H^*(G)$ with the usual convention that $(\emptyset) = 0$. Let $H(r)$ denote $H^*(G)/(x_1, \dots, x_r)$.

Suppose $\operatorname{res}_{G,C_G(E)}(x_{r+1}) \in \operatorname{res}_{G,C_G(E)} H^*(C_G(E))$ is a regular element of

$$H(E,r) = \operatorname{res}_{G,C_G(E)} H^*(G)/(\operatorname{res}_{G,C_G(E)}(x_1), \dots, \operatorname{res}_{G,C_G(E)}(x_r))$$

for all $E \in \mathcal{A}_s(G)$. The restriction maps $\operatorname{res}_{G,C_G(E)} \colon H^*(G) \to H^*(C_G(E))$ induce maps

$$\varphi_{E,r} \colon H(r) \to H(E,r),$$

where $\varphi_{E,r}([x]) = [\operatorname{res}_{G,C_G(E)}(x)]$. The product of these maps,

$$\prod \varphi_{E,r} \colon H(r) \to \prod_{E \in \mathcal{A}_s(G)} H(E,r),$$

is injective since $\operatorname{res}_{G,C_G(E)}((x_1, \dots, x_r)) = (\operatorname{res}_{G,C_G(E)}(x_1), \dots, \operatorname{res}_{G,C_G(E)}(x_n))$ as ideals in $\operatorname{res}_{G,C_G(E)} H^*(G)$. Moreover, the diagram

$$\begin{tikzcd}
H^*(G)/(x_1, \dots, x_r) = H(r) \arrow[r, "\prod \varphi_{E,r}"] \arrow[d, "\cdot x_{r+1}"] & \prod_{E \in \mathcal{A}_s(G)} H(E,r) \arrow[d, "\cdot \prod \operatorname{res}_{G,C_G(E)}(x_{r+1})"] \\
H^*(G)/(x_1, \dots, x_r) = H(r) \arrow[r, "\prod \varphi_{E,r}"] & \prod_{E \in \mathcal{A}_s(G)} H(E,r)
\end{tikzcd}$$

commutes. It follows that x_{r+1} is an $H(r)$-regular element. Hence, it suffices to choose x_{r+1} such that $\operatorname{res}_{G,C_G(E)}(x_{r+1})$ is an $H(E,r)$-regular element for all $E \in \mathcal{A}_s(G)$.

Let $\operatorname{Ass} H(E,r)$ denote the associated primes of $H(E,r)$ as a module over $\operatorname{res}_{G,C_G(E)} H^*(G)$ and let

$$\operatorname{Ass}(r) = \bigcup_{E \in \mathcal{A}_s(G)} \operatorname{Ass} H(E,r).$$

Recall that $\operatorname{Ass} H(E,r)$ is a finite set since $H(E,r)$ is finitely generated as a module over $\operatorname{res}_{G,C_G(E)} H^*(G)$, see proposition A.8. In particular, $\operatorname{Ass}(r)$ is a finite set.

Since the zero divisors of $H(E,r)$ are the union of the associated primes, see proposition A.8, it suffices to choose x_{r+1} such that

$$\operatorname{res}_{G,C_G(E)}(x_{r+1}) \notin \bigcup_{\mathfrak{p}\in \operatorname{Ass}(r)} \mathfrak{p},$$

or equivalently, to choose x_{r+1} such that

$$x_{r+1} \notin \bigcup_{\mathfrak{p}\in \operatorname{Ass}(r)} \operatorname{res}^{-1}_{G,C_G(E)}(\mathfrak{p}).$$

Suppose

$$\bigcup_{\mathfrak{p}\in \operatorname{Ass}(r)} \operatorname{res}^{-1}_{G,C_G(E)}(\mathfrak{p}) = H^+(G),$$

where $H^+(G)$ is the ideal generated by all elements of positive degree. Then lemma A.25 gives that $H^+(G) = \operatorname{res}^{-1}_{G,C_G(E)}(\mathfrak{p})$ for some $\mathfrak{p} \in \operatorname{Ass}(r)$.

Let $\mathfrak{q} \in \operatorname{Ass} H(E,r)$. Using proposition A.33 and proposition A.36,

$$\begin{aligned}\dim H^*(G)/\operatorname{res}^{-1}_{G,C_G(E)}(\mathfrak{q}) &= \dim \operatorname{res}_{G,C_G(E)} H^*(G)/\mathfrak{q} \\ &\geq \operatorname{depth}_{\operatorname{res}_{G,C_G(E)} H^*(G)} H(E,r) \\ &= \operatorname{depth} \operatorname{res}_{G,C_G(E)} H^*(G) - r \\ &\geq s - r > 0.\end{aligned}$$

In particular,

$$\dim H^*(G)/H^+(G) = 0 < \dim H^*(G)/\operatorname{res}^{-1}_{G,C_G(E)}(\mathfrak{p}).$$

Consequently, $H^+(G) \neq \operatorname{res}^{-1}_{G,C_G(E)}(\mathfrak{p})$, i.e., $H^+(G)$ contains an $H(r)$-regular element. □

4 The symmetric and alternating groups

Carlson & Henn [16] determined the depths of the mod p cohomology rings of the symmetric groups and verified Carlson's depth conjecture for these groups. In this section we exploit their results to compute the depths of the cohomology rings of some of the alternating groups and establish the conjecture in these cases. For p odd, we get a complete picture. In the case $p = 2$, the conjecture is verified for "half" of the alternating groups. The remaining cases seem more difficult. The results rely on properties of the Sylow p-subgroups and the ranks of maximal elementary abelian p-subgroups. In addition, we verify the conjecture for the wreath products $\mathbb{Z}/p \wr S_n$, and give some p-fusion properties of the symmetric and the alternating groups.

As usual, p denotes a fixed prime and we only consider mod p cohomology. A few words on the notation. In general, we use standard notation. The symmetric (alternating) group on a finite set Ω is denoted S_Ω (A_Ω). More concretely, the symmetric (alternating) group on the set $\{1, \dots, n\}$ is denoted S_n (A_n). Entries in cycles are separated by commas, e.g., $(1, 2, 3, 4) \in S_4$.

4.1 Sylow p-subgroups of the symmetric groups

The Sylow p-subgroups of the symmetric groups are well known, see e.g. [41]. We begin by determining the order of a Sylow p-subgroup of S_n:

Lemma 4.1. *Let $n = b_0 + b_1 p + \cdots b_m p^m$ be the p-adic expansion of n. The largest power of p dividing $n!$ is*

$$\frac{n - \sum_{i=0}^m b_i}{p-1}.$$

Proof. The number of the integers $1, \dots, n$ divisible by p is $[n/p]$, the number of integers divisible by p^2 is $[n/p^2]$ et cetera. So the largest power of p dividing $n!$ is $[n/p] + [n/p^2] + \cdots [n/p^m]$. Now, if $n = \sum_{i=0}^m b_i p^i$, then $[n/p^j] = \sum_{i=j}^m b_i p^{i-j}$. Hence,

$$\begin{aligned}
[n/p] + [n/p^2] + \cdots [n/p^m] &= \sum_{j=1}^m \sum_{i=j}^m b_i p^{i-j} \\
&= \sum_{i=1}^m b_i (p^{i-1} + \cdots + p + 1) \\
&= \sum_{i=1}^m b_i \frac{p^i - 1}{p-1} \\
&= \frac{n - \sum_{i=0}^m b_i}{p-1}.
\end{aligned}$$

□

To describe the Sylow p-subgroups of the symmetric groups we need the wreath product construction: Let G be a subgroup of the symmetric group S_n and H a subgroup of S_m, both H and G are assumed nontrivial. Then G acts on the product H^n by permutation of tuples. More concretely, define a homomorphism $\varphi\colon G \to \operatorname{Aut}(H^n)$ by

$$\varphi(g)(h_1, \dots, h_n) = (h_{g^{-1}(1)}, \dots, h_{g^{-1}(n)})$$

for $(h_1, \dots, h_n) \in H^n$. It is straightforward to verify that φ is indeed a homomorphism. The wreath product $H \wr G$ of H and G is the semidirect product $H^n \rtimes_\varphi G$. More specifically, $H \wr G$ is the set $H^n \times G$ with multiplication

$$(h_1, \dots, h_n, g)(h'_1, \dots, h'_n, g') = (h_1 h'_{g^{-1}(1)}, \dots, h_n h'_{g^{-1}(n)}, gg').$$

Notice that $|H \wr G| = |H|^n |G|$.

Let $\Lambda = \{1, \dots, m\}$ and $\Omega = \{1, \dots, n\}$. An element $\sigma = (h_1, \dots, h_n, g)$ in $H \wr G$ may be considered as a permutation of the set $\Lambda \times \Omega$ via

$$\sigma(i, j) = (h_j(i), g^{-1}(j))$$

for $(i, j) \in \Lambda \times \Omega$. Consider $\Lambda \times \Omega$ as the ordered set

$$\{\underbrace{\underbrace{(1,1), (2,1), \dots (m,1)}_{m}, \underbrace{(1,2), \dots, (m,2)}_{m}, \dots, \underbrace{(1,n), (2,n), \dots, (m,n)}_{m}}_{n}\},$$

i.e., $\Lambda \times \Omega$ is ordered using a reverse lexicographic order. Consequently, we may consider $H \wr G$ as a subgroup of S_{mn}. Whenever we say $H \wr G$ is a subgroup of a symmetric group we mean via this identification. The next example illustrates the identification.

Example 4.2. Let $G = H = S_2 = \mathbb{Z}/2 = \langle \tau \rangle$ where τ is the nontrivial permutation $(1, 2)$ in S_2. Consider the element $\sigma = (\tau, \tau, 1)$ in $\mathbb{Z}/2 \wr \mathbb{Z}/2$. We compute the corresponding element in S_4 as a permutation of the ordered set $\{(1,1), (2,1), (1,2), (2,2)\}$:

$$\sigma(1,1) = (2,1), \sigma(2,1) = (1,1), \sigma(1,2) = (2,2), \sigma(2,2) = (1,2),$$

i.e., as an element in S_4, σ is the permutation $(1,2)(3,4)$.

Example 4.3. The wreath product $\mathbb{Z}/2 \wr \mathbb{Z}/2$ is isomorphic to the dihedral group of order 8: It is easily verified that $x = (\tau, 1, \tau)$ and $y = (1, \tau, 1)$ generate $\mathbb{Z}/2 \wr \mathbb{Z}/2$ and satisfy the relations $x^4 = y^2 = 1$ and $yxy = x^{-1}$, i.e., $\mathbb{Z}/2 \wr \mathbb{Z}/2$ is the dihedral group of order 8.

Next, we describe the Sylow 2-subgroups of S_{2^n}. Set $W_1 = \mathbb{Z}/2$ and $W_{n+1} = W_n \wr \mathbb{Z}/2$ for $n > 1$. Iteration gives that W_n is a subgroup of S_{2^n}. An easy induction shows that W_n has order $2^{(2^n-1)}$. By lemma 4.1, this is exactly the order of a Sylow 2-subgroup of S_{2^n}. It follows that W_n is a Sylow 2-subgroup of S_{2^n}.

Let $n = 2^{n_1} + \cdots + 2^{n_m}$, $0 \leq n_1 < \cdots < n_m$, be the 2-adic expansion of n. A natural way to view $S_{n_1} \times \cdots \times S_{n_m}$ as a subgroup of S_n is to view S_{n_i} as the subgroup of S_n of permutations which only permutes the subset

$$\{n_1 + \cdots + n_{i-1} + 1, \ldots, n_1 + \cdots + n_i\} \subset \{1, \ldots, n\}.$$

In particular, this gives an embedding of $W_{n_1} \times \cdots \times W_{n_m}$ into S_n. Note that

$$|W_{n_1} \times \cdots \times W_{n_m}| = 2^{2^{n_1}-1} \cdots 2^{2^{n_m}-1} = 2^{2^{n_1}+\cdots+2^{n_m}-m} = 2^{n-m}.$$

By lemma 4.1, the order of a Sylow 2-subgroup of S_n is 2^{n-m}. It follows that $W_{n_1} \times \cdots \times W_{n_m}$ is a Sylow 2-subgroup of S_n.

Let p be an odd prime and $W_1 = \mathbb{Z}/p$ the subgroup of S_p generated by the p-cycle $(1, \ldots, p)$, and $W_{n+1} = W_n \wr \mathbb{Z}/p$ for $n > 1$. Using lemma 4.1, W_n is a Sylow p-subgroup of S_{p^n}. Let $n = b_0 + b_1 p + \cdots + b_m p^m$ be the p-adic expansion of n. As above, consider

$$\underbrace{S_1 \times \cdots \times S_1}_{b_0} \times \underbrace{S_p \times \cdots \times S_p}_{b_1} \times \cdots \times \underbrace{S_{p^m} \times \cdots \times S_{p^m}}_{b_m}$$

as a subgroup of S_n in the natural way. Again, using lemma 4.1, $W_1^{b_1} \times \cdots \times W_m^{b_m}$ has the order of a Sylow p-subgroup of S_n, i.e., it is a Sylow p-subgroup.

Summarizing, we have proved the following theorem. The essential case where n is a prime power is originally due to Kaloujnine [30].

Theorem 4.4. *Let $n = b_0 + b_1 p + \cdots + b_m p^m$ be the p-adic expansion of n. Then the product $W_1^{b_1} \times \cdots \times W_m^{b_m}$ of iterated wreath products is (isomorphic to) a Sylow p-subgroup of S_n.*

Remark 4.5. If $p \nmid n + 1$, then a Sylow p-subgroup of S_n (or A_n) is a Sylow p-subgroup of S_{n+1} (or A_{n+1}). Moreover, since A_n has index 2 in S_n, a Sylow p-subgroup, p odd, of S_n is contained in A_n.

The following result on the center of a Sylow p-subgroup of S_n and its immediate consequences are important to us. These results are surely well known but no explicit reference is known to the author. We begin with a description of the center of a wreath product.

Consider the wreath product $H \wr G$, where H is a subgroup of S_m and G is a subgroup of S_n. For a subgroup K of H, the diagonal of K in H^n is the subgroup $\Delta(K) = \{\, (x, \ldots, x) \mid x \in K \,\}$. Obviously, $\Delta(K)$ is isomorphic to K, and $\Delta(K)$ embeds into $H \wr G$ via the homomorphism $(x, \ldots, x) \mapsto (x, \ldots, x, 1)$. So we may view $\Delta(K)$, and K, as a subgroup of $H \wr G$.

Proposition 4.6. *If G is a transitive subgroup of S_n, then $Z(H\wr G) = \Delta(Z(H))$.*

Proof. The nontrivial inclusion is that the center of $H \wr G$ is contained in the diagonal of the center of H.

Let $\sigma = (h_1, \dots, h_n, g) \in Z(H \wr G)$. For all $x = (x_1, \dots, x_n, f) \in H \wr G$,

$$(h_1 x_{g^{-1}(1)}, \dots, h_1 x_{g^{-1}(n)}, gf) = \sigma x = x\sigma = (x_1 h_{f^{-1}(1)}, \dots, x_n h_{f^{-1}(n)}, fg).$$

In particular, σ commutes with $(h, \dots, h, 1)$ for all $h \in H$, i.e., $h_i h = h h_i$ for all $1 \leq i \leq n$ and all $h \in H$, that is, $h_i \in Z(H)$.

If $(x_1, \dots, x_n, 1) \in H \wr G$, then $h_i x_{g^{-1}(i)} = x_i h_i$. Since $h_i \in Z(H)$, $x_{g^{-1}(i)} = x_i$ for all $1 \leq i \leq n$ and all $(x_1, \dots, x_n) \in H^n$. It follows that g is the identity.

It remains to prove that $h_1 = \cdots = h_n$: For each $1 < i \leq n$, there exits $f \in G$ such that $f^{-1}(1) = i$. Since $\sigma = (h_1, \dots, h_n, 1)$ commutes with $(1, \dots, 1, f)$,

$$(h_{f^{-1}(1)}, \dots, h_{f^{-1}(n)}, g) = (h_1, \dots, h_n, f),$$

i.e., $h_{f^{-1}(1)} = h_i = h_1$ for all i. This finishes the proof. □

The center of the Sylow 2-subgroup W_n of S_{2^n}: The center of $S_2 = \mathbb{Z}/2$ is generated by $\tau = (1, 2)$. By proposition 4.6, the center of $\mathbb{Z}/2 \wr \mathbb{Z}/2$ is $\Delta(\langle\tau\rangle)$, i.e., $\langle(\tau, \tau, 1)\rangle$, where $(\tau, \tau, 1)$ considered as an element in S_4 is the permutation $(1, 2)(3, 4)$, see example 4.2. Assume inductively that the center of W_n is generated by the permutation $\tau' = (1, 2) \cdots (2^n - 1, 2^n)$. As before, the center of W_{n+1} is generated by the element $\sigma' = (\tau', \tau', 1)$. Since

$$\sigma'(1,1) = (2,1), \sigma'(2,1) = (1,1), \dots, \sigma'(2^n,1) = (2^n-1,1),$$
$$\sigma'(1,2) = (2,2), \dots, \sigma'(2^n-1,2) = (2^n,2), \sigma'(2^n,2) = (2^n-1,2),$$

the center of W_{n+1} is generated by the permutation $(1, 2) \cdots (2^n - 1, 2^n)$.

A similar analysis apply for the odd primes. So we have the following result.

Proposition 4.7. *Let p be a prime. The center of W_n is cyclic of order p and is, as a subgroup of S_{p^n}, generated by $(1, \dots, p) \cdots (p^n - p + 1, \dots, p^n)$.*

Corollary 4.8. *Suppose $n \equiv 0, 1 \pmod 4$. Then the center of a Sylow 2-subgroup of S_n is equal to the center of a Sylow 2-subgroup of A_n.*

Proof. We may assume n is divisible by 4. Let $n = 2^{n_1} + \cdots + 2^{n_m}$, $1 < n_1 < \cdots < n_m$, be the 2-adic expansion of n. A Sylow 2-subgroup of S_n is isomorphic to

$$W_{n_1} \times \cdots \times W_{n_m}.$$

Recall that the center of a product is the product of the centers. By proposition 4.7, the center of each factor consists of even permutations. □

Corollary 4.9. *Suppose $n \equiv 2, 3 \pmod 4$. Then a Sylow 2-subgroup of A_n is isomorphic to a Sylow 2-subgroup of S_{n-2}.*

Proof. We may assume $n-2$ is divisible by 4. Let $n = 2 + 2^{n_1} + \cdots + 2^{n_m}$, $1 < n_1 < \cdots < n_m$, be the 2-adic expansion of n. A Sylow 2-subgroup of S_n is isomorphic to

$$P = W_1 \times W_{n_1} \times \cdots \times W_{n_m}.$$

Recall that W_1 is generated by the transposition $(1,2)$. It follows that W_1 is contained in the center of P. Note that P contains a Sylow 2-subgroup Q of A_n, and $P = W_1 Q$ since Q has index 2 in P. Since W_1 and Q are normal subgroups of P and $W_1 \cap Q$ is trivial, P is the product $W_1 \times Q$. Consequently, Q is isomorphic to a Sylow 2-subgroup of S_{n-2}. □

Another situation where wreath products appear naturally is in the description of centralizers in the symmetric groups, see [47] p. 295: Suppose a permutation σ in S_n is a product $\sigma = \sigma_1 \cdots \sigma_m$ of disjoint permutations such that σ_i is a product of r_i s_i-cycles, i.e., $n = r_1 s_1 + \cdots + r_m s_m$. Write

$$\sigma_i = (a(i)_{1,1}, \ldots, a(i)_{1,s_i}) \cdots (a(i)_{r_i,1}, \ldots, a(i)_{r_i,s_i})$$

and $\Omega_i = \{a(i)_{u,v} \mid 1 \le u \le r_i, 1 \le v \le s_i\} \subset \{1, \ldots, n\}$.

Recall that for any $\tau \in S_n$, $\tau\sigma\tau^{-1} = \tau\sigma_1\tau^{-1} \cdots \tau\sigma_m\tau^{-1}$ and

$$\tau\sigma_i\tau^{-1} = (\tau(a(i)_{1,1}), \ldots, \tau(a(i)_{1,s_i})) \cdots (\tau(a(i)_{r_i,1}), \ldots, \tau(a(i)_{r_i,s_i})).$$

Observe that σ and τ commute if and only if $\tau(\Omega_i) = \Omega_i$ and the restriction of τ to Ω_i and σ_i commute for all i. It follows that

$$C_{S_n}(\sigma) = C_{S_{\Omega_1}}(\sigma_1) \times \cdots \times C_{S_{\Omega_m}}(\sigma_m).$$

It remains to consider the case where σ is a product of cycles of the same length:

Proposition 4.10. *Suppose $\sigma \in S_{rs}$ is a product of r disjoint s-cycles. Then $C_{S_{rs}}(\sigma)$ is isomorphic to $\mathbb{Z}/s \wr S_r$.*

Proof. Write

$$\sigma = (a_{1,0}, a_{1,1}, \ldots, a_{1,s-1}) \cdots (a_{r,0}, a_{r,1}, \ldots, a_{r,s-1}).$$

Let $\mathbb{Z}/s$ be the subgroup $\langle (0, \ldots, s-1) \rangle$ of the permutations of $\{0, \ldots, s-1\}$.

Let $\tau \in C_{S_{rs}}(\sigma)$. For $1 \le i \le r$ and $0 \le l \le s-1$,

$$\tau(a_{i,l}) = \tau(\sigma^l(a_{i,0})) = \sigma^l(\tau(a_{i,0})).$$

It follows that τ is determined by its values on the elements $a_{1,0}, \ldots, a_{r,0}$. Furthermore, suppose $\tau(a_{i',0}) = \sigma^l\tau(a_{i,0}) = \tau(a_{i,l})$ for some l. Then $i' = i$ and $l = 0$, i.e., $\tau(a_{1,0}), \ldots, \tau(a_{r,0})$ are in different cycles of σ.

Consequently, setting $\psi(\tau)(i) = j$ if $\tau(a_{i,0}) = a_{j,k}$ defines a permutation $\psi(\tau) \in S_r$. Moreover, define elements $\varphi_i(\tau)$ in $\mathbb{Z}/s$ by $\varphi_i(\tau) = (0, \ldots, s-1)^k$.

Define a map $\theta\colon C_{S_{rs}}(\sigma) \to \mathbb{Z}/s \wr S_r$ by $\theta(\tau) = (\varphi_1(\tau), \dots, \varphi_r(\tau), \psi(\tau))$. The claim is that θ is an isomorphism:

θ homomorphism: Suppose $\tau', \tau \in C_{S_{rs}}(\sigma)$ with $\tau(a_{i,0}) = a_{j,k}$ and $\tau'(a_{j,0}) = a_{j',k'}$. Since

$$\tau'\tau(a_{i,0}) = \tau'(\sigma^k(a_{j,0})) = \sigma^k(\tau'(a_{j,0})) = a_{j',k'+k},$$

it follows that $\psi(\tau'\tau)(i) = j' = \psi(\tau')\psi(\tau)(i)$. Moreover, because $\psi(\tau')^{-1}(j') = j$, we get $\varphi_{\psi(\tau')^{-1}(j')}(\tau) = (0, \dots, s-1)^k$. This shows that $\varphi_{j'}(\tau')\varphi_{\psi(\tau')^{-1}(j')}(\tau) = (0, \dots, m-1)^{k'+k}$. Thus,

$$\begin{aligned}\theta(\tau'\tau) &= (\varphi_1(\tau'\tau), \dots, \varphi_r(\tau'\tau), \psi(\tau'\tau)) \\ &= (\varphi_1(\tau')\varphi_{\psi(\tau')^{-1}(1)}(\tau), \dots, \varphi_r(\tau')\varphi_{\psi(\tau')^{-1}(r)}(\tau), \psi(\tau')\psi(\tau)) \\ &= (\varphi_1(\tau'), \dots, \varphi_r(\tau'), \psi(\tau'))(\varphi_1(\tau), \dots, \varphi_r(\tau), \psi(\tau)) \\ &= \theta(\tau')\theta(\tau),\end{aligned}$$

that is, θ is indeed a homomorphism.

θ injective: Suppose $\theta(\tau) = (1, \dots, 1, 1)$. Then $\tau(a_{i,0}) = a_{i,0}$ for all i, i.e., τ is the identity.

θ surjective: Suppose $(\varphi_{k_1}, \dots, \varphi_{k_r}, \psi) \in \mathbb{Z}/s \wr S_r$, $\varphi_{k_i} = (0, \dots, s-1)^{k_i}$. Consider the permutation τ in S_{rs} defined by $\tau(a_{i,l}) = a_{\psi(i),k_{\psi(i)}+l}$. Then

$$\tau\sigma(a_{i,l}) = \tau(a_{i,l+1}) = a_{\psi(i),k_{\psi(i)}+l+1} = \sigma\tau(a_{i,l})$$

and $\theta(\tau) = (\varphi_{k_1}, \dots, \varphi_{k_r}, \psi)$ by construction. This finishes the proof. □

4.2 Maximal elementary abelian p-subgroups

Consider the elementary abelian group $E_n = (\mathbb{Z}/p)^n$ as a subgroup of S_{p^n} via the left regular representation $\rho\colon E_n \to S_{p^n}$, i.e., the permutation representation given by the transitive action of E_n on the set E_n via left multiplication $\rho(g)(h) = gh$ for $g, h \in E_n$.

Remark 4.11. A characteristic of the regular representation of an elementary abelian p-subgroup is that every nontrivial permutation is a product of n disjoint cycles of length p: Let g be a nontrivial element in E_n. Note that if g has a fixed point then g is the identity; if $gx = x$, $x \in E$, then $g = 1$. So g has no fixed points. The cycle type of g is given by the orbits of the action of $\langle g \rangle$ on E_n. Since the length of an orbit divides $|g| = p$, every orbit has length p.

Theorem 4.12. *Let $n = b_0 + b_1p + \cdots b_mp^m$ be the p-adic expansion of n. If $n = a_0 + a_1p + a_2p^2 + \cdots + a_mp^m$ is a decomposition of n with $0 \le a_0 < p$ and $0 \le a_i$ for $1 \le i \le m$. Then*

$$\underbrace{E_1 \times \cdots \times E_1}_{a_1} \times \cdots \times \underbrace{E_m \times \cdots \times E_m}_{a_m} \subset \underbrace{S_p \times \cdots \times S_p}_{a_1} \times \cdots \times \underbrace{S_{p^m} \times \cdots \times S_{p^m}}_{a_m},$$

as a subgroup of S_n in the natural way, is a maximal elementary abelian p-subgroup of S_n, and different decompositions of n give distinct conjugacy classes.

Furthermore, the maximal p-rank of a maximal elementary abelian p-subgroup is

$$\mathrm{rk}_p(S_n) = \left[\frac{n}{p}\right] = b_1 + b_2 p + \cdots + b_m p^{m-1},$$

and the minimal p-rank is

$$\mathrm{mrk}_p(S_n) = b_1 + 2b_2 + \cdots + m b_m.$$

The minimal p-rank is only obtained by the maximal elementary p-subgroup corresponding to the p-adic expansion of n, except for $p = 2$ and $3 < n < 8$.

The proof of the statement about the conjugacy classes is from [2], see theorem VI.1.3. Concerning the ranks, it is not easy to find a proof in the literature. Especially for the part regarding the minimal rank of a maximal elementary abelian p-subgroup, so we give a somewhat detailed proof here. However, it should not come as a surprise that the minimal rank is determined by the p-adic expansion.

Proof. Let $E \subset S_n$ be an elementary abelian p-subgroup. Furthermore, let $\mathcal{O}_{x_1}, \ldots, \mathcal{O}_{x_m}$ be the orbits of E. Since the length of an orbit $\mathcal{O}_{x_i}$ divides the order of E, every orbit has length a power of p, i.e., $\mathcal{O}_{x_i} = p^{t_i}$ for some t_i. Restriction gives a transitive action of E on each orbit $\mathcal{O}_{x_i}$, or equivalently, a homomorphism $f_i \colon E \to S_{\mathcal{O}_{x_i}}$.

Suppose g is in the stabilizer E_{x_i} of x_i. Then g stabilizes all $x \in \mathcal{O}_{x_i}$ since E abelian. More specifically, if $x = g'x_i$ for some $g' \in E$, then $gx = gg'x_i = g'gx_i = x$. Thus, the kernel of f_i is the stabilizer E_{x_i} of x_i. So f_i induces an injective homomorphism $\tilde{f}_i \colon E/E_{x_i} \to S_{\mathcal{O}_{x_i}}$, and the stabilizer in E/E_{x_i} of every $x \in \mathcal{O}_{x_i}$ is trivial. It follows that $\tilde{f}_i$ is the regular representation of E/E_{x_i}, see e.g. [41] 1.6.7.

Note that $E_{x_1} \cap \cdots \cap E_{x_m}$ is the identity. Consequently, the map

$$E \xrightarrow{\prod f_i} \textstyle\prod_{1 \leq i \leq m} S_{\mathcal{O}_{x_i}} \subset S_n$$

is injective, and it follows that E is, up to conjugacy, one of the listed groups.

Elementary abelian p-subgroups corresponding to different decompositions of n are not conjugated since they contain elements with different cycle type. This proves the statement about the conjugacy classes of maximal elementary abelian p-subgroups of S_n.

Next is the statements about the p-ranks. We may assume p divides n since the Sylow p-subgroups are the same, i.e., $b_0 = a_0 = 0$. Observe that the rank of a maximal elementary abelian p-subgroup corresponding to a given decomposition is

$$a_1 + 2a_2 + \cdots + m a_m.$$

Since $i \leq p^{i-1}$ for $i \geq 1$,

$$\sum_{i=1}^{m} a_i i \leq \sum_{i=1}^{m} a_i p^{i-1} = \frac{n}{p}.$$

Thus, $\mathrm{rk}_p(S_n) = \frac{n}{p}$. In particular, the maximal rank is obtained when a_1 is maximal.

To prove that $\mathrm{mrk}_p(S_n)$ is given by the p-adic expansion we need to prove that

$$b_1 + \cdots (m-1)b_{m-1} + mb_m \leq a_1 + \cdots (m-1)a_{m-1} + ma_m$$

for all decompositions $a_1p + \cdots a_mp^m$ of n. The idea is to iteratively transform the p-adic expansion into any decomposition and keep track of what happens to the ranks of the corresponding elementary abelian p-subgroups. The result is obvious for $m = 1$ since there is only one maximal elementary abelian p-subgroup.

Suppose $n = a_1p + \cdots a_mp^m$ is a decomposition of n with $m > 1$. Change the p-adic expansion by changing b_m to a_m by adding $(b_m - a_m)p$ to b_{m-1}. Thus, the p-adic expansion is changed into the decomposition

$$b_1p + \cdots + (b_{m-1} + (b_m - a_m)p)p^{m-1} + a_mp^m.$$

The rank of the corresponding elementary abelian p-subgroup is

$$b_1 + \cdots + (m-1)(b_{m-1} + (b_m - a_m)p) + ma_m,$$

and

$$b_1 + \cdots + (m-1)b_{m-1} + mb_m \leq b_1 + \cdots + (m-1)(b_{m-1} + (b_m - a_m)p) + ma_m$$

if and only if

$$mb_m \leq (m-1)(b_m - a_m)p + ma_m.$$

Note that $m \leq (m-1)p$ since $m > 1$, and $b_m \geq a_m$ by the greedy nature of the p-adic expansion. Now,

$$\begin{aligned} mb_m \leq (m-1)(b_m - a_m)p + ma_m &\Leftrightarrow m(b_m - a_m) \leq (m-1)(b_m - a_m)p \\ &\Leftrightarrow m \leq (m-1)p. \end{aligned}$$

In other words, the rank of the elementary abelian p-subgroup corresponding to the new decomposition is at least as large as the rank corresponding to the p-adic expansion. Note that equality occur exactly when $m = (m-1)p$.

Observe that

$$b_1p + b_2p^2 + \cdots + (m-1)(b_{m-1} + (b_m - a_m)p)p^{m-1}$$

is the p-adic expansion of $n - a_m p^m$. Repeating the above process gives that

$$\begin{aligned} b_1 + 2b_2 + \cdots + mb_m &\leq b_1 + 2b_2 + \cdots + (m-1)(b_{m-1} + (b_m - a_m)p) + ma_m \\ &\leq \cdots \\ &\leq b_1 + 2c_2 + 3a_3 + \cdots + ma_m \\ &\leq a_1 + 2a_2 + \cdots + ma_m, \end{aligned}$$

where $b_1 p + c_2 p^2$ is the p-adic expansion of $n - a_m p^m - \cdots - a_3 p^3$. This proves that the minimal rank of a maximal elementary abelian p-subgroup correspond to the p-adic expansion.

Finally, we investigate when a decomposition gives the same rank as the p-adic expansion. If $m = 1$, then the p-adic expansion is the only possible decomposition.

Suppose $m > 1$. As noted above, equality occurs exactly when $i = (i-1)p$ for all $1 < i \leq m$. Now, if $i = (i-1)p$ for $i > 1$, then $p = i(p-1)$. Since p prime, $i = 1$ or $p - 1 = 1$. By assumption $i > 1$, so $p = 2$. Note that $i = 2(i-1)$ if and only if $i = 2$. Thus, $i < (i-1)p$ except for $p = i = 2$.

It follows that for p odd the minimal rank of a maximal elementary abelian p-subgroup is only obtained by the p-adic expansion. For $p = 2$ the only cases where a decomposition of n different from the 2-adic expansion obtain the minimal rank is when $m = 2$. More specifically, when the 2-adic expansion has the form $n = b_0 + b_1 2 + b_2 2^2$, that is, $3 < n < 8$. □

Our next theorem on the maximal elementary abelian p-subgroups of A_n is important in determining the depth of the mod p cohomology rings of the alternating groups.

Theorem 4.13. *If p is an odd prime, then the elementary abelian p-subgroups of A_n are precisely the elementary abelian p-subgroups of S_n.*

The maximal elementary abelian 2-subgroups of A_n are the subgroups $E \cap S_n$, where E is a maximal elementary abelian 2-subgroup of S_n.

Let $n = b_0 + b_1 2 + \cdots b_m 2^m$ be the 2-adic expansion of n, and let $n = a_0 + a_1 2 + \cdots + a_m 2^m$ be a decomposition of n with $0 \leq a_0 < 2$ and $0 \leq a_i$ for $1 \leq i \leq m$.

If E is the maximal elementary abelian 2-subgroup of S_n corresponding to the decomposition of n, see theorem 4.12. Then

$$\mathrm{rk}_2(E \cap A_n) = \begin{cases} \mathrm{rk}_2(E), & a_1 = 0 \\ \mathrm{rk}_2(E) - 1, & a_1 > 0. \end{cases}$$

Furthermore,

$$\mathrm{rk}_2(A_n) = \begin{cases} \mathrm{rk}_2(S_n), & n \equiv 0, 1 \,(\mathrm{mod}\, 4) \\ \mathrm{rk}_2(S_n) - 1, & n \equiv 2, 3 \,(\mathrm{mod}\, 4), \end{cases}$$

and

$$\operatorname{mrk}_2(A_n) = \begin{cases} \operatorname{mrk}_2(S_n), & n \equiv 0, 1 \pmod 4 \\ \operatorname{mrk}_2(S_n) - 1, & n \equiv 2, 3 \pmod 4. \end{cases}$$

Proof. For an odd prime p the Sylow p-subgroups of S_n are also the Sylow p-subgroups of A_n. So in this case theorem 4.12 describes the maximal elementary abelian p-subgroups of A_n.

Any maximal elementary abelian 2-subgroup of A_n is contained in a maximal elementary abelian 2-subgroup in S_n, which gives the second statement.

As usual, we may assume n is divisible by 2.

Suppose $a_1 = 0$. Then E contains no transpositions, see remark 4.11. In other words, it is contained in A_n.

Suppose $a_1 > 0$. Then E contains a transposition. Hence, $EA_n = S_n$. By a Noether isomorphism, $[E : E \cap A_n] = [S_n : A_n] = 2$. It follows that $\operatorname{rk}_2(E \cap A_n) = \operatorname{rk}_2(E) - 1$.

Suppose $n \equiv 0 \pmod 4$. Then the decomposition $n = a_2 4 = a_2 2^2$ gives a maximal elementary abelian 2-subgroup of maximal rank $n/2$ in A_n. Note that $b_1 = 0$ in the 2-adic expansion of n. So the corresponding maximal elementary abelian 2-subgroup in S_n is contained in A_n. By theorem 4.12, the 2-adic expansion is the only decomposition with minimal rank except for perhaps $n = 4$. However, S_4 only contains 3 double transpositions which constitutes the only maximal elementary abelian 2-subgroup of A_4.

Suppose $n \equiv 2 \pmod 4$. Then $a_1 \geq 1$ in every decomposition of n. Hence, $\operatorname{rk}_2(E \cap A_n) = \operatorname{rk}_2(E) - 1$ for all maximal elementary abelian 2-subgroups E of S_n. □

4.3 p-fusion in the symmetric and alternating groups

Let H be a subgroup of the finite group G. An element $x \in H^*(H)$ is called stable if

$$\operatorname{res}_{H, H \cap gHg^{-1}}(x) = g \operatorname{res}_{H, g^{-1}Hg \cap H}(x)$$

for all $g \in G$, that is, if the diagram

$$\begin{tikzcd} & H^*(H) \arrow[dl, "\mathrm{res}"'] \arrow[dr, "\mathrm{res}"] & \\ H^*(g^{-1}Hg \cap H) \arrow[rr, "\cdot g"] & & H^*(H \cap gHg^{-1}) \end{tikzcd}$$

commutes for all $g \in G$.

The following theorem by Cartan & Eilenberg, [19] theorem XII.10.1, is classic.

Theorem 4.14. *Let P be a Sylow p-subgroup of G. Then*

$$\operatorname{res}_{G,P} \colon H^*(G) \to H^*(P)$$

is injective and the image consists of the stable elements of $H^*(P)$.

Definition 4.15. *A subgroup H of the group G is said to control p-fusion in G if the following two conditions are satisfied:*

(1) $[G : H]$ is coprime to p, and

(2) if Q is a p-subgroup of H and $g \in G$ is such that $gQg^{-1} \subset H$, then $g = hc$ for some $h \in H$ and $c \in C_G(Q)$.

The requirement that $[G : H]$ is coprime to p gives that H contains a Sylow p-subgroup of G. The following immediate consequence of the theorem is well known, see e.g. [6] proposition 3.8.4.

Proposition 4.16. *Suppose H controls the p-fusion in G. Then*

$$\mathrm{res}_{G,H}\colon H^*(G) \to H^*(H)$$

is an isomorphism.

Proof. Let P be a Sylow p-subgroup of G contained in H. By theorem 4.14, it suffices to show that the stable elements in $H^*(P)$ are the same.

Let $g \in G$. Note that $Q = g^{-1}Pg \cap P$ is a p-subgroup of H such that $gQg^{-1} = P \cap gPg^{-1}$. Since H controls the p-fusion in G, there exists $h \in H$ and $c \in C_G(Q)$ such that $g = hc$.

Suppose $x \in Q$, i.e., $x = g^{-1}yg \in P$ for some $y \in P$. Then

$$x = cxc^{-1} = cg^{-1}ygc^{-1} = h^{-1}yh.$$

Hence, $Q = h^{-1}Ph \cap P$. Furthermore,

$$P \cap gPg^{-1} = gQg^{-1} = hQh^{-1} = h(h^{-1}Ph \cap P)h^{-1} = P \cap hPh^{-1}.$$

Since $c = h^{-1}g$ centralizes Q, $gz = hz$ for all $z \in H^*(Q)$. It follows that the stable elements in $H^*(P)$ are the same. □

Remark 4.17. G. Mislin [35] proved the converse, that if the restriction map $\mathrm{res}_{G,H}\colon H^*(G) \to H^*(H)$ is an isomorphism, then H controls p-fusion in G. It is quite surprising that the cohomology controls the subgroup structure of a group in such a strong way.

The following result on p-fusion in the symmetric groups is widely known. However, it is not easy to find an explicit reference, so we provide a proof here.

Theorem 4.18. *Suppose $p \nmid n + 1$. Then S_n controls p-fusion in S_{n+1}.*

Proof. Consider S_n as the subgroup of S_{n+1} that fixes $n + 1$. Since $p \nmid n + 1$, $[S_{n+1} : S_n]$ and p are coprime. Suppose $Q \subset S_n$ is a p-subgroup and $\sigma \in S_{n+1}$ is such that $\sigma Q\sigma^{-1} \subset S_n$. There is nothing to prove if σ fix $n + 1$. Assume $\sigma(n + 1) \neq n + 1$.

Write $\sigma = \sigma_1 \cdots \sigma_k$ as a product of disjoint cycles such that $\sigma_1, \ldots, \sigma_{k-1} \in S_n$ and σ_k has the form

$$\sigma_k = (a_1, \ldots, a_m, n+1).$$

Let x be an element in Q. If $x(a_m) \neq a_m$, then

$$\sigma x \sigma^{-1}(n+1) = \sigma x(a_m) \neq n+1.$$

This contradicts that $\sigma x \sigma^{-1} \in S_n$. Hence, $x(a_m) = a_m$ for all x in Q. Now,

$$\sigma = \sigma_1 \cdots \sigma_{k-1}(a_1, \ldots, a_m)(a_m, n+1),$$

where $\sigma_1 \cdots \sigma_{k-1}(a_1, \ldots, a_m) \in S_n$ and $(a_m, n+1) \in C_{S_{n+1}}(Q)$ since all elements in Q fix a_m and $n+1$. □

Corollary 4.19. *Let n be a positive integer. Then $H^*(S_{np}) \cong H^*(S_{np+m})$ for $1 \leq m \leq p-1$.*

Note that $H^*(S_n) = \mathbb{F}_p$ for $n < p$. We continue with a result on the p-fusion of the alternating groups.

Theorem 4.20. *Suppose $p \nmid n+1$ and $p \nmid n-1$. Then A_n controls p-fusion in A_{n+1}.*

Proof. Consider A_n as the subgroup of A_{n+1} that fix $n+1$. Since $p \nmid n+1$, $[A_{n+1} : A_n]$ and p are coprime. Suppose $Q \subset A_n$ is a p-subgroup and $\sigma \in A_{n+1}$ is such that $\sigma Q \sigma^{-1} \subset A_n$. We may assume $\sigma(n+1) \neq n+1$.

As in the case of the symmetric group, write $\sigma = \sigma_1 \cdots \sigma_k$ as a product of disjoint cycles such that $\sigma_1, \ldots, \sigma_{k-1} \in S_n$ and σ_k has the form

$$\sigma_k = (a_1, \ldots, a_m, n+1).$$

Recall from the proof of theorem 4.18 that all elements in Q fix a_m and $n+1$. In particular, $Q \subset A_{n-1}$, where A_{n-1} is considered as the subgroup of A_{n+1} that fixes a_m and $n+1$. So Q is contained in a Sylow p-subgroup P of A_{n-1}. Since $p \nmid n-1$, P is conjugate to a Sylow p-subgroup of A_{n-2}, where A_{n-2} is considered as the subgroup of A_{n-1} that fixes an element b in $\{1, \ldots, n+1\} - \{a_m, n+1\}$. Thus, $\tau Q \tau^{-1} \subset A_{n-2}$ for some $\tau \in A_{n-1}$. In other words, $\tau x \tau^{-1}(b) = b$ for all x in Q, that is, $x(\tau^{-1}(b)) = \tau^{-1}(b)$.

Summarizing, all elements in Q fix $n+1$, a_m and $\tau^{-1}(b)$. Thus,

$$\sigma = \sigma_1 \cdots \sigma_{k-1}(a_1, \ldots, a_m)(\tau^{-1}(b), a_m)(\tau^{-1}(b), a_m)(a_m, n+1),$$

where $\sigma_1 \cdots \sigma_{k-1}(a_1, \ldots, a_m)(\tau^{-1}(b), a_m) \in A_n$ and $(\tau^{-1}(b), a_m)(a_m, n+1) \in C_{A_{n+1}}(Q)$ since all elements in Q fix $n+1$, a_m and $\tau^{-1}(b)$. □

Note that it is essential to the proof that $n-1$ is not divisible by p so we can conjugate a Sylow p-subgroup of A_{n-1} to a Sylow p-subgroup of A_{n-2}, providing the crucial extra fixed point. The next example shows that the theorem can not be improved.

Example 4.21. Suppose $p \nmid n+1$ and $p \mid n-1$, i.e., $n-1 = mp$ for some m. Note that p is necessarily an odd prime. Then A_n does not control p-fusion in A_{n+1}: For $1 \leq i \leq m$, let x_i be the p-cycle $((i-1)p+1, \dots, ip)$ and $\Omega_i = \{(i-1)p+1, \dots, ip\}$. The subgroup

$$E = \langle x_1 \rangle \times \cdots \times \langle x_m \rangle$$

is an elementary abelian p-subgroup of $A_{n-1} \subset A_{n+1}$. Note that $E \subset C_{A_{n+1}}(E)$. By proposition 4.10, $\langle x_i \rangle \subset C_{A_{\Omega_i}}(x_i) \subset C_{S_{\Omega_i}}(x_i) = \langle x_i \rangle$. It follows that

$$C_{A_{n+1}}(E) = C_{A_{\Omega_1}}(x_1) \times \cdots \times C_{A_{\Omega_m}}(x_m) \times A_2 = E.$$

Let $\sigma = (1,2)(n,n+1)$. Then $\sigma E \sigma^{-1} \subset A_n$. However, if $\sigma = \tau c$ for some $\tau \in A_n$ and $c \in C_{A_{n+1}}(E) = E$, then $\sigma \in A_n$ which is a contradiction.

Corollary 4.22. *Let n be a positive integer. Then $H^*(A_{np}) \cong H^*(A_{np+1})$ and $H^*(A_{np+2}) \cong H^*(A_{np+m})$ for $2 < m \leq p-1$.*

Note that $H^*(A_n) = \mathbb{F}_p$ for $n < p$.

Theorem 4.23. *Let p be an odd prime. Then A_{np+2} controls p-fusion in S_{np+2}.*

Proof. Suppose $Q \subset A_{np+2}$ is a p-subgroup and $\sigma \in S_{np+2}$ is such that $\sigma Q \sigma^{-1} \subset A_{np+2}$. Assume that $\sigma \notin A_{np+2}$. Consider A_{np} as the subgroup of A_{np+2} that fixes $np+1$ and $np+2$. A Sylow p-subgroup P of A_{np} is a Sylow p-subgroup of A_{np+2}. Since Q is conjugated to a subgroup of P, i.e., $\tau Q \tau^{-1} \subset P$ for some $\tau \in A_{np+2}$. For all $x \in Q$, $\tau x \tau^{-1}(np+1) = np+1$, i.e., $x(\tau^{-1}(np+1)) = \tau^{-1}(np+1)$, and $x(\tau^{-1}(np+2)) = \tau^{-1}(np+2)$. In other words, all elements in Q fix $a = \tau^{-1}(np+1)$ and $b = \tau^{-1}(np+2)$. Consequently, $\sigma = \sigma(a,b)(a,b)$, where $\sigma(a,b) \in A_{np+1}$ since $\sigma \notin A_{np+2}$, and $(a,b) \in C_{S_{np+2}}(Q)$ since all elements in Q fix a and b. □

Corollary 4.24. *Let n be a positive integer. Then $H^*(A_{np+m}) \cong H^*(S_{np})$ for $2 \leq m \leq p-1$.*

4.4 Depth and the symmetric groups

The cohomology rings of the symmetric groups have been much studied. We do not need the actual ring structure to determine the depth as it turns out the depth is completely determined by the Sylow p-subgroups. However, a good introduction to the cohomology of symmetric groups may be found in [2] ch. VI. As an example,

$$H^*(S_6; \mathbb{F}_2) = \mathbb{F}_2[v, x, y, z]/((y+vx)z),$$

where $|v| = 1$, $|x| = 2$ and $|y| = |z| = 3$.

The computation of the depths of the mod p cohomology rings of the symmetric groups is an easy consequence of the following theorem by Carlson & Henn [16].

Theorem 4.25. *If the depth of $H^*(G)$ is d, then the depth of $H^*(G \wr \mathbb{Z}/p)$ is $d+1$.*

Corollary 4.26. *Let $n = b_0 + b_1 p + \cdots + b_m p^m$ be the p-adic expansion of n and P a Sylow p-subgroup of S_n. Then*

$$\operatorname{depth} H^*(S_n) = \operatorname{depth} H^*(P) = b_1 + 2b_2 + \cdots + mb_m,$$

and there exists an associated prime $\mathfrak{p}$ of $H^*(S_n)$ such that the dimension of $H^*(S_n)/\mathfrak{p}$ is equal to the depth.

Proof. Recall that, by theorem 3.9, the depth of $H^*(S_n)$ is greater than or equal to the depth of $H^*(P)$. By theorem 4.4, P is isomorphic to the product $W_1^{b_1} \times \cdots \times W_m^{b_m}$ of iterated wreath products. Hence, $H^*(P)$ is isomorphic to

$$\underbrace{H^*(W_1) \otimes \cdots \otimes H^*(W_1)}_{b_1} \otimes \cdots \otimes \underbrace{H^*(W_m) \otimes \cdots \otimes H^*(W_m)}_{b_m}.$$

Theorem 4.25 implies that $\operatorname{depth} H^*(W_n) = n$, and proposition A.35 gives that

$$\operatorname{depth} H^*(S_n) \geq \operatorname{depth} H^*(P) \geq b_1 + 2b_2 + \cdots + mb_m.$$

Remember that S_n has a maximal elementary abelian p-subgroup of rank $b_1 + 2b_2 + \cdots + mb_m$, see theorem 4.12, and that the prime ideals in $H^*(S_n)$ given by maximal elementary 2-subgroups are always among the associated primes and the dimension of the quotient is equal to the rank, see theorem 2.14. Consequently,

$$\operatorname{depth} H^*(S_n) \leq b_1 + 2b_2 + \cdots + mb_m.$$

This finishes the proof. □

Remark 4.27. Carlson and Henn also proved that if a is the minimum of the dimensions of $H^*(G)/\mathfrak{p}$, $\mathfrak{p} \in \operatorname{Ass} H^*(G)$, then the minimum of the dimensions of $H^*(G \wr \mathbb{Z}/p)/\mathfrak{q}$, $\mathfrak{q} \in \operatorname{Ass} H^*(G \wr \mathbb{Z}/p)$ is at most $a+1$. More concisely, $\omega_a(G \wr \mathbb{Z}/p) \leq \omega_a(G) + 1$. In particular, if G satisfies the conjecture, then $G \wr \mathbb{Z}/p$ also satisfies the conjecture.

Remark 4.28. The center of a Sylow p-subgroup of S_{p^n} has p-rank 1, see proposition 4.7. So the example $\operatorname{depth} H^*(S_{p^n}) = n$ shows that the depth may exceed the p-rank of the center a Sylow p-subgroup, the lower bound from Duflot's theorem, by an arbitrary amount.

Our next result is a kind of reverse to theorem 4.25 in the case of a symmetric group.

Corollary 4.29. *Let $n = b_0 + b_1 p + \cdots + b_m p^m$ be the p-adic expansion of n. Then*

$$\operatorname{depth} H^*(\mathbb{Z}/p \wr S_n) = b_0 + 2b_1 + \cdots + (m+1)b_m.$$

In addition, there exists an associated prime $\mathfrak{p}$ of $H^*(\mathbb{Z}/p \wr S_n)$ such that the dimension of $H^*(\mathbb{Z}/p \wr S_n)/\mathfrak{p}$ is equal to the depth.

Proof. By proposition 4.7, the center of a Sylow p-subgroup P of S_{np} contains a permutation σ which is the product of n disjoint p-cycles. Proposition 4.10 gives that the centralizer $C_{S_{np}}(\sigma)$ is isomorphic to the wreath product $\mathbb{Z}/p \wr S_n$. Note that $np = b_0 p + b_1 p^2 + \cdots + b_m p^{m+1}$. Our improved version of Notbohm's theorem, see theorem 3.18, and corollary 4.26 gives that

$$\begin{aligned}\operatorname{depth} H^*(\mathbb{Z}/p \wr S_n) &= \operatorname{depth} H^*(C_{S_{np}}(\sigma)) \\ &= \operatorname{depth} H^*(S_{np}) = b_0 + 2b_1 + \cdots + (m+1)b_m.\end{aligned}$$

Since $P \subset C_{S_{np}}(\sigma)$, $\operatorname{mrk}_p(\mathbb{Z}/p \wr S_n) = \operatorname{mrk}_p(S_{np}) = \operatorname{depth} H^*(S_{np})$ which finishes the proof. □

4.5 Depth and the alternating groups

After the computation of the depths of the cohomology rings of the symmetric groups, the obvious question is: What is the depths of the cohomology rings of the alternating groups and do the alternating groups satisfy the conjecture? The fact that the alternating groups are simple groups makes an investigation of their cohomology particularly difficult. In general, the mod p cohomology rings of the alternating groups have not yet been computed. See [2] section VI.6 for computations of the mod 2 cohomology of A_n for some small n and [33] for information on the mod p cohomology of A_n for p odd. As an example,

$$H^*(A_6; \mathbb{F}_2) = \mathbb{F}_2[x, y, z]/(yz),$$

where $|x| = 2$, $|y| = |z| = 3$. Notice that $H^1(A_n) = \operatorname{Hom}(A_n, \mathbb{Z}/p) = 0$ since A_n is simple ($n \geq 5$).

For an odd prime p, the depth of the mod p cohomology ring of an alternating group is, not surprisingly, determined by a Sylow p-subgroup.

Proposition 4.30. *Let p be an odd prime and P a Sylow p-subgroup of A_n. Then*

$$\operatorname{depth} H^*(A_n) = \operatorname{depth} H^*(P) = \operatorname{depth} H^*(S_n),$$

and there exists an associated prime $\mathfrak{p}$ of $H^*(A_n)$ such that the dimension of $H^*(A_n)/\mathfrak{p}$ is equal to the depth.

Proof. Follows immediately from the fact that P is a Sylow p-subgroup of S_n and $\operatorname{mrk}_p(S_n) = \operatorname{mrk}_p(A_n)$. □

From now on we only consider mod 2 cohomology. Recall that $H^*(A_{2n}) = H^*(A_{2n+1})$, see corollary 4.22. So we may always assume n is even.

With the results on the properties of the Sylow 2-subgroups of the symmetric and alternating groups, and the ranks of the maximal elementary abelian 2-subgroups, it is easy to establish the conjecture for "half" of the alternating groups. As with the symmetric groups, and the alternating groups for odd primes, the depth of the cohomology ring is determined by a Sylow 2-subgroup:

Proposition 4.31. *Suppose $n \equiv 2, 3 \pmod 4$ and Q is a Sylow 2-subgroup of A_n. Then*

$$\operatorname{depth} H^*(A_n) = \operatorname{depth} H^*(Q) = \operatorname{depth} H^*(S_n) - 1.$$

In addition, there exists an associated prime $\mathfrak{p}$ of $H^*(A_n)$ such that the dimension of $H^*(A_n)/\mathfrak{p}$ is equal to the depth.

Proof. By corollary 4.9, a Sylow 2-subgroup Q of A_n is isomorphic to a Sylow 2-subgroup of S_{n-2}. Theorem 4.26 gives that

$$\operatorname{depth} H^*(Q) = \operatorname{depth} H^*(S_{n-2}) = \operatorname{depth} H^*(S_n) - 1.$$

Noting that A_n contains a maximal elementary abelian 2-subgroup of rank $\operatorname{mrk}_2(S_n) - 1 = \operatorname{depth} H^*(S_n) - 1$, see theorem 4.13, finishes the proof. □

The key point in the proof is corollary 4.9 which relied on the fact the center of a Sylow 2-subgroup of S_n contained a transposition. However, if n is divisible by 4, the center of a Sylow 2-subgroup of S_n coincides with the center of A_n, see corollary 4.8. Thus, a similar approach does not apply in this case.

In fact, the result also follows from a certain short exact sequence involving the mod 2 cohomology rings of the symmetric and alternating groups. The discovery of these results was actually the first breakthrough in the author's attempt to compute the depths of the mod 2 cohomology rings of the alternating groups. Since these results might be useful in determining the depth of $H^*(A_n)$ where 4 divides n, we give a brief introduction, see [2] section VI.6 for details.

Lemma 4.32. *Let G be a group. Suppose $v \in H^1(G, \mathbb{Z}/2) = \operatorname{Hom}(G, \mathbb{Z}/2)$ is nonzero, and let $H \subset G$ denote its kernel. Then there is a long exact sequence*

$$\begin{tikzcd} \cdots \arrow[r] & H^n(G) \arrow[r, "\cdot v"] & H^{n+1}(G) \arrow[r, "\mathrm{res}"] & H^{i+1}(H) \arrow[r, "\mathrm{tr}"] & H^{n+1}(G) \arrow[r] & \cdots . \end{tikzcd}$$

In particular, there is a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & H^*(G)/(v) \arrow[r, "\mathrm{res}"] & H^*(H) \arrow[r, "\mathrm{tr}"] & \operatorname{Ann}_{H^*(G)}(v) \arrow[r] & 0 \end{tikzcd}$$

of $H^*(G)$-modules via restriction.

Corollary 4.33. *Let v be the generator of $H^1(S_n) = \mathrm{Hom}(S_n, \mathbb{Z}/2) = \mathbb{Z}/2$. Then*

$$\begin{tikzcd}0 \arrow[r] & H^*(S_n)/(v) \arrow[r, "\mathrm{res}"] & H^*(A_n) \arrow[r, "\mathrm{tr}"] & \mathrm{Ann}_{H^*(S_n)}(v) \arrow[r] & 0\end{tikzcd}$$

is a short exact sequence of $H^*(S_n)$-modules.

Proposition 4.34. *If $n \equiv 2, 3 \pmod 4$, then the restriction map $H^*(S_n) \to H^*(A_n)$ is onto. In particular, $H^*(A_n) \cong H^*(S_n)/(v)$, where v is a generator of $H^1(S_n)$.*

Note that v is a regular element because $\mathrm{Ann}_{H^*(S_n)}(v) = 0$. It follows that

$$\operatorname{depth} H^*(A_n) = \operatorname{depth} H^*(S_n)/(v) = \operatorname{depth} H^*(S_n) - 1,$$

see proposition A.36, which gives another proof of the statement concerning the depth in proposition 4.31. Of course, to verify that the alternating groups in these cases satisfy Carlson's depth conjecture we still need the results of the ranks of the elementary abelian 2-subgroups.

Perhaps the most powerful consequence of the previous proposition is that it determines the mod 2 cohomology of the alternating groups from the cohomology of the symmetric groups, e.g., the example with S_6 and A_6 above. The proof of the proposition relies heavily on topological methods. This led the author to search for a more elementary proof of proposition 4.31. The search ended with the above proof which only uses properties of the Sylow 2-subgroups of the symmetric and alternating groups.

The remaining case of n divisible by 4 seems more difficult and the author has unfortunately not been able to determine the depth. Remember that $\operatorname{depth} H^*(S_n) = \mathrm{mrk}_2(S_n) = \mathrm{mrk}_2(A_n)$ in this case. For small n the situation is as follows.

A Sylow 2-subgroup of A_4 is a maximal elementary abelian 2-subgroup of rank 2, i.e., $\operatorname{depth} H^*(A_4) = 2$. A Sylow 2-subgroup of A_8 has order 64 with Hall-Senior number 259 or Magma small group library number 138 which, by [14] or [26], has depth 3. Since $\mathrm{mrk}_2(A_8) = 3$, the depth of $H^*(A_8)$ is 3. The table below lists some information about S_n and A_n for small n.

We end with a question:

Question 4.35. *Suppose $n \equiv 0, 1 \pmod 4$. Let P and Q be Sylow 2-subgroups of S_n and A_n, respectively. Is*

$$\operatorname{depth} H^*(A_n) = \operatorname{depth} H^*(Q) = \operatorname{depth} H^*(P) = \operatorname{depth} H^*(S_n)?$$

n	depth(S_n)	mrk$_2(S_n)$	rk$_2(S_n)$	depth(A_n)	mrk$_2(A_n)$	rk$_2(A_n)$
4	2	2	2	2	2	2
6	3	3	3	2	2	2

n	depth(S_n)	mrk$_2(S_n)$	rk$_2(S_n)$	depth(A_n)	mrk$_2(A_n)$	rk$_2(A_n)$
8	3	3	4	3	3	4
10	4	4	5	3	3	4
12	5	5	6	-	5	6
14	6	6	7	5	5	6
16	4	4	8	-	4	8
18	5	5	9	4	4	8
20	6	6	10	-	6	10
22	7	7	11	6	6	10
24	8	8	12	-	8	12
26	9	9	13	8	8	12
28	10	10	14	-	10	14
30	11	11	15	10	10	14
32	5	5	16	-	5	16

A Graded commutative ring theory

This fairly lengthy appendix provides background theory from commutative ring theory in the context of graded commutative rings. As we shall see, the so called graded commutative Noetherian rings with a field in degree zero, e.g., the mod p cohomology ring of a finite group, behave like local rings in the strictly commutative world.

The objective is not to develop graded commutative ring theory from scratch. Instead, many results, e.g., matters concerning prime ideals, are reduced to their well known commutative counterparts and in these cases we in general provide a reference where the interested reader can locate a proof. Concerning depth it is not obvious how to reduce results to the known results from the commutative case so more details are provided. The exposition is primarily based on [5], [13], [18] and [34].

Let k be a field. All rings are nontrivial unitary rings, and the identity element is denoted by 1 and the zero element by 0.

We begin with a very brief introduction to graded rings and modules. The main purpose is to establish terminology and the reader unfamiliar with these concepts can find a thorough and excellent exposition in [32]. It should be noted that we work with internal grading whereas [32] work with external grading.

Definition A.1. *A graded ring is a ring R with a direct sum decomposition $R = \bigoplus_{i\in\mathbb{N}_0} R^i$ of abelian subgroups such that $R^iR^j \subset R^{i+j}$ for all $i, j \in \mathbb{N}_0$.*

A graded (right) R-module is an R-module M with a direct sum decomposition $M = \bigoplus_{i\in\mathbb{N}_0} M^i$ of abelian subgroups such that $R^iM^j \subset M^{i+j}$ ($M^iR^j \subset M^{i+j}$) for all $i, j \in \mathbb{N}_0$.

A graded algebra over a graded ring R is an R-algebra A which is both a graded R-module and a graded ring.

An element $x \in M$ is called homogeneous if $x \in M^i$ for some i which is called the degree of x. We write $|x| = i$ to denote that x is homogeneous of degree i. The zero element is by definition homogeneous of arbitrary degree. A ring homomorphism $\varphi\colon R \to S$ of graded rings is called homogeneous if $\varphi(R^i) \subset S^i$ for all $i \in \mathbb{N}_0$. Similarly for a homomorphism of R-modules. Note that R^0 is a subring of R and each M^i is an R^0-module.

A submodule $N \subset M$ is called homogenous if N is generated be homogeneous elements, or equivalently, if $x \in N$ each homogenous term of x is in N, i.e., $N = \bigoplus_{i\in\mathbb{N}_0}(N \cap M^i)$. If N is a homogeneous submodule of M then

$$M/N = \bigoplus_{i\in\mathbb{N}_0} M^i/(N \cap M^i)$$

is a graded R-module. The homogeneous submodules of R are called homogeneous ideals. The homogenous elements of positive degree generate an ideal which is denoted R^+.

Any ring S may trivially be considered as a graded ring R with $R^0 = S$ and $R^i = 0$ for $i > 0$. A graded algebra over the trivially graded ring k is simply called a graded k-algebra.

Example A.2. The graded polynomial algebra over k generated by an indeterminate x of degree $d > 0$ is denoted $k[x]$ and is defined by

$$k[x]^i = \begin{cases} 0, & d \nmid i \\ \text{the free } k \text{ module generated by } x^j, & i = jd \end{cases}$$

with product given by $x^i x^j = x^{i+j}$ and x^0 as the identity. Disregarding the grading $k[x]$ is just the ordinary polynomial algebra in x with coefficients in k. In $k[x]$ the ideal (x) is homogeneous but the ideal $(1 + x)$ is not homogeneous. In fact, both ideals are maximal ideals in $k[x]$ since they are the kernel of the evaluation homomorphism $\epsilon_a \colon k[x] \to k$, $f \mapsto f(a)$, $a \in k$, which is surjective and the kernel of ϵ_a is $(x - a)$. The exterior algebra over k generated by x of odd degree $d > 0$, denoted $\wedge_k(x)$, is the quotient algebra $k[x]/(x^2)$.

Definition A.3. *A graded ring R is called graded commutative if*

$$xy = (-1)^{|x||y|} yx$$

for all homogenous elements x, y in R.

Of course, a graded ring may be commutative in the usual sense and we say it is commutative graded. For example, a graded polynomial algebra on one generator is graded commutative if and only if the generator has even degree, but it is always commutative graded.

Graded commutative rings are very close to being commutative. Since the left and right ideals coincide, the notions of Noetherian ring and prime ideals act as in the commutative case. More generally, left modules are the same as right modules. Specifically, every left R-module M is also a right module via the formula $mr = (-1)^{|r||m|} rm$ for homogeneous elements $r \in R$ and $m \in M$. Henceforth we only consider left modules.

Note that elements of even degree always commute, and if 2 is invertible, then the square of an element of odd degree is zero. In particular, R^0 is a commutative subring of R, i.e., R is a graded R^0-algebra.

If R and S are graded commutative k-algebras, the tensor product $R^i \otimes_k S^j$ for all i and j is a k-module. The graded tensor product $R \otimes_k S$ is the graded k-module with $(R \otimes_k S)^n = \bigoplus_{i+j=n} R^i \otimes_k S^j$. The tensor product becomes a graded commutative k-algebra with product defined by

$$(r \otimes s)(r' \otimes s') = (-1)^{|s||r'|} (rr' \otimes ss').$$

Example A.4. The graded polynomial algebra on generators $x_1, \dots, x_n$ of even degree is the commutative graded k-algebra $k[x_1, \dots, x_n] = k[x_1] \otimes_k \cdots \otimes_k k[x_n]$.

The homogeneous elements of degree i are the homogeneous polynomials of degree i. Similarly, the exterior algebra $\wedge_k(x_1, \dots, x_n)$ on generators $x_1, \dots, x_n$ of odd degree is $\wedge_k(x_1) \otimes_k \cdots \otimes_k \wedge_k(x_n)$.

Proposition A.5. *If a graded commutative ring R is Noetherian then R^0 is Noetherian and R is finitely generated as a ring over R^0 by homogeneous elements.*

Proof. Since R is Noetherian and $R/R^+ = R^0$, R^0 is Noetherian. The ideal R^+ is finitely generated. Each generator is a finite sum of homogeneous elements hence R^+ is generated by a finite number of homogeneous elements $x_1, \dots x_n$. Thus, R is generated as a ring over R^0 by $x_1, \dots, x_n$ and 1. □

In fact, the converse is also true when $R^0 = k$ is a field, see remark A.17 below. In the situation of the previous proposition R is a finitely generated graded commutative R^0-algebra. Note that if R is a graded commutative Noetherian ring with R^0 a field, then from a purely graded perspective the ring is (graded commutative) local with maximal ideal R^+.

A.1 The prime ideal spectrum

Let R be a graded commutative Noetherian ring with $R^0 = k$ a field. As usual, $\operatorname{Spec} R$ denotes the set of prime ideals in R, and is also called the prime ideal spectrum of R.

Let $\varphi\colon R \to S$ be a ring homomorphism. If $\mathfrak{p}$ is a prime ideal of S, then $f^{-1}(\mathfrak{p})$ is a prime ideal of R, i.e., f induces a map of sets

$$f^{-1}\colon \operatorname{Spec} S \to \operatorname{Spec} R.$$

In other words, $R \mapsto \operatorname{Spec} R$ is a contravariant functor from the category of rings to the category of sets.

For an ideal I of R the set of prime ideals containing I is called the variety of I and is denoted $V(I)$, that is,

$$V(I) = \{\, \mathfrak{p} \in \operatorname{Spec} R \,|\, I \subset \mathfrak{p} \,\}.$$

Furthermore, the set

$$\sqrt{I} = \{\, x \in R \,|\, x^n \in I \text{ for some } n \,\}$$

is an ideal of R, which is called the radical of I. The nilpotent elements in R, or the nilradical of R, is the radical of the zero ideal and is also denoted $\operatorname{Nil}(R)$.

If k has characteristic 2, R is strictly commutative. If k has characteristic different from 2, every element of odd degree square to zero, i.e., the elements of odd degree are contained in the nilradical which is contained in every prime ideal of R. In other words, the prime ideal spectrum of R and $R/\operatorname{Nil}(R)$ coincide. Furthermore, if I is an ideal of R, then $V(I) = V(I + \operatorname{Nil}(R))$, i.e., $V(I)$

and $V((I+\operatorname{Nil}(R))/\operatorname{Nil}(R))$ also coincide. Note that $R/\operatorname{Nil}(R)$ is a commutative graded ring since the nilradical is homogeneous by the following proposition. Summarizing, we may assume that R is strictly commutative in matters concerning prime ideals and thus apply well known results from commutative algebra.

First some elementary properties of radicals and varieties.

Proposition A.6.

(1) If I is a homogeneous ideal in R, then the radical $\sqrt{I}$ is also a homogeneous ideal.

(2) If I is an ideal of R, then $\sqrt{I} = \bigcap_{\mathfrak{p}\in V(I)} \mathfrak{p}$. In particular, if $\mathfrak{p}$ is a prime ideal of R, then $\sqrt{\mathfrak{p}} = \mathfrak{p}$.

Proof. (1) It is difficult to find a reference for this fact, so we give a proof: Suppose $x = x_1 + \cdots + x_m \in \sqrt{I}$, $|x_1| < \cdots < |x_m|$, i.e., $x^n \in I$ for some n. Since I is homogeneous, each homogeneous term of x^n is in I. In particular, the homogeneous term x_1^n of x^n of smallest degree is in I. So $x_1 \in \sqrt{I}$ and $y = x - x_1 \in \sqrt{I}$. Iterating gives that $x_1, \ldots, x_m \in \sqrt{I}$. Thus, $\sqrt{I}$ is homogeneous.

(2) see [34] p. 3. □

Proposition A.7.

(1) If I and J are ideals in R, then $V(I) \cup V(J) = V(I \cap J) = V(IJ)$.

(2) If $\{I_\lambda\}_{\lambda\in\Lambda}$ is any family of ideals in R, then

$$\bigcap_{\lambda\in\Lambda} V(I_\lambda) = V(\bigoplus_{\lambda\in\Lambda} I_\lambda).$$

(3) If I is an ideal, then $V(I) = V(\sqrt{I})$.

Proof. (1)-(2) see [34] p. 24. (3) by proposition A.6. □

Recall that for any R-module M the annihilator of an element m in M is the ideal

$$\operatorname{Ann}_R(m) = \{\, r \in R \,|\, rm = 0 \,\},$$

and the annihilator of M is the ideal

$$\operatorname{Ann}_R M = \bigcap_{m\in M} \operatorname{Ann}_R(m),$$

i.e., the elements in R which annihilate all elements in M. The union of all annihilators of nonzero elements in M is the set of zero divisors of M.

An ideal in R is said to be associated to the R-module M if it is the annihilator of some nonzero element in M. An associated prime ideal, or simply an associated prime, of M is a prime ideal associated to M. The set of prime ideals associated to M is denoted $\operatorname{Ass}_R M$, that is,

$$\operatorname{Ass}_R M = \{\, \mathfrak{p} \in \operatorname{Spec} R \,|\, \mathfrak{p} = \operatorname{Ann}_R(m) \text{ for some } m \in M \,\}.$$

The associated primes of R is simply denoted $\operatorname{Ass} R$.

It is not clear that we may reduce questions about associated primes to questions in $R/\operatorname{Nil}(R)$. Instead we shall just note that the proofs of the statements of the following proposition in the commutative case goes verbatim through to the graded commutative case. The diligent reader should have no problems verifying this.

Proposition A.8. *Suppose M is a graded R-module.*

(1) Every maximal element in the set $\{\operatorname{Ann}_R(m) \,|\, 0 \neq m \in M\}$, ordered under inclusion, is an associated prime of M. In particular, every nontrivial module has an associated prime.

(2) The set of zero divisors of M is the union of all associated primes of M.

(3) If M is finitely generated, then $\operatorname{Ass}_R M$ is a finite set.

(4) If M is finitely generated, then the minimal elements, ordered under inclusion, of $\operatorname{Ass}_R M$ and $V(\operatorname{Ann}_R M)$ coincide. In particular, the minimal prime ideals of R are associated primes.

(5) Any associated prime ideal of M is homogeneous and the annihilator of a homogeneous element in M.

Proof. (1)-(2): [34] theorem 6.1. (3)-(4): [5] proposition 2.2.5. (5): [13] lemma 1.5.6. □

Proposition A.9. *Suppose $\mathfrak{p}$ is a prime ideal of R. Let $\mathfrak{p}^*$ be the ideal generated by all homogeneous elements in $\mathfrak{p}$. Then $\mathfrak{p}^*$ is a prime ideal of R.*

Proof. Notice that $(\mathfrak{p}/\operatorname{Nil}(R))^* = \mathfrak{p}^*/\operatorname{Nil}(R)$ since $\operatorname{Nil}(R)$ is homogeneous. By the commutative case, see [13] lemma 1.5.6, $\mathfrak{p}^*/\operatorname{Nil}(R)$ is a prime ideal which implies that $\mathfrak{p}^*$ is a prime ideal. □

A.2 Krull dimension

Let R be a graded commutative Noetherian ring with $R^0 = k$ a field.

Definition A.10. *The Krull dimension, or simply the dimension, of the ring R is denoted $\dim R$ and is defined to be the supremum of lengths n of strictly increasing chains of prime ideals*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

in R. For an R-module M the dimension of M is defined to be the dimension of $R/\operatorname{Ann}_R M$ and is denoted $\dim_R M$.

As an example, the dimension of a graded polynomial algebra $k[x_1, \dots, x_n]$ is n, see e.g. [5] proposition 1.4.1. An immediate consequence of proposition A.8(4):

Proposition A.11. *Suppose M is a finitely generated R-module. Then*

$$\dim_R M = \max\{\, \dim R/\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Ass}_R M \,\}.$$

For reference we collect a few elementary properties.

Proposition A.12.

(1) For an ideal I in R, $\dim_R R/I = \dim R/I = \dim R/\sqrt{I}$. In particular, if $I \subset \operatorname{Nil}(R) = \sqrt{0}$, then $\dim R = \dim R/I$.

(2) If $I \subset J$ are ideals in R, then $\dim R/I \geq \dim R/J$. In particular, $\dim_R M \leq \dim R$ for all R-modules M.

(3) If $I_1, \dots, I_n$ are ideals in R, then

$$\dim R/(I_1 \cap \dots \cap I_n) = \max\{\dim R/I_j \mid 1 \leq j \leq n\,\}.$$

Proof. (1) since $\operatorname{Ann}_R R/I = I$ and $V(I) = V(\sqrt{I})$, see proposition A.7. (2) since $V(J) \subset V(I)$. (3) follows from the fact that $V(I_1 \cap \dots \cap I_n) = V(I_1) \cup \dots \cup V(I_n)$, see proposition A.7. □

Let $R \subset S$ be an extension of rings. Then we may consider S as an R-module. An element $x \in S$ is called integral over R if x is a root of a monic polynomial with coefficients in R. If every element in S is integral over R we say that S is integral over R or that $R \subset S$ is an integral extension. More generally, if $\varphi\colon R \to S$ is a homomorphism of rings, then S is an R-module via φ, that is, $rs = \varphi(r)s$ for $r \in R$ and $s \in S$ and we say S is integral over R if S is integral over the image of φ.

All nilpotent elements in S are trivially integral over R. The canonical homomorphism $\varphi\colon R/\operatorname{Nil}(R) = R/(\operatorname{Nil}(S) \cap R) \to S/\operatorname{Nil}(S)$, $\varphi([x]) = [x]$, is injective, and we may consider $R/\operatorname{Nil}(R)$ as a subring of $S/\operatorname{Nil}(S)$. It is straightforward to check that $R/\operatorname{Nil}(R) \subset S/\operatorname{Nil}(S)$ is an integral extension if and only if $R \subset S$ is an integral extension. Thus, in matters involving integral extensions and prime ideals we may assume the rings are strictly commutative.

Theorem A.13. *Let $R \subset S$ be an extension of rings.*

(1) If S is finitely generated as an R-module, then S is integral over R.

(2) The subset of S of integral elements over R is a subring containing R.

Proof. Both statements follow easily from the commutative case, see [34] theorem 9.1.

(1) If S is finitely generated as a module over R, then $S/\operatorname{Nil}(S)$ is finitely generated as a module over $R/\operatorname{Nil}(R)$. By the commutative case, $S/\operatorname{Nil}(S)$ is integral over $R/\operatorname{Nil}(R)$, i.e., S integral over R.

(2) If $x, y \in S$ are integral over R, then $[x], [y] \in S/\operatorname{Nil}(S)$ are integral over $R/\operatorname{Nil}(R)$. Thus, $[xy]$ and $[x \pm y]$ are integral over $R/\operatorname{Nil}(R)$, hence xy and $x \pm y$ are integral over R. □

For an extension $R \subset S$ of rings, a prime ideal $\mathfrak{q}$ of S is said to lie over a prime ideal $\mathfrak{p}$ in R if $\mathfrak{q} \cap R = \mathfrak{p}$.

Theorem A.14. *Let $R \subset S$ be an integral extension.*

(1) If $\mathfrak{p}$ is a prime ideal of R, then there exists a prime ideal $\mathfrak{q}$ of S lying over $\mathfrak{p}$, and there are no strict inclusions between prime ideals lying over $\mathfrak{p}$.

(2) Suppose $\mathfrak{p} \subset \mathfrak{p}'$ are prime ideals of R and $\mathfrak{q}$ is a prime ideal lying over $\mathfrak{p}$. Then there exists a prime ideal $\mathfrak{q}'$ of S lying over $\mathfrak{p}$ with $\mathfrak{q} \subset \mathfrak{q}'$.

Proof. [34] theorem 9.4. □

An immediate consequence is that dimension is preserved by integral extensions.

Corollary A.15. *Let $R \subset S$ be an integral extension. If I is an ideal of S, then $\dim S/I = \dim R/(I \cap R)$. In particular, if $R \subset S$ is an integral extension, then $\dim R = \dim S$.*

Proof. Replace S/I by S and $R/(I \cap R)$ by R, that is, we may assume $I = 0$. Now, use theorem A.14. □

Proposition A.16. *Let k be a field of characteristic $p > 0$. Suppose $\varphi\colon R \to S$ is an F-isomorphism of k-algebras, that is, the kernel of φ consists of nilpotent elements and for each $x \in S$ there exists $n \geq 0$ such that $x^{p^n} \in R$. Then $\varphi^{-1}\colon \operatorname{Spec} S \to \operatorname{Spec} R$ is a bijection.*

Proof. We may assume R is commutative. Since $R/\operatorname{Ker}\varphi$ is isomorphic to $\operatorname{Im}\varphi$, and $\operatorname{Spec} R$ and $\operatorname{Spec} R/\operatorname{Ker}\varphi$ coincide we may assume φ is an inclusion, i.e., $R \subset S$.

φ^{-1} surjective: By theorem A.14 since S is clearly integral over R.

φ^{-1} injective: Let $\mathfrak{p}$ be a prime ideal of R. Consider the set

$$\mathfrak{q} = \{\, x \in S \mid x^{p^n} \in \mathfrak{p} \text{ for some } n \geq 0 \,\}.$$

Suppose $\mathfrak{q}$ is prime ideal of S contained in any prime ideal of S lying over $\mathfrak{p}$. Since there are no strict inclusions between prime ideals lying over $\mathfrak{p}$, $\mathfrak{q}$ is the only prime ideal lying over $\mathfrak{p}$. In other words, φ^{-1} is injective. Thus, it remains to prove the two statements about $\mathfrak{q}$.

Suppose $\mathfrak{p}'$ lies over $\mathfrak{p}$. If $x \in \mathfrak{q}$, then $x^q \in \mathfrak{p} \subset \mathfrak{p}'$ for some power q of p. It follows that $x \in \mathfrak{p}'$ since $\mathfrak{p}'$ is prime ideal, i.e., $\mathfrak{q} \subset \mathfrak{p}'$.

$\mathfrak{q}$ prime ideal: Let $x, y \in \mathfrak{q}$, i.e., $x^{p^m}, y^{p^n} \in \mathfrak{p}$ for some $m, n \geq 0$. Using that the Frobenius map is a homomorphism in characteristic p,

$$(x+y)^{p^{m+n}} = x^{p^{m+n}} + y^{p^{m+n}} \in \mathfrak{p}.$$

Furthermore, if $s \in S$, i.e., $s^{p^l} \in R$ for some $l \geq 0$, then

$$(sx)^{p^{l+m}} = s^{p^{l+m}} x^{p^{l+m}} \in \mathfrak{p}.$$

Thus, $\mathfrak{q}$ is an ideal of S.

Let $s' \in S$ and $ss' \in \mathfrak{q}$, i.e., $(ss')^q \in \mathfrak{p}$ for some power q of p. Then $s^q(s')^q \in \mathfrak{p}$. Since $\mathfrak{p}$ is a prime ideal in R, s^q or $(s')^q$ is in $\mathfrak{p}$. In any event, s or s' is in $\mathfrak{q}$. It follows that $\mathfrak{q}$ is a prime ideal. □

Another way of dealing with the graded commutativity when the characteristic of k is different from 2 is to use the subring R^{ev} of R consisting of the elements in even degree, i.e., $R^{ev} = \bigoplus_{i \geq 0} R^{2i}$. In case of the characteristic of k is 2 we set $R^{ev} = R$.

Note that R^{ev} is a finitely generated commutative graded k-algebra. It is generated as a k-algebra by the k-algebra generators of R of even degree and the products of pairs of generators of R of odd degree. Furthermore, R is finitely generated as a module over R^{ev}. This follows since the k-algebra generators of R of odd degee square to zero hence there are only finite many nontrivial products of these.

Remark A.17. A partial converse to proposition A.5: Suppose R is a finitely generated graded commutative R^0-algebra with $R^0 = k$ a field. Hilbert's basis theorem implies that R^{ev} is Noetherian. Since R is finitely generated as a module over R^{ev}, R is Noetherian as a R^{ev}-module, i.e., R is Noetherian as a ring.

Using this approach we can prove a graded commutative version of Noether normalization using the commutative graded version, see [5] theorem 2.2.7.

Let M be a graded R-module. Observe that no nontrivial element in $k = R^0$ is in $\operatorname{Ann}_R M$ and the image of $k = R^0$ in $R/\operatorname{Ann}_R M$ is isomorphic to k. We implicitly use this identification in the following theorem. Similarly for R^{ev}.

Theorem A.18. *Let R be a graded commutative Noetherian ring with $R^0 = k$ and M a finitely generated graded R-module. Then there exists homogeneous elements $x_1, \ldots, x_n$ of positive degree in R which are algebraically independent over k in $R/\operatorname{Ann}_R M$ such that M is a finitely generated module over the polynomial subring $k[x_1, \ldots, x_n]$ of $R/\operatorname{Ann}_R M$ and n is the dimension of M.*

If $R = M$ is an integral domain, then n is equal to the transcendence degree (the maximal number of algebraically independent elements) of R over k.

Proof. Applying the commutative version of Noether normalization to the R^{ev}-module M gives homogeneous elements $x_1, \dots, x_n$ in R^{ev} with the properties of the theorem. We also write x_i for the image of x_i in $R/\operatorname{Ann}_R M$ or $R^{ev}/\operatorname{Ann}_{R^{ev}} M$.

Suppose $f(x_1, \dots, x_n) = 0$ in $R/\operatorname{Ann}_R M$ for some polynomial f with coefficients in k, that is, $f(x_1, \dots, x_n) \in \operatorname{Ann}_R M$. Noting that $x_1, \dots, x_n$ are elements in R^{ev} gives that $f(x_1, \dots, x_n) \in \operatorname{Ann}_R M \cap R^{ev} = \operatorname{Ann}_{R^{ev}} M$ which contradicts the algebraic independence of $x_1, \dots, x_n$ in $R^{ev}/\operatorname{Ann}_{R^{ev}} M$. It follows that $x_1, \dots, x_n$ are algebraically independent over k in $R/\operatorname{Ann}_R M$.

Remember that R is finitely generated as a module over R^{ev} and $\operatorname{Ann}_{R^{ev}} M = \operatorname{Ann}_R M \cap R^{ev}$. Corollary A.15 gives that

$$\dim_R M = \dim R/\operatorname{Ann}_R M = \dim R^{ev}/\operatorname{Ann}_{R^{ev}} M = \dim_{R^{ev}} M = n.$$

Finally, the statement about finite generation is clear. □

A homogeneous system of parameters of a finitely generated graded module M over R is a sequence of homogeneous elements $x_1, \dots, x_n$ satisfying the conditions of the theorem.

A.3 Regular sequences and depth

As usual, let R be a graded commutative Noetherian ring with $R^0 = k$ a field. Recall that R^+ denotes the ideal generated by the elements of positive degree and R^{ev} denotes the ideal generated by the elements of even degree.

Definition A.19. *Let M be a finitely generated graded R-module.*

A homogeneous element $x \in R^+$ is called an M-regular element in R if x is not a zero divisor of M, or equivalently, if multiplication by x is injective.

A sequence $x_1, \dots, x_n$ of homogeneous elements in R^+ is called an M-regular sequence in R if x_i is $M/(x_1, \dots, x_{i-1})M$-regular for $1 \leq i \leq n$, where $(\emptyset) = 0$.

An M-regular sequence $x_1, \dots, x_n$ is said to be maximal if $x_1, \dots, x_n, x_{n+1}$ is not an M-regular sequence for all $x_{n+1} \in R^+$.

An R-regular element is simply called regular. Similarly, an R-regular sequence is simply called a regular sequence. Concentration on homogeneous elements is not a restriction as we shall see later.

Recall that the set of zero divisors of M is the union of the finitely many associated primes of M. In other words, choosing regular elements is about avoiding the finite union of associated primes.

Note that, if $x_1, \dots, x_n$ is an M-regular sequence, then

$$(x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, x_2, \dots, x_n)$$

is a strictly ascending chain of ideals in R: Suppose $x_{i+1} \in (x_1, \ldots, x_i) = I$. Then $x_{i+1}M \subset IM$, that is, M/IM is annihilated by x_{i+1} which contradicts that x_{i+1} is M/IM-regular. In particular, since R is Noetherian there exist maximal M-regular sequences.

Observe that nilpotent elements can not be regular elements, so every regular element is in R^{ev}. Usually, for more general definitions of regular sequences it is also required that $M/(x_1, \ldots, x_n)M \neq 0$. This is not necessary in the present situation by the following graded version of Nakayama's lemma.

Lemma A.20. *If M is a graded R-module with $R^+M = M$, then $M = 0$.*

Proof. Suppose $M \neq 0$. Choose i minimal such that $M^i \neq 0$. Consider a nontrivial element $x \in M^i$. Since $R^+M = M$, there exist homogeneous elements $r_j \in R^+$ and $x_j \in M$ such that $x = \sum x_j m_j$. But, $|r_j| > 0$ whence $|m_j| < i$, that is, $m_j = 0$. It follows that $x = 0$. □

Remark A.21. Multiplication by a homogeneous element x in R is in general not an R-module map $M \to M$ for an R-module M. However, one may construct an R-module map $\mu_x \colon M \to M$ with the same image and kernel as multiplication by x as a map of sets. For a homogeneous element $m \in M$ define $\mu_x(m) = (-1)^{|x||m|}xm$. Now, for a homogeneous element r in R,

$$\mu_x(rm) = (-1)^{|x|(|r|+|m|)}xrm = r(-1)^{|x||m|}xm = r\mu_x(m).$$

Extending linearly gives an R-module map, also for x not homogeneous. Of course, if x has even degree then multiplication by x is indeed an R-module map.

Next is a few properties of regular sequences.

Theorem A.22. *Let M be a finitely generated graded R-module. A sequence of homogeneous elements $x_1, \ldots, x_n$ in R^+ is an M-regular sequence if and only if $x_1, \ldots, x_n$ are algebraically independent over k in R and M is a free module over $k[x_1, \ldots, x_n]$.*

We give a detailed version of the proof given in [18], see proposition 12.2.1, which is a slightly modified version of a proof in [24], see proposition 10.3.4. It should be noted that neither of the authors address the issue of algebraic independence over k of a regular sequence. The author do not find this to be clear from the definitions. Kaplansky [31], see the concluding remarks, gives a sketch of a direct proof in the case of a regular sequence for the ring. The proof does not seem to generalize to the case of a regular sequence for a module. However, we may appeal to the well known fact for commutative graded Noetherian rings with a field in degree zero, any regular sequence may be extended to a homogeneous system of parameters, see e.g. [5]. More specifically, see the proof of theorem 2.2.7 for the construction of a homogeneous system of parameters. Since an M-regular sequence in R is contained in R^{ev}, it follows that it is an M-regular sequence in R^{ev}, i.e., the sequence forms an algebraic independent set over k.

Proof of theorem A.22. Suppose $x_1, \dots, x_n$ is an M-regular sequence in R. We use induction on n to prove that M is a free module over $k[x_1, \dots, x_n]$.

Let $n = 1$. Choose homogeneous elements $\{e_i\}_{i\in I}$ in M such that the set $\{[e_i]\}_{i\in I}$ of cosets is a k-basis for M/x_1M. The claim is that $\{e_i\}_{i\in I}$ is a $k[x_1]$-basis for M.

$M = k[x_1]\{e_i\}_{i\in I}$: Let $[m] \in M/x_1M$, m homogeneous. Since $[m] = \sum_i c_i[e_i]$ for some $c_i \in k$, it follows that $m = \sum_i c_ie_i + x_1m_1$ for some homogeneous m_1. Note that $|m_1| < |m|$ since $|x_1| > 0$. Now, $[m_1] = \sum_i c_{1,i}[e_i]$, that is, $m_1 = \sum_i c_{1,i}e_i + x_1m_2$ for some m_2. Iterating gives the result.

The set $\{e_i\}_{i\in I}$ is $k[x_1]$-linear independent: Suppose $\sum_{i\in J} f_ie_i = 0$, $J \subset I$ finite subset, is a linear relation with coefficients in $k[x_1]$. Each homogeneous term is zero and has the form

$$y = c_0e_{i_0} + c_1x_1e_{i_1} + c_lx_1^le_{i_l},$$

for some $c_l \in k$. Since the image in M/x_1M is $c_0[e_{i_0}] = 0$, it follows that $c_0 = 0$. Thus,

$$y = c_1x_1e_{i_1} + c_lx_1^le_{i_l} = x_1(c_1e_{i_1} + c_lx_1^{l-1}e_{i_l}) = 0.$$

Note that $y/x_1 = 0$ since x_1 is a regular element. As before we conclude that $c_1 = 0$. Iterating gives that $c_0 = c_1 = \cdots = c_l = 0$. Applying this to each homogeneous term gives that $f_i = 0$ for all $i \in J$.

This proves that M is a free module over $k[x_1]$.

Let $n > 1$. Set $I_n = (x_1, \dots, x_{n-1}) \subset k[x_1, \dots, x_n]$. By induction, M is a free module over $k[x_1, \dots, x_{n-1}]$ and M/IM is a free module over $k[x_n]$.

Choose homogeneous elements $\{e_i\}_{i\in I}$ in M such that $\{[e_i]\}_{i\in I}$ is a $k[x_n]$-basis for M/I_nM. Let F be the free $k[x_1, \dots, x_n]$-module on symbols $\{f_i\}_{i\in I}$. Consider the canonical homomorphism $f\colon F \to M$, $f_i \mapsto e_i$. Let K be the kernel of f which is a graded $k[x_1, \dots, x_n]$-submodule of F. Thus, there is an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r] & F \arrow[r, "f"] & M \arrow[r] & 0 \end{tikzcd}$$

of $k[x_1, \dots, x_n]$-modules. Since M is free over $k[x_1, \dots, x_{n-1}]$, this sequence splits considered as a sequence of $k[x_1, \dots, x_{n-1}]$-modules.

For a graded module N over $k[x_1, \dots, x_{n-1}]$ we have that $N \otimes_{k[x_1,\dots,x_{n-1}]} k$ is isomorphic to N/I_nN. To see this apply $- \otimes_{k[x_1,\dots,x_{n-1}]} N$ to the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & I_n \arrow[r] & k[x_1, \dots, x_{n-1}] \arrow[r] & k \arrow[r] & 0, \end{tikzcd}$$

and use the right exactness of the tensor product, and that the image of $I_n \otimes_{k[x_1,\dots,x_{n-1}]} N$ in $k[x_1, \dots, x_{n-1}] \otimes_{k[x_1,\dots,x_{n-1}]} N = N$ is I_nN.

Since the tensor product sends split sequences to exact sequences,

$$\begin{tikzcd} 0 \arrow[r] & K/I_nK \arrow[r] & F/I_nF \arrow[r, "f"] & M/I_nM \arrow[r] & 0 \end{tikzcd}$$

is an exact sequence of $k[x_1, \ldots, x_{n-1}]$-modules.

By construction, the map $f\colon F/I_nF \to M/I_nM$ induced by f is an isomorphism of $k[x_n]$-modules, i.e., $K/I_nK = 0$. It follows that $K = 0$. The latter follows by using the grading, looking at elements of K of lowest degree and that elements of I_n have degree greater than zero, the details are left to the reader.

Conversely, suppose $x_1, \ldots, x_n$ are algebraically independent over k in R and M free over $k[x_1, \ldots, x_n]$. Since $x_1, \ldots, x_n$ is a regular sequence in $k[x_1, \ldots, x_n]$ it is clear that it is an M-regular sequence. □

Corollary A.23. *If $x_1, \ldots, x_n$ is an M-regular sequence, then so is $x_1^{e_1}, \ldots, x_n^{e_n}$ for all positive integers $e_1, \ldots, e_n$.*

Proof. Since $x_1, \ldots, x_n$ are algebraically independent over k, $x_1^{e_1}, \ldots, x_n^{e_n}$ are also algebraically independent over k. Note that $k[x_1, \ldots, x_n]$ is a free module over $k[x_1^{e_1}, \ldots, x_n^{e_n}]$. Since M is a free module over $k[x_1, \ldots, x_n]$, M is a free module over $k[x_1^{e_1}, \ldots, x_n^{e_n}]$. □

The following theorem gives a homological characterization of regular sequences.

Theorem A.24. *Let M be a finitely generated graded R-module and $x_1, \ldots, x_n$ an M-regular sequence. Then there exists an $M/(x_1, \ldots, x_n)M$-regular element in R^+ if and only if $\operatorname{Ext}_R^n(k, M) = 0$.*

In particular, all maximal M-regular sequences have the same length, namely

$$\min\{\, n \mid \operatorname{Ext}_R^n(k, M) \neq 0 \,\},$$

and any regular sequence may be extended to a maximal M-regular sequence.

Of course, this is well known from commutative algebra. The usual arguments apply in the graded commutative case. Since it can not be found in the literature, we briefly go through the details. In the following identify R/R^+ and k, and $\operatorname{Hom}_R(k, M)$ denotes the group of R-homomorphisms $k \to M$. The theorem follows from a series of lemmas.

Lemma A.25. *Suppose an ideal I is contained in a finite union of prime ideals $\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$. Then $I \subset \mathfrak{p}_i$ for some i.*

Proof. Suppose $n > 1$ and I is not contained in the union of any proper subset of $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. Choose $x \in I$ such that $x \notin \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_{n-1}$, i.e., $x \in \mathfrak{p}_n$. Also choose elements $y \in I$ with $y \notin \mathfrak{p}_n$, and $z_i \in \mathfrak{p}_i$ with $z_i \notin \mathfrak{p}_n$ for $1 \leq i \leq n$. Now, $x + yz_1 \cdots z_{n-1} \in I$ but is not in $\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$. □

Lemma A.26. *Suppose M is a finitely generated graded R-module. Then R^+ consists of zero divisors of M if and only if R^+ is an associated prime of M.*

Proof. Suppose R^+ consists of zero divisors. If $x \in R^+$, then x annihilates an element m of M, i.e., $x \in \operatorname{Ann}_R(m)$. Since maximal annihilators are associated primes, x is in some associated prime of M. It follows that R^+ is contained in the union of all associated primes of M. However, there are only a finite number of associated primes, and since $k = R^0$ is a field they are all contained in R^+. In other words, R^+ is a finite union of associated primes. By lemma A.25, R^+ is one of the associated primes.

Conversely, if $R^+ = \operatorname{Ann}_R(m)$ for some $m \in M$, then every element in R^+ is a zero divisor of m. □

Lemma A.27. *Let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ be a set of pairwise distinct prime ideals of R. Suppose $R^+ \neq \mathfrak{p}_i$ for all i. Then there exists a homogeneous element $x \notin \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$.*

Proof. Clearly, we may assume the prime ideals are homogeneous. Using induction on n, assume $\mathfrak{p}_n$ is minimal in $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ and $x' \notin \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_{n-1}$. If $x' \notin \mathfrak{p}_n$, we are done. Suppose $x' \in \mathfrak{p}_n$. Since $\mathfrak{p}_n$ is minimal, there exists an element $r \in \bigcap_{1 \leq i \leq n-1} \mathfrak{p}_i - \mathfrak{p}_n$. Choose $y \in R^+ - \mathfrak{p}_n$. Consequently, $x = (x')^u + (ry)^v$ is homogeneous for some u, v. Note that $ry \in \mathfrak{p}_i$ for all $1 \leq i \leq n-1$ and $ry \notin \mathfrak{p}_n$. If $x \in \mathfrak{p}_n$, then $x - (x')^u = (ry)^v \in \mathfrak{p}_n$, a contradiction. If $x \in \mathfrak{p}_i$, $1 \leq i \leq n-1$, then $x - (ry)^v = (x')^u \in \mathfrak{p}_i$, a contradiction. Thus, $x \notin \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$. □

Lemma A.28. *Let M be a finitely generated R-module. Then every homogeneous element in R^+ is a zero divisor of M if and only if R^+ consists of zero divisors of M.*

Proof. Obviously, if R^+ consists of zero divisors, then every homogeneous element is a zero divisor.

Conversely, if R^+ do not consist of zero divisors, then R^+ is not equal to any of the finitely many associated primes of M, see lemma A.26. By lemma A.27, the exists a homogeneous element not contained in the union of the associated primes, i.e., there exists a homogeneous M-regular element. □

Lemma A.29. *Let M be a finitely generated graded R-module. Then R^+ contains an M-regular element if and only if* $\operatorname{Hom}_R(k, M) = 0$.

Proof. Suppose R^+ consists of zero divisors. Then, by lemma A.26, R^+ is an associated prime of M, i.e., $R^+ = \operatorname{Ann}_R(m)$ for some nonzero m in M. It follows that the homomorphism $R \to M$, $r \mapsto rm$, induces a nontrivial homomorphism $k \to M$.

Conversely, let x be an M-regular element and $f \in \operatorname{Hom}_R(k, M)$. Since $xy = 0$ for all y in k, $0 = f(xy) = xf(y)$, i.e., $f(y) = 0$ since multiplication by x is injective. □

Lemma A.30. *Let M be a finitely generated graded R-module, and $x_1, \dots, x_n$ an M-regular sequence. Then* $\operatorname{Hom}_R(k, M/(x_1, \dots, x_n)M) \cong \operatorname{Ext}^n_R(k, M)$.

Proof. The proof is induction on n. The case $n = 0$ follows from the fact that $\operatorname{Hom}_R(k, M) \cong \operatorname{Ext}^0_R(k, M)$.

Let $n > 0$. By induction,

$$\operatorname{Ext}^{n-1}_R(k, M) \cong \operatorname{Hom}_R(k, M/(x_1, \dots, x_{n-1})M).$$

Lemma A.29 gives that $\operatorname{Ext}^{n-1}_R(k, M) = 0$ since x_n is $M/(x_1, \dots, x_{n-1})M$-regular.

The exact sequence of R-modules

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "x_1"] & M \arrow[r] & M/x_1M \arrow[r] & 0 \end{tikzcd}$$

gives an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Ext}^{n-1}_R(k, M/x_1M) \arrow[r] & \operatorname{Ext}^n_R(k, M) \arrow[r, "x_1"] & \operatorname{Ext}^n_R(k, M). \end{tikzcd}$$

Since x_1 annihilates the R-module $k = R/R^+$ and Ext is an additive functor, the map $\operatorname{Ext}^*_R(k, M) \to \operatorname{Ext}^*_R(k, M)$ induced by multiplication by x_1 is the trivial map.

Hence,

$$\operatorname{Ext}^{n-1}_R(k, M/x_1M) \cong \operatorname{Ext}^n_R(k, M).$$

Note that $x_2, \dots, x_n$ is an M/x_1M-regular sequence. So, by induction,

$$\operatorname{Ext}^{n-1}_R(k, M/x_1M) \cong \operatorname{Hom}_R(k, M/(x_1, \dots, x_n)M).$$

This finishes the proof. □

Combining lemma A.29 and lemma A.30 proves theorem A.24. Using theorem A.24 we have the usual definition and homological characterization of depth in case of a graded commutative ring.

Definition A.31. *The depth of a finitely generated R-module M is the length of a maximal M-regular sequence and is denoted* $\operatorname{depth}_R M$. *The depth of R is simply denoted* $\operatorname{depth} R$.

Theorem A.32. *If M is a finitely generated graded R-module, then*

$$\operatorname{depth}_R M = \min\{\, n \mid \operatorname{Ext}^n_R(k, M) \neq 0 \,\}.$$

Proposition A.33. *If M is a finitely generated graded R-module, and $\mathfrak{p}$ is an associated prime of M, then* $\operatorname{depth}_R M \leq \dim R/\mathfrak{p}$. *In particular,*

$$\operatorname{depth}_R M \leq \min\{\dim R/\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Ass}_R M \,\}.$$

Proof. Suppose $\mathfrak{p} = \operatorname{Ann}_R(m)$, $m \in M$, is an associated prime of M. Since $\mathfrak{p}$ is homogeneous, $R/\mathfrak{p}$ is a finitely generated graded integral domain. Let $d = \operatorname{depth}_R M$. Thus, there exists an M-regular sequence $x_1, \dots, x_d$ in R such that $x_1, \dots, x_d$ are algebraically independent over k and M is a free $k[x_1, \dots, x_d]$-module. Hence, $k[x_1, \dots, x_d] \cong k[x_1, \dots, x_d] \cdot m \subset Rm$. Furthermore, $Rm \cong R/\operatorname{Ann}_R(m) = R/\mathfrak{p}$, i.e., the images of $x_1, \dots, x_d$ in $R/\mathfrak{p}$ are algebraically independent over k. Since the dimension of $R/\mathfrak{p}$ is the maximal number of algebraically independent elements over k, see theorem A.18, it follows that $d \leq \dim R/\mathfrak{p}$. □

Corollary A.34. *If M is a finitely generated R-module, then* $\operatorname{depth}_R M \leq \dim_R M$.

Proof. Propositions A.11 and A.33. □

For example, the sequence $x_1, \dots, x_n$ is a regular sequence in the graded polynomial algebra $k[x_1, \dots, x_n]$. Since the depth cannot exceed the dimension, the sequence is maximal. In this example the depth is equal to the dimension. A ring or module with this property is called Cohen-Macaulay. Cohen-Macaulay rings are an interesting class of rings, see [13].

Proposition A.35. *Let R and S be graded commutative Noetherian rings with $R^0 = S^0 = k$. Then* $\operatorname{depth} R \otimes_k S \geq \operatorname{depth} R + \operatorname{depth} S$.

Proof. Let $x_1, \dots, x_m$ be an R-regular sequence and $y_1, \dots, y_n$ an S-regular sequence. By theorem A.22, R is a free module over the polynomial subring $k[x_1, \dots, x_m]$ and S is a free module over the polynomial subring $k[y_1, \dots, y_n]$. It is straightforward to verify that $R \otimes_k S$ is a free module over the polynomial subring $k[x_1, \dots, x_m] \otimes_k k[y_1, \dots, y_n]$ of $R \otimes_k S$. □

Proposition A.36. *Let M be a finitely generated graded R-module. If $x_1, \dots, x_n$ is an M-regular sequence, then* $\operatorname{depth}_R M/(x_1, \dots, x_n)M = \operatorname{depth}_R M - n$.

Proof. By induction it suffices to consider the case $n = 1$, which follows from the fact that $\operatorname{Ext}_R^{n-1}(k, M/xM) \cong \operatorname{Ext}_R^n(k, M)$, see the proof of lemma A.30. □

Proposition A.37. *Suppose M and N are finitely generated R-modules. Then*

$$\operatorname{depth}_R M \oplus N = \min\{\operatorname{depth}_R M, \operatorname{depth}_R N\}.$$

Proof. Follows immediately from the homological characterization of depth and the fact that Ext is an additive functor. □

Proposition A.38. *Let R and S be graded commutative Noetherian rings with $R^0 = S^0 = k$. Suppose $R \subset S$ and S is finitely generated as a module over R. If M is a finitely generated S-module, then*

$$\operatorname{depth}_R M = \operatorname{depth}_S M.$$

In particular, $\operatorname{depth}_R S = \operatorname{depth} S$.

Proof. Clearly, any M-regular sequence in R is an M-regular sequence in S. Thus, it suffices to prove that any maximal M-regular sequence in R is a maximal M-regular sequence in S. So let $x_1, \ldots, x_d$ be a maximal M-regular sequence in R.

Suppose $y \in S^n$ is a regular element of $\overline{M} = M/(x_1, \ldots, x_d)M$. Since S is finitely generated as a module over R, y is a root of a monic polynomial f with coefficients in R, that is,

$$f(y) = y^m + a_{m-1}y^{m-1} + \cdots a_1 y + a_0 = 0$$

for some $a_0, a_1, \ldots, a_{m-1} \in R$. Since $f(y) = 0$, the homogeneous parts of $f(y)$ are also zero. In particular, the part of degree $|y^m| = mn$, which is a monic polynomial in y with homogeneous coefficients, is zero. In other words, we may assume that a_i is homogeneous of degree $(m - i)n$.

Note that any element of R^+ is a zero divisor of $\overline{M}$. By lemma A.26, R^+ is an associated prime of $\overline{M}$, i.e., $R^+ = \mathrm{Ann}_R(\overline{m})$ for some nonzero $\overline{m}$ in $\overline{M}$. Since a_i is homogeneous of positive degree,

$$0 = f(y)\overline{m} = y^m \overline{m},$$

that is, y^m, and consequently y, is not a regular element on $\overline{M}$. This finishes the proof. □

We end this appendix with an investigation of what happens if we allow nonhomogeneous elements in the definition of regular sequences. Let M be a finitely generated graded R-module. Nowhere in the homological characterization of regular sequences, c.f. theorem A.24, did we use that M is graded and M-regular sequences consisted of homogenous elements. We only used that multiplication by a regular element is an R-module map, see e.g. the proof of lemma A.30, which follows from the fact that a homogeneous regular element has even degree. However, the proofs go through if we replace multiplication by an element with the corresponding R-module map, see remark A.21. In other words, theorem A.24 is also true if we allow nonhomogeneous elements. Hence, it is not a restriction to only consider homogeneous regular sequences.

B Cohomology rings of D_8 and Q_8

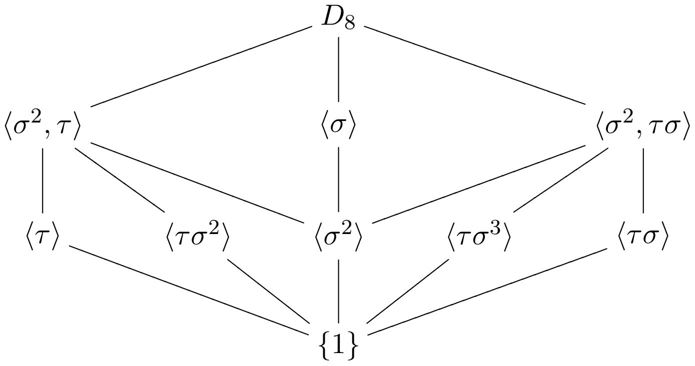
In this appendix we give a detailed computation using the Lyndon-Hochschild-Serre spectral sequence of the mod 2 cohomology ring of the dihedral group D_8 of order 8. Beside the actual ring structure, the restriction maps to the elementary abelian 2-subgroups are determined. For quick reference, there is a review of the results at the end of the section on the dihedral group. The computation of the cohomology of the quaternion group is similar and we do not present the details. The reader should, however, have no problem providing the details. We only consider mod 2 cohomology hence the coefficients will be omitted from the notation.

B.1 The dihedral group of order 8

One presentation of the dihedral group of order 8 is

$$D_8 = \langle\, \sigma, \tau \,|\, \sigma^4 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \,\rangle.$$

The subgroups of D_8 are


D_8
$\langle\sigma^2,\tau\rangle$
$\langle\sigma\rangle$
$\langle\sigma^2,\tau\sigma\rangle$
$\langle\tau\rangle$
$\langle\tau\sigma^2\rangle$
$\langle\sigma^2\rangle$
$\langle\tau\sigma^3\rangle$
$\langle\tau\sigma\rangle$
$\{1\}$

and there are only two conjugacy classes containing more than one subgroup, namely $\{\langle\tau\rangle, \langle\tau\sigma^2\rangle\}$ and $\{\langle\tau\sigma\rangle, \langle\tau\sigma^3\rangle\}$.

Note that $Z(D_8) = [D_8, D_8] = \langle\sigma^2\rangle$ is cyclic of order 2, where $[D_8, D_8]$ denotes the commutator subgroup. Furthermore,

$$D_8/Z(D_8) = D_8/[D_8, D_8] = \langle[\sigma], [\tau]\rangle = \{1, [\sigma], [\tau], [\tau\sigma]\} = \mathbb{Z}/2 \times \mathbb{Z}/2,$$

with cosets $1 = \{1, \sigma^2\}$, $[\sigma] = \{\sigma, \sigma^3\}$, $[\tau] = \{\tau, \tau\sigma^2\}$ and $[\tau\sigma] = \{\tau\sigma, \tau\sigma^3\}$.

We shall apply the Lyndon-Hochschild-Serre spectral sequence to the central group extension

$$\begin{tikzcd} 1 \arrow[r] & Z(D_8) \arrow[r] & D_8 \arrow[r] & D_8/Z(D_8) \arrow[r] & 1. \end{tikzcd}$$

Recall that

$$H^1(D_8) = \mathrm{Hom}(D_8, \mathbb{Z}/2) = \mathrm{Hom}(D_8/[D_8, D_8], \mathbb{Z}/2) = \mathbb{Z}/2 \times \mathbb{Z}/2.$$

In other words, $H^1(D_8)$ is the dual space of the $\mathbb{F}_2$-vector space $D_8/[D_8, D_8]$.

Let $x, y\colon D_8/[D_8, D_8] \to \mathbb{Z}/2$ be the dual basis, that is,

$$x([\sigma]) = 1, x([\tau]) = 0 \text{ and } y([\sigma]) = 0, y([\tau]) = 1.$$

In particular, $H^*(D_8/Z(D_8)) = \mathbb{F}_2[x, y]$ with x and y in degree one.

Remember that the restrictions of elements in degree one are easily determined using the natural identification of the first cohomology group and group homomorphisms, a technique we use implicitly.

The quotient $D_8/Z(D_8)$ acts trivially on $H^q(Z(D_8)) = \mathbb{Z}/2$. This follows from the fact that any p-group, p prime, acts trivially on $\mathbb{Z}/p$: Suppose G is a p-group acting on $\mathbb{Z}/p$, that is, there is a homomorphism

$$\varphi\colon G \to \operatorname{Aut}(\mathbb{Z}/p) = \mathbb{Z}/p^\times.$$

So $|\varphi(g)|$ is a power of p and divides $p - 1$, that is, $\varphi(g)$ is the identity. Of course, this is also a well known property of the spectral sequence of a central extension.

Recall that $H^*(Z(D_8)) = \mathbb{F}_2[w]$ with w in degree one. Since $D_8/Z(D_8)$ acts trivially on the cohomology of $Z(D_8)$, the universal coefficient theorem gives that the E_2-page of the Lyndon-Hochschild-Serre spectral sequence of the group extension

$$\begin{tikzcd}
1 \arrow[r] & Z(D_8) \arrow[r] \arrow[d, phantom, "\shortparallel"] & D_8 \arrow[r] & \langle[\sigma], [\tau]\rangle \arrow[r] \arrow[d, phantom, "\shortparallel"] & 1 \\
 & \mathbb{Z}/2 & & \mathbb{Z}/2 \times \mathbb{Z}/2 &
\end{tikzcd}$$

is

$$\begin{aligned} E^2 &= H^*(D_8/Z(D_8); H^*(Z(D_8))) \\ &\cong H^*(Z(D_8)) \otimes H^*(D_8/Z(D_8)) \\ &= \mathbb{F}_2[w, x, y], \end{aligned}$$

where $|w| = |x| = |y| = 1$. The reader is advised to draw the pages of the spectral sequence.

To determine the differential d_2 it suffices, since the differential is a derivation, to determine $d_2\colon E_2^{0,1} \to E_2^{2,0}$. Since $E_\infty^{1,0} = E_2^{1,0} = \mathbb{Z}/2 \times \mathbb{Z}/2 = H^1(D_8)$, it follows that $d_2(w) \neq 0$. The $\mathbb{F}_2$-vector space $E_2^{2,0}$ is generated by the homogeneous polynomials in x and y of degree two. So

$$d_2(w) = ax^2 + bxy + cy^2$$

for some $a, b, c \in \mathbb{F}_2$.

To compute $d_2(w)$ we exploit the subgroup structure of D_8 and the naturality of the spectral sequence.

Consider the obvious map of group extensions

$$\begin{tikzcd}
1 \arrow[r] & Z(D_8) \arrow[r] & D_8 \arrow[r] & \langle[\sigma],[\tau]\rangle \arrow[r] & 1 \\
1 \arrow[r] & \langle\sigma^2\rangle \arrow[r] \arrow[u, equal] & \langle\sigma\rangle \arrow[r] \arrow[u] & \langle[\sigma]\rangle \arrow[r] \arrow[u] & 1.
\end{tikzcd}$$

The restriction map

$$\mathrm{res}_\sigma = \mathrm{res}_{\langle[\sigma],[\tau]\rangle,\langle[\sigma]\rangle}\colon H^1(\langle[\sigma],[\tau]\rangle) \to H^1(\langle[\sigma]\rangle)$$

maps x to a generator of $H^1(\langle[\sigma]\rangle)$ and y to zero. To get further we need to investigate the spectral sequence of the group extension

$$\begin{tikzcd}
1 \arrow[r] & \langle\sigma^2\rangle \arrow[r] \arrow[d, equal] & \langle\sigma\rangle \arrow[r] \arrow[d, equal] & \langle[\sigma]\rangle \arrow[r] \arrow[d, equal] & 1. \\
 & \mathbb{Z}/2 & \mathbb{Z}/4 & \mathbb{Z}/2 &
\end{tikzcd}$$

As above, the action of $\langle[\sigma]\rangle$ on $H^q(\langle\sigma\rangle)$ is trivial. So the initial page is

$${}^{\sigma}\!E_2 = H^*(\langle\sigma^2\rangle) \otimes H^*(\langle[\sigma]\rangle) = H^*(\mathbb{Z}/2 \times \mathbb{Z}/2)$$

which is a polynomial algebra in two indeterminates of degree one. Note that

$$H^1(\langle\sigma\rangle) = \mathrm{Hom}(\mathbb{Z}/4, \mathbb{Z}/2) = \mathbb{Z}/2.$$

It follows that ${}^{\sigma}d_2\colon {}^{\sigma}\!E_2^{0,1} \to {}^{\sigma}\!E_2^{2,0}$ is nonzero, otherwise $H^1(\mathbb{Z}/4) = \mathbb{Z}/2 \times \mathbb{Z}/2$. Naturality of the spectral sequence gives the commutative diagram

$$\begin{tikzcd}
E_2^{0,1} \arrow[r, "d_2"] \arrow[d, equal] & E_2^{2,0} \arrow[d, "\mathrm{res}_\sigma"] \\
{}^{\sigma}\!E_2^{0,1} \arrow[r, "{}^{\sigma}d_2"] & {}^{\sigma}\!E_2^{2,0}.
\end{tikzcd}$$

Since ${}^{\sigma}d_2$ is nonzero,

$$\mathrm{res}_\sigma(d_2(w)) = \mathrm{res}_\sigma(ax^2 + bxy + cy^2) = a\,\mathrm{res}_\sigma(x)^2 \neq 0,$$

that is, $a = 1$.

Next, consider the map of group extensions

$$\begin{tikzcd}
1 \arrow[r] & Z(D_8) \arrow[r] & D_8 \arrow[r] & \langle[\sigma],[\tau]\rangle \arrow[r] & 1 \\
1 \arrow[r] & \langle\sigma^2\rangle \arrow[r] \arrow[u, equal] & \langle\sigma^2,\tau\rangle \arrow[r] \arrow[u] & \langle[\tau]\rangle \arrow[r] \arrow[u] & 1.
\end{tikzcd}$$

The restriction map

$$\mathrm{res}_\tau = \mathrm{res}_{\langle[\sigma],[\tau]\rangle,\langle[\tau]\rangle}\colon H^1(\langle[\sigma],[\tau]\rangle) \to H^1(\langle[\tau]\rangle)$$

maps x to zero and y to a generator of $H^1(\langle[\tau]\rangle)$. The spectral sequence of the group extension

$$\begin{tikzcd}
1 \arrow[r] & \langle\sigma^2\rangle \arrow[r] \arrow[d, phantom, "\shortparallel"] & \langle\sigma^2,\tau\rangle \arrow[r] \arrow[d, phantom, "\shortparallel"] & \langle[\tau]\rangle \arrow[r] \arrow[d, phantom, "\shortparallel"] & 1 \\
 & \mathbb{Z}/2 & \mathbb{Z}/2\times\mathbb{Z}/2 & \mathbb{Z}/2 &
\end{tikzcd}$$

has initial page

$$^{\tau}E_2 = H^*(\langle\sigma^2\rangle)\otimes H^*(\langle[\tau]\rangle) = H^*(\mathbb{Z}/2\times\mathbb{Z}/2)$$

which is a polynomial algebra in two indeterminates of degree one. Since $^{\tau}E_2 = H^*(\langle\sigma^2,\tau\rangle)$ the spectral sequence collapses at the $^{\tau}E_2$-page. In particular, the differential $^{\tau}d_2$ is zero.

Naturality of the spectral sequence gives that

$$0 = {}^{\tau}d_2(w) = \mathrm{res}_\tau(d_2(w)) = \mathrm{res}_\tau(ax^2+bxy+cy^2) = c\,\mathrm{res}_\tau(y)^2.$$

Since $\mathrm{res}_\tau(y)^2$ is a generator of $H^2(\langle\tau\rangle)$, we get that $c=0$.

Next, consider the map of group extensions

$$\begin{tikzcd}
1 \arrow[r] & Z(D_8) \arrow[r] & D_8 \arrow[r] & \langle[\sigma],[\tau]\rangle \arrow[r] & 1 \\
1 \arrow[r] & \langle\sigma^2\rangle \arrow[r] \arrow[u, equal] & \langle\sigma^2,\tau\sigma\rangle \arrow[r] \arrow[u] & \langle[\tau\sigma]\rangle \arrow[r] \arrow[u] & 1.
\end{tikzcd}$$

The restriction map

$$\mathrm{res}_{\tau\sigma} = \mathrm{res}_{\langle[\sigma],[\tau]\rangle,\langle[\tau\sigma]\rangle}\colon H^1(\langle[\sigma],[\tau]\rangle)\to H^1(\langle[\tau\sigma]\rangle)$$

maps x and y to a generator z of $H^1(\langle[\tau\sigma]\rangle)$. As above, it follows that

$$0 = \mathrm{res}_{\tau\sigma}(d_2(w)) = \mathrm{res}_{\tau\sigma}(ax^2+bxy+cy^2) = (a+b+c)z^2,$$

i.e., $a+b+c=0$.

Summarizing we have that $a=1$, $c=0$ and $a+b+c=0$, which implies that $b=1$. Thus,

$$d_2(w) = x^2+xy.$$

As noted above this allows us to compute d_2. In details, for positive integers i,j,k,

$$\begin{aligned}
d_2(w^{2k}) &= 2kw^{2k-1}d_2(w) = 0,\\
d_2(w^{2k+1}) &= d_2(w)w^{2k} + wd_2(w^{2k}) = d_2(w)w^{2k},\\
d_2(w^{2k}x^iy^j) &= d_2(w^{2k})x^iy^j + w^{2k}d_2(x^iy^j) = 0 \text{ and}\\
d_2(w^{2k+1}x^iy^j) &= d_2(w^{2k+1})x^iy^j + w^{2k+1}d_2(x^iy^j) = d_2(w)w^{2k}x^iy^j.
\end{aligned}$$

Consequently,

$$E_3 = \mathbb{F}_2[w^2,x,y]/(x^2+xy).$$

Let $\beta = Sq^1$ be the Bockstein homomorphism. Steenrod operations commute with the transgression, see e.g. [7] theorem 4.8.1. Since w^2 is transgressive, it follows that

$$d_3(w^2) = \beta d_2(w) = \beta(x^2 + xy) = 2x\beta(x) + x^2y + xy^2 = x^2y + xy^2 = d_2(wy),$$

Consequently, $d_3(w^2) = 0$, and therefore $d_3 = 0$. Note that $d_r(w^2) = 0$ for $r > 3$, i.e.,

$$d_r((w^2)^k) = kw^{2(k-1)}d_r(w^2) = 0$$

for $k > 0$ and $r > 3$.

It follows that $E_\infty = E_3$ and we have computed the cohomology ring of D_8 up to a filtration of $H^*(D_8)$. Since $x^2 + xy$ is zero in $E_\infty^{2,0} \subset H^2(D_8)$, there are no filtration problems.

All in all,

$$H^*(D_8) = \mathbb{F}_2[v, x, y]/(x^2 + xy)$$

with $|v| = 2$ and $|x| = |y| = 1$.

Of course, v is only determined up to filtration. Below we shall see that we may choose v such that it restricts to zero on the subgroups $\langle\tau\rangle$ and $\langle\tau\sigma\rangle$. Before we continue we list the restrictions of x and y to the elementary abelian 2-subgroups of D_8.

The restrictions of x and y to the two maximal elementary abelian 2-subgroups: As usual, $H^1(\langle\sigma^2, \tau\rangle) = \mathrm{Hom}(\langle\sigma^2, \tau\rangle, \mathbb{Z}/2)$. Let e_1 be dual to σ^2 and e_2 dual to τ. Then the restriction map

$$\mathrm{res}_{D_8,\langle\sigma^2,\tau\rangle} \colon H^*(D_8) \to H^*(\langle\sigma^2, \tau\rangle) = \mathbb{F}_2[e_1, e_2]$$

maps x to zero and y to e_2. Similarly, the restriction map

$$\mathrm{res}_{D_8,\langle\sigma^2,\tau\sigma\rangle} \colon H^*(D_8) \to H^*(\langle\sigma^2, \tau\sigma\rangle) = \mathbb{F}_2[f_1, f_2],$$

where f_1 is dual to σ^2 and f_2 is dual to $\tau\sigma$, maps both x and y to f_2. In particular, $x + y$ restricts to zero.

The restrictions of x and y to the subgroups $\langle\tau\rangle$, $\langle\tau\sigma\rangle$ and $\langle\sigma^2\rangle$: The restriction map

$$\mathrm{res}_{D_8,\langle\tau\rangle} \colon H^*(D_8) \to H^*(\langle\tau\rangle) = \mathbb{F}_2[g_\tau]$$

maps x to zero and y to the generator. The restriction map

$$\mathrm{res}_{D_8,\langle\tau\sigma\rangle} \colon H^*(D_8) \to H^*(\langle\tau\sigma\rangle) = F_2[g_{\tau\sigma}]$$

maps both x and y to the generator. The restriction map

$$\mathrm{res}_{D_8,\langle\sigma^2\rangle} \colon H^*(D_8) \to H^*(\langle\sigma^2\rangle) = F_2[g_{\sigma^2}]$$

maps both x and y to zero. Since $\langle\tau\rangle$ and $\langle\tau\sigma^2\rangle$ are conjugate, the restriction to $\langle\tau\sigma^2\rangle$ follows from the restriction to $\langle\tau\rangle$. Similarly for $\langle\tau\sigma\rangle$ and $\langle\tau\sigma^3\rangle$.

Now, we show that we may choose v such that it restricts to zero on the subgroups $\langle\tau\rangle$ and $\langle\tau\sigma\rangle$: Note that $\mathbb{F}_2\{w^2\} = E_\infty^{0,2} = H^2(D_8)/E_\infty^{2,0}$ and $E_\infty^{2,0} = \mathbb{F}_2\{xy, y^2\}$, the latter since $x^2 = xy$. So we can choose v among the elements

$$v = w^2 + axy + by^2,$$

$a, b \in \mathbb{F}_2$. Now,

$$\operatorname{res}_{D_8,\langle\tau\rangle}(v) = \operatorname{res}_{D_8,\langle\tau\rangle}(w^2) + bg_\tau$$

and

$$\operatorname{res}_{D_8,\langle\tau\sigma\rangle}(v) = \operatorname{res}_{D_8,\langle\tau\sigma\rangle}(w^2) + (a+b)g_{\tau\sigma}.$$

Clearly, it is possible to choose a and b, depending on whether the restrictions of w^2 is zero or not, such that the restrictions of v to the subgroups $\langle\tau\rangle$ and $\langle\tau\sigma\rangle$ are zero. It follows that the restrictions of v to $\langle\tau\sigma^2\rangle$ and $\langle\tau\sigma^3\rangle$ are also zero.

We finish with determining the restriction of v to the remaining elementary abelian 2-subgroups. Up to the natural isomorphism from the universal coefficient theorem, we may identify $H^2(Z(D_8)) = H^2(\langle\sigma^2\rangle)$ and $E_\infty^{0,2}$. It should be clear that the restriction of v to $\langle\sigma^2\rangle$ is the square of a generator g_{σ^2} of $H^*(\langle\sigma^2\rangle)$.

The restriction of v to $\langle\sigma^2,\tau\rangle$: The $\mathbb{F}_2$-vector space $H^2(\langle\sigma^2,\tau\rangle)$ is equal to $\mathbb{F}_2\{e_1^2, e_1e_2, e_2^2\}$. So

$$\operatorname{res}_{D_8,\langle\sigma^2,\tau\rangle}(v) = ae_1^2 + be_1e_2 + ce_2^2$$

for some $a, b, c \in \mathbb{F}_2$. To determine a, b and c we compute the restriction to the subgroups of $\langle\sigma^2,\tau\rangle$:

$$\begin{aligned}
&0 = \operatorname{res}_{D_8,\langle\tau\rangle}(v) = \operatorname{res}_{\langle\sigma^2,\tau\rangle,\langle\tau\rangle}(\operatorname{res}_{D_8,\langle\sigma^2,\tau\rangle}(v)) = cg_\tau^2,\\
&0 \neq \operatorname{res}_{D_8,\langle\sigma^2\rangle}(v) = \operatorname{res}_{\langle\sigma^2,\tau\rangle,\langle\sigma^2\rangle}(\operatorname{res}_{D_8,\langle\sigma^2,\tau\rangle}(v)) = ag_{\sigma^2}^2 \text{ and}\\
&0 = \operatorname{res}_{D_8,\langle\tau\sigma^2\rangle}(v) = \operatorname{res}_{\langle\sigma^2,\tau\rangle,\langle\tau\sigma^2\rangle}(\operatorname{res}_{D_8,\langle\sigma^2,\tau\rangle}(v)) = (a+b+c)g_{\tau\sigma}.
\end{aligned}$$

Summing up, $a+b+c = 0$, $a = 1$ and $c = 0$, which implies that $\operatorname{res}_{D_8,\langle\sigma^2,\tau\rangle}(v) = e_1^2 + e_1e_2$. A similar computation gives that $\operatorname{res}_{D_8,\langle\sigma^2,\tau\rangle}(v) = f_1^2 + f_1f_2$.

Summarizing, the mod 2 cohomology of D_8 is

$$H^*(D_8;\mathbb{F}_2) = \mathbb{F}_2[x,y,v]/(x(x+y))$$

with x and y in degree 1 and v in degree 2. The following tables contain information about the restriction maps to the conjugacy classes of elementary abelian 2-subgroups. Note that the kernels of the restriction are equal to their radicals. This follows since they are prime ideals, see proposition A.6.

	$H^*(\langle\sigma^2,\tau\rangle) = \mathbb{F}_2[e_1,e_2]$	$H^*(\langle\sigma^2,\tau\sigma\rangle) = \mathbb{F}_2[f_1,f_2]$
x	0	f_2
y	e_2	f_2
v	$e_1^2 + e_1e_2$	$f_1^2 + f_1f_2$
Ker res	(x)	$(x+y)$

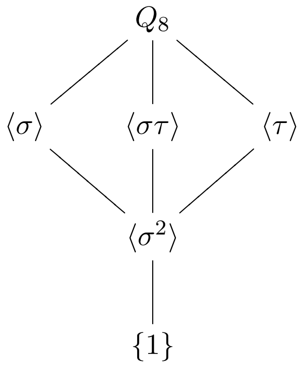
	$H^*(\langle\tau\rangle) = \mathbb{F}_2[g_\tau]$	$H^*(\langle\tau\sigma\rangle) = \mathbb{F}_2[g_{\tau\sigma}]$	$H^*(\langle\sigma^2\rangle) = \mathbb{F}_2[g_{\sigma^2}]$
x	0	$g_{\tau\sigma}$	0
y	g_τ	$g_{\tau\sigma}$	0
v	0	0	$g_{\sigma^2}^2$
Ker res	(x, v)	$(x + y, v)$	(x, y)

B.2 The quaternion group

A presentation of the quaternion group is

$$Q_8 = \langle\, \sigma, \tau \mid \sigma^4 = 1, \sigma^2 = \tau^2, \tau\sigma\tau^{-1} = \sigma^{-1} \,\rangle.$$

The subgroups of Q_8 are



and all subgroups are normal.

Note that $Z(Q_8) = [Q_8, Q_8] = \langle\sigma^2\rangle$. Applying the Lyndon-Hochschild-Serre spectral sequence to the central extension

$$\begin{tikzcd} 1 \arrow[r] & Z(Q_8) \arrow[r] & Q_8 \arrow[r] & Q_8/Z(Q_8) \arrow[r] & 1, \end{tikzcd}$$

using the techniques from the computation of the mod 2 cohomology ring of D_8, gives that

$$H^*(Q_8; \mathbb{F}_2) = \mathbb{F}_2[x, y, v]/(x^2 + xy + y^2, x^2y + xy^2)$$

with x and y in degree 1 and v in degree 4. Note that the spectral sequence in this case collapses at the E_4-page. It should not come as a surprise that v restricts to the 4th power of a generator of $H^*(\langle\sigma^2\rangle)$. This gives the information about the restriction to $\langle\sigma^2\rangle$ in the following table.

	$H^*(\langle\sigma^2\rangle) = \mathbb{F}_2[g]$
x	0
y	0
v	g^4

In particular, $\operatorname{Ker}\operatorname{res}_{Q_8,\langle\sigma^2\rangle} = (x, y)$. Since (x, y) is a prime ideal, proposition A.6 gives that $\sqrt{\operatorname{Ker}\operatorname{res}_{Q_8,\langle\sigma^2\rangle}} = \operatorname{Ker}\operatorname{res}_{Q_8,\langle\sigma^2\rangle}$. In fact, (x, y) is an associated prime:

$(x, y) = \operatorname{Ann}_{H^*(Q_8;\mathbb{F}_2)}(x^2y)$: It is clear that the annihilator of x^2y is contained in (x, y). Conversely, note that

$$0 = x(x^2 + xy + y^2) = x^3 + x^2y + xy^2 = x^3.$$

Similarly, $y^3 = 0$. So x annihilate x^2y and y annihilate $xy^2 = x^2y$, i.e., (x, y) is contained in the annihilator of x^2y.

C Depth and small groups

Carlson [14] and Green [26] computed the mod p cohomology of some small p-groups using computer calculations. In particular, they computed the depth of these rings and verified that the groups satisfy Carlson's depth conjecture. Using these computations and various theoretical results it is often possible to determine the depth of the mod p cohomology and verify the conjecture of a small finite group. This appendix gives a brief description of the key functions of a program written in the Magma computer algebra system[1] to automatize this process. The program is included in appendix D and is also freely available (at the time of writing) at

`http://www.math.ku.dk/~morten/thesis/smallgroupdepth.magma`.

Beside some auxiliary functions the program also contains a database of the depth computations of Carlson and Green. For full details see the source code.

Let G be the group of order o and number n in the Magma small group library. Moreover, let p be a prime and P a Sylow p-subgroup of G. As usual, $H^*(G)$ denotes the mod p cohomology of G.

The function `SmallGroupDepth(o,n,p)` tries to determine the depth of the mod p cohomology ring of G by going through the following steps:

(1) If $|G|$ is coprime to p, then $H^*(G) = \mathbb{F}_p$ in degree zero, i.e., the depth of $H^*(G)$ is zero.

(2) If $\mathrm{rk}_p(Z(P)) = \mathrm{mrk}_p(G) = d$, then $\operatorname{depth} H^*(G) = d$.

(3) If G is a p-group, then we only know the depth of $H^*(G)$ if it has been computed by Carlson or Green.

(4) If $\operatorname{depth} H^*(P) = \mathrm{mrk}_p(G) = d$, then $\operatorname{depth} H^*(G) = d$.

(5) If N is a normal subgroup of G and $|N|$ is coprime to p, then the Lyndon-Hochschild-Serre spectral sequence collapses at the E_2-page and $E_2 = H^*(G/N; \mathbb{F}_p) \cong H^*(G; \mathbb{F}_p)$. Thus, $\operatorname{depth} H^*(G) \cong \operatorname{depth} H^*(G/N)$. Try to determine the depth of $H^*(G/N)$.

(6) If the depth of $H^*(C_G(E))$ is known and equal to d for some central elementary abelian p-subgroup E of P, then $\operatorname{depth} H^*(G) = d$, see theorem 3.18.

(7) If none of these steps determined the depth of $H^*(G)$, we give up and return the value -1.

The function `CheckDepthConjecture(o,n,p)` tries to check if G satisfies Carlson's depth conjecture by going through the following steps:

[1] `http://magma.maths.usyd.edu.au/magma/`

(1) If $|G|$ is coprime to p there is nothing to check.

(2) If G is a p-group in the database of the computations by Carlson and Green, then G satisfies the conjecture.

(3) If $\mathrm{rk}_p(G) \leq 2$, then G satisfies the conjecture, see theorem 3.50.

(4) If $\mathrm{rk}_p(Z(P)) = \mathrm{mrk}_p(G)$, then G satisfies the conjecture.

(5) If $\operatorname{depth} H^*(G) = \mathrm{mrk}_p(G)$, then G satisfies the conjecture.

(6) If N is a normal subgroup of G and $|N|$ is coprime to p, then as above, $H^*(G) \cong H^*(G/N)$. Try to determine if G/N satisfies the conjecture.

(7) If none of these steps determined if G satisfies the conjecture, we give up and return the boolean value false.

Note that a false result only means that the function could not determine if the group satisfies the conjecture.

The following table contains information about the 69 out of the 3775 non-abelian groups of order strictly less than 256 but not a power of 2 for which the program is not able to determine whether or not they satisfy the conjecture at the prime $p = 2$. The group G given by the pair (o, n) denotes the group of order o and number n in Magma small group library, and P denotes a Sylow 2-subgroup of G.

Group	$\mathrm{rk}_2(G)$	$\mathrm{mrk}_2(G)$	$\operatorname{depth} H^*(G)$	$\operatorname{depth} H^*(P)$	$\mathrm{rk}_2(Z(P))$
(48,30)	3	3	2	2	2
(96,65)	3	3	2	2	2
(96,71)	3	3	2	2	2
(96,185)	3	3	2	2	2
(96,189)	3	3	-	2	2
(96,193)	3	3	-	2	1
(96,194)	4	4	3	3	3
(144,33)	3	3	2	2	2
(144,123)	3	3	2	2	2
(144,126)	3	3	2	2	2
(192,4)	3	3	-	1	1
(192,180)	3	3	2	2	2
(192,182)	3	3	2	2	2
(192,184)	4	3	2	2	1
(192,185)	3	3	2	2	1
(192,186)	3	3	2	2	2
(192,191)	5	5	3	3	3

Group	$\mathrm{rk}_2(G)$	$\mathrm{mrk}_2(G)$	$\operatorname{depth} H^*(G)$	$\operatorname{depth} H^*(P)$	$\mathrm{rk}_2(Z(P))$
(192,195)	4	4	3	3	3
(192,197)	4	4	3	3	3
(192,198)	4	4	3	3	3
(192,202)	3	3	-	2	1
(192,951)	3	3	-	2	2
(192,952)	3	3	-	2	2
(192,953)	3	3	-	2	2
(192,954)	3	3	-	2	2
(192,957)	3	3	2	2	2
(192,959)	3	3	2	2	2
(192,960)	3	3	2	2	2
(192,965)	3	3	-	1	1
(192,966)	3	3	-	2	1
(192,967)	4	4	3	3	3
(192,968)	4	4	2	2	2
(192,969)	4	4	3	3	3
(192,970)	4	4	3	3	3
(192,971)	4	4	3	3	3
(192,973)	4	4	2	2	2
(192,975)	3	3	2	2	2
(192,978)	3	3	-	2	2
(192,979)	3	3	-	2	2
(192,982)	3	3	-	2	1
(192,984)	3	3	-	2	2
(192,987)	3	3	-	1	1
(192,991)	5	5	3	3	3
(192,994)	5	5	4	4	4
(192,998)	3	3	-	2	2
(192,1001)	4	4	3	3	3
(192,1009)	4	4	2	2	2
(192,1011)	4	4	3	3	3
(192,1013)	3	3	-	2	1
(192,1015)	4	4	3	3	3
(192,1021)	4	4	-	2	2
(192,1023)	4	4	2	2	2
(192,1024)	4	4	-	2	2
(192,1468)	4	4	3	3	3
(192,1475)	4	4	-	3	3
(192,1476)	3	3	-	2	2
(192,1479)	3	3	-	2	2

Group	$\mathrm{rk}_2(G)$	$\mathrm{mrk}_2(G)$	depth $H^*(G)$	depth $H^*(P)$	$\mathrm{rk}_2(Z(P))$
(192,1481)	4	4	-	3	2
(192,1482)	3	3	-	2	1
(192,1485)	3	3	-	2	1
(192,1487)	5	5	4	4	4
(192,1489)	3	3	2	2	2
(192,1491)	3	3	-	2	1
(192,1492)	3	3	-	1	1
(192,1495)	5	5	3	3	3
(240,91)	3	3	2	2	2
(240,104)	3	3	2	2	2
(240,107)	3	3	2	2	2
(240,192)	3	3	2	2	2

D Program

```
// Depth and small groups by Morten Poulsen, 2007.

// Database of depths of the mod p cohomology of some small p-groups.
// Thanks to J. F. Carlson and D. J. Green.
// DD[q][o][n] is the depth of the mod p = Primes[q][1]
// cohomology ring of the group of order p^o and number n in the
// Magma small group library. If depth is unknown the value is -1
DD := [];

Primes := [ <2,7>, <3,5>, <5,4>, <7,3> ];

// Initialize database of depth computations
for p in [1..#Primes] do
    DD[p] := [];
   for o in [1..Max([ Primes[i][2] : i in [1..#Primes]])] do
      DD[p][o] := [];
      max := Max([ NumberOfSmallGroups(i) : i in [ Primes[k][1]^j :
                j in [1..Primes[k][2]], k in [1..#Primes]]]);
      for n in [1..max] do
         DD[p][o][n] := -1;
      end for;
   end for;
end for;

// Depths of the mod 2 cohomology of groups of order 2^1
DD[1][1][1] := 2;

// Depths of the mod 2 cohomology of groups of order 2^2
DD[1][2][1] := 1; DD[1][2][2] := 2;

// Depths of the mod 2 cohomology of groups of order 2^3
DD[1][3][1] := 1; DD[1][3][2] := 2; DD[1][3][3] := 2;
DD[1][3][4] := 1; DD[1][3][5] := 3;

// Depths of the mod 2 cohomology of groups of order 2^4
DD[1][4][1] := 1; DD[1][4][2] := 2; DD[1][4][3] := 2;
DD[1][4][4] := 2; DD[1][4][5] := 2; DD[1][4][6] := 1;
DD[1][4][7] := 2; DD[1][4][8] := 1; DD[1][4][9] := 1;
DD[1][4][10] := 3; DD[1][4][11] := 3; DD[1][4][12] := 2;
DD[1][4][13] := 2; DD[1][4][14] := 4;

// Depths of the mod 2 cohomology of groups of order 2^5
DD[1][5][1] := 1; DD[1][5][2] := 3; DD[1][5][3] := 2;
DD[1][5][4] := 2; DD[1][5][5] := 2; DD[1][5][6] := 2;
DD[1][5][7] := 1; DD[1][5][8] := 1; DD[1][5][9] := 2;
DD[1][5][10] := 2; DD[1][5][11] := 2; DD[1][5][12] := 2;
```

```
DD[1][5][13] := 2; DD[1][5][14] := 2; DD[1][5][15] := 1;
DD[1][5][16] := 2; DD[1][5][17] := 1; DD[1][5][18] := 2;
DD[1][5][19] := 1; DD[1][5][20] := 1; DD[1][5][21] := 3;
DD[1][5][22] := 3; DD[1][5][23] := 3; DD[1][5][24] := 2;
DD[1][5][25] := 3; DD[1][5][26] := 2; DD[1][5][27] := 3;
DD[1][5][28] := 3; DD[1][5][29] := 2; DD[1][5][30] := 2;
DD[1][5][31] := 2; DD[1][5][32] := 2; DD[1][5][33] := 2;
DD[1][5][34] := 3; DD[1][5][35] := 2; DD[1][5][36] := 3;
DD[1][5][37] := 2; DD[1][5][38] := 2; DD[1][5][39] := 3;
DD[1][5][40] := 2; DD[1][5][41] := 2; DD[1][5][42] := 2;
DD[1][5][43] := 2; DD[1][5][44] := 1; DD[1][5][45] := 4;
DD[1][5][46] := 4; DD[1][5][47] := 3; DD[1][5][48] := 3;
DD[1][5][49] := 3; DD[1][5][50] := 2; DD[1][5][51] := 5;

// Depths of the mod 2 cohomology of groups of order 2^6
DD[1][6][1] := 1; DD[1][6][2] := 2; DD[1][6][3] := 2;
DD[1][6][4] := 2; DD[1][6][5] := 2; DD[1][6][6] := 2;
DD[1][6][7] := 2; DD[1][6][8] := 3; DD[1][6][9] := 2;
DD[1][6][10] := 2; DD[1][6][11] := 2; DD[1][6][12] := 2;
DD[1][6][13] := 2; DD[1][6][14] := 2; DD[1][6][15] := 2;
DD[1][6][16] := 2; DD[1][6][17] := 3; DD[1][6][18] := 1;
DD[1][6][19] := 1; DD[1][6][20] := 2; DD[1][6][21] := 3;
DD[1][6][22] := 2; DD[1][6][23] := 3; DD[1][6][24] := 2;
DD[1][6][25] := 1; DD[1][6][26] := 2; DD[1][6][27] := 2;
DD[1][6][28] := 1; DD[1][6][29] := 2; DD[1][6][30] := 1;
DD[1][6][31] := 2; DD[1][6][32] := 2; DD[1][6][33] := 1;
DD[1][6][34] := 2; DD[1][6][35] := 1; DD[1][6][36] := 1;
DD[1][6][37] := 1; DD[1][6][38] := 2; DD[1][6][39] := 2;
DD[1][6][40] := 2; DD[1][6][41] := 2; DD[1][6][42] := 1;
DD[1][6][43] := 1; DD[1][6][44] := 2; DD[1][6][45] := 1;
DD[1][6][46] := 1; DD[1][6][47] := 2; DD[1][6][48] := 2;
DD[1][6][49] := 1; DD[1][6][50] := 2; DD[1][6][51] := 1;
DD[1][6][52] := 2; DD[1][6][53] := 1; DD[1][6][54] := 1;
DD[1][6][55] := 3; DD[1][6][56] := 4; DD[1][6][57] := 3;
DD[1][6][58] := 3; DD[1][6][59] := 3; DD[1][6][60] := 3;
DD[1][6][61] := 3; DD[1][6][62] := 3; DD[1][6][63] := 3;
DD[1][6][64] := 3; DD[1][6][65] := 3; DD[1][6][66] := 3;
DD[1][6][67] := 4; DD[1][6][68] := 3; DD[1][6][69] := 3;
DD[1][6][70] := 3; DD[1][6][71] := 3; DD[1][6][72] := 3;
DD[1][6][73] := 4; DD[1][6][74] := 3; DD[1][6][75] := 3;
DD[1][6][76] := 3; DD[1][6][77] := 3; DD[1][6][78] := 3;
DD[1][6][79] := 3; DD[1][6][80] := 3; DD[1][6][81] := 3;
DD[1][6][82] := 3; DD[1][6][83] := 3; DD[1][6][84] := 3;
DD[1][6][85] := 2; DD[1][6][86] := 2; DD[1][6][87] := 3;
DD[1][6][88] := 2; DD[1][6][89] := 3; DD[1][6][90] := 3;
DD[1][6][91] := 2; DD[1][6][92] := 2; DD[1][6][93] := 2;
DD[1][6][94] := 2; DD[1][6][95] := 3; DD[1][6][96] := 3;
DD[1][6][97] := 3; DD[1][6][98] := 3; DD[1][6][99] := 2;
```

```
DD[1][6][100] := 2; DD[1][6][101] := 3; DD[1][6][102] := 2;
DD[1][6][103] := 3; DD[1][6][104] := 2; DD[1][6][105] := 2;
DD[1][6][106] := 3; DD[1][6][107] := 3; DD[1][6][108] := 2;
DD[1][6][109] := 2; DD[1][6][110] := 2; DD[1][6][111] := 1;
DD[1][6][112] := 2; DD[1][6][113] := 2; DD[1][6][114] := 2;
DD[1][6][115] := 3; DD[1][6][116] := 2; DD[1][6][117] := 2;
DD[1][6][118] := 3; DD[1][6][119] := 2; DD[1][6][120] := 2;
DD[1][6][121] := 2; DD[1][6][122] := 2; DD[1][6][123] := 3;
DD[1][6][124] := 2; DD[1][6][125] := 2; DD[1][6][126] := 2;
DD[1][6][127] := 2; DD[1][6][128] := 3; DD[1][6][129] := 3;
DD[1][6][130] := 3; DD[1][6][131] := 2; DD[1][6][132] := 2;
DD[1][6][133] := 2; DD[1][6][134] := 3; DD[1][6][135] := 2;
DD[1][6][136] := 1; DD[1][6][137] := 2; DD[1][6][138] := 3;
DD[1][6][139] := 2; DD[1][6][140] := 3; DD[1][6][141] := 2;
DD[1][6][142] := 2; DD[1][6][143] := 2; DD[1][6][144] := 2;
DD[1][6][145] := 2; DD[1][6][146] := 2; DD[1][6][147] := 3;
DD[1][6][148] := 2; DD[1][6][149] := 2; DD[1][6][150] := 2;
DD[1][6][151] := 2; DD[1][6][152] := 1; DD[1][6][153] := 2;
DD[1][6][154] := 1; DD[1][6][155] := 2; DD[1][6][156] := 2;
DD[1][6][157] := 2; DD[1][6][158] := 2; DD[1][6][159] := 2;
DD[1][6][160] := 2; DD[1][6][161] := 2; DD[1][6][162] := 2;
DD[1][6][163] := 2; DD[1][6][164] := 2; DD[1][6][165] := 2;
DD[1][6][166] := 2; DD[1][6][167] := 2; DD[1][6][168] := 2;
DD[1][6][169] := 2; DD[1][6][170] := 2; DD[1][6][171] := 2;
DD[1][6][172] := 2; DD[1][6][173] := 2; DD[1][6][174] := 3;
DD[1][6][175] := 2; DD[1][6][176] := 2; DD[1][6][177] := 2;
DD[1][6][178] := 2; DD[1][6][179] := 2; DD[1][6][180] := 2;
DD[1][6][181] := 2; DD[1][6][182] := 2; DD[1][6][183] := 3;
DD[1][6][184] := 2; DD[1][6][185] := 2; DD[1][6][186] := 3;
DD[1][6][187] := 2; DD[1][6][188] := 2; DD[1][6][189] := 2;
DD[1][6][190] := 2; DD[1][6][191] := 1; DD[1][6][192] := 4;
DD[1][6][193] := 4; DD[1][6][194] := 4; DD[1][6][195] := 3;
DD[1][6][196] := 4; DD[1][6][197] := 3; DD[1][6][198] := 3;
DD[1][6][199] := 3; DD[1][6][200] := 2; DD[1][6][201] := 3;
DD[1][6][202] := 4; DD[1][6][203] := 4; DD[1][6][204] := 3;
DD[1][6][205] := 3; DD[1][6][206] := 3; DD[1][6][207] := 3;
DD[1][6][208] := 3; DD[1][6][209] := 3; DD[1][6][210] := 2;
DD[1][6][211] := 4; DD[1][6][212] := 3; DD[1][6][213] := 3;
DD[1][6][214] := 2; DD[1][6][215] := 3; DD[1][6][216] := 3;
DD[1][6][217] := 2; DD[1][6][218] := 3; DD[1][6][219] := 2;
DD[1][6][220] := 2; DD[1][6][221] := 3; DD[1][6][222] := 2;
DD[1][6][223] := 2; DD[1][6][224] := 2; DD[1][6][225] := 2;
DD[1][6][226] := 4; DD[1][6][227] := 3; DD[1][6][228] := 3;
DD[1][6][229] := 3; DD[1][6][230] := 3; DD[1][6][231] := 3;
DD[1][6][232] := 2; DD[1][6][233] := 2; DD[1][6][234] := 3;
DD[1][6][235] := 2; DD[1][6][236] := 2; DD[1][6][237] := 2;
DD[1][6][238] := 2; DD[1][6][239] := 2; DD[1][6][240] := 2;
DD[1][6][241] := 3; DD[1][6][242] := 2; DD[1][6][243] := 2;
```

```
DD[1][6][244] := 2; DD[1][6][245] := 2; DD[1][6][246] := 4;
DD[1][6][247] := 3; DD[1][6][248] := 3; DD[1][6][249] := 2;
DD[1][6][250] := 4; DD[1][6][251] := 3; DD[1][6][252] := 3;
DD[1][6][253] := 3; DD[1][6][254] := 3; DD[1][6][255] := 2;
DD[1][6][256] := 2; DD[1][6][257] := 3; DD[1][6][258] := 2;
DD[1][6][259] := 2; DD[1][6][260] := 5; DD[1][6][261] := 5;
DD[1][6][262] := 4; DD[1][6][263] := 4; DD[1][6][264] := 4;
DD[1][6][265] := 3; DD[1][6][266] := 3; DD[1][6][267] := 6;

// Depths of the mod 2 cohomology of groups of order 2^7
DD[1][7][928] := 3; DD[1][7][937] := 2; DD[1][7][2023] := 2;

// Depths of the mod 3 cohomology of groups of order 3^1
DD[2][1][1] := 1;

// Depths of the mod 3 cohomology of groups of order 3^2
DD[2][2][1] := 1; DD[2][2][2] := 2;

// Depths of the mod 3 cohomology of groups of order 3^3
DD[2][3][1] := 1; DD[2][3][2] := 2; DD[2][3][3] := 2;
DD[2][3][4] := 1; DD[2][3][5] := 3;

// Depths of the mod 3 cohomology of groups of order 3^4
DD[2][4][1] := 1; DD[2][4][2] := 2; DD[2][4][3] := 2;
DD[2][4][4] := 2; DD[2][4][5] := 2; DD[2][4][6] := 1;
DD[2][4][7] := 2; DD[2][4][8] := 1; DD[2][4][9] := 2;
DD[2][4][10] := 1; DD[2][4][11] := 3; DD[2][4][12] := 3;
DD[2][4][13] := 2; DD[2][4][14] := 1; DD[2][4][15] := 4;

// Depths of the mod 3 cohomology of groups of order 3^5
DD[2][5][1] := 1; DD[2][5][2] := 3; DD[2][5][10] := 2;
DD[2][5][16] := 1; DD[2][5][23] := 2; DD[2][5][26] := 2;
DD[2][5][31] := 3; DD[2][5][48] := 3; DD[2][5][61] := 4;
DD[2][5][67] := 5;

// Depths of the mod 5 cohomology of groups of order 5^1
DD[3][1][1] := 1;

// Depths of the mod 5 cohomology of groups of order 5^2
DD[3][2][1] := 1; DD[3][2][2] := 2;

// Depths of the mod 5 cohomology of groups of order 5^3
DD[3][3][1] := 1; DD[3][3][2] := 2; DD[3][3][3] := 1;
DD[3][3][4] := 1; DD[3][3][5] := 3;

// Depths of the mod 5 cohomology of groups of order 5^4
DD[3][4][1] := 1; DD[3][4][2] := 2; DD[3][4][3] := 2;
DD[3][4][4] := 2; DD[3][4][5] := 2; DD[3][4][6] := 1;
```

```
DD[3][4][8] := 1; DD[3][4][9] := 1; DD[3][4][10] := 1;
DD[3][4][11] := 3; DD[3][4][12] := 2; DD[3][4][13] := 2;
DD[3][4][14] := 1; DD[3][4][15] := 4;

// Depths of the mod 7 cohomology of groups of order 7^1
DD[4][1][1] := 1;

// Depths of the mod 7 cohomology of groups of order 7^2
DD[4][2][1] := 1; DD[4][2][2] := 2;

// Depths of the mod 7 cohomology of groups of order 7^3
DD[4][3][1] := 1; DD[4][3][2] := 2; DD[4][3][3] := 1;
DD[4][3][4] := 1; DD[4][3][5] := 3;

// Lookup a group in DD
LookupDepth := function(o,n,p);
   error if not CanIdentifyGroup(o) or n gt NumberOfSmallGroups(o),
      "LookupDepth: Group out of range!";
   error if not IsPrime(p),
      "LookupDepth: Third argument not prime number!";

   // Trivial case, p does not divide the order of G
   if not IsDivisibleBy(o,p) then
      return 0;
   end if;

   if not p in [ Primes[i][1] : i in [1..#Primes] ] or
      not o in [ Primes[i][1]^j :
            j in [1..Primes[i][2]], i in [1..#Primes] ] then
      return -1;
   end if;

   // The index l of p in Primes
   for i in [1..#Primes] do
      if p eq Primes[i][1] then l := i; break; end if;
   end for;

   // Find k such that o = p^k
   k := Max({i : i in [1..Primes[l][2]] | IsDivisibleBy(o,p^i)});

   return DD[l][k][n];
end function;

// Returns L, EL, maxEL, oeas -
// L: The subgroups
// EL: The elementary abelian p-subgroups
// maxEL: The maximal elementary abelian p-subgroups
// oeas: The orders of the maximal elementary abelian p-subgroups
```

```
ElementaryAbelianSubgroupsInfo := function(G,p);
   L := SubgroupLattice(G : Properties:=true);

   EL := [ i : i in [1..#L] | IsElementaryAbelian(L[i]) and
      IsDivisibleBy(#L[i],p) ];

   maxEL := [ i : i in EL | not(exists{j : j in EL | L!i lt L!j}) ];

   oeas := [ #L[i] : i in maxEL ];

   return L, EL, maxEL, oeas;
end function;

// Returns oeas, zrk, mrk, dim -
// oeas: The orders of the maximal elementary abelian p-subgroups
// zrk: The p-rank of the center of a Sylow p-subgroup
// mrk: The minimal p-rank amongst the maximal p-subgroups
// dim: The p-rank of the group
GroupInfo := function(G,p);
   L, EL, maxEL, oeas := ElementaryAbelianSubgroupsInfo(G,p);
   P := SylowSubgroup(G,p);
   PZL, _, maxPZEL, _ := ElementaryAbelianSubgroupsInfo(Center(P),p);

   // Maximal order of a maximal elementary abelian subgroup
   dim := Max({e : e in [0..#G] | IsDivisibleBy(#maxEL eq 0
      select 1 else Max([ #L[i] : i in maxEL ]),p^e)});

   // Minimal order of a maximal elementary abelian subgroup
   mrk := Max({e : e in [0..#G] | IsDivisibleBy(#maxEL eq 0
      select 1 else Min([ #L[i] : i in maxEL ]),p^e)});

   // Rank of the center of a Sylow p-subgroup
   zrk := Max({e : e in [0..#P] | IsDivisibleBy(#maxPZEL eq 0
      select 1 else Max([ #PZL[i] : i in maxPZEL ]),p^e)});

   return oeas, zrk, mrk, dim;
end function;

// Returns -1 if the depth can not be determined
SmallGroupDepth := function(o,n,p);
   error if not CanIdentifyGroup(o) or n gt NumberOfSmallGroups(o),
      "SmallGroupDepth: Group out of range!";
   error if not IsPrime(p),
      "SmallGroupDepth: Third argument not prime number!";

   // Trivial case if p does not divide the order of G
   if not IsDivisibleBy(o,p) then
      return 0;
```

```
end if;

d := LookupDepth(o,n,p);

// If the order is a prime power, then the only hope is the database
if IsPrimePower(o) then
   return d;
end if;

G := SmallGroup(o,n);
oel, zrk, mrk, dim := GroupInfo(G,p);

// A trivial case
if zrk eq mrk then
   return mrk;
end if;

// Check if the depth can be determined by the depth of a
// Sylow p-subgroup
P := SylowSubgroup(G,p);
error if not CanIdentifyGroup(Order(P)),
   "SmallGroupDepth: Can not identify Sylow subgroup!";
IP := IdentifyGroup(P);
op := IP[1]; np := IP[2];
dp := LookupDepth(op,np,p);

// If dp equals mrk, then this is the depth of G
if mrk eq dp then
   return dp;
end if;

// Check if the depth can be determined by using the
// Lyndon-Hochschild-Serre spectral sequence, i.e.,
// if G has normal subgroup N of order prime to p,
// then the cohomology rings of G and G/N are iso
NS := NormalSubgroups(G);
for i in [1..#NS] do
   N := NS[i]`subgroup;
   if Order(N) gt 1 and not IsDivisibleBy(Order(N),p) then
      error if not CanIdentifyGroup(Order(G/N)),
         "SmallGroupDepth: Can not identify quotient group!";
      Q := IdentifyGroup(G/N);
      oq := Q[1]; nq := Q[2];
      dq := LookupDepth(oq,nq,p);

      // If the depth of G/N is known, then this is the depth of G
      if dq gt 0 then
         return dq;
         end if;

         // If the depth of G/N is not known,
         // then try recursively to determine it
          d := $$(oq,nq,p);
         if d gt 0 then
            return d;
         end if;
      end if;
   end for;

   // Check if the depth can be determined by the improved version
   // of Notbohm's result
   ZL, ZEL, _, _ := ElementaryAbelianSubgroupsInfo(Center(P),p);
   for i in ZEL do
      C := ZL[i];
         Cent := Centralizer(G,C);
         error if not CanIdentifyGroup(Order(Cent)),
            "SmallGroupDepth: Can not identify centralizer!";
         CC := IdentifyGroup(Centralizer(G,C));
         occ := CC[1]; ncc := CC[2];
         // Only try to get the depths of proper centralizers
         // or infinite loop
         if occ lt o then
            dcc := $$(occ,ncc,p);
            if dcc gt 0 then
               return dcc;
            end if;
         end if;
   end for;

   // We give up...
   return -1;
end function;

// Returns false if it can not be determined whether or not
// the group satisfies Carlson's depth conjecture
CheckDepthConjecture := function(o,n,p);
   error if not CanIdentifyGroup(o) or n gt NumberOfSmallGroups(o),
      "CheckDepthConjecture: Group out of range!";
   error if not IsPrime(p),
      "CheckDepthConjecture: Third argument not prime number!";

   // Trivial case if p does not divide the order of G
   if not IsDivisibleBy(o,p) then
      return true;
   end if;
   // All p-groups in the database satisfy the conjecture
   if IsPrimePower(o) and LookupDepth(o,n,p) gt 0 then
      return true;
   end if;

   G := SmallGroup(o,n);
   oel, zrk, mrk, dim := GroupInfo(G,p);

   // Groups of p-rank less than or equal to 2 satisfy the conjecture
   if dim le 2 then
      return true;
   end if;

   // A well known case
   if zrk eq mrk then
      return true;
   end if;

   d := SmallGroupDepth(o,n,p);

   // Another well known case
   if d eq mrk then
      return true;
   end if;

   // As in SmallGroupDepth try the cohomology ring of G/N,
   // N normal subgroup of G of order prime to p
   NS := NormalSubgroups(G);
   for i in [1..#NS] do
      N := NS[i]`subgroup;

      if Order(N) gt 1 and not IsDivisibleBy(Order(N),p) then
         error if not CanIdentifyGroup(Order(G/N)),
            "CheckDepthConjecture: Can not identify quotient group!";
         Q := IdentifyGroup(G/N);
         oq := Q[1]; nq := Q[2];
         if $$(oq,nq,p) then
            return true;
         end if;
      end if;
   end for;

   // We give up...
   return false;
end function;

// The dimension of the kernel of the restriction maps on H^1 and H^2
// of the centralizers of elementary abelian subgroups of rank r
```

```
CheckRes12 := function(o,n,r,p);
   error if not CanIdentifyGroup(o) or n gt NumberOfSmallGroups(o),
      "CheckRes12: Group out of range!";
   error if not IsPrime(p),
      "CheckRes12: Fourth argument not prime number!";

   G := SmallGroup(o,n);
   L, EL, _, _ := ElementaryAbelianSubgroupsInfo(G,p);

   // The elementary abelian p-subgroup of rank r
   rEL := [ i : i in EL | Order(L[i]) eq p^r ];

   error if #rEL eq 0,
      "CheckRes12: No elementary abelian subgroups of rank", r, ".";

   MG := TrivialModule(G,GF(p));
   CMG := CohomologyModule(G,MG);
   H1G := CohomologyGroup(CMG,1);
   H2G := CohomologyGroup(CMG,2);
   gen1G := [ OneCocycle(CMG,H1G.j) : j in [1..Ngens(H1G)] ];
   gen2G := [ TwoCocycle(CMG,H2G.j) : j in [1..Ngens(H2G)] ];

   Ker1 := H1G;
   for E in [ L[i] : i in rEL ] do
      H := Centralizer(G,E);
      MH := Restriction(MG,H);
      CMH := CohomologyModule(H,MH);
      H1H := CohomologyGroup(CMH,1);
      im := [ IdentifyOneCocycle(CMH,func< u | MH!gen1G[j](u) >) :
         j in [1..Ngens(H1G)] ];
      res1 := hom< H1G -> H1H | im>;
      Ker1 := Ker1 meet Kernel(res1);
   end for;

   Ker2 := H2G;
   for E in [ L[i] : i in rEL ] do
      H := Centralizer(G,E);
      MH := Restriction(MG,H);
      CMH := CohomologyModule(H,MH);
      H2H := CohomologyGroup(CMH,2);
      im := [ IdentifyTwoCocycle(CMH,func< u | MH!gen2G[j](u) >) :
         j in [1..Ngens(H2G)] ];
      res2 := hom< H2G -> H2H | im>;
      Ker2 := Ker2 meet Kernel(res2);
   end for;

   return Dimension(Ker1), Dimension(Ker2);
end function;
```

List of notation

Sets	
X, Y	Sets.
$X - Y$	Set difference.
$X \subset Y$	X is a subset of Y.
$X \subsetneq Y$	X is a proper subset of Y.
Rings & modules	
R, I, M	A graded ring, an ideal of R and an R-module.
R^+	The ideal generated by homogeneous elem. of degree > 0.
$R^{\geq i}$	The ideal generated by homogeneous elem. of degree $\geq i$.
$\operatorname{Ann}_R(x)$	The annihilator of an element $x \in M$.
$\operatorname{Ann}_R M$	The annihilator of M.
$\operatorname{Ker} \varphi$	The kernel of a homomorphism φ of R-modules.
$\operatorname{Im} \varphi$	The image of a homomorphism φ of R-modules.
$\operatorname{Spec} R$	The set of prime ideals of R.
$\operatorname{Ass}_R M$	The associated primes of M.
$V(I)$	The prime ideals of R containing I.
$\sqrt{I}$	The radical of I.
$\operatorname{Nil}(R)$	The nilradical of R, i.e., the nilpotent elements in R.
$\dim_R M$	The (Krull) dimension of M.
$\operatorname{depth}_R M$	The depth of M.
Groups & cohomology of groups	
G, H, g	A finite group, a subgroup of G and an element of G.
$H < G$	H is a proper subgroup of G.
p	A prime number.
$\mathbb{Z}/n$	The cyclic group of order n.
$\operatorname{rk}_p(G)$	The p-rank of G.
$\operatorname{mrk}_p(G)$	The minimal rank amongst the maximal elementary abelian p-subgroups of G.
c_g	Conjugation by g, $c_g \colon H \to gHg^{-1}$, $c_g(h) = ghg^{-1}$.
$Z(G)$	The center of G.
$C_G(H)$	The centralizer of H in G.
$N_G(H)$	The normalizer of H in G.
$\mathcal{A}(G)$	The Quillen category.
$\mathcal{A}_s(G)$	The elementary abelian p-subgroups of G of rank s.
$\mathcal{H}_s(G)$	The set $\{\, C_G(E) \mid E \in \mathcal{A}_s(G) \,\}$.
$\mathbb{F}_p$	The Galois field with p elements.
$H^*(G)$	The mod p cohomology ring $H^*(G; \mathbb{F}_p)$ of G.
$\cdot g$	The homomorphism $H^*(H) \to H^*(gHg^{-1})$ induced by $c_{g^{-1}}$.
β	The Bockstein of the sequence $0 \to \mathbb{Z}/p \to \mathbb{Z}/p^2 \to \mathbb{Z}/p \to 0$.
Sq^i	The Steenrod square of degree i, $p = 2$.
P^i	The Steenrod reduced power of degree $n + 2i(p-1)$, p odd.

References

[1] J. F. Adams and C. W. Wilkerson, *Finite H-spaces and algebras over the Steenrod algebra*, Ann. of Math. **111** (1980), 95–143.

[2] A. Adem and R. J. Milgram, *Cohomology of finite groups*, second ed., Grundlehren der Mathematischen Wissenschaften, vol. 309, Springer-Verlag, Berlin, 2004.

[3] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, Reading, 1969.

[4] D. J. Benson, *The image of the transfer map*, Arch. Math. **61** (1993), 7–11.

[5] ———, *Polynomial invariants of finite groups*, London Math. Soc. Lecture Note Series, vol. 190, Cambridge University Press, Cambridge, 1993.

[6] ———, *Representations and cohomology. I*, second ed., Cambridge Studies in Advanced Mathematics, vol. 30, Cambridge University Press, Cambridge, 1998.

[7] ———, *Representations and cohomology. II*, second ed., Cambridge Studies in Advanced Mathematics, vol. 31, Cambridge University Press, Cambridge, 1998.

[8] ———, *Commutative algebra in the cohomology of groups*, Trends in commutative algebra, Math. Sci. Res. Inst. Publ., vol. 51, Cambridge Univ. Press, Cambridge, 2004, pp. 1–50.

[9] D. J. Benson and J. F. Carlson, *Diagrammatic methods for modular representations and cohomology*, Comm. Algebra **15** (1987), 53–121.

[10] N. Bourbaki, *Algèbre. Chapitres 1 à 3*, Hermann, Paris, 1970.

[11] C. Broto and H.-W. Henn, *Some remarks on central elementary abelian p-subgroups and cohomology of classifying spaces*, Quart. J. Math. **44** (1993), 155–163.

[12] K. S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York, 1994, Corrected reprint of the 1982 original.

[13] W. Bruns and J. Herzog, *Cohen-Macauley rings*, Cambridge studies in advanced mathematics, vol. 39, Cambridge University Press, Cambridge, 1993.

[14] J. F. Carlson, *The mod-2 cohomology of 2-groups*, `http://www.math.uga.edu/~lvalero/cohointro.html`.

[15] ———, *Depth and transfer maps in the cohomology of groups*, Math. Z. **218** (1995), 461–468.

[16] J. F. Carlson and H.-W. Henn, *Depth and the cohomology of wreath products*, Manuscripta Math. **87** (1995), 145–151.

[17] ———, *Cohomological detection and regular elements in group cohomology*, Proc. Amer. Math. Soc. **124** (1996), 665–670.

[18] J. F. Carlson, L. Townsley, L. Valeri-Elizondo, and M. Zhang, *Cohomology rings of finite groups*, Kluwer Academic Publishers, Dordrecht, 2003.

[19] H. Cartan and S. Eilenberg, *Homological algebra*, Princeton University Press, Princeton, N. J., 1956.

[20] J. Duflot, *Depth and equivariant cohomology*, Comment. Math. Helv. (1981), 627–637.

[21] ———, *The associated primes of $H_G^*(X)$*, J. Pure Appl. Algebra **30** (1983), 131–141.

[22] D. Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995.

[23] L. Evens, *The cohomology ring of a finite group*, Trans. Amer. Math. Soc. **101** (1961), 224–239.

[24] ———, *The cohomology of groups*, Oxford University Press, New York, 1991.

[25] E. Golod, *The cohomology ring of a finite p-group*, Dokl. Akad. Nauk SSSR **125** (1959), 703–706.

[26] D. J. Green, *Cohomology rings of some small p-groups*, `http://www.math.uni-wuppertal.de/~green/Coho_v2/`.

[27] ———, *On Carlson's depth conjecture in group cohomology*, Math. Z. **244** (2003), 711–723.

[28] A. Hatcher, *Algebraic topology*, Cambridge University Press, Cambridge, 2002.

[29] H.-W. Henn, J. Lannes, and L. Schwartz, *Localizations of unstable A-modules and equivariant mod p cohomology*, Math. Ann. **301** (1995), 23–68.

[30] L. Kaloujnine, *La structure des p-groupes de Sylow des groupes symétriques finis*, Ann. Sci. École Norm. Sup. (3) **65** (1948), 239–276.

[31] I. Kaplansky, *R-sequences and homological dimension*, Nagoya Math. J. **20** (1962), 195–199.

[32] S. Mac Lane, *Homology*, Springer-Verlag, Berlin, 1995, Reprint of the 1975 edition.

[33] B. J. Mann, *The cohomology of the alternating groups*, Michigan Math. J. **32** (1985), 267–277.

[34] H. Matsumura, *Commutative ring theory*, Cambridge studies in advanced mathematics, vol. 8, Cambridge University Press, Cambridge, 1989.

[35] G. Mislin, *On group homomorphisms inducing mod-p cohomology isomorphisms*, Comment. Math. Helv. **65** (1990), 454–461.

[36] D. Notbohm, *Depth and homology decompositions*, Preprint, 2006.

[37] D. Quillen, *A cohomological criterion for p-nilpotence*, J. Pure Appl. Algebra **1** (1971), 361–372.

[38] ———, *The spectrum of an equivariant cohomology ring. I, II*, Ann. Math. **94** (1971), 549–602.

[39] ———, *On the cohomology and K-theory of the general linear groups over a finite field*, Ann. Math. **96** (1972), 552–586.

[40] D. Quillen and B. B. Venkov, *Cohomology of finite groups and elementary abelian subgroups*, Topology **11** (1972), 317–318.

[41] D. J. S. Robinson, *A course in the theory of groups*, second ed., Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1996.

[42] J. J. Rotman, *An introduction to the theory of groups*, fourth ed., Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995.

[43] D. J. Rusin, *The cohomology of the groups of order* 32, Math. Comp. **53** (1989), 359–385.

[44] L. Schwartz, *Unstable modules over the Steenrod algebra and Sullivan's fixed point set conjecture*, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, 1994.

[45] J.-P. Serre, *Sur la dimension cohomologique des groupes profinis*, Topology **3** (1965), 413–420.

[46] L. Smith, *Polynomial invariants of finite groups*, A. K. Peters, Wellesley, MA, 1995.

[47] M. Suzuki, *Group theory. I*, Grundlehren der Mathematischen Wissenschaften, vol. 247, Springer-Verlag, Berlin, 1982.

[48] B. B. Venkov, *Cohomology algebras for some classifying spaces*, Dokl. Akad. Nauk SSSR **127** (1959), 943–944.

[49] C. A. Weibel, *An introduction to homological algebra*, Cambridge studies in advanced mathematics, vol. 38, Cambridge University Press, Cambridge, 1994.