DET NATURVIDENSKABELIGE FAKULTET
KØBENHAVNS UNIVERSITET

Master Thesis in Mathematics

Amalie Høgenhaven

Quillen Stratification in Group Cohomology

Advisor: Jesper Grodal

May 16, 2013

Abstract

Let G be a finite group and let k be a field of prime characteristic p. The purpose of this thesis is to examine the ring structure of the cohomology ring $H^*(G,k)$ by relating it via restriction maps to the cohomology rings of the elementary abelian p-subgroups of G. We prove that $H^*(G,k)$ is a finitely generated graded commutative k-algebra, so one can apply concepts from commutative algebra, such as Krull dimension and nilpotency, to $H^*(G,k)$ and ask for a group theoretic interpretation. We prove that the Krull dimension of the cohomology ring $H^*(G,k)$ is the maximal rank of the elementary abelian p-subgroups of G. We then turn our attention to Quillen's Stratification Theorems, which state that the maximal ideal spectrum of $H^*(G,k)$ decomposes into disjoint pieces corresponding to the elementary abelian p-subgoups of G. We conclude the thesis by reinterpreting the result achieved about maximal ideals spectra in order to show that the cohomology ring $H^*(G,\mathbb{F}_p)$ can be described up to nilpotency phenomena as a ring cooked up from the elementary abelian p-subgroups of G and inner monomorphisms between them.

Resumé

Lad G være en endelig gruppe, og lad k være et legeme af primtalskarakteristik p. Formålet med dette speciale er at undersøge ringstrukturen af gruppekohomologiringen $H^*(G,k)$ ved at relatere den via restriktionsafbildninger til de elementære abelske p-undergruppers kohomologiringe. Vi viser at $H^*(G,k)$ er en endelig frembragt gradueret kommutativ ring, så man kan anvende begreber fra kommutativ algebra såsom Krull-dimension og nilpotens på $H^*(G,k)$ og spørge efter en gruppeteoretisk fortolkning. Vi viser, at Krull-dimensionen af gruppekohomologiringen $H^*(G,k)$ er den maksimale rang blandt de elementære abelske p-undergrupper. Dernæst vender vi vores opmærksomhed mod Quillen's Stratification Sætninger, som garanterer, at maksimalidealspektret af $H^*(G,k)$ tillader en dekomposition i disjunkte dele svarende til de elementære abelske p-undergrupper i G. Vi afslutter dette speciale med at genfortolke resultaterne om maksimalidealspektret for at vise, at kohomologiringen $H^*(G,\mathbb{F}_p)$ kan beskrives op til nilpotens som en ring konstrueret af de elementære abelske p-undergrupper i G og indre monomorfier mellem dem.

Contents

Introduction

In 1971 Quillen published two important articles [16] which describes the mod p group cohomology ring of a compact Lie group for a fixed prime p. Quillen's approach was to investigate the cohomology ring $H^*(G, \mathbb{F}_p)$ in terms of the elementary abelian p-subgroups of G, that is subgroups isomorphic to $(\mathbb{Z}_p)^d$ for some $d \geq 0$. This thesis evolves around the results of Quillen in the case of a finite group.

Given a finite group G and a fixed prime p, there are two equivalent approaches to defining the mod p cohomology ring of G. The algebraic approach, which applies to discrete groups, defines the cohomology ring to be $\mathrm{Ext}^*_{\mathbb{F}_pG}(\mathbb{F}_p, \mathbb{F}_p)$. The topological approach, which applies to topological groups in general, uses the notion of a classifying space. If G is finite, this is an Eilenberg-Maclane space $K(G, 1)$, and the group cohomology ring of G is defined as $H^*(K(G, 1), \mathbb{F}_p)$.

A fundamental result in group cohomology is the Evens-Venkov theorem which states that $H^*(G, \mathbb{F}_p)$ is a finitely generated graded commutative $\mathbb{F}_p$-algebra. In 1959 Venkov [19] proved the theorem for all compact Lie groups using topological methods. A few years later, in 1961, Evens [5] gave a purely algebraic proof for all finite groups. The result suggests that one may use methods from commutative algebra in order to study $H^*(G, \mathbb{F}_p)$. Of course one would like to understand the result in terms of the group theory of G. With his 1971 articles [16] Quillen took a substantial step in this direction. He proved that the Krull dimension of the cohomology ring $H^*(G, \mathbb{F}_p)$ equals the maximal rank of the elementary abelian p-subgroups of G which was conjectured by Atiyah and Swan. Moreover, Quillen described $H^*(G, \mathbb{F}_p)$ up to nilpotency phenomena via the elementary abelian p-subgroups. More precisely, Quillen considered the category $\mathcal{C}_G$ whose objects are the elementary abelian p-subgroups of G and whose morphisms are inclusions of one subgroup into another followed by conjugations by an element in G. Then $E \mapsto H^*(E, \mathbb{F}_p)$ defines a functor from $\mathcal{C}_G^{op}$ to graded commutative $\mathbb{F}_p$-algebras, and the restriction maps induce a homomorphism

$$q_G : H^*(G, \mathbb{F}_p) \to \lim_{E} H^*(E, \mathbb{F}_p).$$

Quillen proved that the map is an F-isomorphism i.e., the kernel is nilpotent and there is some $a \geq 0$ such that for all $x \in \lim_E H^*(E, \mathbb{F}_p)$, $x^{p^a} \in \mathrm{Im}(q_G)$. The inverse limit is reasonably accessible since the cohomology rings of elementary abelian p-groups are well-known and, as we shall see, the homomorphism contains a great deal of information about the structure of $H^*(G, \mathbb{F}_p)$.

Quillen's articles take on a topological approach and use G-spaces and equivariant cohomology. His results hold for compact Lie groups in general, and if one is only interested in the finite case the results are obtained as corollaries of the general case. In this thesis we shall stay in an algebraic setting and thus limiting our results to finite groups.

Structure of the Thesis

The first section of this thesis contains an introduction to group cohomology via classifying spaces. We follow Venkov's topological proof of the finite generation of the cohomology ring $H^*(G,k)$, which exploits the fact that any finite group embeds in the unitary group $U(n)$.

Throughout the rest of the thesis our approach to group cohomology will be strictly algebraic. Section two is dedicated to setting up the basic machinery of algebraic group cohomology, and we will determine the cohomology rings of elementary abelian p-groups.

Let H be a subgroup of G of finite index n. The purpose of the third section is to introduce a transfer-like map, called Evens' norm map,

$$N_{H,G}\colon H^r(H,R) \to H^{rn}(G,R),$$

as constructed by Evens [6]. We will use the norm map to prove a theorem of Serre which states that if G is a finite p-group which is not elementary abelian then there exist non-zero elements $x_1,\dots,x_r \in H^1(G,\mathbb{F}_p)$ for some $r \geq 1$, such that the product of the Bocksteins is zero.

The fourth section is dedicated to determine the Krull dimension of $H^*(G,\mathbb{F}_p)$. We use algebraic methods, as done by Quillen and Venkov [15], to prove that if $u \in H^*(G,\mathbb{F}_p)$ restricts to zero on every elementary abelian p-subgroup, u is in fact nilpotent. It now follows easily that the Krull dimension of $H^*(G,\mathbb{F}_p)$ is the maximal rank of the elementary abelian p-subgroups of G. This approach differs completely from Quillen's original approach that uses G-spaces and equivariant cohomology.

In section five, we turn our attention to the maximal ideal spectrum of G and prove the Quillen Stratification Theorems. The first theorem provides a decomposition of the maximal ideal spectrum of G into disjoint pieces corresponding to the conjugacy classes of elementary abelian p-subgroups of G while the second theorem gives a more detailed description of the pieces going into the decomposition.

We conclude this thesis (section six) by proving that the map

$$q_G : H(G,\mathbb{F}_p) \to \lim_{E} H(E,\mathbb{F}_p).$$

is an F-isomorphism. It turns out that this statement is equivalent to the results proven in the previous section. This equivalence was established by Quillen [16].

Appendix A provides the necessary background from commutative algebra, and appendix B contains some very basic facts about finite p-groups that we shall use in section three.

In order to fully comprehend this text, the reader should be familiar with basic homological algebra such as the derived functor Ext, the universal coefficient theorem, and the Künneth formula. A reference for this is [9]. Furthermore the first section requires a basic background in algebraic topology. We will assume that the reader is familiar with the basic results in homotopy theory, Serre fibrations, and the Serre spectral sequence. Two references here are [8] and [13].

Acknowledgements

My warmest thanks are due to my supervisor, Professor Jesper Grodal, who has been a great inspiration and support in writing this thesis. I also wish to thank Kristian Moi, Jens Jakob Kjær, James Gabe and Kristian Knudsen Olesen for comments and advise along the road.

1 Topological Group Cohomology

This section contains an introduction to group cohomology via classifying spaces. Let R be a Noetherian ring. The main result of this section is Theorem 1.13 which states that the cohomology ring of a finite group G with coefficients in R is a finitely generated graded commutative R-algebra. Throughout this section a map between topological spaces will always mean a continuous map, and all topologies are assumed to be Hausdorff.

1.1 Classifying Spaces

If G is a topological group, a principal G-bundle $p : E \to B$ is roughly speaking a locally trivial free G-space E with orbit space B. Under mild hypotheses, there exists a classifying space BG, such that isomorphism classes of principal G-bundles over B are in natural bijective correspondence with homotopy classes of maps $[B, BG]$. This section will contain no actual proofs, the reader may consult [14] for details. Instead we will emphasize a working understanding of the concepts, allowing us to apply the theory right away. To that end, we have made some simplifying adjustments regarding the functorial properties of the classifying space.

Definition 1.1. A topological group G is a set G equipped with a topology and a group structure such that the functions $G \times G \to G$ given by $(s, t) \mapsto st$ and $G \to G$ given by $s \mapsto s^{-1}$ are continuous. A map of topological groups $\phi : G \to G'$ is a continuous group homomorphism.

For simplicity, we assume that all topological groups are CW-complexes. Any group G can be made into a topological group by equipping G with the discrete topology. The general linear group $GL_n(\mathbb{C})$, consisting of all invertible $n \times n$ matrices with complex entries, is a topological group when equipped with the topology obtained by identifying $GL_n(\mathbb{C})$ with a subspace of the Euclidean space $\mathbb{C}^{n^2}$ in the obvious way. Likewise, the unitary group $U(n)$, consisting of all $n \times n$ matrices with complex entries whose columns form orthonormal bases of $\mathbb{C}^n$ with the usual inner product, is a topological group. Note that any finite topological group must be discrete in order for the topology to be Hausdorff.

Definition 1.2. A right G-space is a topological space X equipped with a continuous right G-action $X \times G \to X$. A G-map is a map of right G-spaces $f : X \to Y$ satisfying $f(xg) = f(x)g$ for all $g \in G$ and $x \in X$. We let X/G denote the orbit space, which is the set of G-orbits in X equipped with the quotient topology with respect to the canonical surjection $\pi : X \to X/G$.

Definition 1.3. Let B be a topological space and let E be a right G-space. Let $p : E \to B$ be a G-map, where G acts trivially on B. We call $E \xrightarrow{p} B$ a principal G-bundle over B if there exist an open cover $\{U_\alpha\}$ of B and G-homeomorphisms h_α such that the following diagram commutes

$$\begin{tikzcd}
p^{-1}(U_\alpha) \arrow[rr, "h_\alpha"] \arrow[dr, "p"'] & & U_\alpha \times G \arrow[dl, "\pi"] \\
& U_\alpha. &
\end{tikzcd}$$

Here, $U_\alpha \times G$ is equipped with the G-action $(u, g)h = (u, gh)$ and π is the projection map onto the first coordinate. We call E the total space and B the base space of the bundle. Note that G must act freely on E. Each fibre $p^{-1}(b)$ is carried homeomorphically onto $\{b\} \times G$ by a G-map, hence the fibre is isomorphic as a G-space to G. Furthermore p induces a bijection $E/G \to B$, which is in fact a homeomorphism. Locally the map

$$U_\alpha \xrightarrow{id \times 1_G} U_\alpha \times G \xrightarrow{h_\alpha^{-1}} p^{-1}(U_\alpha)$$

is an inverse. Let $p : E \to B$ and $p' : E' \to B$ be principal G-bundles over B. A map of principal G-bundles over B is a G-map $\mu : E \to E'$ such that $p'\mu = p$.

Example 1.4. Given a topological space B and a topological group G, we may form the product bundle $B \times G \to B$, which is referred to as the trivial bundle.

For a more interesting example, let G be a discrete group. Then a principal G-bundle with path-connected total space is the same thing as a regular covering map with G as the group of deck transformations. We assume that covering maps have path-connected total space by definition. Indeed, if $p : E \to B$ is a principal G-bundle, then it is a local product with discrete fibre hence a covering map. Any element $g \in G$ gives rise to a deck transformation $E \to E$ by $e \mapsto eg$, hence $G \subset G(E)$, where $G(E)$ denotes the group of deck transformations. Let $f \in G(E)$ and $e \in E$. Then e and $f(e)$ is in the same fibre, hence there is a $g \in G$ such that $eg = f(e)$. Since a deck transformation is determined by its action on a single point, $f = g$ hence $G = G(E)$. Since G acts transitively on each fibre the covering is regular. Conversely, if $\pi : E \to B$ is a regular covering with G as the group of deck transformations, it is easy to see that it is a principal G-bundle.

The above characterization leads to another class of examples. If G is a finite group, then any path-connected Hausdorff space X on which G acts freely gives rise to a principal G-bundle. Letting $x \in X$, we may find disjoint open neighbourhoods U_g around xg and define an open neighbourhood of x by $U_x = \bigcap_{g \in G} U_g g^{-1}$. Clearly $U_x g \cap U_x h = \emptyset$ for any $g \neq h$, so the action is properly discontinuous and thus $X \to X/G$ is a normal covering with G acting as the deck transformations.

Given a principal G-bundle $E \xrightarrow{p} B$ and a map $f : B' \to B$ we can form the pull-back bundle $f^*(p)$ fitting in the ordinary pull-back diagram

$$\begin{tikzcd}
E_f \arrow[r] \arrow[d, "f^*(p)"'] & E \arrow[d, "p"] \\
B' \arrow[r, "f"] & B.
\end{tikzcd}$$

One may verify that $f^*(p)$ inherits a canonical principal G-bundle structure from p such that $E_f \to E$ becomes a G-map.

Theorem 1.5. *Let $E \xrightarrow{p} B$ be a principal G-bundle, and let B' be a CW-complex. If $f, g : B' \to B$ are homotopic maps then $f^*(p)$ and $g^*(p)$ are isomorphic as principal G-bundles over B'.*

The proof is omitted, but can be found in [14, Prop. 7.1].

Definition 1.6. A universal G-bundle is a principal G-bundle $p_G : EG \to BG$ such that for all CW-complexes B, the map

$$[B; BG] \to \mathrm{Princ}_G(B) \quad \text{given by} \quad f \mapsto f^*(p_G)$$

from homotopy classes of maps $B \to BG$ to isomorphism classes of principal G-bundles over B, is a bijection.

The following theorem states that a CW base space BG of a universal G-bundle is in fact unique up to homotopy equivalence. We will refer to such a CW-complex as the classifying space of G.

Theorem 1.7. *Let $p : EG \to BG$ and $p' : EG' \to BG'$ be universal G-bundles with BG and BG' CW-complexes. Then BG and BG' are canonically homotopy equivalent.*

Proof. Let $f : BG \to BG'$ represent the homotopy class corresponding to the isomorphism class containing p, hence $f^*(p') = p$. Likewise, let $f' : BG' \to BG$ correspond to p', hence $(f')^*(p) = p'$. We have the following commutative diagram

$$\begin{tikzcd}
EG \arrow[r] \arrow[d, "p"] & EG' \arrow[r] \arrow[d, "p'"] & EG \arrow[d, "p"] \\
BG \arrow[r, "f"] & BG' \arrow[r, "f'"] & BG,
\end{tikzcd}$$

where the two squares are pull-back squares. But then the outer rectangle is also a pull-back square, hence $(f' \circ f)^*(p) = p$. Since $id^*(p) = p$, it follows from the bijection $[BG; BG] \cong Princ_G(BG)$ that $f' \circ f \cong id_{BG}$. Likewise, we see that $f \circ f' \cong id_{BG'}$, hence $f : BG \to BG'$ is the desired homotopy equivalence. □

A principal G-bundle is in particular a Serre fibration. Since the pull-back of a Serre fibration along a homotopy equivalence is a weak homotopy equivalence, it follows from the proof above that EG and EG' are weakly homotopy equivalent. Before we can make use of the theory of classifying spaces we need the following theorem, which is due to Milnor. Given a topological group G, Milnor provides an explicit functorial construction of a classifying space.

Theorem 1.8. *Let G be a topological group. Then there exists a classifying space BG. The total space EG in Milnor's construction is a contractible CW-complex.*

Sketch of Milnor's construction. Recall that if X and Y are topological spaces, then the join $X * Y$ is the quotient of the product space $X \times I \times Y$ by the equivalence relation

$$\begin{aligned} (x, 0, y) &\sim (x', 0, y) \quad \text{for all } x, x' \in X, y \in Y, \\ (x, 1, y) &\sim (x, 1, y') \quad \text{for all } x \in X, y, y' \in Y. \end{aligned}$$

Intuitively $X * Y$ is formed by taking the disjoint union of the two spaces and attaching a line segment joining every point in X to every point in Y.

We define EG to be the union of all finite joins with the colimit topology topology, i.e.

$$EG := \bigcup_{n \in \mathbb{N}} \underbrace{G * \cdots * G}_{n}.$$

Since G is a CW-complex, so is EG. The underlying set of EG consists of formal elements $(t_1 g_1, t_2 g_2, \dots)$ with each $t_i \in [0, 1]$, $t_i = 0$ for all but finitely many i and $\sum t_i = 1$, modulo the equivalence relation given by

$$(t_1 g_1, t_2 g_2, \dots) \sim (t_1 g_1', t_2 g_2', \dots)$$

provided $g_i = g_i'$ whenever $t_i \neq 0$. A free right G-action on EG is given by

$$(t_1 g_1, t_2 g_2, \dots) g = (t_1 g_1 g, t_2 g_2 g, \dots),$$

and we take BG to be the orbit space $BG = EG/G$. One may consult [3, Thm. 2.4.6] for a proof that $EG \to BG$ is universal. It is easily seen that EG is contractible. Since S^n is compact any map $f : S^n \to EG$ has image in some finite subjoin $G * \cdots * G$ (r times). The join of $(r + 1)$ copies of G

contains the join $G * \cdots * G * (1_G)$ which is a cone, thus contractible. Hence f factors through a contractible subspace and is therefore homotopic to the constant map. Thus EG is weakly contractible and therefore contractible by the Whitehead theorem. □

If G is a topological group we let EG_M and BG_M denote the total space and the base space of Milnor's construction. Let $\phi : G \to G'$ be a map of topological groups. We obtain an induced continuous map $EG_M \to EG'_M$ by mapping

$$(t_1g_1, t_2g_2, \dots) \mapsto (t_1\phi(g_1), t_2\phi(g_2), \dots).$$

Since $(t_1g_1, t_2g_2, \dots)g \mapsto (t_1\phi(g_1), t_2\phi(g_2), \dots)\phi(g)$ we get an induced map of classifying spaces $\phi^* : BG_M \to BG'_M$. Hence $G \mapsto BG_M$ defines a functor from the category of topological groups to the category of topological spaces.

If $E \to B$ is a universal G bundle with B a CW-complex, then E is weakly equivalent to the space EG in Milnor's construction, hence it is weakly contractible. The converse statement is also true, see [14, Thm. 7.4], leading to the following useful characterization.

Theorem 1.9. *Suppose $p : E \to B$ is a principal G-bundle with B a CW-complex. Then $E \to B$ is a universal G-bundle if and only if E is weakly contractible.*

If G be a discrete group, then the classifying space of G is an Eilenberg-MacLane space $K(G,1)$. Indeed, let $p : EG \to K(G,1)$ be the universal cover of $K(G,1)$. This is a regular covering space with G as the group of deck transformations, hence a principal G-bundle. Since EG is simply connected and p induces an isomorphism on the n'th homotopy group when $n \geq 2$, EG is indeed weakly contractible.

The classifying space of $U(n)$ The Steifel manifold $V^n(\mathbb{C}^k)$ is the set of ordered n-tuples of orthonormal vectors in $\mathbb{C}^k$, topologized as a subset of $(\mathbb{C}^k)^n$. The elements of $V^n(\mathbb{C}^k)$ are called n-frames in $\mathbb{C}^k$. The Grassmann manifold $G_n(\mathbb{C}^k)$ is the set of n-dimensional subspaces of $\mathbb{C}^k$ and there is a surjection

$$p : V^n(\mathbb{C}^k) \to G^n(\mathbb{C}^k)$$

sending an n-frame to the subspace it spans. The set $G^n(\mathbb{C}^k)$ is topologized as a quotient space of $V^n(\mathbb{C}^k)$. The fibres of the map are the spaces of n-frames in a fixed n-plane in $\mathbb{C}^k$, and so they are homeomorphic to $V^n(\mathbb{C}^n)$. Since an n-frame in $\mathbb{C}^n$ is the same as a unitary $n \times n$ matrix, viewing the columns of the matrix as an n-frame, the fibres can also be identified with the unitary group $U(n)$. We note that there is no problem in allowing $k = \infty$ in these definitions, and in fact $V^n(\mathbb{C}^\infty) = \cup_k V^n(\mathbb{C}^k)$ and $G^n(\mathbb{C}^\infty) = \cup_k G^n(\mathbb{C}^k)$ with the colimit topologies.

The projection $p : V^n(\mathbb{C}^k) \to G^n(\mathbb{C}^k)$ is a fibre bundle. Indeed, fix an n-plane $P \in G^n(\mathbb{C}^k)$ and pick an orthonormal basis for P. We obtain continuously varying orthonormal bases for all n-planes P' in a neighbourhood U of P by projecting the basis for P orthogonally onto P' and then applying the Gram-Schmidt process. Now we may identify an n-plane P' in U with $\mathbb{C}^n$ according to the orthonormal basis, hence n-frames in these n-planes are identified with n-planes in $\mathbb{C}^n$ such that $p^{-1}(U)$ is identified with $U \times V_n(\mathbb{C}^n)$.

There is a right action of the unitary group $U(n)$ on $V^n(\mathbb{C}^k)$. Given an $n \times n$ unitary matrix W and an n-frame in $\mathbb{C}^k$, we obtain a new n-frame by linear substitutions according to the matrix W. The orbits of $U(n)$ are exactly the fibres of p, thus $V^n(\mathbb{C}^\infty) \to G^n(\mathbb{C}^\infty)$ is a principal $U(n)$-bundle. Since $G^n(\mathbb{C}^\infty)$ admits a CW-structure, it follows from Theorem 1.9 that the bundle is universal if $V^n(\mathbb{C}^\infty)$ is weakly contractible. To this end define a homotopy $H : \mathbb{C}^\infty \times I \to \mathbb{C}^\infty$ by

$$H_t(x_1, x_2, \dots) = (1-t)(x_1, x_2, \dots) + t(0, x_1, x_2, \dots).$$

For a fixed t, this is a linear injective map $\mathbb{C}^\infty \to \mathbb{C}^\infty$. Thus if we apply H_t to an n-tuple of orthonormal vectors in $\mathbb{C}^\infty$ we obtain an n-tuple of linear independent vectors in $\mathbb{C}^\infty$. Applying the Gram-Schmidt process to this tuple makes it orthonormal. Thus we have a deformation retract of $V^n(\mathbb{C}^\infty)$ onto the subspace of n-frames with first coordinate zero. If we repeat the procedure n-times we deform into the subspace of n-frames with first n-coordinates zero. For such an n-frame, we define a homotopy by

$$F_t(v_1, \dots, v_n) = (1-t)(v_1, \dots, v_n) + t(e_1, \dots, e_n),$$

where e_i is the i'th standard basis vector in $\mathbb{C}^\infty$. The homotopy preserves linear independence since v_i has the first n-coordinates zero, so after applying Gram-Schmidt we have a deformation through n-frames onto a fixed n-frame, hence $V^n(\mathbb{C}^\infty)$ is contractible. We conclude that $BU(n) \cong G^n(\mathbb{C}^\infty)$.

The cohomology of the infinite complex Grassmanian with coefficients in a commutative Noetherian ring is well-known and we state the result in the following theorem. See [11, section 20.3].

Theorem 1.10. *Let R be a commutative Noetherian ring. Then*

$$H^*(BU(n), R) \cong R[c_1, \dots, c_n]$$

with $deg(c_i) = 2i$.

1.2 Group Cohomology

Definition 1.11. Let G be a topological group, let BG be a classifying space of G and let R be a commutative ring. The cohomology ring of G with coefficients in R is the cohomology ring $H^*(BG, R)$ with the cup product structure, thus $H^*(BG, R)$ is a graded commutative ring.

We note that $H^*(BG, R)$ is only defined up to canonical isomorphism. If BG and $\tilde{B}G$ are both classifying spaces of G, then they are canonically homotopy equivalent via a map $f : BG \to \tilde{B}G$ determined up to homotopy. Since homotopic maps induces the same map in cohomology, we obtain a canonical isomorphism $f^* : H^*(\tilde{B}G, R) \to H^*(BG, R)$.

Functorial Properties Let $\phi : G \to G'$ be a map of topological groups and let BG and BG' be classifying spaces of G and G' respectively. Let $\phi_M : BG_M \to BG'_M$ denote the induced map on Milnor's classifying spaces. Composing with the canonical homotopy equivalences we obtain a map

$$\overline{f} : BG \xrightarrow{f} BG_M \xrightarrow{\phi_M} BG'_M \xrightarrow{f'} BG',$$

which induces a unique ring homomorphism $f^* : H(BG', R) \to H^*(BG, R)$. The induced map f^* is easily seen to be compatible with the canonical isomorphisms by drawing up the appropriate pull-back diagrams. Let $H \leq G$ be a subgroup. The inclusion $H \hookrightarrow G$ induces a map in cohomology called the restriction map, $\mathrm{res}_{G,H} : H^*(BG, R) \to H^*(BH, R)$.

Given a finite group G fix an inclusion $G \hookrightarrow U(n)$. If we choose the classifying spaces cleverly it will be easy to verify that we have a choice of map $BG \to BU(n)$ inducing the restriction map in cohomology which is a Serre fibration whose fibre is the orbit space $U(n)/G$. This fibration will be the key to the proof of the finite generation of the cohomology ring. We state this in the following theorem.

Theorem 1.12. *Let G be a finite group. There exist a choice of classifying spaces BG and $BU(n)$, and a map $i : BG \to BU(n)$ inducing the restriction map in cohomology, such that*

$$U(N)/G \to BG \xrightarrow{i} BU(n)$$

is a fibre sequence.

Proof. The inclusion $i : G \hookrightarrow U(n)$ induces a map on Milnor's classifying spaces, which is the bottom row in the commutative diagram

$$\begin{tikzcd}
(G * G * \cdots) \arrow[r, hook] \arrow[d] & (U(n) * U(n) * \cdots) \arrow[r, equal] \arrow[d] & (U(n) * U(n) * \cdots) \arrow[d] \\
(G * G * \cdots)/G \arrow[r, "i"] & (U(n) * U(n) * \cdots)/G \arrow[r, "i'"] & (U(n) * U(n) * \cdots)/U(n).
\end{tikzcd}$$

Since $U(n)$ acts freely on the contractible CW-complex $EU(n)_M$, so does G. Since G is finite, we may choose the CW-structure on $EU(n)_M$ such that G acts cellularly ensuring that the coset space $EU(n)_M/G$ is again a CW-complex. Hence the middle column $EU(n)_M \to EU(n)_M/G$ is a universal G-bundle by Theorem 1.9. The left square is easily seen to be a pull back diagram. Indeed, let $y \in (U(n)*U(n)*\cdots)$ such $y \cdot g = x$ for some $x \in (G*G*\cdots)$. By definition of the G-action we must have $y \in (G*G*\cdots)$. Hence the map i is the canonical homotopy equivalence between the two G-classifying spaces BG_M and $EU(n)_M/G$. Let $j : EU(n)_M/G \to BG_M$ denote a homotpy inverse, giving us homotopic maps

$$EU(n)_M/G \xrightarrow{i'} BU(n)_M \qquad \text{and} \qquad EU(n)_M/G \xrightarrow{j} BG_M \xrightarrow{i' \circ i} BU(n)_M.$$

The right hand map induces the restriction map in cohomology, hence so does the left hand map. It is clear that $i' : EU(n)_M/G \to EU(n)_M/U(n)$ is a local product with fibre the coset space $U(n)/G$. Since local products are Serre fibrations, the theorem follows. □

1.3 Finite Generation of the Cohomology Ring

Let G be a finite group and let R be commutative Noetherian ring. In this section we will prove that the cohomology ring $H^*(BG, R)$ is a finitely generated R-algebra following a proof of Venkov as reformulated in [3, Section 3.10]. The restriction map

$$\mathrm{res}_{U(n),G} : H^*(BU(n), R) \to H^*(BG, R)$$

gives $H^*(BG, R)$ the structure of a $H^*(BU(n), R)$-module. We prove that $H^*(BG, R)$ is finitely generated as a $H^*(BU(n), R)$-module and obtain the desired statement as a corollary.

Theorem 1.13. *Suppose G is a finite group and R is a commutative Noetherian ring. Then $H^*(BG, R)$ is a finitely generated $H^*(BU(n), R)$-module.*

Proof. It follows from Theorem 1.12 that we have a fibre sequence of the form

$$U(N)/G \to BG \xrightarrow{i} BU(n),$$

where i induces the restriction map in cohomology. We have a map of fibrations as illustrated in the commutative diagram

$$\begin{tikzcd}
* \arrow[r] & BU(n) \arrow[r, "="] & BU(n) \\
U(n)/G \arrow[r] \arrow[u] & BG \arrow[r, "i"] \arrow[u, "i"] & BU(n). \arrow[u, "="']
\end{tikzcd}$$

Both rows give rise to Serre spectral sequences. Since the Serre spectral sequence is natural with respect to maps of fibrations as in the diagram above, we obtain maps between the spectral sequences as in the diagram below:

$$\begin{tikzcd}
H^*(BU(n), R)) \arrow[r, dashed] \arrow[d] & H^*(BU(n), R) \arrow[d, "\mathrm{res}_{U(n),G}"'] \\
H^*(BU(n), H^*(U(n)/G, R)) \arrow[r, dashed] & H^*(BG, R).
\end{tikzcd}$$

The diagram turns the spectral sequence arising from the bottom fibration into a spectral sequence of $H^*(BU(n), R)$-modules, and the $H^*(BU(n), R)$-module structure on $H^*(BG, R)$ is induced by the module structure on filtration quotients on the E_∞ page. So in order to determine the desired module structure, we start by investigating the module structure on the E_2 page and then, since R is Noetherian, we will be able to work our way to the E_∞ page.

Recall that

$$H^*(BU(n), R) = R[c_1, \ldots, c_n]$$

with $\deg(c_i) = 2i$. Since R is Noetherian it follows from Hilbert's Basis Theorem that $H^*(BU(n), R)$ is Noetherian as well. The E_2 page of the lower spectral sequence is of the form $H^*(BU(n), H^*(U(n)/G, R))$. There are no local coefficients involved since $BU(n)$ is simply connected. Moreover, we have isomorphisms

$$\begin{aligned} H^*(BU(n); H^*(U(n)/G; R)) &\cong H^*(BU(n); R) \otimes_R H^*(U(n)/G, R) \\ &\cong H^*(U(n)/G, R)[c_1, \ldots, c_n], \end{aligned}$$

since the cohomology of $BU(n)$ is a finitely generated free R-module in each dimension. The $H^*(BU(n), R)$-module structure on the E_2-page is induced by the identity map $BU(n) \to BU(n)$ and the map $U(n)/G \to *$, hence we view $H^*(U(n)/G, R)[c_1, \ldots, c_n]$ as a module over the subring $R[c_1, \ldots, c_n]$. It is well known that $U(n)$ has the structure of a finite CW-complex, i.e., a CW-complex with finitely many cells. Since G is finite, we can choose the finite CW-structure such that G acts cellularly, ensuring that the orbit space $U(n)/G$ has the structure of a finite CW-complex. Hence $H^*(U(n)/G, R)$ is finitely generated as an R-module. It follows that the E_2 page of the lower spectral sequence is a finitely generated Noetherian $H^*(BU(n), R)$-module.

The E_∞ page is a sub-quotient of the E_2-page. Since $H^*(BU(n), R)$ is Noetherian it follows that E_∞ is a finitely generated $H^*(BU(n), R)$-module. Hence $H^*(BG, R)$ has a finite filtration of finitely generated $H^*(BU(n), R)$-modules and is therefore finitely generated over $H^*(BU(n), R)$. □

Corollary 1.14. *$H^*(BG, R)$ is a finitely generated graded commutative R-algebra.*

Proof. This is clear since $H^*(BG, R)$ is finitely generated as a module over $H^*(BU(n), R)$ and $H^*(BU(n), R) \cong R[c_1, \dots, c_n]$. □

Definition 1.15. A ring homomorphism $R \to S$ is called finite if S is finitely generated as a module over the image of R.

Theorem 1.13 yields the following important corollary that will play an important role throughout the rest of this thesis.

Corollary 1.16. *Let H be a subgroup of G and let R be a commutative Noetherian ring. Then the restriction map*

$$res_{G,H} : H^*(BG, R) \to H^*(BH, R)$$

is finite.

Proof. We have an embedding of H into $U(n)$ via $H \hookrightarrow G \hookrightarrow U(n)$. Hence the restriction $\mathrm{res}_{U(n),G} : H^*(BU(n), R) \to H^*(BG, R)$ factors as the composition

$$H^*(BU(n), R) \xrightarrow{\mathrm{res}_{U(n),G}} H^*(BG, R) \xrightarrow{\mathrm{res}_{G,H}} H^*(BH, R).$$

Since $H^*(BH, R)$ is finitely generated as a module over $H^*(BU(n), R)$ it is in particular finitely generated as a module over $H^*(BG, R)$. □

2 Algebraic Group Cohomology

Throughout the rest of this thesis our approach to group cohomology will be strictly algebraic, and G will denote a discrete group which we write multiplicatively. The element $1 \in G$ will denote the identity element. Let p be a fixed prime. An elementary abelian p-group is a group isomorphic to $(\mathbb{Z}_p)^d$ for some $d \geq 0$. The purpose of this section is to introduce algebraic group cohomology and present the basic tools of this theory. We will present examples along the way enabling us to determine the group cohomology rings of elementary abelian p-groups. We will end this section with a brief indication on how to connect the two different notions of group cohomology.

2.1 Basic Definitions

Let G be a group and let R be a commutative ring. We will always assume that R is a PID. The most important examples are when $R = \mathbb{Z}$ or when R a field. Let RG denote the group ring of G over R. All RG-modules are assumed to be left RG-modules. Note that an RG-module is nothing more than an R-module on which G acts R-linearly. We will call a RG-module trivial if G acts as the identity. When the ring R is implicitly understood we will refer to an RG-module as a G-module. Likewise we will refer to a morphism of RG-module as a G-module map.

Let G_1 and G_2 be groups, let M a be a G_1-module and let N be a G_2-module. We turn the R-modules $\mathrm{Hom}_R(M,N)$ and $M \otimes_R N$ into $(G_1 \times G_2)$-modules by defining a R-linear action as follows

$$\begin{aligned} ((g_1,g_2)f)(m) &= g_2 f(g_1^{-1}m), \\ (g_1,g_2)(m \otimes n) &= g_1 m \otimes g_2 n, \end{aligned}$$

for $m \in M$, $n \in N$, $f \in \mathrm{Hom}_R(M,N)$, and $(g_1,g_2) \in G_1 \times G_2$. Let $d : G \to G \times G$ denote the diagonal map $g \mapsto g \times g$. Given G-modules M and N, we may regard $\mathrm{Hom}_R(M,N)$ and $M \otimes_R N$ as G-modules via d.

Let X be a chain complex of abelian groups

$$X: \quad \cdots X_n \xrightarrow{\partial} X_{n-1} \xrightarrow{\partial} \cdots \xrightarrow{\partial} X_1 \xrightarrow{\partial} X_0 \to 0.$$

We refer to X as a G-chain complex (or some times just G-complex) if the X_i's are G-modules and the differential ∂ is a G-module map. We will refer to a morphism of G-chain complexes as a G-chain map. If X is a G-chain complex, M is a G-module and we have an augmentation map $\epsilon_0 : X_0 \to M$ we simple write $X \to M$, and call it a G-resolution of M. We say that $X \to M$ is a free/projective G-resolution if all the X_i's are free/projective G-modules. Let A be a ring which is also a G-module. If the multiplication $A \otimes_R A \to A$ is a G-module map we call A a G-ring.

Definition 2.1. Let G be a group and let M be a G-module. We define the n'th cohomology group of G with coefficient in M by

$$H^n(G,M) = \operatorname{Ext}^n_{RG}(R,M),$$

where R is thought of as a trivial G-module.

The definition may seem to depend on the base ring R, but the ring homomorphism $\mathbb{Z} \to R$ given by $1 \mapsto 1$ induces an isomorphism

$$\operatorname{Ext}^n_{RG}(R,M) \cong \operatorname{Ext}^n_{\mathbb{Z}G}(\mathbb{Z},M)$$

where we view M as a $\mathbb{Z}G$-module via $\mathbb{Z} \to R$. See [7, Section 1.1] for details.

Example 2.2. Let $G = \langle x \rangle$ be a cyclic group of order t with generator x, and let N denote the element $1 + x + \cdots + x^{t-1} \in RG$. Define $\varepsilon : RG \to R$ by $\varepsilon(x) = 1$. Then

$$F: \quad \cdots \xrightarrow{\cdot N} RG \xrightarrow{\cdot(x-1)} RG \xrightarrow{\cdot N} RG \xrightarrow{\cdot(x-1)} RG \xrightarrow{\varepsilon} R \to 0$$

is a free G-resolution of R. For a G-module M, $\operatorname{Hom}_{RG}(RG,M) \cong M$, hence the complex $\operatorname{Hom}_{RG}(F,M)$ is isomorphic to the complex

$$0 \to M \xrightarrow{\cdot(x-1)} M \xrightarrow{\cdot N} M \xrightarrow{\cdot(x-1)} M \xrightarrow{\cdot N} \cdots .$$

Now we may calculate the cohomology of G with coefficients in M to be

$$H^n(G,M) = \begin{cases} M^G & \text{if } n = 0, \\ \ker(\cdot N)/\operatorname{Im}(\cdot(x-1)) & \text{if } n > 0,\ n \text{ odd}, \\ \ker(\cdot(x-1))/\operatorname{Im}(\cdot N) & \text{if } n > 0,\ n \text{ even}, \end{cases}$$

where $M^G = \{m \in M \mid gm = m \text{ for all } g \in G\}$. If $M = \mathbb{Z}$ we obtain

$$H^n(G,\mathbb{Z}) = \begin{cases} \mathbb{Z} & \text{if } n = 0, \\ 0 & \text{if } n > 0,\ n \text{ odd}, \\ \mathbb{Z}_t & \text{if } n > 0,\ n \text{ even}. \end{cases}$$

If P is a cyclic group of prime order p and $M = k$ is a field of characteristic p, then both maps $\cdot(x-1)$ and $\cdot N$ are zero. Hence $H^n(P,k) = k$ (as an additive group) for all $n \geq 0$.

Functorial Properties We may view $H^*(-,-)$ as a functor from the following category: An object in $\mathcal{C}$ is a pair (G,M) where G is a group and M is a G-module. A morphism in $\mathcal{C}$, $(G,M) \to (G',M')$, is a pair of compatible maps $(\phi : G \to G', f : M' \to M)$, i.e., ϕ is a map of groups and f is a G-module map when we view M' as a G-module via ϕ. Given projective resolutions F and F' of R over G and G' respectively, we may regard F'

as a G-complex via ϕ. In this case F' is acyclic though not necessarily projective. It is a fundamental result in introductory homological algebra that there exists an augmentation preserving G-chain map $\Phi : F \to F'$, and that such is map is unique up to homotopy. We thus obtain a chain map

$$\mathrm{Hom}(\Phi, f) : \mathrm{Hom}_{RG'}(F', M') \to \mathrm{Hom}_{RG}(F, M)$$

which is also unique up to homotopy. Since homotopic chain maps induce the same maps in cohomology, we get a well-defined morphism $(\alpha, f)^* : H^*(G', M') \to H^*(G, M)$ making $H^*(-,-)$ into a contravariant functor on $\mathcal{C}$. If $M' = M$ and $f = id$ we simply write α^* for the induced map. Note that for a trivial G-module A, we may regard $H^n(-, A)$ as a contravariant functor on the category of groups.

Low Degree Cohomology We refer a few result from [7, Section 2.3] to give some intuition about low degree group cohomology. If M is a G-module, then $H^0(G, M) = M^G$ and if M is a trivial G-module then $H^1(G, M) = \mathrm{Hom}(G, M)$. It is easily verified that if $\phi : G \to G'$ is a group homomorphism then the induced map in cohomological dimension 1 can be identified with pre-composition by ϕ.

Remark 2.3. We recall a useful result from homological algebra known as the Künneth formula. Let A and B be free R-chain complexes. The tensor product $A \otimes_R B$ is an R-chain complex with differential

$$d(a \otimes b) = da \otimes b + (-1)^{\mathrm{deg} a} a \otimes db.$$

The Künneth formula tells us that there is an exact sequence

$$0 \to H_*(A) \otimes_R H_*(B) \to H_*(A \otimes_R B) \to \mathrm{Tor}_1^R(H_*(A), H_*(B)) \to 0.$$

The left hand map is defined as follows. Let a and b represent homogeneous elements in $H_*(A)$ and $H_*(B)$ respectively. Then the image is represented by $a \otimes b$. We will refer to this map as the Künneth map.

The Ring Structure of $H^*(G, R)$ The cohomology complex $H^*(G, R)$ may be endowed with a multiplicative structure, turning it into a graded commutative ring. Here graded commutative means that the multiplication satisfies the commutation rule

$$\alpha\beta = (-1)^{pq}\beta\alpha$$

for $\alpha \in H^p(G, R)$ and $\beta \in H^q(G, R)$. We introduce the product, often referred to as the cup-product, in a slightly more general setting. Given G-modules M and N the cup-product will be a collection of homomorphsims

$$H^r(G, M) \otimes_R H^s(G, N) \to H^{r+s}(G, M \otimes_R N).$$

If we in addition are given a G-module L and a map of G-modules $M \otimes_R N \to L$, then we may compose the cup-product with the induced map and obtain a collection of pairings

$$H^r(G, M) \otimes_R H^s(G, N) \to H^{r+s}(G, L).$$

In particular if $M = N = L$ is a G-ring, then the cup-product gives $H^*(G, M)$ the structure of a graded ring. More generally, if A is a G-ring and M is a G-module, which is also an A-module in a compatible way, i.e., the action $A \otimes_R M \to A$ is a map of G-modules, then $H^*(G, M)$ is a module over $H^*(G, A)$. We will only sketch the construction of the cup-product. Verification of the various properties of the cup-product may be found in [7, Chapter 3].

Let G and H be groups and let M be a G-module and N an H-module. Also let $X \to R$ be a projective G-resolution and let $Y \to R$ be an projective H-resolution. One may verify that $X \otimes_R Y \to R \otimes_R R \cong R$ is a projective resolution of R as a $G \times H$-module. Define the cross product

$$\mathrm{Hom}_{RG}(X, M) \otimes_R \mathrm{Hom}_{RH}(Y, N) \xrightarrow{\times} \mathrm{Hom}_{R(G\times H)}(X \otimes_R Y, M \otimes_R N).$$

by

$$(f \times g)(x \otimes y) = f(x) \otimes g(y).$$

This induces a map in cohomology when composed with the Künneth map gives rise to a degree preserving homomorphism

$$\times : H^*(G, M) \otimes_R H^*(H, N) \to H^*(G \times H, M \otimes_R N).$$

We will call this map *the cross product.* If $\alpha \in H^r(G, M)$ and $\beta \in H^s(H, N)$ we will denote the image of $\alpha \otimes \beta$ in $H^{r+s}(G \times H, M \otimes_R N)$ by $\alpha \times \beta$. Let $d : G \to G \times G$ denote the diagonal map. The cup-product is defined as the composition of d^* with the cross product. Hence if $\alpha \in H^r(G, M)$ and $\beta \in H^s(G, N)$ then the cup-product $\alpha\beta \in H^{r+s}(G, M \otimes_R N)$ is given by $\alpha\beta := d^*(\alpha \times \beta)$. We state the following theorem describing the properties of the cup-product.

Theorem 2.4. *If A is a commutative G-ring, then $H^*(G, A)$ is an associative commutative graded ring with identity $1 \in H^0(G, A) = A^G$, i.e., $\alpha\beta = (-1)^{pq}\beta\alpha$ for $\alpha \in H^p(G, A)$ and $\beta \in H^q(G, A)$. If M is an A-module, which is also a G-module with consistent action, then $H^*(G, M)$ is a graded $H^*(G, A)$-module with 1 acting as the identity. All maps induced in cohomology are graded ring homomorphisms (or module homomorphism in the module case).*

Describing the cup product on the level of cochains boils down to describing the map d^* at cochain level. Let $X \to R$ be a projective G-resolution.

Then $X \otimes_R X \to R$ is a projective $G \times G$-resolution. Thus to describe the map $d^* : H^*(G \times G, M \otimes_R N) \to H^*(G, M \otimes_R N)$, we need a chain map $D : X \to X \otimes_R X$ such that $D(gx) = d(x)D(x)$. Such a map is unique up to homotopy and will be called a diagonal map.

Example 2.5. Let $G = \langle x \rangle$ be a cyclic group of order t with generator x. We have a projective G-resolution of R given by $X_n = RGx_n$, $\epsilon(x_0) = 1$, $d_n(x_n) = (x-1) \cdot x_{n-1}$ for n odd and $d_n(x_n) = N \cdot x_{n-1}$ for n even, $n > 0$, as in Example 2.2. The following map is a diagonal map:

$$D = \sum D_{r,s} \quad \text{where} \quad D_{r,s} : X_{r+s} \to X_r \otimes_R X_s \quad \text{is given by}$$

$$D_{r,s}(x_{r+s}) = \begin{cases} x_r \otimes x_s & r \text{ even}, \\ x_r \otimes xx_s & s \text{ even}, r \text{ odd}, \\ \sum_{0 \le i < j < t} x^i x_r \otimes x^j x_s & r, s \text{ odd}. \end{cases}$$

The verification is rather long and tedious and will be omitted here. Let M and N be G-modules, let $m \in M$ represent a cohomology class in degree r and let $n \in N$ represent a cohomology class in degree s. Then the cup product of these classes is represented by

$$\begin{array}{rl} m \otimes n & \text{if } r \text{ or } s \text{ is even}, \\ \displaystyle\sum_{0 \le i < j < t} x^i m \otimes x^j n & \text{if } r \text{ and } s \text{ are odd}, \end{array}$$

because $n \in \ker(\cdot(x-1))$ if s is even. Let M be a trivial G-ring and let $m, n \in M$ represent cohomology classes of degree r and s respectively. It follows that the cup product of these classes is represented by

$$\begin{array}{rl} mn, & \text{if } r \text{ or } s \text{ is even}, \\ \dfrac{t(t-1)}{2} mn, & \text{if } r \text{ and } s \text{ are odd}. \end{array}$$

If we combine this information with Example 2.2 we obtain

$$H^*(P, \mathbb{Z}) = \mathbb{Z}[\chi \mid p\chi = 0, \ \deg\chi = 2],$$

if P is cyclic of prime order p. If k is a field of characteristic p then

$$H^*(P, k) = \begin{cases} k[\nu, \varepsilon \mid \deg\nu = 1, \deg\varepsilon = 2, \nu^2 = 0] & \text{if } p > 2, \\ k[\nu \mid \deg\nu = 1] & \text{if } p = 2, \end{cases}$$

Since $H^1(P, k) = \mathrm{Hom}(P, k)$ we may choose ν as the homomorphism given by $\nu(x) = 1$. Given a G-module M, $H^*(G, M)$ is a graded module over $H^*(G, k)$. If $p > 2$ then multiplication by ε is an isomorphism $H^q(G, M) \to H^{q+2}(G, M)$ for $q > 0$ and an epimorphism for $q = 0$. Likewise, for $p = 2$ multiplication by ν is an isomorphism $H^q(G, M) \to H^{q+1}(G, M)$ for $q > 0$ and an epimorphism for $q = 0$.

Restriction, Corestriction and Inflation Maps Let $H \leq G$ be a subgroup and let M be a G-module. The inclusion $H \hookrightarrow G$ induces a map in cohomology, called the restriction map,

$$\mathrm{res}_{G,H} : H^*(G, M) \to H^*(H, M).$$

If $X \to R$ is a free G-resolution, then $X \to R$ is also an free H-resolution since RG is RH-free. On cochain level the restriction map is induced by the inclusion

$$\mathrm{Hom}_{RG}(X, M) \subseteq \mathrm{Hom}_{RH}(X, M).$$

Assume that H is a subgroup of finite index n. In this case we may construct a map going in the other direction called the corestriction. If $f \in \mathrm{Hom}_{RH}(X_i, M)$ we define $\mathrm{co}(f) \in \mathrm{Hom}_{RG}(X_i, M)$ by

$$\mathrm{co}(f)(x) = \sum_{g_i \in G/H} g_i f(g_i^{-1} x), \quad x \in X_i,$$

where G/H denotes a set of left coset representatives. Let $(G/H)'$ denote another set of representatives, hence for $g_i' \in (G/H)'$ we have $g_i' = g_j h$ for a unique $g_j \in G/H$ and $h \in H$. Then

$$g_j \alpha(g_j^{-1} x) = g_j \alpha(h g_i'^{-1} x) = g_j h \alpha(g_i'^{-1} x) = g_i' \alpha(g_i'^{-1} x),$$

so summing over all representatives we see that $\mathrm{co}(f)$ is independent of the choice of coset representatives. To see that $\mathrm{co}(f)$ is a map of G-modules consider a term of the form $g_i \alpha(g_i^{-1} g x)$. For $g_i \in G/H$ we have $g_i^{-1} g = h g_j^{-1}$ for a unique $g_j \in G/H$ and $h \in H$. Then

$$g_i f(g_i^{-1} g x) = g_i f(h g_j^{-1} x) = g_i h f(g_j^{-1} x) = g g_j f(g_j^{-1} x),$$

thus summing over all cosets yields the linearity. Thus $\mathrm{co} : \mathrm{Hom}_H(X, M) \to \mathrm{Hom}_G(X, M)$ induces a map in cohomology

$$\mathrm{cor}_{H,G} : H^*(H, M) \to H^*(G, M),$$

which is easily seen to be independent of resolution X. If we have subgroups of finite index $K \leq H \leq G$ then $\mathrm{cor}_{K,H} \circ \mathrm{cor}_{H,G} = \mathrm{cor}_{K,G}$, which is verified by using the fact that if S is a set of left coset representatives of K in H and T is a set of left coset representatives of H in G, then the set of products TS is a set of left coset representatives of K in G. The next theorem follows directly from the definitions on cochain level.

Theorem 2.6. *Let $H \leq G$ be a subgroup of finite index. Then the composition*

$$cor_{H,G} \circ res_{G,H} : H^*(G, M) \to H^*(G, M)$$

is multiplication by $[G : H]$.

Corollary 2.7. *Let p be a prime dividing $|G|$ and let H be a subgroup of finite index such that p does not divide $[G:H]$. Then the restriction map*

$$res_{G,H} : H^*(G, \mathbb{F}_p) \to H^*(H, \mathbb{F}_p)$$

is injective.

Proof. Since the element $[G:H] \in H^0(G, \mathbb{F}_p) = \mathbb{F}_p$ is invertible, it follows that the composition $\mathrm{cor}_{H,G} \circ \mathrm{res}_{G,H}$ is injective, hence $\mathrm{res}_{G,H}$ is injective. □

In particular if $|G| < \infty$ the restriction to any non-trivial Sylow-p-subgroup is injective. Finally, we obtain another useful corollary.

Corollary 2.8. *If G is a finite group and M is a G-module, then*

$$|G|H^n(G, M) = \{0\}$$

for all $n > 0$.

Proof. By Theorem 2.6 multiplication by $|G| = [G : \{1\}]$ factors through $H^n(\{1\}, M) = \{0\}$. □

Theorem 2.9. *Let $H \leq G$ be a subgroup of finite index and let M be a G-module. Then*

$$cor_{H,G}(res_{G,H}(\alpha)\beta) = \alpha cor_{H,G}(\beta).$$

for $\alpha \in H^*(G, M)$ and $\beta \in H^*(H, M)$.

Proof. Let $X \to R$ be a projective G-resolution, let $g \in \mathrm{Hom}_{RH}(H, M)$ represent β and let $f \in \mathrm{Hom}_{RG}(X, M)$ represent α, then $f \in \mathrm{Hom}_{RH}(X, M)$ represents $\mathrm{res}_{G,H}(\alpha)$. We may view $X \otimes_R X \to R$ as a projective G-resolution via $d : G \to G \times G$. We can use the identity $X \otimes_R X \to X \otimes_R X$ to compute products, where the complex on the left is viewed as a G-complex and the complex on the right is viewed as a $G \times G$-complex (and similar for H). With these identifications $f \times g \in \mathrm{Hom}_{RH}(X \otimes_R X, M \otimes_R M)$ represents $\mathrm{res}_{G,H}(\alpha)\beta$, hence $\mathrm{co}(f \times g) \in \mathrm{Hom}_{RG}(X \otimes_R X, M \otimes_R M)$ represents $\mathrm{cor}_{H,G}(\mathrm{res}_{G,H}(\alpha)\beta)$, while $f \times \mathrm{co}(g) \in \mathrm{Hom}_{RG}(X \otimes_R X, M \otimes_R M)$ represents $\alpha \mathrm{cor}_{H,G}(\beta)$. By comparing the two maps on an element $x \otimes y \in X \otimes_R X$, the statement follows. □

Finally, we are left with only one more useful map to introduce. Let N be a normal subgroup of G and let M be a G-module. If $f : G \to G/N$ denote the quotient map and if $\iota : M^G \to M$ is the inclusion, then the induced map $(f, \iota)^* = \mathrm{inf}_{G/N,G} : H(G/N, M^G) \to H(G, M)$ is called the inflation map.

Conjugation Maps Fix $g \in G$, let H be a subgroup of G and let M be a G-module. Define a morphism $(f : gHg^{-1} \to H, \alpha : M \to M)$ by

$$f(h) = g^{-1}hg, \ h \in gHg^{-1}; \qquad \alpha(m) = gm, \ m \in M.$$

It induces an isomorphism in cohomology $g^* : H^*(H, M) \to H^*(gHg^{-1}, M)$. On the level of cochains, g^* is induced by the map

$$\begin{aligned} &g' : \mathrm{Hom}_{RH}(X, M) \to \mathrm{Hom}_{R(gHg^{-1})}(X, M) \\ &\text{given by} \quad (g'f)(x) = gf(g^{-1}x), \end{aligned}$$

where $X \to R$ denotes a projective G-resolution. It is easy to check that $(g_1g_2)^* = g_1^*g_2^*$, so if H is a normal subgroup we obtain a R-linear action of G on $H^*(H, M)$. Clearly $h^* = id$ for $h \in H$, so if H is a normal subgroup of G, this actually defines a G/H-action on $H^*(H, M)$ giving $H^*(H, M)$ the structure of a G/H-module. If $G = H$ we get the following theorem.

Theorem 2.10. *G acts trivially on $H^*(G, M)$.*

Bockstein Homomorphisms Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of G-modules. This gives rise to a long exact sequence in cohomology with boundary maps

$$\delta : H^n(G, M'') \to H^{n+1}(G, M'),$$

which are referred to as Bockstein homomorphisms. The most important ones are $\beta : H^n(G, \mathbb{Z}_p) \to H^{n+1}(G, \mathbb{Z}_p)$ arising from the short exact sequence

$$0 \to \mathbb{Z}_p \xrightarrow{\cdot p} \mathbb{Z}_{p^2} \to \mathbb{Z}_p \to 0$$

and $\hat{\beta} : H^n(G, \mathbb{Z}_p) \to H^{n+1}(G, \mathbb{Z})$ arising from the short exact sequence

$$0 \to \mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z} \to \mathbb{Z}_p \to 0.$$

Note that β is obtained by composing $\hat{\beta}$ with the map induced by the projection $\mathbb{Z} \to \mathbb{Z}_p$. Another useful Bockstein arises from the short exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0.$$

If G is a finite group, then by Corollary 2.8 $|G|H^n(G, \mathbb{Q}) = \{0\}$ for $n > 0$. Since $H^n(G, \mathbb{Q})$ is a vector space over $\mathbb{Q}$, $H^n(G, \mathbb{Q}) = \{0\}$ for all $n > 0$, the connecting homomorphism

$$\delta : H^n(G, \mathbb{Q}/\mathbb{Z}) \to H^{n+1}(G, \mathbb{Z})$$

is an isomorphism for $n > 0$. In particular

$$H^2(G, \mathbb{Z}) \cong H^1(G, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}).$$

Remark 2.11. The following useful observation is an application of the universal coefficient theorem in homology. Let k be a field, let X be a k-complex and let M be a k-module. The universal coefficient theorem then provides an isomorphism

$$H_*(X) \otimes_k M \cong H_*(X \otimes_k M),$$

since the Tor part vanishes. Next, let G be a group, let $Y \to k$ be a projective kG-resolution and let M be a trivial kG-module. One may easily verify that we have an isomorphism of co-chain complexes

$$\mathrm{Hom}_{kG}(Y, k) \otimes_k M \cong \mathrm{Hom}_{kG}(Y, M).$$

Setting $X = \mathrm{Hom}_{kG}(Y, k)$ we obtain an isomorphism $H^*(G, k) \otimes M \cong H^*(G, M)$ which is easy to describe. Let $f : P \to k$ be a cocycle representing a class $\alpha \in H^*(G, k)$ and let $m \in M$. Define $F : P \to M$ by $F(p) = f(p)m$. Then F is a again a cocycle and we map $\alpha \otimes m$ to the class represented by F.

If k is a field of characteristic p, it is an $\mathbb{F}_p$-algebra and the universal coefficient theorem provides an isomorphism $H^*(G, \mathbb{F}_p) \otimes_{\mathbb{F}_p} k \cong H^*(G, k)$, which is easily seen to be an isomorphism of k-algebras. Thus hence we have an embedding $H^*(G, \mathbb{F}_p) \hookrightarrow H^*(G, k)$ given by $x \mapsto x \otimes 1$. We abuse notation slightly and let β denote the composition

$$H^1(E, \mathbb{F}_p) \xrightarrow{\beta} H^2(E, \mathbb{F}_p) \hookrightarrow H^2(E, k),$$

where $\beta : H^1(E, \mathbb{F}_p) \to H^2(E, \mathbb{F}_p)$ is the Bockstein. If $\phi : G \to G'$ is a group homomorphism, then it is straight forward to verify that the induced map $\phi^* \otimes id$ on the left hand side corresponds to the induced map ϕ^* on the right hand side.

2.2 The Cohomology Ring of Elementary Abelian p-Groups

Let G and H be finite groups. Then $H^*(G, R) \otimes H^*(H, R)$ becomes an R-algebra when equipped with the multiplication

$$(a \otimes b)(c \otimes d) = (-1)^{\deg(b)\deg(c)} ac \otimes bd.$$

Recall that we have the external product

$$H^*(G, R) \otimes_R H^*(H, R) \to H^*(G \times H, R),$$

which is easily seen to be a map of R-algebras. Using the Künneth formula, one may verify that the map is injective. If $R = k$ is a field, then it is actually an isomorphism, see [7, p.17]. The restriction to finite groups appears because we want to ensure the existence of a free resolution of R over G and

H respectively in which each module is finitely generated. The observation allows us to determine the cohomology ring of any finite abelian group with field coefficients, since we have calculated the cohomology of cyclic groups.

Let $P = \langle x \rangle$ be a cyclic group of prime order p with generator x. Since we know the cohomology groups of P with $\mathbb{Z}$ and $\mathbb{Z}_p$ coefficients we are able to compute a segment of the long exact sequence arising from $\mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z} \to \mathbb{Z}_p$

$$\cdots 0 \to H^1(P, \mathbb{Z}_p) \xrightarrow{\hat{\beta}} H^2(P, \mathbb{Z}) \xrightarrow{p=0} H^2(P, \mathbb{Z}) \to H^2(P, \mathbb{Z}_p) \xrightarrow{\hat{\beta}} 0 \cdots$$

We see that $\hat{\beta} : H^1(P, \mathbb{Z}_p) \to H^2(P, \mathbb{Z})$ and the projection map $H^2(P, \mathbb{Z}) \to H^2(P, \mathbb{Z}_p)$ are isomorphisms. Since β is the composition of these two maps, $\beta : H^1(P, \mathbb{Z}_p) \to H^2(P, \mathbb{Z}_p)$ is an isomorphism as well. Now, a generator $\nu \in H^1(P, \mathbb{Z}_p) = \operatorname{Hom}(P, \mathbb{Z}_p)$ may be characterized by $\nu(x) = 1$, thus $\beta(\nu)$ generates $H^2(P, \mathbb{Z}_p)$.

Let $E = P^d$, for P a cyclic group of prime order p, let k be a field of characteristic p and define $(E)^* = \operatorname{Hom}(E, k)$. The above discussion combined with Example 2.5 tell us that for $p > 2$

$$H^*(E, k) \cong H^*(P, k)^{\otimes d} \cong \Lambda[\nu_1, \ldots, \nu_d] \otimes k[\varepsilon_1, \ldots, \varepsilon_d],$$

where $\deg(\nu_i) = 1$ and $\deg(\varepsilon_i) = 2$, and $\{\nu_1, \ldots, \nu_d\}$ forms a basis for $(E)^*$. Let $p_i : E \to P_i$ be the projection onto the i'th factor. Since the long exact sequence in cohomology is natural the following diagram commutes

$$\begin{tikzcd}
\operatorname{Hom}(P_i, \mathbb{F}_p) \arrow[r, "\circ p_i"] \arrow[d, "\beta"] & \operatorname{Hom}(E, \mathbb{F}_p) \arrow[d, "\beta"] \\
H^2(P_i, \mathbb{F}_p) \arrow[r, "p_i^*"] & H^2(E, \mathbb{F}_p),
\end{tikzcd}$$

hence $\varepsilon_i = \beta(\nu_i)$ just as in the cyclic case. For $p = 2$

$$H^*(E, k) \cong H^*(P, k)^{\otimes d} \cong k[\nu_1, \ldots, \nu_d].$$

To summarize we may write

$$H^*(E, k) \cong \begin{cases} S_k(E^*, 1) & \text{if } p = 2, \\ \Lambda_k(E^*, 1) \otimes_k S_k(E^*, 2) & \text{if } p > 2, \end{cases}$$

where $S_k(E^*, i)$ is a symmetric graded algebra over k with E^* in degree i and similarly $\Lambda_k(E^*, i)$ is a graded exterior algebra over k with E^* in degree i.

If we consider integral coefficients, we only obtain a ring monomorphism

$$H^*(P,\mathbb{Z})^{\otimes d} \hookrightarrow H^*(E,\mathbb{Z}).$$

Thus $H^*(E,\mathbb{Z})$ contains a subring of the form $\mathbb{Z}[\chi_1,\dots,\chi_d \mid p\chi_i = 0]$ where $\{\chi_1,\dots,\chi_d\}$ form a basis for $H^2(E,\mathbb{Z}) = \mathrm{Hom}(E,\mathbb{Q}/\mathbb{Z})$. This subring may be described as the symmetric graded algebra over $\mathbb{Z}$ with $\hat{E} = \mathrm{Hom}(E,\mathbb{Q}/\mathbb{Z})$ in degree 2. Thus we have a monomorphism

$$S_{\mathbb{Z}}(\hat{E},2) \hookrightarrow H^*(E,\mathbb{Z}).$$

2.3 Equivalence with the Topological Definition

Given a discrete group G, we have two different definitions of group cohomology. Luckily, they are equivalent. We will briefly sketch how this equivalence arises and show that the n'th cohomology group defined via classifying spaces is isomorphic to the n'th cohomology group defined algebraically. The equivalence is of course far more comprehensive, the product structure and the induced maps are compatible, so the results achieved via topological methods apply in the algebraic setting.

Before we can exhibit the equivalent nature of the two approaches we recall the definition of cohomology with local coefficients which is a generalization of ordinary cohomology. Let X be a path-connected space having a universal cover $\tilde{X}$ and fundamental group π. The group π acts on $\tilde{X}$ as deck transformations and this induces an action on the chains of X sending an n-simplex $\sigma : \triangle^n \to \tilde{X}$ to the composition $\triangle^n \xrightarrow{\sigma} \tilde{X} \xrightarrow{\gamma} \tilde{X}$ for $\gamma \in \pi$. This makes $C_*(\tilde{X})$ into a chain-complex of $\mathbb{Z}\pi$-modules. Let M be a left $\mathbb{Z}\pi$-module. The cohomology groups of X with local coefficients in M is defined as the cohomology of the cochain-complex $\mathrm{Hom}_{\mathbb{Z}\pi}(C_*(\tilde{X}),M)$, i.e.,

$$H^n(X,\underline{M}) := H^n(\mathrm{Hom}_{\mathbb{Z}\pi}(C_*(\tilde{X}),M)).$$

When M is a trivial $\mathbb{Z}\pi$-module, $H^n(X,\underline{M})$ is just ordinary cohomology with coefficients in the abelian group M. The basic properties of ordinary cohomology extend to cohomology with local coefficients.

Let X be a free G-set and turn the free abelian group $\mathbb{Z}X$ into a $\mathbb{Z}G$-module by extending the action of G on X to a $\mathbb{Z}$-linear action on $\mathbb{Z}X$. We may write X as the disjoint union of orbits $X = \coprod_{x\in I} G_x$, where I is a set of representatives for the orbits. Since the action is free, each orbit is isomorphic to G, and so as a G-set $X \cong \coprod_I G$. In this way we obtain an isomorphism of $\mathbb{Z}G$-modules $\mathbb{Z}X \cong \oplus_I \mathbb{Z}G$. To summarize, we have proven the following theorem.

Theorem 2.12. *Let X be a free G-set and let E be a set of representatives of the G-orbits in X. Then $\mathbb{Z}X$ is a free $\mathbb{Z}G$-modules with basis E.*

Now, let $\tilde{Y} \xrightarrow{p} Y$ be a regular covering map with G as the group of deck transformations. If Y is a CW-complex then $\tilde{Y}$ naturally inherits a CW-structure. The open cells of $\tilde{Y}$ lying over an open cell $\sigma \in Y$ are simply the connected components of $p^{-1}(\sigma)$. The cells are permuted freely and transitively by G and each is mapped homeomorphically onto σ by p. Hence G permutes the cells of the same dimension, so $C_*(\tilde{Y})$ becomes a chain complex of $\mathbb{Z}G$-modules and by Theorem 2.12 each $C_n(\tilde{Y})$ is a free $\mathbb{Z}G$-modules with one basis element for each n-cell of Y. Define an augmentation map $C_0(\tilde{Y}) \to \mathbb{Z}$ by $v \mapsto 1$ for every 0-cell v of $\tilde{Y}$. We obtain a chain complex of $\mathbb{Z}G$-modules

$$\cdots \to C_n(\tilde{Y}) \to C_{n-1}(\tilde{Y}) \to \cdots \to C_0(\tilde{Y}) \to \mathbb{Z} \to 0.$$

If $\tilde{Y}$ is contractible then $\tilde{H}_*(\tilde{Y}) = \tilde{H}_*(*)$ and the chain-complex is exact.

Now it should be clear how we should compare the two definitions of group cohomology. We know that $K(G,1)$ is a classifying space of G and we let $\tilde{X} \to K(G,1)$ be the universal cover. This is a regular covering map with G as the group of deck transformations and $\tilde{X}$ is contractible. Hence the cellular chain-complex $C_*(\tilde{X})$ is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}G$.

Theorem 2.13. *Let M be a G-module. Then we have an isomorphisms of abelian groups $H^n(G,M) \cong H^n(BG,\underline{M})$.*

Proof. Let $\tilde{X} \to K(G,1)$ be the universal cover. By definition the cohomology of G with coefficients in M is the cohomology of the chain complex $\mathrm{Hom}_G(C_*(\tilde{X}), M)$. But since the chain-complex $C_*(\tilde{X})$ is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}G$ this is the exact same chain complex as the one used for the algebraic definition of group cohomology. □

3 Evens' Norm Map

Let G be a group and let H a subgroup of finite index n. The purpose of this section is to introduce a map called Evens' norm map

$$N_{H,G} \colon H^r(H, R) \to H^{rn}(G, R),$$

as done by Evens in [7, section 5 and 6]. The norm was originally constructed by Evens in [6]. We will sketch the construction of the norm map and state its properties. First we will take some time to investigate how Evens' norm map acts on elementary abelian p-groups. Afterwards we will prove a theorem of Serre, Theorem 3.8, that provides a rings structural difference between the cohomology ring of an elementary abelian p-groups and the cohomology ring of a p-group which is not elementary abelian. The understanding of the norm map on elementary abelian p-groups will be crucial to the proof.

3.1 Wreath Products and the Monomial Embedding

Let S_n denote the permutation group on n letters. Then S_n acts from the left on $H^{\times n}$ by permuting the factors

$$(h_1, \ldots, h_n)\sigma = (h_{\sigma(1)}, \cdots, h_{\sigma(n)}),$$

and we define the wreath product $S_n \int H$ to be the semi-direct product $S \ltimes H^{\times n}$. Thus $S_n \int H$ consists of tuples $(\sigma, h_1, \ldots, h_n)$ with $\sigma \in S_n$, $h_i \in H$ and multiplication is given by

$$(\sigma, h_1, \ldots, h_n)(\sigma', h'_1, \ldots, h'_n) = (\sigma \circ \sigma', h_{\sigma'(1)}h'_1, \ldots, h_{\sigma'(n)}h'_n).$$

We want to embed G into the wreath product $S_n \int H$. Fix a set $T = \{t_1, \ldots, t_n\}$ of left coset representatives and an element $g \in G$. Then for $t_i \in T$

$$gt_i = t_j h_{g,i}$$

for a unique representative $t_j \in T$ and an element $h_{g,i} \in H$. Thus g gives rise to a permutation $\pi(g) \in S_n$ by setting $\pi(g)(i) = j$. Define $\phi : G \to S_n \int H$ by

$$\Phi(g) = (\pi(g), h_{g,1}, \ldots h_{g,n}).$$

It is easy to verify that Φ is a group monomorphism, called the monomial embedding. If we choose another set of left coset representatives, we obtain a conjugate embedding. Indeed, let $T' = \{t'_1, \ldots, t'_n\}$ denote another set of let coset representatives. The equations

$$t'_i = t_{\alpha(i)} h_i,$$

gives rise to a permutation $\alpha \in S_n$ and elements $h_i \in H$. Consider the element $u = (\alpha, h_1, \ldots, h_n) \in S_n \int H$. For $g \in G$ the following rather cumbersome calculations yields the desired result. First

$$\begin{aligned} u^{-1}\Phi(g)u &= \Big(\alpha^{-1}, h^{-1}_{\alpha^{-1}(1)}, \ldots, h^{-1}_{\alpha^{-1}(n)}\Big)\Big(\pi(g), h_{g,1}, \ldots h_{g,n}\Big)\Big(\alpha, h_1, \ldots, h_n\Big) \\ &= \Big(\alpha^{-1} \circ \pi(g) \circ \alpha, h^{-1}_{\alpha^{-1}\circ\pi(g)\circ\alpha(1)} h_{g,\alpha(1)} h_1, \ldots, h^{-1}_{\alpha^{-1}\circ\pi(g)\circ\alpha(n)} h_{g,\alpha(n)} h_n\Big) \end{aligned}$$

and since

$$gt'_i = gt_{\alpha(i)}h_i = t_{\pi(g)(\alpha(i))}h_{g,\alpha(i)}h_i = t'_{\alpha^{-1}\circ\pi(g)\circ\alpha(i)} h^{-1}_{\alpha^{-1}\circ\pi(g)\circ\alpha(i)} h_{g,\alpha(i)} h_i$$

we conclude that $u\Phi u^{-1} = \Phi'$. The inclusion $\Phi : G \to S_n \int H$ associated to a specific choice of coset representatives gives rise to a restriction map $H^*(S_n \int H, k) \to H^*(G, k)$. If we change the set of coset representatives we obtain an inclusion of the form $\Phi' = u \circ \Phi$, where $u : S_n \int H \to S_n \int H$ is conjugation by u. By Theorem 2.10, $u^* = id$ in cohomology, hence the restriction map is independent of the choice of coset representatives.

3.2 Evens' Norm Map

We may now define Evens' norm map $N_{H,G} \colon H^r(H, R) \to H^{rn}(G, R)$. There is some sign twist involved when r is odd, which we will ignore completely by assuming that r is even. Given a cohomology class $\alpha \in H^r(H, \mathbb{Z})$ we will first map it to a cohomology class in $H^{rn}(S_n \int H, R)$, which we may roughly describe as the product of α with itself n times. By restricting this cohomology class along the monomial embedding, we obtain a cohomology class in $H^{rn}(G, R)$.

Let $\nu : U \to R$ be a projective H-resolution. Then $\nu^{\otimes n} : U^{\otimes n} \to R^{\otimes n} \cong R$ is a projective resolution of R as an $H^{\times n}$-module. Let $\varepsilon : W \to R$ be a projective S_n-resolution. They fit together

$$\varepsilon \otimes \nu^{\otimes n} : W \otimes_R U^{\otimes n} \to R \otimes_R R^{\otimes n} \cong R$$

as a projective resolution of R as a $(S_n \int H)$-module, see [7, prop. 2.5.1]. Let $f : U_r \to R$ be a cocycle representing $\alpha \in H^r(H, R)$. Then the map

$$\varepsilon \otimes f^{\otimes n} : W \otimes_R U^{\otimes n} \to R \otimes_R R^{\otimes n} \cong R$$

is a cocycle and thus defines a cohomology class in $H^{rn}(S_n \int H, R)$. Let $1 \int \alpha$ denote this class. One needs to verify that the cohomology class $1 \int \alpha$ is independent of resolutions U and W and the map f representing α. The independence of f will follow from the following lemma. The reader may consult [7, section 5.3] for an argument concerning independence of resolutions.

Lemma 3.1. *Let $F, G : U \to L$ be chain homotopic maps of H-complexes. Then*

$$id \otimes F^{\otimes n},\ id \otimes G^{\otimes n} \colon W \otimes_R U^{\otimes n} \to W \otimes_R L^{\otimes n}$$

are chain homotopic maps of $S_n \int H$-complexes.

Proof. Let I denote the chain complex of R-modules with $I_0 = Ra \oplus Rb$, $I_1 = Rc$ and $I_n = 0$ for all other n. Define a differential by $\partial(c) = a - b$. Then $I \otimes_R U$ is a chain complex of H-modules. A chain homotopy from F to G is the same as a map of H-chain complexes $P : I \otimes_R U \to L$ such that $P(a \otimes u) = F(u)$ and $P(b \otimes u) = G(u)$. First, assume that we are given P as above and define a H-chain map $p : U \to L$ by $p(u) = P(c \otimes u)$. Then

$$\begin{aligned} F(u) - G(u) &= P(a \otimes u) - P(b \otimes u) \\ &= P(\partial^I(c) \otimes u) \\ &= P(\partial(c \otimes u) + c \otimes \partial^U(u)) \\ &= \partial^L(P(c \otimes u)) + P(c \otimes \partial^U(u)) \\ &= \partial^L(p(u)) - p(\partial^U(u)), \end{aligned}$$

hence p is a chain homotopy from F to G. Likewise, if $p : U \to L$ is a chain homotopy from F to G we may define a chain map $P : I \otimes_R U \to L$ with the desired properties in the following way. Since

$$(I \otimes_R U)_n = (Ra \otimes_R U_n) \oplus (Rb \otimes_R U_n) \oplus (Rc \otimes_R U_{n-1}),$$

we define P to be $F \oplus G \oplus p$. One may verify that the chain-homotopy relation is equivalent to saying that P commutes with the differentials.

By assumption, we have a map of H-chain complexes $P : I \otimes_R U \to L$ such that $P(a \otimes u) = F(u)$ and $P(b \otimes u) = G(u)$. The above argument is general, hence to prove that $id \otimes F^{\otimes n}$ and $id \otimes G^{\otimes n}$ are chain-homotopic, it suffices to construct an $S_n \int H$-chain map

$$Q \colon I \otimes_R W \otimes_R U^{\otimes n} \to W \otimes_R L^{\otimes n},$$

which on $a \otimes W \otimes U^{\otimes n}$ is $id \otimes F^{\otimes n}$ and on $b \otimes W \otimes U^{\otimes n}$ is $id \otimes G^{\otimes n}$. Assume that we had constructed an S_n-map $J \colon I \otimes_R W \to I^{\otimes n} \otimes_R W$ such that

$$J(a \otimes w) = a^{\otimes n} \otimes w \quad \text{and} \quad J(b \otimes w) = b^{\otimes n} \otimes w.$$

Then we could take Q to be the composition

$$\begin{aligned} I \otimes_k W \otimes_R U^{\otimes n} &\xrightarrow{J \otimes id} I^{\otimes n} \otimes_R W \otimes_R U^{\otimes n} \cong W \otimes_R I^{\otimes n} \otimes_R U^{\otimes n} \\ &\cong W \otimes_R (I \otimes_R U)^{\otimes n} \xrightarrow{id \otimes P^{\otimes n}} W \otimes_R L^{\otimes n}, \end{aligned}$$

where the two middle maps are change of order. The composition takes $a \otimes w \otimes (\otimes u_i)$ to $a^{\otimes n} \otimes w \otimes (\otimes u_i)$, then to $w \otimes (\otimes(a \otimes u_i))$ and finally to $w \otimes (\otimes F(u_i))$. Similar equalities hold for b. We are able to ignore signs since each twisting involves an element of even degree.

To construct J, we proceed as follows. $I_0 \otimes_R W$ is a subcomplex of $I \otimes_R W$, and J is already defined here by the given conditions. The idea is to show that we can extend J to all of $I \otimes_R W$ degree by degree. Let $A = I \otimes_R W$, hence $A = A' \oplus A''$ where $A' = I_0 \otimes_R W$ and $A'' = I_1 \otimes_R W$. Let $B = I^{\otimes n} \otimes_R W$. In degree 0, $A_0 = A'_0$ so no extension is needed. If J has been defined up to degree s, then we have the following commutative diagram

$$\begin{tikzcd}
A''_{s+1} \arrow[r, "\partial^A"] \arrow[d, dashed, "J''_{s+1}"] & A_s \arrow[r, "\partial^A"] \arrow[d, "J_s"] & A_{s-1} \arrow[d, "J_{s-1}"] \\
B_{s+1} \arrow[r, "\partial^B"'] & B_s \arrow[r, "\partial^B"'] & B_{s-1}.
\end{tikzcd}$$

The composition $A''_{s+1} \to A_s \to A_{s-1}$ is trivial, so the same is true for $\partial^B \circ J_s \circ \partial^A$, thus

$$J_s(\partial^A(A''_{s+1})) \subseteq \ker \partial^B = \partial^B(B_{s+1}).$$

Since A''_{s+1} is a projective S_n-module, we may define a S_n-map $J''_{s+1} : A''_{s+1} \to B_{s+1}$ making the diagram commute. Setting $J_{s+1} = J'_{s+1} \oplus J''_{s+1}$ extends the map J one degree further. □

We apply the lemma as follows. Assume that the cocycles $f, g : U_r \to R$ both represent the class α. Define a chain complex L by letting $L_n = R$ and $L_i = 0$ for all $i \neq n$. Then f and g may be viewed as chain homotopic maps of H-complexes $U \to L$. It follows from the lemma that $id \otimes f^{\otimes n}, id \otimes g^{\otimes n} : W \otimes_R U^{\otimes n} \to W \otimes_R L^{\otimes n}$ are chain homotopic maps of $S_n \int H$-complexes. Composing with $\varepsilon \otimes id$, we see that $\varepsilon \otimes f^{\otimes n}, \varepsilon \otimes g^{\otimes n} : W \otimes_R U^{\otimes n} \to L^{\otimes n}$ are chain homotopic maps of $S_n \int H$-complexes. Since $L^{\otimes n}$ only has one non-trivial component, namely R in degree rn, we may identify these maps with $\varepsilon \int f$ and $\varepsilon \int g$. To say that they are chain homotopic is simply saying that they are cohomologous since the differential in L is trivial.

Non-homogeneous elements If $\alpha \in H^*(H, R)$ is non-homogeneous but instead a sum of homogeneous elements of even degree, we can use essentially the same method to construct an inhomogeneous class $1 \int \alpha \in H^*(S_n \int H, R)$. Let $\alpha, \beta \in H^*(H, R)$ be homogeneous elements of even degrees and suppose f is a cocyle representing α and g is a cocycle representing

β. Define the cohomology class $1 \int (\alpha+\beta)$ to be the class represented by

$$\varepsilon \otimes (f+g)^{\otimes n}.$$

This is a sum of terms of the form

$$\varepsilon \otimes (h_1 \otimes \cdots \otimes h_n),$$

where each h_i is either f or g. The term with all $h_i = f$ represents the class $1 \int \alpha$, while term with all $h_i = g$ represents the class $1 \int \beta$.

Definition 3.2. Let G be a group, let H a subgroup a finite index n and let $\Phi : G \hookrightarrow S_n \int H$ be the monomial embedding. If $\alpha \in H^*(H,R)$ is an element of even degree, i.e., α is a sum of homogeneous elements of even degree, we define the norm map $N_{H,G} : H^*(H,R) \to H^*(G,R)$ by

$$N_{H,G}(\alpha) = \Phi^*(1 \int \alpha).$$

It is clear from the definition that $N_{G,G} = id$, and if $\alpha \in H^0(H,k)$ then $N_{H,G}(\alpha) = \alpha^n$.

Theorem 3.3. *Evens' norm map has the following properties*

1. *If H is a subgroup of K and K is a subgroup of G, then for $\alpha \in H^*(H,R)$ of even degree*

$$N_{K,G}(N_{H,K}(\alpha)) = N_{H,G}(\alpha).$$

2. *Let H be a subgroup of G. If $\alpha, \beta \in H^*(H,R)$ are of even degree, then*

$$N_{H,G}(\alpha\beta) = N_{H,G}(\alpha) N_{H,G}(\beta).$$

3. *If $G = \cup_{x \in D} KxH$ is a double coset decomposition of G, then for $\alpha \in H^*(H,R)$ of even degree*

$$res_{G,K}(N_{H,G}(\alpha)) = \prod_{x \in D} N_{K \cap xHx^{-1},K}(res_{xHx^{-1},K \cap xHx^{-1}}(x^*\alpha)).$$

The order of the elements in the product is irrelevant since everything is of even degree.

4. *If H is normal in G, then for $\alpha \in H^*(H,R)$ of even degree*

$$res_{G,H}(N_{H,G}(\alpha)) = \prod_{y \in G/H} y^*(\alpha).$$

The order of the elements in the product is irrelevant since everything is of even degree.

5. *Let H be a subgroup of G and let H' be a subgroup of G'. Let $\phi : G' \to G$ be a homomorphism such that $\phi(H') \subseteq H$, and ϕ induces a one-to-one correspondence $G'/H' \cong G/H$. Let ϕ' denote the restriction of ϕ to H'. Then for $\alpha \in H^*(H, R)$ of even degree*

$$N_{H',G'}(\phi'^*(\alpha)) = \phi^*(N_{H,G}(\alpha)).$$

The third property is often referred to as the double coset formula. A proof can be found in [7, section 6.2]. The properties 1. and 2. follow from investigating the norm on the level of resolutions. To obtain the second property one starts by proving the formula $1 \int (\alpha\beta) = (1 \int \alpha)(1 \int \beta)$ in $H^*(S_n \int H, k)$. Property 3. requires more work, while property 4. follows immediately afterwards when we note that for a normal subgroup H, a double coset decomposition is the same as a single coset decomposition. Property 5. follows from the fact that $1 \int \alpha$ is natural with respect to the group homomorphism $S_n \int H' \to S_n \int H$ arising from $\phi' : H' \to H$.

The norm map satisfies some additivity rules, which are useful when making calculations. A proof may be found in [7, section 6.2].

Theorem 3.4. *Let $H \leq G$ be a subgroup of finite index n, and let $\alpha, \beta \in H^*(H, R)$ be homogeneous of even degrees. Then*

$$N_{H,G}(1 + \alpha) = 1 + cor_{H,G}(\alpha) + \cdots + N_{H,G}(\alpha),$$

where the intermediate terms are elements of degrees between deg(α) and deg$(\alpha)n$. If H is normal in G of prime index p, then

$$N_{H,G}(\alpha + \beta) = N_{H,G}(\alpha) + cor_{H,G}(\nu) + N_{H,G}(\beta)$$

for some $\nu \in H^*(H, R)$.

3.3 The Norm Map on Elementary Abelian p-Groups

Let p be a fixed prime. Let $E = P \times P$, where P is a cyclic group of prime order p. Recall that the Künneth formula provides a ring monomorphism

$$S_{\mathbb{Z}}(\hat{P}, 2) \otimes_k S_{\mathbb{Z}}(\hat{P}, 2) \cong S_{\mathbb{Z}}(\hat{E}, 2) \hookrightarrow H^*(E, \mathbb{Z}),$$

where $\hat{P} = \mathrm{Hom}(P, \mathbb{Q}/\mathbb{Z})$ and $\hat{E} = \mathrm{Hom}(E, \mathbb{Q}/\mathbb{Z})$. Since the cohomology ring $H^*(P, \mathbb{Z})$ is trivial in odd degrees, the monomorphism is an isomorphism in even degree, since every Tor term will involve an odd degree term, thus

$$\bigoplus_{i+j=p} H^{2i}(P, \mathbb{Z}) \otimes H^{2j}(P, \mathbb{Z}) \cong H^{2p}(E, \mathbb{Z}).$$

The element $a \otimes b$ on the left hand side corresponds to the element $a \times b$ on the right hand side. Since $H^*(P, \mathbb{Z}) = \mathbb{Z}[\chi \mid p\chi = 0]$ it follows that an element in $H^{2p}(E, \mathbb{Z})$ can be written uniquely on the form

$$\sum_{i+j=p} a_{i,j} \chi^i \times \chi^j,$$

with $a_{ij} \in \mathbb{F}_p$.

Theorem 3.5. *Let F denote the subgroup $\{1\} \times P \subset P \times P = E$. Then*

$$N_{F,E}(\chi) = 1 \times \chi^p - \chi^{p-1} \times \chi.$$

Proof. Let $\varepsilon = \chi \times 1$ and let $\mu = 1 \times \chi$. Since E is elementary abelian, we may view $H^2(E, \mathbb{Z}) = \operatorname{Hom}(E, \mathbb{Q}/\mathbb{Z})$ as an $\mathbb{F}_p$-vector space with basis $\{\varepsilon, \mu\}$. We think of ε and μ as homomorphisms $E \to \mathbb{Q}/\mathbb{Z}$, hence $\ker \varepsilon = F$. We wish to determine the homogeneous polynomial of degree p

$$N_{F,E}(\chi) = \sum_{j=0}^{p} a_j \mu^j \varepsilon^{p-j}.$$

Let $F_i = \ker(\mu - i\varepsilon)$ for $i = 1, \ldots, p-1$. These are subgroups of degree p and $F_i \cap F = \{1\}$ for all i. Since $E = F_i F$, it follows by the double coset formula, Theorem 3.3 part 3, that

$$\operatorname{res}_{E,F_i} N_{F,E}(\chi) = N_{\{1\},F_i} \operatorname{res}_{F,\{1\}}(\chi) = 1.$$

Recall that $H^*(F_i, \mathbb{Z}) = S_{\mathbb{Z}}(\hat{F_i})$. Since $N_{F,E}(\chi)$ is in the subring $S_{\mathbb{Z}}(\hat{E})$, we are interested in determining the kernel of the restriction map on this subring, $S_{\mathbb{Z}}(\hat{E}) \to S_{\mathbb{Z}}(\hat{F_i})$. Here, the restriction map is induced by the map of dual spaces $\hat{E} \to \hat{F_i}$ induced by the inclusion $F_i \hookrightarrow E$, hence

$$S_{\mathbb{Z}}(\hat{E}) \cap \ker(\operatorname{res}_{E,F_i}) = (\mu - i\epsilon),$$

where $(\mu - i\epsilon)$ denotes the principal ideal generated by $\mu - i\epsilon$. Thus $N_{F,E}(\chi)$ is divisible by $\mu - i\varepsilon$ for all i and therefore also by their product, which is

$$\prod_{i=0}^{p-1} (\mu - i\varepsilon) = \mu^p - \varepsilon^{p-1}\mu.$$

Hence $N_{F,E}(\chi)$ is on the form $c(\mu^p - \varepsilon^{p-1}\mu)$ for some $c \in \mathbb{F}_p$. By Theorem 3.3 part 4, $\operatorname{res}_{E,F} N_{F,E}(\chi) = \chi^p$ since the conjugation action is trivial because E is abelian. The restriction map $\operatorname{res}_{E,F}$ on the subring $S_{\mathbb{Z}}(\hat{E})$ is induced by the map of dual spaces $\hat{E} \to \hat{F}$ given by $\varepsilon \mapsto 0$ and $\nu \mapsto \chi$. Thus $c = 1$, and we have the desired result.

□

Corollary 3.6. *Let E be an elementary abelian p-group and let F be a subgroup. Then for each $\chi \in H^2(F, \mathbb{Z})$, we have*

$$N_{F,E}(\chi) = \prod_{res_{E,F}(\nu)=\chi} \nu.$$

Proof. We start by reducing to the case $[E : F] = p$. Suppose $E \geq E' \geq F$, and that the corollary has been established for the pairs E, E' and E', F. Then by Theorem 3.3 part 1 and part 3,

$$\begin{aligned} N_{F,E}(\chi) &= N_{E',E}(N_{F,E'}(\chi)) \\ &= N_{E',E}\Big(\prod_{\mathrm{res}_{E',F}(\nu')=\chi} \nu' \Big) \\ &= \prod_{\mathrm{res}_{E',F}(\nu')=\chi} N_{E',E}(\nu') \\ &= \prod_{\mathrm{res}_{E',F}(\nu')=\chi} \ \prod_{\mathrm{res}_{E,E'}(\nu)=\nu'} \nu \\ &= \prod_{\mathrm{res}_{E,F}(\nu)=\chi} \nu. \end{aligned}$$

Thus we may assume that F has index p. If $\chi = 0$, the corollary clearly holds, so we may assume that χ is non-trivial. As before, we identify χ with a non-trivial homomorphism $\chi : F \to \mathbb{Q}/\mathbb{Z}$, and, since F is an elementary abelian p-group, χ has image $\langle 1/p \rangle \mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}_p$. Let F_1 denote the kernel of χ. Since χ factors through F/F_1, we have $\chi = \inf_{F/F_1,F}(\chi_1)$ for some $\chi_1 \in H^2(F/F_1, \mathbb{Z})$. Since $[E : F] = [E/F_1 : F/F_1] = p$, it follows from Theorem 3.3 part 5 that

$$N_{F,E}(\chi) = N_{F,E}(\inf_{F/F_1,F}(\chi_1)) = \inf_{E/F_1,E}(N_{F/F_1,E/F_1}(\chi_1)).$$

If the theorem holds for the pair $E/F_1, F/F_1$, then

$$N_{F,E}(\chi) = \prod_{\mathrm{res}_{E/F_1,F/F_1}(\nu_1)=\chi_1} \inf_{E/F_1,E}(\nu_1).$$

There are p elements in $H^2(E/F_1, \mathbb{Z})$ such that $\mathrm{res}_{E/F_1,F/F_1}(\nu_1) = \chi_1$. Also, there are p elements in $H^2(E, \mathbb{Z})$ such that $\mathrm{res}_{E,F}(\nu) = \chi$, and these are the inflations of p elements in $H^2(E/F_1, \mathbb{Z})$, clearly restricting to χ_1 on F/F_1. Hence the p elements appearing in the product above equal the p elements going into the product in the statement, thus proving the corollary.

It only remains to prove the corollary for the pair $E/F_1, F/F_1$. Since $|E/F_1| = p^2$ and $|F/F_1| = p$, it thus suffices to verify the corollary in the case where $|E| = p^2$ and $|F| = p$. This is exactly the case considered in Theorem 3.5. Using the same notation, we saw that

$$N_{F,E}(\chi) = \prod_{i=0}^{p-1} (\mu - i\varepsilon).$$

The elements $\mu - i\varepsilon$ are exactly the p elements of $H^2(E, \mathbb{Z})$ restricting to χ on $H^2(F, \mathbb{Z})$, thus finishing the proof. □

3.4 Serre's Theorem

Let p be a fixed prime. A finite p-group is a group of order p^a for some $a \geq 0$. Serre's theorem states that if G is a finite p-group, which is not elementary abelian, then there exist non-zero elements $x_1, \ldots, x_r \in H^1(G, \mathbb{F}_p)$ for some $r \geq 1$, such that the product of the Bocksteins is zero;

$$\beta(x_1)\beta(x_2) \cdots \beta(x_r) = 0 \in H^{2r}(G, \mathbb{F}_p).$$

If G is elementary abelian, then the Bocksteins of the degree one generators form a polynomial subring of $H^*(G, \mathbb{F}_p)$ and therefore no such relation exists. Serre's original proof [17] uses Steenrod operations. We shall instead follow a proof by Evens as given in [7], which relies partly on work by Okuyama and Sasake and uses Evens' norm map. The idea behind the proof is to reduce to the case where $|G| = p^3$ and exploit that the cohomology rings of such groups are fairly well-known.

Let G be a finite p-group. We say that a proper subgroup $H \leq G$ is maximal, if it is not contained in any proper subgroup of G different from H. The following are equivalent for a subgroup $H \leq G$.

1. H is maximal and normal.

2. H is maximal.

3. $[G : H] = p$.

See Corollary B.4. An element of order p in $H^2(G, \mathbb{Z})$ is a homomorphism $\beta : G \to \mathbb{Q}/\mathbb{Z}$ with image $\langle 1/p \rangle \mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}_p$, hence $[G : \ker\beta] = p$ so the kernel is a maximal subgroup of G. Likewise, any maximal subgroup of G occurs as the kernel of an element of order p in $H^2(G, \mathbb{Z})$. Moreover, if $\beta, \beta' \in H^2(G, \mathbb{Z})$ of order p have the same kernel, then they must differ by multiplication by an integer r with $(r, p) = 1$. We abuse notation slightly and write β_H for any β with kernel H. We will need the following result concerning finite p-groups.

Lemma 3.7. *Let N be a non-trivial normal subgroup of a finite p-group G. Then $[G, N]N^p$ is a normal subgroup of G, and $N/([G, N]N^p)$ is non-trivial.*

A proof can be found in [10, Chapter III, Theorem 2.6]. Let G_2 denote the Frattini subgroup of G, i.e. the intersection of all maximal subgroups of G. Since all maximal subgroups are normal, G_2 is normal. If M is a maximal subgroup, then G/M has order p, hence $[G,G]G^p \leq M$ so $[G,G]G^p \leq G_2$, thus the Frattini quotient G/G_2 is elementary abelian. Let H be a normal subgroup of G such that the quotient group G/H is elementary abelian, hence G/H is generated by n cosets x_iH each of degree p

$$G/H = \langle x_1 H \rangle \times \cdots \times \langle x_n H \rangle .$$

Then $\overline{H}_i = \langle x_j H \mid j \neq i \rangle$ are n maximal subgroups of G/H with $\cap_i \overline{H_i} = \{1\}$, and their pre-images in G are n maximal subgroups H_i with $\cap_i H_i = H$. Since the Frattini subgroup is the intersection of all maximal subgroups, $G_2 \leq H$, thus the Frattini subgroup is the smallest normal subgroup such that the factor group is elementary abelian. Since $[G,G]G^p \leq G_2$ and $G/([G,G]G^p)$ is elementary abelian, we thus have $G_2 = [G,G]G^p$.

Let $r : G \to G/G_2$ be the quotient map. The inflation map in cohomological dimension 2 is pre-composition with r

$$\inf_{G/G_2,G} : \mathrm{Hom}(G/G_2, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}),$$

which is clearly injective. Any $\alpha : G/G_2 \to \mathbb{Q}/\mathbb{Z}$ satisfies $p\alpha = 0$ since G/G_2 is elementary abelian. Likewise, any $\beta : G \to \mathbb{Q}/\mathbb{Z}$ of order p has kernel a maximal subgroup of G, hence it factors trough G/G_2, so the inflation map surjects onto the subgroup of all β with $p\beta = 0$.

Theorem 3.8. *Let G be a finite p-group, which is not elementary abelian. Then there exist maximal subgroups $H_1, \cdots, H_k$ such that*

$$\beta_{H_1}\beta_{H_2}\cdots\beta_{H_k} = 0$$

in $H^*(G,\mathbb{Z})$.

Proof. Since G is not elementary abelian, $G_2 \neq \{1\}$. We start by reducing to the case where G_2 is cyclic of order p. Let $G_3 = [G, G_2]G_2^p$. By Lemma 3.7, G_2/G_3 is a non-trivial p-group, so we can find a subgroup $M/G_3 \leq G_2/G_3$ of index p. The pre-image M is a subgroup in G such that $[G_2 : M] = p$. Since G_2/G_3 is central in G/G_3 by construction, M is a normal subgroup of G. The inflation map

$$\inf_{G/M,G} : H^2(G/M,\mathbb{Z}) = \mathrm{Hom}(G/M,\mathbb{Q}/\mathbb{Z}) \to H^2(G,\mathbb{Z}) = \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$$

is a monomorphism, so if there is non-trivial elements $\overline{\beta}_i \in H^2(G/M,\mathbb{Z})$ of order p with product 0, their inflations $\beta_i \in H^2(G,\mathbb{Z})$ are non-trivial elements of order p with product 0. G/M is not elementary abelian and since

$(G/M)/(G_2/M) \cong G/G_2$ is elementary abelian, the Frattini subgroup of G/M must be contained in G_2/M. Since G_2/M is cyclic of order p, we must have $(G/M)_2 = G_2/M$. Thus it suffices to verify the theorem for groups with Frattini subgroups cyclic of order p.

Suppose that G contains a subgroup K, such that K is not elementary abelian, $K_2 = G_2$, and the theorem is true for K. Then the theorem holds for G. Indeed, choose non-trivial elements $\beta_1, \dots, \beta_r$ of order p in $H^2(K, \mathbb{Z})$ with product 0. Since $K_2 = G_2$ and the inflation map surjects onto the elements of order p, we have $\beta_i = \inf_{K/G_2 \to K}(\overline{\beta}_i)$ for non-trivial elements $\overline{\beta}_i \in (K/G_2, \mathbb{Z})$. Since $[G : K] = [G/G_2 : K/G_2]$, it follows from Theorem 3.3 part 5 that

$$\begin{aligned} 0 &= N_{K,G}\Big(\prod \beta_i\Big) \\ &= N_{K,G}\Big(\prod \inf_{K/G_2,K}(\overline{\beta}_i)\Big) \\ &= N_{K,G}\Big(\inf_{K/G_2,K}\Big(\prod \overline{\beta}_i\Big)\Big) \\ &= \inf_{G/G_2,G}\Big(N_{K/G_2,G/G_2}\Big(\prod \overline{\beta}_i\Big)\Big) \\ &= \inf_{G/G_2,G}\Big(\prod N_{K/G_2,G/G_2}(\overline{\beta}_i)\Big). \end{aligned}$$

By Corollary 3.6, each $N_{K/G_2,G/G_2}(\overline{\beta}_i)$ is a product of non-trivial elements of $H^2(G/G_2, \mathbb{Z})$, necessarily of order p. Inflating to G we obtain the desired result.

It thus remains to prove the existence of the subgroup K. First assume that G contains a cyclic subgroup K of order p^2. Since K_2 is a non-trivial subgroup of G_2, and G_2 is cyclic of order p, $K_2 = G_2$. The group $H^2(K, \mathbb{Z}) = \operatorname{Hom}(K, \mathbb{Q}/\mathbb{Z})$ is generated by an element ξ of order p^2, so $\beta = p\xi$ is of order p and satisfies $\beta^2 = p^2\xi^2 = 0$ as desired. If G does not contain a cyclic subgroup of order p^2, then every non-trivial element of G has order p. Since G is not elementary abelian, G cannot be abelian. Let x and y be non-commuting elements of G, and let K denote the non-abelian subgroup they generate. As above, we must have $K_2 = G_2 = [K, K]$, hence

$$|K/G_2| \leq p^2 \quad \text{and} \quad |K| \leq p^3.$$

These inequalities are actually strict. The center of a non-trivial p-group is non-trivial, hence $K/Z(K)$ must be either of order $1, p$ or p^2. In all cases $K/Z(K)$ is abelian, hence $G_2 = [K, K] \leq Z(K)$. The elements $1, x, \dots, x^{p-1}$ represent different cosets in K/G_2, for otherwise $x \in Z(K)$, which is not the case. But y represents yet another coset, otherwise $yx^i \in Z(K)$ for some $1 \leq i \leq p-1$. But then $y^2x^i = yx^iy$, hence $yx^i = x^iy$. Since x has order p, this forces x and y to commute, which is not the case. Thus K/G_2 has at least $p+1$ elements, thus $|K/G_2| = p^2$ and $|K| = p^3$. Proving the theorem for the subgroup K finishes the proof.

We have reduced to the case $|K| = p^3$, $|K_2| = p$ and every non-trivial element of K has order p. Let H be a maximal subgroup of K, hence H is elementary abelian of rank 2. Again, we view $H^2(H, \mathbb{Z}) = \text{Hom}(H, \mathbb{Q}/\mathbb{Z})$ as an $\mathbb{F}_p$-vector space with basis $\{\mu, \varepsilon\}$, where μ and ε are homomorphisms $H \to \mathbb{Q}/\mathbb{Z}$. Let xH denote a generator of the cyclic p-group K/H, hence

$$K = H \cup xH \cup \cdots \cup x^{p-1}H.$$

Conjugation by x gives rise to a non-trivial automorphism $x : H \to H$, otherwise K would be abelian. The element x acts on $H^*(H, \mathbb{Z})$ via the map induced by conjugation $x^* : H^*(H, \mathbb{Z}) \to H^*(H, \mathbb{Z})$. The action in cohomological dimension 2 is pre-composition with x, $\text{Hom}(H, \mathbb{Q}/\mathbb{Z}) \to \text{Hom}(H, \mathbb{Q}/\mathbb{Z})$, hence x acts non-trivially. It follows from linear algebra that, up to change of basis, there is only one way an element of order p can act non-trivially on a rank 2 $\mathbb{F}_p$-vector space, hence

$$\begin{aligned} x^*(\mu) &= \mu, \\ x^*(\varepsilon) &= \mu + \varepsilon. \end{aligned}$$

Let yK_2 denote a generator of the cyclic p-group H/K_2. As noted earlier $K_2 \leq Z(K)$. Since

$$H = K_2 \cup yK_2 \cup \cdots \cup y^{p-1}K_2$$

and conjugation by x is non-trivial on H, $[x, y]$ is a non-trivial element in K_2, thus it generates K_2. We see that

$$\mu([x, y]) = \mu(x^{-1}yxy^{-1}) = \mu(x^{-1}yx) - \mu(y) = x^*(\mu(y)) - \mu(y) = 0$$

so $\mu(K_2) = 0$. Hence $\mu = \inf_{H/K_2,H}(\overline{\mu})$, where $\overline{\mu} \in H^2(H/K_2, \mathbb{Z})$. Since $[K : H] = [K/K_2 : H/K_2]$, it follows from Theorem 3.3 part 5 that

$$N_{H,K}(\mu) = N_{H,K}(\inf_{H/K_2,H}(\overline{\mu})) = \inf_{K/K_2,K}(N_{H/K_2,K/K_2}(\overline{\mu})),$$

and by Corollary 3.6, $N_{H/K_2,K/K_2}(\overline{\mu})$ is a product of non-trivial elements of $H^2(K/K_2, \mathbb{Z})$. Thus $N_{H,K}(\mu)$ is a product of non-trivial elements of order p in $H^2(K, \mathbb{Z})$. Choose $\alpha \in H^2(K, \mathbb{Z})$ with kernel H. If we can show that $\alpha N_{H,K}(\mu) = 0$, then the theorem holds for K. Since x acts trivially on $H^*(K, \mathbb{Z})$, it follows from Theorem 3.3 part 5 and the additivity formula 3.4 that

$$\begin{aligned} N_{H,K}(\varepsilon) &= x^*(N_{H,K}(\varepsilon)) = N_{H,K}(x^*(\varepsilon)) = N_{H,K}(\mu + \varepsilon) \\ &= N_{H,K}(\mu) + \text{cor}_{H,K}(\nu) + N_{H,K}(\varepsilon) \end{aligned}$$

for some $\nu \in H^*(H, \mathbb{Z})$. Hence $N_{H,K}(\mu) = -\mathrm{cor}_{H,K}(\nu)$. By Theorem 2.9

$$\alpha N_{H,K}(\mu) = -\alpha \mathrm{cor}_{H,K}(\nu) = -\mathrm{cor}_{H,K}(\mathrm{res}_{K,H}(\alpha)\nu) = 0$$

since $\mathrm{res}_{K,H}(\alpha) = 0$, which finishes the proof of Serre's theorem. □

Corollary 3.9. *Let G be a finite p-group which is not elementary abelian. Then there exist non-trivial elements $\alpha_1, \dots, \alpha_r \in H^1(G, \mathbb{F}_p)$ such that*

$$\beta(\alpha_1) \cdots \beta(\alpha_r) = 0.$$

Proof. We have the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z} \arrow[r, "\cdot p"] \arrow[d, "="] & \mathbb{Z} \arrow[r] \arrow[d, "\cdot \frac{1}{p}"] & \mathbb{Z}_p \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & \mathbb{Z} \arrow[r, hook] & \mathbb{Q} \arrow[r] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0,
\end{tikzcd}$$

where we identify $\mathbb{Z}_p \cong \langle 1/p \rangle \mathbb{Z}/\mathbb{Z}$. By naturality of the long exact sequence in cohomology, the diagram gives rise to a commutative square

$$\begin{tikzcd}
\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\cong"] & H^2(G, \mathbb{Z}) \\
\mathrm{Hom}(G, \mathbb{F}_p) \arrow[r, "\hat{\beta}"] \arrow[u, "\circ i"] & H^2(G, \mathbb{Z}) \arrow[u, "="]
\end{tikzcd}$$

where i denotes the inclusion $\mathbb{F}_p \cong \langle 1/p \rangle \mathbb{Z}/\mathbb{Z} \hookrightarrow \mathbb{Q}/\mathbb{Z}$. By the above theorem there exist non-trivial elements of degree p, $\gamma_1, \dots, \gamma_r \in H^2(G, \mathbb{Z})$ such that $\gamma_1 \cdots \gamma_r = 0$. Since $\gamma_1, \dots, \gamma_r$ have images contained in $\langle 1/p \rangle \mathbb{Z}/\mathbb{Z}$, there exist $\alpha_1, \dots, \alpha_r \in H^1(G, \mathbb{F}_p)$ such that $\hat{\beta}(\alpha_i) = \gamma_i$. Let $r : \mathbb{Z} \to \mathbb{Z}_p$ denote the reduction module p. Since $\beta = r^* \circ \hat{\beta}$, and r^* is a ring homomorphism, it follows that $\beta(\alpha_1) \cdots \beta(\alpha_r) = 0$.

□

4 The Quillen-Venkov Lemma

Let G be a finite group and let p be a fixed prime. Consider the product of the restriction maps

$$\Pi \mathrm{res}_{G,E} : H^*(G, \mathbb{F}_p) \to \prod_{E \leq G} H^*(E, \mathbb{F}_p),$$

where E ranges over the elementary abelian p-subgroups of G. The main theorem of this section is Theorem 4.5 which states that the kernel of this map is nilpotent. We give an algebraic proof by Quillen and Venkov [15], which uses the Lyndon-Hochschild-Serre spectral sequence and Serre's theorem. The approach distinguishes from Quillen's original proof, which involved G-spaces and equivariant cohomology. As a consequence of this theorem we see the Krull dimension of $H^*(G, \mathbb{F}_p)$ is the maximal rank of the elementary abelian p-subgroups of G.

4.1 The Lyndon-Hochschild-Serre Spectral Sequence

A spectral sequence is a strong algebraic tool allowing us to express relations between certain cohomology groups. The Lyndon-Hochschild-Serre spectral sequence relates the cohomology of a group to that of a normal subgroup and that of the factor group. We will not go into details with the proof but merely sketch the idea behind the construction. We assume that the reader is familiar with the notion of a spectral sequence and how a spectral sequence is associated with a filtered complex.

Definition 4.1. A double complex E is a collection of abelian groups and maps arranged as in the following diagram

$$\begin{tikzcd}
\vdots & \vdots & \vdots & \\
E_0^{0,2} \arrow[u] \arrow[r, "d_1"] & E_0^{2,2} \arrow[u] \arrow[r, "d_1"] & E_0^{2,2} \arrow[u] \arrow[r] & \cdots \\
E_0^{0,1} \arrow[u, "d_0"'] \arrow[r, "d_1"] & E_0^{1,1} \arrow[u, "d_0"'] \arrow[r, "d_1"] & E_0^{2,1} \arrow[u, "d_0"'] \arrow[r] & \cdots \\
E_0^{0,0} \arrow[u, "d_0"'] \arrow[r, "d_1"] & E_0^{1,0} \arrow[u, "d_0"'] \arrow[r, "d_1"] & E_0^{2,0} \arrow[u, "d_0"'] \arrow[r] & \cdots
\end{tikzcd}$$

such that

1. each row satisfies $d_1 \circ d_1 = 0$,

2. each column satisfies $d_0 \circ d_0 = 0$,

3. each square satisfies $d_0 \circ d_1 + d_1 \circ d_0 = 0$.

The total complex $\mathrm{Tot}(E)$ of the double complex is given by

$$\mathrm{Tot}(E)^n = \bigoplus_{i+j=n} E_0^{ij}$$

with differential $d_0 + d_1 : \mathrm{Tot}(E)^n \to \mathrm{Tot}(E)^{n+1}$.

The total complex is filtered as follows:

$$F_I^p \mathrm{Tot}(E)^n = \oplus_{r \geq p} E^{r,n-r}, \quad F_{II}^p \mathrm{Tot}(E)^n = \oplus_{r \geq p} E^{n-r,r}$$

F_I^* may be thought of as a "column-wise" filtration, while F_{II}^* may be thought of as a "row-wise" filtration. Since $E^{p,q} = 0$ when $p < 0$ or $q < 0$, the filtrations are bounded. The two filtrations then give rise to two spectral sequences, both converging to $H^*(\mathrm{Tot}(E))$. It is often a useful strategy to compare the two spectral sequences, especially if one has a simple E_2 with a lot of trivial terms and the other does not. This is exactly what happens in the proof of the Lyndon-Hochchilds-Serre spectral sequence. The above construction and definitions are natural with respect to almost any property involving a double complex. In particular, E could be a double graded algebra such that d_0 and d_1 are both derivations with respect to the total degree. Then the multiplicative structure is inherited at each stage of the spectral sequence, the d_r are derivations, and all the relevant morphisms are consistent with the multiplicative structures.

Theorem 4.2 (The LHS Spectral Sequence)**.** *Let G be a group, N a normal subgroup and M an RG-module. There exists a spectral sequence with E_2-term $H^*(G/N, H^*(N, M))$, which converges to $H^*(G, M)$. Explicitly we have a spectral sequence $\{E_r^{p,q}, d_r\}$ with*

1. $d_r : E_r^{p,q} \to E^{p+r,q-r+1}$ and $E_{r+1}^{p,q} = kerd_r/Imd_r$ at $E_r^{p,q}$,

2. $E_2^{p,q} \cong H^p(G/N, H^q(N, M))$,

3. stable terms $E_\infty^{p,n-p}$ isomorphic to the successive quotients F_p^n/F_{p+1}^n in a filtration $0 \subset F_n^n \subset \cdots \subset F_0^n = H^n(G, M)$ of $H^n(G, M)$.

Rough sketch of proof. The spectral sequence will arise from a double complex that we construct as follows. Let $X \xrightarrow{\partial} R$ be a projective RG-resolution and let $Y \xrightarrow{\partial'} R$ be a projective $R(G/N)$-resolution. Then $X \to R$ is also an projective RN-resolution. Recall that G acts on $\mathrm{Hom}_{RN}(X, M)$ by setting $(gf)(x) = g(f(g^{-1}x))$. Since N acts trivially, we obtain a R-linear action of G/N on $\mathrm{Hom}_{RN}(X,M)$, making $\mathrm{Hom}_{RN}(X,M)$ into a complex of $R(G/N)$-modules. Form the double complex

$$E_0^{pq} = \mathrm{Hom}_{R(G/H)}(Y_p, \mathrm{Hom}_{RN}(X_q, M))$$

with

$$\begin{aligned} d_0 &= \mathrm{Hom}(\partial'_p, \mathrm{Hom}(id, id)), \\ d_1 &= (-1)^p \mathrm{Hom}(id, \mathrm{Hom}(\partial_q, id)). \end{aligned}$$

The double complex gives rise to two spectral sequences. One may verify that the first spectral sequence has E_2 page $H^*(G/H, H^*(H,M))$. It turns out that the second spectral sequence has a very simple form, most of the E_2 page is trivial, which makes it possible to identify the cohomology of the total complex with $H^*(G,M)$. See [7, Section 7.2]. □

As indicated the spectral sequence behaves well with respect to the cup-product structure. A proof can be found in [7, Section 7.3].

Theorem 4.3. *Let $M = R$. Then the spectral sequence can be endowed with a bilinear product $E_r^{p,q} \times E_r^{s,t} \to E_r^{p+s,q+t}$ such that*

1. *each d_r is a derivation and the product on the E_{r+1} page is induced by the product on the E_r page,*
2. *the multiplicative structure on the E_2 page agrees up to sign with the cup-product in $H^*(G/N, H^*(N,R))$,*
3. *the cup-product in $H^*(G,R)$ restrict to maps $F_p^m \times F_s^n \to F_{p+s}^{m+n}$. These induce quotient maps $E_\infty^{p,m-p} \times E_\infty^{s,n-s} \to E_\infty^{p+s,m+n-p-s}$ which agree with the product on the E_∞ page.*

We have a map

$$H^n(G/N, M^N) \cong E_2^{n,0} \to E_3^{n,0} \to \cdots \to E_\infty^{n,0} \cong F_n^n \subseteq H^n(G,M)$$

since $E_i^{n,0} \cong E_{i-1}^{n,0}/\mathrm{Im}(d_{i-1})$. Likewise, we have a map

$$H^n(G,M) \to H^n(G,M)/F_1^n \cong E_\infty^{0,n} \hookrightarrow E_2^{0,2} \cong H^n(N,M)^{G/N} \subseteq H^n(N,M)$$

since we have inclusions $E_i^{0,n} = \ker(d_{i-1}) \subseteq E_{i-1}^{0,n}$. These maps are called edge homomorphisms and the following theorem provides an identification of theme. For a proof, see [7, Prop. 7.2.2].

Theorem 4.4. *Let G be a group, let N be a normal subgroup and let M be a G-module. The horizontal edge homomorphism*

$$H^*(G/N, M^N) \cong E_2^{*,0} \to E_\infty^{*,0} \subseteq H^*(G,M)$$

is $\mathit{inf}_{G/N,G}$. The vertical edge homomorphism

$$H^*(G,M) \to E_2^{0,*} \cong H^*(N,M)^{G/H} \subseteq H^*(N,M)$$

is $\mathit{res}_{G,N}$.

4.2 The Quillen-Venkov Lemma

Let G be a finite group and let p be a fixed prime.

Theorem 4.5 (The Quillen-Venkov Lemma)**.** *Suppose $\alpha \in H^*(G, \mathbb{F}_p)$ and α restricts to zero on every elementary abelian p-subgroup of G. Then α is nilpotent.*

Let v be a non-zero element in $H^1(G, \mathbb{F}_p) = \operatorname{Hom}(G, \mathbb{F}_p)$, hence $v : G \to \mathbb{F}_p$ is surjective. Let G' denote the kernel of v, thus $G/G' \cong P$, where P is a cyclic group of order p. Before we can prove the Quillen-Venkov Lemma we need the following result.

Lemma 4.6. *If $u \in H^*(G, \mathbb{F}_p)$ restricts to zero on G', then $u^2 \in H^*(G, \mathbb{F}_p) \cdot \beta(v)$, where β is the Bockstein homomorphism.*

Proof of lemma. By Theorem 4.2, there exists a spectral sequence converging to $H^*(G, \mathbb{F}_p)$ with

$$E_2^{p,q} = H^p(P, H^q(G', \mathbb{F}_p)).$$

As usual let $\nu \in H^1(P, \mathbb{F}_p) = \operatorname{Hom}(P, \mathbb{F}_p)$ denote the generator characterized by $\nu(x) = 1$, where $P = \langle x \rangle$ and let $\varepsilon = \beta(\nu) \in H^2(P, \mathbb{F}_p)$. Since the long exact sequence in cohomology is natural, the following diagram commutes

$$\begin{tikzcd}
\operatorname{Hom}(P, \mathbb{F}_p) \arrow[r, "\circ v"] \arrow[d, "\beta"] & \operatorname{Hom}(G, \mathbb{F}_p) \arrow[d, "\beta"] \\
H^2(P, \mathbb{F}_p) \arrow[r, "v^*"] & H^2(G, \mathbb{F}_p),
\end{tikzcd}$$

hence $v^*(\varepsilon) = \beta(v)$. Since $\varepsilon \in H^2(P, \mathbb{F}_p) = E_2^{2,0}$ and $d_r^{2,0} = 0$ for all r, the element ε represents a residue class in $E_r^{2,0}$ which we will denote ε_r. The multiplicative structure on the spectral sequence induces a map on each page

$$E_r^{p,q} \xrightarrow{\cdot \varepsilon_r} E_r^{p+2,q}.$$

Since $d_r(x\varepsilon_r) = xd_r(\varepsilon_r) + (-1)^2 d_r(x)\varepsilon_r = d_r(x)\varepsilon_r$ for $x \in E_r^{p,q}$, the map commutes with the differentials. We claim that the map is surjective for $p \geq 0$ and injective for $p \geq r - 1$ and in order to prove this we proceed by induction on r. It is true for $r = 2$, since it is the map

$$H^p(P, H^q(G', \mathbb{F}_p)) \xrightarrow{\cdot \varepsilon} H^{p+2}(P, H^q(G', \mathbb{F}_p)),$$

which we investigated in Example 2.5. Now assume that the statement holds on the $r - 1$'th page. Given an element $\overline{x} \in E_r^{p+2,q}$, choose an inverse image $x \in E_{r-1}^{p+2,q}$ such that $d_{r-1}(x) = 0$. By the inductive hypothesis $x = y\varepsilon_{r-1}$ for some $y \in E_{r-1}^{p,q}$. Then $d_{r-1}(y)\varepsilon_{r-1} = d_{r-1}(y\varepsilon_{r-1}) = 0$ and since $d_{r-1}(y) \in$

$E_{r-1}^{p+r-1,q-r+2}$ it follows from the inductive hypothesis about injectivity that $d_{r-1}(y) = 0$. Thus $\overline{y} \in E_r^{p,q}$ is an element with $\overline{y}\varepsilon_r = \overline{x}$, so multiplication by ε_r is indeed surjective. Next, let $\overline{x} \in E_r^{p,q}$ with $p \geq r-1$ such that $\overline{x}\varepsilon_r = 0$. Choose an inverse image $x \in E_{r-1}^{p+2,q}$ such that $d_{r-1}(x) = 0$. Then $x\varepsilon_{r-1} = d_{r-1}(y)$ for some $y \in E_{r-1}^{p-r+3,q+r}$. Since $p-r+3 \geq 2$, we may write $y = z\varepsilon_{r-1}$ for some $z \in E_{r-1}^{p-r+1,q+r}$ by the inductive hypothesis. Then

$$(x - d_{r-1}(z))\varepsilon_{r-1} = d_{r-1}(y) - d_{r-1}(z\varepsilon_{r-1}) = 0$$

and by injectivity $x = d_{r-1}(z)$, hence $\overline{x} = 0$ as desired.

By decreasing induction on s we see that $F_s^n \cdot \beta(v) = F_{s+2}^{n+2}$. Indeed, by Theorem 4.3 multiplication by ε_∞ on the E_∞ page is induced by multiplication by $v^*(\varepsilon) = \beta(v)$ on the filtration coefficients, hence

$$F_{n+2}^{n+2} = E_\infty^{n+2,0} = E_\infty^{n,0} \cdot \varepsilon_\infty = F_n^n \cdot \beta(v).$$

Next, assume that the statement holds for $s+1$. Since

$$F_{s+2}^{n+2}/F_{s+3}^{n+2} = E_\infty^{s+2,n-s} = E_\infty^{s,n-s} \cdot \varepsilon_\infty = F_s^n/F_{s+1}^{n+1} \cdot \varepsilon_\infty$$

the equality follows. Finally, if $u \in H^*(G, \mathbb{F}_p)$ restricts to zero on G' then, by Theorem 4.4, $u \in F_1^i$ for some $i \geq 0$. Hence $u^2 \in F_2^i = H^i(G, \mathbb{F}_p) \cdot \beta(v)$. □

Proof of theorem 4.5. We do induction on the order of G, hence we may assume that the theorem is true for groups of smaller order. Let $u \in H^*(G, \mathbb{F}_p)$ restrict to zero on any elementary abelian p-subgroup. By assumption the restriction of u to any proper subgroup $H < G$ is nilpotent. By raising u to a power if necessary, we may assume that u restrict to zero on any proper subgroup. If G is not a p-group, then u restrict to zero on a Sylow-p-subgroup P, hence $u = 0$ by Corollary 2.7, and the theorem holds. Next assume that G is a p-group. If G is elementary abelian the theorem trivially holds, hence we assume further that G is not elementary abelian. For any non-zero $v \in H^1(G, \mathbb{F}_p)$ the restriction of u to the kernel of v is zero, hence by the lemma, u^2 is divisible by $\beta(v)$. Thus for any sequence of non-zero elements $v_1, \ldots, v_m \in H^1(G, \mathbb{F}_p)$, u^{2m} is divisible by $\prod \beta(v_i)$. By Serre's Theorem 3.9 there exists such a sequence with $\prod \beta(v_i) = 0$, hence u is nilpotent. □

Let k be a field of characteristic p. Since we have a k-algebra isomorphism $H^*(G, \mathbb{F}_p) \otimes_{\mathbb{F}_p} k \cong H^*(G, k)$, we are able to expand the previous result to hold k-coefficients in general.

Corollary 4.7. *Let k be a field of characteristic p. Then the product of the restriction maps*

$$\Pi res_{G,E} : H^*(G, k) \to \prod_{E \leq G} H^*(E, k)$$

has nilpotent kernel.

Proof. Let $y \in H^*(G,k)$ be a homogeneous element with trivial image. We may write $y = x \otimes s$ with $x \in H(G,\mathbb{F}_p)$ and $s \in k$. If $s = 0$, then $y = 0$. If $s \neq 0$, then the element $(1 \otimes s^{-1})(x \otimes s) = x \otimes 1$ also restricts to zero. By Theorem 4.5, x is nilpotent and therefore y is nilpotent as desired. □

4.3 The Krull Dimension of $H(G,k)$

Let k denote a field of characteristic p. The cohomology ring $H^*(G,k)$ is graded commutative. The area of commutative ring theory provides a very rich setting for investigating the cohomology rings, so we face the problem of either reinterpreting the classical concepts in a graded setting or somehow alternate our objects to obtain a strictly commutative structure. We have chosen the last option. Let $H(G,k)$ denote the usual cohomology ring $H^*(G,k)$ if $p = 2$, and the subring ring of elements of even degree $H^{ev}(G,k)$ if $p > 2$. Then $H(G,k)$ is a commutative k-algebra. Recall that if E is an elementary abelian p-group, then

$$H^*(E,k) \cong \begin{cases} S(E^*,1) & \text{if } p = 2, \\ \Lambda(E^*,1) \otimes_k S(E^*,2) & \text{if } p > 2, \end{cases}$$

where $E^* = \mathrm{Hom}(E,k)$. Hence

$$H(E,k) \cong \begin{cases} S(E^*,1) & \text{if } p = 2, \\ S(E^*,2) \oplus J & \text{if } p > 2, \end{cases}$$

where J is the nilpotent ideal generated by $H^1(E,k)^2 \subset H^2(E,k)$.

Definition 4.8. Let A be a commutative ring. The Krull dimension of A, denoted $\dim A$, is the largest number of sharp inclusion appearing in a chain of prime ideals

$$\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_n$$

in A. If no such upper bound exists, we set $\dim A = \infty$.

We have gathered some basic facts about Krull dimension in the appendix section A.2. In particular $\dim k[x_1,\ldots,x_n] = n$, thus if E is an elementary abelian p-group of rank n, then $\dim H(E,k) = n$. Now we may prove the first theorem relating the cohomology ring of G to the elementary abelian p-subgroups of G.

Theorem 4.9. *The Krull dimension of $H(G,k)$ is equal to the maximal rank of an elementary abelian p-subgroup in G.*

Proof. The restriction map induces a map on subrings

$$\Pi\mathrm{res}_{G,E} : H(G,k) \to \prod_{E \leq G} H(E,k).$$

By Corollary 4.7, the kernel is nilpotent. Since a prime ideal must contain all nilpotent elements it follows that $\dim H(G,k) = \dim(\Pi\mathrm{res} H(G,k))$. By Corollary, 1.16 $H^*(E,k)$ is finitely generated as a module over $\Pi\mathrm{res}H^*(G,k)$, thus the same holds for the product ring. By Theorem A.16 in the appendix, this still holds when we pass to the subrings of even degree elements, hence $\prod_{E\leq G} H(E,k)$ is integral over $\Pi\mathrm{res}\,(H(G,k)$, so by Theorem A.11 the two rings have the same dimension. Since the dimension of a product of rings is the maximal dimension amongst the factors, the theorem follows. □

5 Quillen's Stratification Theorems

In this section we prove Quillen's Stratification Theorems, which states that the maximal ideal spectrum of $H^*(G,k)$ decomposes into disjoint pieces corresponding to the elementary abelian p-subgroups of G and gives a very nice description of the pieces going into the decomposition. We will start this section with a brief introduction to algebraic geometry. Throughout this section k will denote an algebraically closed field of characteristic p, and all rings are assumed to be finitely generated commutative k-algebras.

5.1 A Brief Introduction to Algebraic Geometry

The maximal ideal spectrum Let A be a finitely generated commutative k-algebra and let $\max(A)$ denote the set of maximal ideals in A. If $I \subseteq A$ is an ideal, let $V(I) \subseteq \max(A)$ be the set of maximal ideals containing I. The $V(I)$'s form the closed sets of a topology on $\max(A)$, called the Zariski topology. The maximal ideal spectrum of A is the topological space $\max(A)$ with the Zariski topology.

If $f \in A$ we write $V(f)$ for the closed set given by the principal ideal (f). Let $X_f = \max(A) - V(f)$, hence X_f consists of all maximal ideals not containing f. The sets X_f form an open basis for the topology on $\max(A)$.

Since A is a finitely generated commutative k-algebra, A has the form $k[x_1,\dots,x_n]/I_A$ for some ideal I_A in the polynomial ring $k[x_1,\dots,x_n]$. Thus the maximal ideals in A are in one-to-one correspondence with the maximal ideals in $k[x_1,\dots,x_n]$ containing I_A. Each point $(a_1,\dots,a_n) \in \mathbb{A}^n_k$, where $\mathbb{A}^n_k$ denotes the affine space of dimension n over k, determines a surjective k-algebra homomorphism

$$k[x_1,\dots,x_n] \to k \quad \text{given by} \quad x_i \mapsto a_i,$$

and the kernel is a maximal ideal in $k[x_1,\dots,x_n]$. Since polynomial functions separate points in $\mathbb{A}^n_k$, distinct points give rise to distinct maximal ideals. Moreover, it follows from Hilbert's Nullstellensatz that every maximal ideal in the polynomial ring $k[x_1,\dots,x_n]$ is determined by a point $(a_1,\dots,a_n) \in \mathbb{A}^n_k$ as above. The maximal ideal determined by $\phi : k[x_1,\dots,x_n] \to k$ will contain I_A if and only if ϕ factors through $k[x_1,\dots,x_n]/I_A$. Thus there is a one-to-one correspondence

$$\mathrm{Hom}_{k\text{-alg}}(A,k) \cong \max(A).$$

It is natural to view an element $a \in A$ as a function on $\max(A)$ by evaluating the corresponding algebra homomorphism at a. Let I be an ideal in A. With this interpretation, the set $V(I)$ corresponds to the subset of $\max(A)$ where I vanishes.

Induced Maps Let $\phi : A \to B$ be a k-algebra homomorphism and let $\mathfrak{m} \in \max(B)$. Then $\phi^{-1}(\mathfrak{m})$ is a maximal ideal in A, hence ϕ induces a map of maximal ideal spectra

$$\phi^* : \max(B) \to \max(A).$$

It is clear that $(\phi^*)^{-1}(X_f) = X_{\phi(f)}$ for all $f \in A$, hence ϕ^* is continuous.

Remark 5.1. Let $I \subset A$ be an ideal. The quotient map $A \to A/I$ induces a map on maximal ideal spectra $\max(A/I) \to \max(A)$, which is easily seen to be a homeomorphism onto the closed set $V(I) \subset \max(A)$. Let $f \in A$ be non-nilpotent. One may verify that the canonical map $A \to A[f^{-1}]$ induces a homeomorphism of $\max(A[f^{-1}])$ onto its image. The image of $\max(A[f^{-1}])$ is the open set X_f, so this gives a very nice description of the basis elements of the Zariski topology.

Theorem 5.2. *Let $A \subseteq B$ with B integral over A. Then the map induced by the inclusion $i^* : max(B) \to max(A)$ is a surjective, closed map.*

Proof. The induced map $i^* : \max(B) \to \max(A)$ is given by

$$\mathfrak{m} \mapsto \mathfrak{m} \cap A.$$

By Theorem A.7, this map is surjective. If I is an ideal in B we claim that $i^*(V_B(I)) = V_A(I \cap A)$. If $\mathfrak{m} \in V_B(I)$ then by definition we have $I \subseteq \mathfrak{m}$, hence $I \cap A \subseteq \mathfrak{m} \cap A$, hence $\mathfrak{m} \cap A \in V_A(I \cap A)$. Conversely, if $\mathfrak{m} \in V_A(I \cap A)$ then $\mathfrak{m}$ corresponds uniquely to a maximal ideal $\mathfrak{m}/(I \cap A)$ in $A/(I \cap A)$. Since B/I is integral over $A/(I \cap A)$ there exists some maximal ideal $\mathfrak{m}' \in V_B(I)$ such that $(\mathfrak{m}'/I) \cap (A/(I \cap A)) = \mathfrak{m}/(I \cap A)$. Since

$$(\mathfrak{m}' \cap A)/(I \cap A) = \big(\mathfrak{m}'/I\big) \cap (A/(I \cap A)) = \mathfrak{m}/(I \cap A),$$

the maximal ideals $\mathfrak{m}' \cap A$ and $\mathfrak{m}$ correspond to the same ideal in the residue ring, hence $\mathfrak{m}' \cap A = \mathfrak{m}$. Thus $\mathfrak{m} \in i^*(V_B(I))$ as desired. □

Given a finitely generated commutative k-algebra A, we write $A^{[p^a]}$ for the subring consisting of the p^a'th power of elements in A. We have the following corollary to the above theorem.

Corollary 5.3. *Let $A \subseteq B$ such that $B^{[p^a]} \subseteq A$ for some $a \geq 0$. Then the induced map $i^* : max(B) \to max(A)$ is a homeomorphism.*

Proof. Clearly the inclusion $B^{[p^a]} \subseteq A$ is integral, and in fact so is the inclusion $A \subseteq B$. Indeed, if $b \in B$ then b is root in the monic polynomial $x^{p^a} - b^{p^a}$ which has coefficients in A. Thus the induced maps on maximal ideal spectra are continuous, closed and surjective, hence so is the composition

$$\max(B) \to \max(A) \to \max(B^{[p^a]}).$$

The composition is induced by the inclusion $B^{[p^a]} \hookrightarrow B$. Since k is an algebraically closed field of characteristic p, it is perfect, hence the Fröbenius map $s \mapsto s^{p^a}$ is an isomorphism on k. Let $\phi, \psi \in \mathrm{Hom}_{k\text{-alg}}(B, k)$ such that $\phi(b) \neq \psi(b)$ for some $b \in B$. Then $\phi(b^{p^a}) \neq \phi(b^{p^a})$, hence ϕ and ψ have different images in $\max(B^{[p^a]})$ as desired. Thus the induced map is a closed bijection, hence a homeomorphism. $\square$

Suppose a finite group G acts as automorphisms on a finitely generated commutative k-algebra A and let $\mathfrak{m} \in \max(A)$. By letting $g \cdot \mathfrak{m} = g(\mathfrak{m})$ we obtain a G-action on the maximal ideal spectra.

Theorem 5.4. *Suppose a finite group G acts as automorphisms on a finitely generated commutative k-algebra A. Then the fixed point subalgebra A^G is a finitely generated k-algebra over which A is integral. The variety max(A^G) is the quotient of max(A) by the action of G.*

Proof. Let $a \in A$ and consider the monic polynomial

$$f_a(x) = \prod_{g \in G}(x - g(a)),$$

which has coefficients in A^G. Since $f_a(a) = 0$, A is integral over A^G. Choose a finite set $\{a_1, \ldots, a_n\}$ of k-algebra generators of A and consider the monic polynomials $\{f_{a_1}, \ldots, f_{a_n}\}$. Let B be the subalgebra of A^G generated by all coefficients appearing in the polynomials. Then B is a finitely generated k-algebra, hence Noetherian. Since each generator a_i is integral over B, it follows from Corollary A.3 that $A = k[a_1, \ldots, a_n]$ is a finitely generated B-module. Then the sub-B-module A^G is finitely generated as a B-module as well and is therefore a finitely generated k-algebra.

By Theorem 5.2 the inclusion $A^G \hookrightarrow A$ induces a surjective map $\max(A) \to \max(A^G)$. It is clear that if $\mathfrak{m}$ and $\mathfrak{m}'$ are G-conjugate maximal ideals in A, then $\mathfrak{m} \cap A^G = \mathfrak{m}' \cap A^G$. Thus the map factors as

$$\max(A) \to \max(A)/G \xrightarrow{i} \max(A^G)$$

with i surjective. Assume that $\mathfrak{m}$ and $\mathfrak{m}'$ are maximal ideals in A, which are not G-conjugate. Then there exists $a \in \mathfrak{m}$ such that $a \notin g(\mathfrak{m}')$ for any $g \in G$. Otherwise, we would have $\mathfrak{m} \subseteq \cup_{g \in G} g(\mathfrak{m}')$, and since the union is finite $\mathfrak{m} \subseteq g(\mathfrak{m}')$ for some $g \in G$. Hence $\prod_{g \in G} g(a)$ is an element of A^G lying in $\mathfrak{m}$ but not in $\mathfrak{m}'$. We conclude that i is a continuous closed bijection and therefore a homeomorphism. $\square$

5.2 Quillen's Stratification Theorems

Let G be a finite group and let k be an algebraically closed field of characteristic p. Again, $H(G, k)$ denotes $H^*(G, k)$ if $p = 2$ and $H^{ev}(G, k)$ if $p > 2$.

Recall that if E is an elementary abelian p-group, then

$$H(E,k) \cong \begin{cases} S(E^*,1) & \text{if } p = 2, \\ S(E^*,2) \oplus J & \text{if } p > 2, \end{cases}$$

where J is the nilpotent ideal generated by $H^1(E,k)^2 \subset H^2(E,k)$.

Let V_G denote the maximal ideal spectrum of $H(G,k)$. If H is a subgroup of G, we have a restriction map $\mathrm{res}_{G,H} : H(G,k) \to H(H,k)$, which induces a map of maximal ideal spectra $\mathrm{res}^*_{G,H} : V_H \to V_G$.

Theorem 5.5. *We have*

$$V_G = \bigcup_{E \leq G} res^*_{G,E} V_E,$$

where E ranges over all elementary abelian p-subgroups of G.

Proof. By Corollary 4.7, the product of the restriction maps

$$\Pi\mathrm{res}_{G,E} : H(G,k) \to \Pi\mathrm{res}\,(H(G,k) \hookrightarrow \prod_{E \leq G} H(E,k)$$

has nilpotent kernel, hence the left map induces a surjective map on spectra. As noted in the proof of Theorem 4.9, $\prod_{E \leq G} H(E,k)$ is integral over $\Pi\mathrm{res}\,(H(G,k)$, so the right map induces a surjective map on spectra by Theorem 5.2, and the theorem follows. □

The Quillen Stratification Theorems 5.9 and 5.10 are refinements of the above theorem.

Remark 5.6. Let $E \leq G$ be an elementary abelian p-subgroup and consider the image $\mathrm{res}^*_{G,E}(V_E) \subseteq V_G$. We claim that

$$\mathrm{res}^*_{G,E}(V_E) = V(\ker(\mathrm{res}_{G,E})) \subseteq V_G,$$

in particular $\mathrm{res}^*_{G,E}(V_E)$ is a closed subset of V_G. It is clear that any maximal ideal in $\mathrm{res}^*_{G,E}(V_E)$ must contain the kernel of the restriction map. Conversely, let $\mathfrak{m}$ be a maximal ideal in $H(G,k)$ such that $\ker(\mathrm{res}_{G,E}) \subseteq \mathfrak{m}$. We have the following commutative diagram, where the lower map is an isomorphism

$$\begin{tikzcd}
H(G,k) \arrow[r, "\mathrm{res}_{G,E}"] \arrow[d, two heads] & H(E,k). \\
H(G,k)/\ker(\mathrm{res}_{G,E}) \arrow[r] & \mathrm{res}_{G,E}\,(H(G,k)) \arrow[u, hook]
\end{tikzcd}$$

Thus $\mathfrak{m}$ corresponds uniquely to a maximal ideal $\overline{\mathfrak{m}}$ in $\mathrm{res}_{G,E}\,(H(G,k))$. Since $H(E,k)$ is integral over $\mathrm{res}_{G,E}\,(H(G,k))$, it follows from Theorem A.7 and Theorem A.5, that there exists a maximal ideal $\mathfrak{m}'$ in $H(E,k)$ such that $\mathfrak{m}' \cap \mathrm{res}_{G,E}\,(H(G,k)) = \overline{\mathfrak{m}}$. Hence $\mathrm{res}^*_{G,E}(\mathfrak{m}') = \mathfrak{m}$.

Remark 5.7. Now it is easily seen why we must restrict our attention to conjugacy classes of elementary abelian p-subgroups if we hope to use the sets $\mathrm{res}^*_{G,E}(V_E)$ to construct a decomposition of V_G. If $g \in G$ then we have an obvious commutative diagram

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

where g is conjugation. Since g induces the identity on $H(G,k)$, the following two maps are identical

$$\begin{aligned}
\mathrm{res}_{G,E} &: H(G,k) \to H(E,k), \\
g^* \circ \mathrm{res}_{G,gEg^{-1}} &: H(G,k) \to H(gEg^{-1},k) \to H(E,k).
\end{aligned}$$

In particular $\ker(\mathrm{res}_{G,gEg^{-1}}) = \ker(\mathrm{res}_{G,E})$, so by the above discussion

$$\mathrm{res}^*_{G,E}(V_E) = \mathrm{res}^*_{G,gEg^{-1}}(V_{gEg^{-1}}).$$

Recall that β denotes the composition

$$H^1(E,\mathbb{F}_p) \xrightarrow{\beta} H^2(E,\mathbb{F}_p) \hookrightarrow H^2(E,k).$$

Define an element in $H(E,k)$ by

$$\sigma_E = \begin{cases} \prod \beta(\varepsilon) & \text{if } p > 2, \\ \prod \varepsilon & \text{if } p = 2, \end{cases}$$

where ε ranges over all non-trivial elements in $H^1(E,\mathbb{F}_p) = \mathrm{Hom}(E,\mathbb{F}_p)$. Clearly σ_E is invariant under any automorphism of E. Moreover, since every proper subgroup $F < E$ is contained in a subspace of codimension 1, and all these subspaces occur as kernels of homomorphisms in $\mathrm{Hom}(E,\mathbb{F}_p)$, the restriction of σ_E to any proper subgroup is trivial.

Lemma 5.8. *Suppose that E is an elementary abelian p-subgroup of G such that $|N_G(E):E| = p^\alpha h$, where $(p,h) = 1$. Then the following hold:*

1. *If $y \in H(E,k)$ is invariant under the action of $N_G(E)$, then there exists an element $y' \in H(G,k)$ with $\mathrm{res}_{G,E}(y') = (\sigma_E \cdot y)^{p^\alpha}$.*

2. *There exists an element $\rho_E \in H(G,k)$ such that $res_{G,E}(\rho_E) = (\sigma_E)^{p^\alpha}$, and such that if E is not conjugate to a subgroup of an elementary abelian p-group E', then $res_{G,E'}(\rho_E) = 0$.*

Proof. To proof the first statement, let $y \in H(E,k)^{N_G(E)}$. Without loss of generality we may assume that y is homogeneous and we let

$$z = N_{E,G}(1 + \sigma_E y).$$

By the double coset formula, Theorem 3.3 part 3,

$$\mathrm{res}_{G,E}(z) = \prod_{g \in D} N_{(gEg^{-1} \cap E),E}(\mathrm{res}_{gEg^{-1},(gEg^{-1}\cap E)}(1 + g^*(\sigma_E y))),$$

where $G = \cup_{g \in D} EgE$ is a double coset decomposition. Now g^* carries $\mathrm{Hom}(E, \mathbb{F}_p)$ isomorphically onto $\mathrm{Hom}(gEg^{-1}, \mathbb{F}_p)$, hence $g^*(\sigma_E) = \sigma_{gEg^{-1}}$. Since the restriction of $\sigma_{gEg^{-1}}$ to any proper subgroup is zero, the only terms in the product, which are not equal to 1, are those for which $gEg^{-1} = E$, i.e., those indexed by $g \in N_G(E)$. Since y is invariant under the action of $N_G(E)$, $g^*(\sigma_E y) = \sigma_E \cdot y$ for all $g \in N_G(E)$, hence

$$\begin{aligned}\mathrm{res}_{G,E}(z) &= (1 + \sigma_E y)^{p^\alpha h} = (1 + (\sigma_E y)^{p^\alpha})^h \\ &= 1 + h(\sigma_E y)^{p^\alpha} + \text{ terms of higher degree.}\end{aligned}$$

Now take y' as the homogeneous part of z of degree $p^\alpha \mathrm{deg}(\sigma_E y)$ divided by h.

To prove the second statement, choose $y = 1$ and write ρ_E for the element y' obtained as above. Let E' be an elementary abelian p-subgroup. By the double coset formula, Theorem 3.3 part 3,

$$\mathrm{res}_{G,E'}(z) = \prod_{g \in D} N_{(gEg^{-1} \cap E'),E'}(\mathrm{res}_{gEg^{-1} \to (gEg^{-1}\cap E')}(1 + g^*(\sigma_E))).$$

If E is not conjugate to any subgroup of E' then for all $g \in D$

$$\mathrm{res}_{gEg^{-1} \to gEg^{-1} \cap E'}(g^*(\sigma_E)) = 0,$$

hence $\mathrm{res}_{G,E'}(z) = 1$ and $\mathrm{res}_{G,E'}(\rho_E) = 0$ as desired. □

Define

$$V_E^+ = V_E - \bigcup_{F < E} \mathrm{res}^*_{E,F} V_F,$$

where F ranges over all proper subgroups of E. Since every proper subgroup is contained in a subspace of codimension 1, we may restrict the above union to $\mathbb{F}_p$-hyperplanes. Let F denote such a hyperplane. There are exactly $p-1$

homomorphisms in $\mathrm{Hom}(E, \mathbb{F}_p) \subset \mathrm{Hom}(E, k) = E^*$ with kernel F. Now let ν_F be such a homomorphism. Since

$$S(E^*) \cap \ker(\mathrm{res}_{E,F}) = (\nu_F),$$

where (ν_F) denotes the principal ideal generated by ν_F, $\mathrm{res}^*_{E,F}(V_F)$ consists of all maximal ideals in $H(E, k)$ which contain ν_F. Thus $\bigcup_{F<E} \mathrm{res}^*_{E,F} V_F$ consists of all maximal ideals in $H(E, k)$ containing the element

$$\prod_{F \text{ is a } \mathbb{F}_p\text{-hyperplane}} \nu_F.$$

If we for each F replace ν_F with the product of all $p-1$ homomorphisms in $\mathrm{Hom}(E, \mathbb{F}_p)$ having F as kernel, we do not change the closed set, hence

$$\bigcup_{F<E} \mathrm{res}^*_{E,F} V_F = V\left(\sigma_E\right).$$

Thus V_E^+ corresponds to the maximal ideals of $H(E, k)$ not containing σ_E, and the inclusion $H(E, k) \hookrightarrow H(E, k)[\sigma_E^{-1}]$ induces a homeomorphism

$$\max\left(H(E, k)[\sigma_E^{-1}]\right) \to V_E^+.$$

Define

$$V_{G,E}^+ = \mathrm{res}^*_{G,E}(V_E) - \bigcup_{F<E} \mathrm{res}^*_{G,F}(V_F).$$

Clearly $V_{G,E}^+ \subseteq \mathrm{res}^*_{G,E}(V_E^+)$. Let U be the subset of all ideals in $\mathrm{res}^*_{G,E}(V_E)$ not containing ρ_E. Note that all ideals in the union $\bigcup_{F<E} \mathrm{res}^*_{G,F}(V_F)$ contain ρ_E. Indeed, since E is not conjugate to a subgroup of F, the second part of Lemma 5.8 implies that $\mathrm{res}_{G,F}(\rho_E) = 0$, so $U \subseteq V_{G,E}^+$. Since $\mathrm{res}_{G,E}(\rho_E) = \sigma_E^{p^\alpha}$, it is clear that $\mathrm{res}_{G,E}(V_E^+) \subseteq U$. Thus we may conclude that

$$V_{G,E}^+ = \mathrm{res}_{G,E}(V_E^+) = U.$$

Note that $V_{G,E}^+$ is locally closed since it is the intersection of the closed set $\mathrm{res}^*_{G,E}(V_E)$ and the open set $V_G - V(\rho_E)$.

Theorem 5.9. *The maximal ideal spectrum V_G is the disjoint union of the locally closed subsets $V_{G,E}^+$, one for each conjugacy class of elementary abelian p-subgroups E in G. Moreover, $V_{G,E}^+$ is itself homeomorphic to the maximal ideal spectrum of a suitably chosen ring.*

Proof. It is clear from Theorem 5.5 and the discussion above that

$$V_G = \bigcup_{E \in I} V_{G,E}^+,$$

where I denotes a family of elementary abelian p-subgroups, one from each conjugacy class. To see that the sets $V^+_{G,E}$ are disjoint, let $E, E' \in I$, hence E and E' are not conjugate. If E is conjugate to a subgroup $F' < E'$, then $\mathrm{res}^*_{G,E}(V_E) = \mathrm{res}^*_{G,F'}(V'_F)$, hence $V^+_{G,E}$ and $V^+_{G,E'}$ are disjoint by definition. If E is not conjugate to a subgroup of E', then by the second part of Lemma 5.8, $\mathrm{res}_{G,E'}(\rho_E) = 0$, hence everywhere zero on $V^+_{G,E'}$. Since $V^+_{G,E}$ is the intersection of $\mathrm{res}^*_{G,E}(V_E)$ and $V_G - V(\rho_E)$, ρ_E is everywhere non-zero on $V^+_{G,E}$, thus the sets are disjoint.

By the second part of Lemma 5.8, the restriction $\mathrm{res}_{G,E} : H(G,k) \to H(E,k)$ induces a map on fraction rings

$$\mathrm{res}_{G,E} : H(G,k)[\rho_E^{-1}] \to H(E,k)[\sigma_E^{-1}],$$

so $\mathrm{res}_{G,H}$ induces an isomorphism of rings

$$\left(H(G,k)/\ker(\mathrm{res}_{G,E})\right)[\rho_E^{-1}] \xrightarrow{\sim} \mathrm{res}_{G,E}\left(H(G,k)[\rho_E^{-1}]\right).$$

The composition

$$H(G,k) \to H(G,k)/\ker(\mathrm{res}_{G,E}) \hookrightarrow \left(H(G,k)/\ker(\mathrm{res}_{G,E})\right)[\rho_E^{-1}]$$

induces a homeomorphism onto the set of maximal ideals in $H(G,k)$ which contain the kernel $\ker(\mathrm{res}_{G,E})$ but do not contain ρ_E. This is exactly $V^+_{G,E}$. Hence we have a homeomorphism induced by the restriction map

$$V^+_{G,E} \to \max\left(\mathrm{res}_{G,E}\left(H(G,k)[\rho_E^{-1}]\right)\right).$$

□

Recall that $g \in N_G(E)$ acts on $H(E,k)$ as an automorphism $g^* : H(E,k) \to H(E,k)$. An element in the centralizer $C_G(E)$ acts trivially, so we obtain an action of $W_G(E) = N_G(E)/C_G(E)$ on $H(E,k)$.

Theorem 5.10. *The group $W_G(E) = N_G(E)/C_G(E)$ acts on V^+_E and the restriction map induces a homeomorphism*

$$V^+_E/W_G(E) \to V^+_{G,E}.$$

Proof. As before we have a map of fraction rings

$$\mathrm{res}_{G,E} : H(G,k)[\rho_E^{-1}] \to H(E,k)[\sigma_E^{-1}].$$

Since $W_G(E)$ acts trivially on $H(G,k)$, we must have

$$\mathrm{res}_{G,E}\left(H(G,k)[\rho_E^{-1}]\right) \subseteq \left(H(E,k)[\sigma_E^{-1}]\right)^{W_G(E)}. \qquad (\star)$$

By the first part of Lemma 5.8, we have an inclusion

$$\left(\left(H(E,k)[\sigma_E^{-1}]\right)^{W_G(E)}\right)^{[p^\alpha]} \subseteq \mathrm{res}_{G,E}\left(H(G,k)[\rho_E^{-1}]\right).$$

Hence by Theorem 5.3, the inclusion $(\star)$ induces a homeomorphism

$$\max\left(\left(H(E,k)[\sigma_E^{-1}]\right)^{W_G(E)}\right) \to \max\left(\mathrm{res}_{G,E}\left(H(G,k)[\rho_E^{-1}]\right)\right).$$

By Theorem 5.4, the left hand side is homeomorphic to the quotient of V_E^+ by the action of $W_G(E)$, and we saw in the proof of Theorem 5.9 that the right hand side is homeomorphic to $V_{G,E}^+$ via the restriction map. □

In order to further describe the maximal ideal spectrum of $H(G,k)$, we consider the following category.

Definition 5.11. Let $\mathcal{C}_G$ denote the category whose objects are the elementary abelian p-subgroups of G and whose morphisms are all group homomorphisms which can be induced by conjugation by an element in G. Hence a group homomorphism $\varphi : E \to E'$ is a morphism in $\mathcal{C}_G$ if there exists a $g \in G$ such that $\varphi(e) = geg^{-1}$ for all $e \in E$.

Define a functor from $\mathcal{C}_G$ to the category of topological spaces by

$$E \mapsto V_E, \qquad (E \xrightarrow{\varphi} E') \mapsto (V_E \xrightarrow{\varphi^*} V_E').$$

We saw in Remark 5.7 that for all elementary abelian p-subgoups $E \leq G$ and $g \in G$, we have $\mathrm{res}_{G,E} = g^* \circ \mathrm{res}_{G,gEg^{-1}}$. Hence the restriction maps $\mathrm{res}^*_{G,E} : V_E \to V_G$ induce a map $\mathrm{colim}_E V_E \to V_G$.

Theorem 5.12. *The map*

$$\underset{E}{colim} V_E \to V_G$$

induced by the restriction maps is a homeomorphism.

Proof. By definition

$$\underset{E}{\mathrm{colim}} V_E = \bigsqcup_{E \leq G} V_E / \sim$$

where $\sim$ is the equivalence relation generated by the relation that identifies $x_E \in V_E$ and $x_{E'} \in V_{E'}$ if there exists a morphism in $\mathcal{C}_G$, $\varphi : E \to E'$, such that $\varphi^*(x_E) = x_{E'}$. If two subgroups are conjugated, they are identified by that conjugation morphism in $\mathcal{C}_G$, hence we may restrict the disjoint union to a family I of elementary abelian subgroups, one from each conjugacy class. Likewise, we may replace V_E by V_E^+ since this overlap arises from the inclusions in $\mathcal{C}_G$. Hence

$$\underset{E}{\mathrm{colim}} V_E = \bigsqcup_{E \in I} V_E^+ / \sim .$$

The only identifications left are those arising from conjugation of smaller subgroups into bigger subgroups, hence

$$\operatorname*{colim}_{E} V_E = \bigsqcup_{E \in I} V_E^+ / W_G(E).$$

Theorem 5.10 implies that the restriction map induces a homeomorphism $V_E^+/W_G(E) \to V_{G,E}^+$, and since V_G is the disjoint union of the pieces $V_{G,E}^+$, the theorem follows. □

6 Quillen's F-Isomorphism

Consider the product of the restriction maps

$$\Pi \mathrm{res}_{G,E} : H(G, \mathbb{F}_p) \to \prod_{E \leq G} H(E, \mathbb{F}_p).$$

We have seen that the kernel of this map is nilpotent. It is clear that elements in the target of this map must satisfy certain compatibility conditions related to inclusions and conjugations in G. Define a functor from $\mathcal{C}_G^{op}$ to the category of graded $\mathbb{F}_p$-algebras by

$$E \mapsto H(E, \mathbb{F}_p), \qquad \alpha \mapsto \alpha^*.$$

We saw in Remark 5.7 that $\mathrm{res}_{G,E} = g^* \circ \mathrm{res}_{G,gEg^{-1}}$ for all $g \in G$. Hence the restriction maps induce a homomorphism

$$q_G : H(G, \mathbb{F}_p) \to \lim_{E} H(E, \mathbb{F}_p),$$

which we shall call the Quillen homomorphism. The purpose of this section is to show the following theorem.

Theorem 6.1. *The Quillen homomorphism*

$$q_G : H(G, \mathbb{F}_p) \to \lim_{E} H(E, \mathbb{F}_p)$$

is an F-isomorphism.

Theorem 5.12 from the previous section is actually equivalent to the theorem above. We reformulate Theorem 5.12 below and the rest of this section is occupied with showing the equivalence of the two statements. This equivalence was established by Quillen in his paper [16, prop. B.8, B.9].

Theorem 6.2. *The Quillen homomorphism $q_G : H(G, \mathbb{F}_p) \to \lim_{E} H(E, \mathbb{F}_p)$ induces a bijection*

$$q_G^* : \mathit{Hom}_{\mathbb{F}_p\text{-}alg}(\lim_{E} H(E, \mathbb{F}_p), k) \to \mathit{Hom}_{\mathbb{F}_p\text{-}alg}(H(G, \mathbb{F}_p), k)$$

for all algebraically closed fields k of characteristic p.

It is not true in general that the functor $\mathrm{Hom}_{\mathbb{F}_p\text{-alg}}(-, k)$ take limits to colimits, but in this case the canonical map

$$\operatorname*{colim}_{E} \mathrm{Hom}_{\mathbb{F}_p\text{-alg}}(H(E, \mathbb{F}_p), k) \xrightarrow{\cong} \mathrm{Hom}_{\mathbb{F}_p\text{-alg}}(\lim_{E} H(E, \mathbb{F}_p), k)$$

is indeed a bijection. For a proof, see [16, Lemma 8.11]. The proof uses that the category $\mathcal{C}_G$ is finite and that all the rings in question are finite modules over the Noetherian ring $H(G, \mathbb{F}_p)$.

Proof of theorem 6.2. We have an isomorphism of k-algebras $H(G,k) \cong H(G,\mathbb{F}_p) \otimes_{\mathbb{F}_p} k$, giving us a bijection of sets

$$\begin{aligned}\mathrm{Hom}_{\mathbb{F}_p\text{-alg}}(H(G,\mathbb{F}_p),k) &\cong \mathrm{Hom}_{k\text{-alg}}(H(G,k),k)\\ &\cong V_G.\end{aligned}$$

Likewise, we have a bijection of sets

$$\begin{aligned}\mathrm{Hom}_{\mathbb{F}_p\text{-alg}}(\lim_E H(E,\mathbb{F}_p),k) &\cong \operatorname*{colim}_E \mathrm{Hom}_{\mathbb{F}_p\text{-alg}}(H(E,\mathbb{F}_p),k)\\ &\cong \operatorname*{colim}_E \mathrm{Hom}_{k\text{-alg}}(H(E,k),k)\\ &\cong \operatorname*{colim}_E V_E.\end{aligned}$$

Under these identifications the Quillen homomorphism $q_G : H(G,\mathbb{F}_p) \to \lim_E H(E,\mathbb{F}_p)$ corresponds to the map $V_G \to \operatorname*{colim}_E V_E$ induced by the restriction maps $\mathrm{res}^*_{G,E}$. This is a homeomorphism by Theorem 5.12, hence q^*_G is bijective. □

We proceed to show the equivalence of the two theorems. For the rest of this section we assume that all rings are $\mathbb{F}_p$-algebras.

Theorem 6.3. *Let A be a Noetherian ring and let $f : A \to B$ be homomorphism such that B is finitely generated as a module over the image of A. Then the induced map*

$$f^* : Hom_{\mathbb{F}_p\text{-}alg}(B,k) \to Hom_{\mathbb{F}_p\text{-}alg}(A,k)$$

is a bijection for all algebraically closed fields k of characteristic p, if and only if f is an F-isomorphism.

If $\mathfrak{p}$ be a prime ideal in A, then the integral domain $A/\mathfrak{p}$ embeds in its field of fractions $Q(A/\mathfrak{p})$. Fields of this form are referred to as residue fields of A. Letting $\overline{Q}(A/\mathfrak{p})$ denote the algebraic closure, the composition

$$\phi_{\mathfrak{p}} : A \to A/\mathfrak{p} \hookrightarrow Q(A/\mathfrak{p}) \hookrightarrow \overline{Q}(A/\mathfrak{p})$$

is a ring homomorphism from A to an algebraically closed field of characteristic p with kernel $\mathfrak{p}$.

Lemma 6.4. *Let $A \subseteq B$ with A Noetherian and B finitely generated as a module over A. Suppose that the map induced by the inclusion*

$$Hom_{\mathbb{F}_p\text{-}alg}(B,k) \to Hom_{\mathbb{F}_p\text{-}alg}(A,k)$$

is a bijection for all algebraically closed fields k of characteristic p. Then for each prime ideal $\mathfrak{p}$ in A, there exists a unique prime ideal $\mathfrak{q}$ in B such that $\mathfrak{q} \cap A = \mathfrak{p}$. Moreover, for each such $\mathfrak{p}$ and $\mathfrak{q}$, $(B/\mathfrak{q})^{[p^a]}$ is contained in the residue field of $A/\mathfrak{p}$ for some $a \geq 0$.

Before we prove the lemma we recall some basic facts about field extensions.

Definition 6.5. Let $L \subseteq K$ be a finite field extension of a field of characteristic p. An element $a \in K$ is said to be purely inseparable over L if there is an integer $m \geq 0$ such that $a^{p^m} \in L$. We call the extension purely inseparable, if every element in K is purely inseparable over L.

Given a finite normal extension $L \subseteq K$, we let $G(K/L)$ be the set of all L-automorphisms of K. The order of the group $G(K/L)$ is closely related to the separability of the extension $L \subseteq K$, in particular one may prove that the extension is purely inseparable if and only if $G(K/L)$ is trivial. The relation between the two concepts that we shall need is contained in the following theorem. A proof can be found in [12, Chapter I, Thm. 21].

Theorem 6.6. *Let $L \subseteq K$ be a finite normal extension. Let $a \in K$ and suppose that a is left fixed by each element of $G(K/L)$. Then a is purely inseparable over L.*

Proof of Lemma 6.4. Let $\mathfrak{p}$ be a prime ideal in A. Since B is finitely generated as an A-module, it follows from Theorem A.7 that there exists a prime ideal $\mathfrak{q}$ in B with $\mathfrak{q} \cap A = \mathfrak{p}$. We want to show that $\mathfrak{q}$ is unique with this property. Let $\mathfrak{q}_1$ and $\mathfrak{q}_2$ be prime ideals in B such that

$$\mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A = \mathfrak{p}.$$

Consider the commutative diagram

$$\begin{tikzcd}
 & B \arrow[r, "\phi_{\mathfrak{q}_1}"] & \overline{Q}(B/\mathfrak{q}_1) \\
A \arrow[ur, hook] \arrow[dr, hook] \arrow[rr, "\phi_{\mathfrak{p}}"] & & \overline{Q}(A/\mathfrak{p}) \arrow[u, hook] \arrow[d, hook] \\
 & B \arrow[r, "\phi_{\mathfrak{q}_2}"] & \overline{Q}(B/\mathfrak{q}_2).
\end{tikzcd}$$

.

Since an algebraically closed field has no proper finite extensions,

$$\overline{Q}(A/\mathfrak{p}) = \overline{Q}(B/\mathfrak{q}_1) = \overline{Q}(B/\mathfrak{q}_2).$$

By assumption, the map $\phi_{\mathfrak{p}}$ factors uniquely through B, hence $\phi_{\mathfrak{q}_1} = \phi_{\mathfrak{q}_2}$ and therefore $\mathfrak{q}_1 = \mathfrak{q}_2$ as desired.

Let $\mathfrak{p}$ be a prime ideal in A and let $\mathfrak{q}$ be the unique prime ideal in B lying over A. Consider the finite field extension $Q(A/\mathfrak{p}) \subseteq Q(B/\mathfrak{q})$. Let $Q(B/\mathfrak{q})_N$ denote the normal closure of $Q(B/\mathfrak{q})$ which is a finite field extension of $Q(A/\mathfrak{p})$. We have the following commutative diagram

$$\begin{tikzcd}
A \arrow[r, hook] \arrow[d, "\phi_{\mathfrak{p}}"'] & B \arrow[d, "\phi_{\mathfrak{q}}"'] & & \\
Q(A/\mathfrak{p}) \arrow[r, hook] & Q(B/\mathfrak{q}) \arrow[r, hook] & Q(B/\mathfrak{q})_N \arrow[r, hook] & \overline{Q}(A/\mathfrak{p}).
\end{tikzcd}$$

Let $x \in Q(B/\mathfrak{p})$. If there exists a $Q(A/\mathfrak{p})$-automorphism of $Q(B/\mathfrak{q})_N$ which does not fix x, then the map $A \to \overline{Q}(A/\mathfrak{p})$ allows two distinct factorizations through B. This is false by assumption, hence no such automorphism exists. By Theorem 6.6 the extension $Q(A/\mathfrak{p}) \subseteq Q(B/\mathfrak{q})$ is purely inseparable, hence for each $x \in B/\mathfrak{p}$ there exists some $b \geq 0$ such that $x^{p^b} \in Q(A/\mathfrak{p})$. Since $B/\mathfrak{p}$ is finitely generated as a module over $A/\mathfrak{p}$, there exists some $a \geq 0$ such that $(B/\mathfrak{p})^{[p^a]} \subseteq Q(A/\mathfrak{p})$. □

Proof of Theorem 6.3. Let $a \in A$ be non-nilpotent. Since the intersection of all prime ideals in A equals the ideal of nilpotent elements, there exists some prime ideal $\mathfrak{p}$ in A such that $a \notin \mathfrak{p}$. By assumption there exists some $\psi : B \to \overline{Q}(A/\mathfrak{p})$ such that $\psi \circ f = \phi_{\mathfrak{p}}$, thus a is not in the kernel of f.

We may divide out by the nil-radicals and reduce to the case where f is an inclusion. Consider the ideals in A given by

$$I_d = \left\{ a \in A \mid a\left(B^{[p^d]}\right) \subseteq A \right\}.$$

Let $a \in I_d$. Then for all $b \in B$, $ab^{p^{d+1}} = a(b^p)^{p^d} \in A$, hence $I_d \subseteq I_{d+1}$, so the ideals form an ascending chain. Since A is Noetherian there exists some d such that $I_{d'} = I_d$ for all $d' \geq d$. Our claim is that $I_d = A$. Assume for contradiction that I_d is a proper ideal in A. Since A is Noetherian, I_d allows a primary decomposition, so we may choose a minimal prime ideal $\mathfrak{p}$ in A containing I_d. It is clear that $(I_d)_{\mathfrak{p}} = (I_{d'})_{\mathfrak{p}}$ for all $d' \geq d$. One may verify that for each d'

$$(I_{d'})_{\mathfrak{p}} = \left\{ a \in A_{\mathfrak{p}} \mid a\left(B_{\mathfrak{p}}^{[p^d]}\right) \subseteq A_{\mathfrak{p}} \right\}.$$

The localization of I_d is a proper ideal in $A_{\mathfrak{p}}$. If $1 \in (I_d)_{\mathfrak{p}}$, then $1 = \frac{a}{\tau}$ for some $a \in I_d$ and $\tau \in A - \mathfrak{p}$, hence $\tau'\tau = \tau' a$ for some $\tau' \in A - \mathfrak{p}$. But this is impossible since the left hand side is in $A - \mathfrak{p}$, while the right hand side is in $\mathfrak{p}$. Because of the minimality of $\mathfrak{p}$, there are no prime ideals strictly contained in $\mathfrak{p}$ that contain I_d. Hence the only prime ideal in the localization $A_{\mathfrak{p}}$ which contains $(I_d)_{\mathfrak{p}}$ is the maximal ideal $\mathfrak{p}_{\mathfrak{p}}$. Since the radical of $(I_d)_{\mathfrak{p}}$ is the intersection of all prime ideals containing it, we must have $\sqrt{(I_d)_{\mathfrak{p}}} = \mathfrak{p}_{\mathfrak{p}}$.

The localization $A_{\mathfrak{p}}$ is Noetherian and $B_{\mathfrak{p}}$ is certainly finitely generated as a module over $A_{\mathfrak{p}}$. It is easy to verify that the inclusion $A_{\mathfrak{p}} \subseteq B_{\mathfrak{p}}$ still induces a bijection

$$\mathrm{Hom}_{\mathbb{F}_p\text{-alg}}(B_{\mathfrak{p}}, k) \to \mathrm{Hom}_{\mathbb{F}_p\text{-alg}}(A_{\mathfrak{p}}, k)$$

for all algebraically closed fields k of characteristic p. If $B_{\mathfrak{p}}^{[p^s]} \subseteq A_{\mathfrak{p}}$ for some s, then $I_{d'}$ would not be proper for sufficiently large d', which would give us the desired contradiction. Thus we may reduce to the case where A is a local ring with maximal ideal $\mathfrak{p}$, which is the radical of I_d.

By Theorem A.5 in the appendix, an ideal in B is maximal if and only if its contraction to A is maximal. By Lemma 6.4, there is a unique prime ideal $\mathfrak{q}$ in B lying over $\mathfrak{p}$, hence B is a local ring with maximal ideal $\mathfrak{q}$. Any prime ideal in B containing $\mathfrak{p}B$ must contract to $\mathfrak{p}$, hence $\mathfrak{q}$ is the only prime ideal containing $\mathfrak{p}B$, so $\sqrt{\mathfrak{p}B} = \mathfrak{q}$. Since B is a finite module over a Noetherian ring, B is itself Noetherian as a ring. In a Noetherian ring, any ideal contains a power of its radical, thus there is some p-power n_1 such that $\mathfrak{q}^{[n_1]} \subseteq \mathfrak{p}B$. Similarly, since A is Noetherian, there is some p-power n_2 such that $\mathfrak{p}^{[n_2]} \subseteq I_d$, which implies $\mathfrak{p}^{[n_2]}B^{[p^d]} \subseteq A$. Let $n_3 = \max(n_2, p^d)$. Then

$$(\mathfrak{p}B)^{[n_3]} = \mathfrak{p}^{[n_3]}B^{[n_3]} \subseteq \mathfrak{p}^{[n_2]}B^{[p^d]} \subseteq A.$$

By Lemma 6.4, $(B/\mathfrak{q})^{[m]}$ is contained in $A/\mathfrak{p}$ for some p-power m. Hence $B^{[m]} \subseteq A + \mathfrak{q}$. Putting all this together we see that

$$B^{[mn_1n_3]} \subseteq A^{[n_1n_3]} + \mathfrak{q}^{[n_1n_3]} \subseteq A,$$

which is the desired contradiction. Hence f is an F-isomorphism.

Conversely let $f : A \to B$ be an F-isomorphism and let k be an algebraically closed field of characteristic p. To establish surjectivity of the induced map, let $\phi : A \to k$ be a ring homomorphism. Since all nilpotent elements must have trivial image, ϕ factors as

$$A \to A/\mathrm{ker(f)} \xrightarrow{\phi} k.$$

Now f induces an isomorphism $A/\mathrm{ker(f)} \cong f(A)$, so to prove that the induced map f^* is surjective, we need to extend $\phi : f(A) \to k$ to all of B. The kernel of ϕ is a prime ideal $\mathfrak{p}$ in $f(A)$. Since B is a finite $f(A)$-module, it follows from Theorem A.7 that there exists a prime ideal $\mathfrak{q}$ in B lying over $\mathfrak{p}$ and the field extension $Q(f(A)/\mathfrak{p}) \subseteq Q(B/\mathfrak{q})$ is finite. We have the following commutative diagram

$$\begin{tikzcd}
f(A) \arrow[r] \arrow[d, hook] & f(A)/\mathfrak{p} \arrow[r, hook] \arrow[d, hook] & \overline{Q}(f(A)/\mathfrak{p}) \arrow[r, hook] \arrow[d, equal] & k \\
B \arrow[r] & B/\mathfrak{q} \arrow[r, hook] & \overline{Q}(B/\mathfrak{q}). &
\end{tikzcd}$$

Since an algebraically closed field has no proper finite extension, it follows that $\overline{Q}(f(A)/\mathfrak{p}) = \overline{Q}(B/\mathfrak{q})$, hence ϕ extends to all of B. To establish injectivity let $\phi, \psi : B \to k$ such that $\phi(b) \neq \psi(b)$ for some $b \in B$. Since k is algebraically closed, the Fröbenius map $s \to s^{p^n}$ is an isomorphism, hence $\phi(b^{p^n}) \neq \psi(b^{p^n})$. By assumption there exists an $a \in A$ such that $f(a) = b^{p^n}$. But then $\phi \circ f(a) \neq \psi \circ f(a)$ as desired. □

Having established equivalence between the Theorems 6.1 and 6.3, it follows that the Quillen homomorphisms is indeed an F-isomorphism. This is still the case if we replace the ring $H(G, \mathbb{F}_p)$ with $H^*(G, \mathbb{F}_p)$ since all odd degree elements are nilpotent.

Example 6.7. Let $G = \langle x \rangle$ be a cyclic group of order p^2 with generator x, hence G has only one elementary abelian p-subgroup, namely a cyclic subgroup $P = \langle x^p \rangle$ of order p. The Quillen homomorphism is then

$$\mathrm{res}_{G,P} : H^*(G, \mathbb{F}_p) \to H^*(P, \mathbb{F}_p).$$

In cohomological dimension 1 this is pre-composition by the inclusion

$$\mathrm{Hom}(G, \mathbb{F}_p) \xrightarrow{\circ i} \mathrm{Hom}(P, \mathbb{F}_p),$$

which is the zero-map, showing that the Quillen homomorphism is neither injective nor surjective in general.

A Commutative Algebra

The appendix contains various results from commutative algebra. Throughout this section all rings are associative, commutative, unital rings.

A.1 Integral Dependence

Definition A.1. Let $A \subseteq B$ be rings. An element $x \in B$ is called integral over A if it is a root of a monic polynomial with coefficients in A, hence satisfies an equation of the form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0, \quad a_i \in A.$$

Theorem A.2. *Let $A \subseteq B$ be rings. The following are equivalent*

1. *$x \in B$ is integral over A.*
2. *$A[x]$ is a finitely generated A-module.*
3. *$A[x]$ is contained in a subring C of B such that C is finitely generated as an A-module.*

A proof of the above theorem can be found in [1, Prop. 5.1]. An easy consequence of the above theorem is the following.

Corollary A.3. *Let $x_1, \ldots, x_n$ be elements of B, each of which is integral over A. Then $A[x_1, \ldots, x_n]$ is a finitely generated A-module.*

Let C denote the elements of B which are integral over A. If $x, y \in C$ then $A[x, y]$ is finitely generated as an A-module, hence $x \pm y$ and xy are elements of C by Theorem A.2 part 3, and we conclude that C is a subring of B. The subring C is called the integral closure of A in B. If $C = A$ then A is called integrally closed, and if $C = B$, we say that B is integral over A. Let $A \subseteq B$ be commutative rings. The above theorems combine to the following two statements:

- If B is a finitely generated A-module, then B is integral over A.
- If B is integral over A and B is a finitely generated A-algebra, then B is a finitely generated A-module.

If I is an ideal in B, then $I \cap A$ is an ideal in A. If B is integral over A, then clearly $B/\mathfrak{a}$ is integral over $A/(I \cap A)$ since we may just reduce a given equation modulo I. Likewise, one may verify that if B is integral over A and S is a multiplicatively closed subset of A, then $S^{-1}B$ is integral over $S^{-1}A$.

Theorem A.4. *Let $A \subseteq B$ be integral domains, B integral over A. Then B is a field if and only if A is a field.*

Proof. Assume that A is a field and let $b \in B$, $b \neq 0$. Let

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

be an equation of integral dependence of minimal degree, in particular $b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1 \neq 0$. Since

$$b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) = -a_0$$

and B is an integral domain, we must have $a_0 \neq 0$. But then $-a_0^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1)$ is an inverse of b, hence B is a field. Conversely assume that B is a field and let $a \in A$, $a \neq 0$. Then $a^{-1} \in B$, hence we have an equation

$$a^{-n} = a_{n-1}a^{1-n} + \cdots + a_1 a^{-1} + a_0.$$

Multiplying the equation by a^{n-1}, we see that $a^{-1} = a_{n-1} + \cdots + a_1 a^{n-2} + a_0 a^{n-1} \in A$, hence A is a field. □

Corollary A.5. *Let $A \subseteq B$ be rings, B integral over A. Let $\mathfrak{p}$ be a prime ideal in B. Then $\mathfrak{p}$ is a maximal ideal in B if and only if $\mathfrak{p} \cap A$ is a maximal ideal in A.*

Proof. Since $B/\mathfrak{p}$ and $A/(\mathfrak{p} \cap A)$ are both integral domains, and $B/\mathfrak{p}$ is integral over $A/(\mathfrak{p} \cap A)$, the corollary follows immediately from the theorem. □

Theorem A.6. *Let $A \subseteq B$ be rings, B integral over A. Let $\mathfrak{p}, \mathfrak{p}'$ be a prime ideals in B such that $\mathfrak{p} \subseteq \mathfrak{p}'$. If $\mathfrak{p} \cap A = \mathfrak{p}' \cap A$ then $\mathfrak{p} = \mathfrak{p}'$.*

Proof. Let $\mathfrak{q}$ denote the ideal $\mathfrak{p} \cap A = \mathfrak{p}' \cap A$. Since the contraction of a prime ideal is prime, $S = A - \mathfrak{q}$ is a multiplicatively closed subset of A. Hence $B_\mathfrak{q}$ is integral over $A_\mathfrak{q}$. Let $\mathfrak{m}$ be the extension of $\mathfrak{q}$ in $A_\mathfrak{q}$ and let $\mathfrak{n}, \mathfrak{n}'$ be the extensions of $\mathfrak{p}, \mathfrak{p}'$ in $B_\mathfrak{q}$. Then $\mathfrak{m}$ is a maximal ideal of $A_\mathfrak{q}$, $\mathfrak{n} \subseteq \mathfrak{n}'$ and $\mathfrak{n} \cap A_\mathfrak{q} = \mathfrak{n}' \cap A_\mathfrak{q} = \mathfrak{m}$. By Theorem A.5, $\mathfrak{n} \subseteq \mathfrak{n}'$ are both maximal so $\mathfrak{n} = \mathfrak{n}'$. We conclude that $\mathfrak{p} = \mathfrak{p}'$. □

Theorem A.7. *Let $A \subseteq B$ be rings, B integral over A. Let $\mathfrak{p}$ be a prime ideal of A. Then there exists a prime ideal $\mathfrak{q}$ in B such that $\mathfrak{q} \cap A = \mathfrak{p}$.*

Proof. As before $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$. We have the following commutative diagram

$$\begin{tikzcd}
A \arrow[r, hook] \arrow[d, "\alpha"'] & B \arrow[d, "\beta"] \\
A_\mathfrak{p} \arrow[r, hook] & B_\mathfrak{p}
\end{tikzcd}$$

Recall that there is a one-to-one correspondence between the prime ideals in A not meeting $\mathfrak{p}$ and the prime ideals in $A_\mathfrak{p}$

$$\mathfrak{q} \subseteq A_\mathfrak{p} \leftrightarrow \alpha^{-1}(\mathfrak{q}) \subseteq A.$$

The prime ideal $\mathfrak{p}$ corresponds to the unique maximal ideal in the local ring $A_\mathfrak{p}$. Let $\mathfrak{m}$ be a maximal ideal of $B_\mathfrak{p}$. Then $\mathfrak{n} = \mathfrak{m} \cap A_\mathfrak{p}$ is the unique maximal ideal in $A_\mathfrak{p}$ by Corollary A.5. Let $\mathfrak{q} = \beta^{-1}(\mathfrak{m})$. Then $\mathfrak{q}$ is a prime ideal in B and $\alpha^{-1}(\mathfrak{n}) = \mathfrak{q} \cap A$. Hence $\mathfrak{q} \cap A = \mathfrak{p}$ as desired. □

Theorem A.8 (Going-up Theorem)**.** *Let $A \subseteq B$ be rings, B integral over A. Let $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_n$ be a chain of prime ideals in A and let $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_m$ be a chain of prime ideals in B with $m < n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$. Then the chain in B can be extended to a chain of length n, $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_m$, with $\mathfrak{q}_i \cap A = \mathfrak{p}_i$.*

Proof. By induction it is enough to consider the case where $m = 1$ and $n = 2$. Since $\mathfrak{q}_1 = \mathfrak{p}_1 \cap A$, $B/\mathfrak{q}_1$ is integral over $A/\mathfrak{p}_1$. Let $\overline{\mathfrak{p}}_2$ denote the image of $\mathfrak{p}_2$ in the quotient ring $A/\mathfrak{p}_1$. By Theorem A.7, there exist a prime ideal $\overline{\mathfrak{q}}_2$ in $B/\mathfrak{q}_1$ such that $\overline{\mathfrak{q}}_2 \cap A/\mathfrak{p}_1 = \overline{\mathfrak{p}}_2$. The pre-image of $\overline{\mathfrak{q}}_2$ is a prime ideal in B with the desired properties. □

A.2 Krull Dimension

Definition A.9. Let A be a ring. The Krull dimension of A, denoted dim$A$, is the largest number of sharp inclusion appearing in a chain of prime ideals

$$\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_n$$

in A. If no such upper bound exists, we set dim$A = \infty$.

We refer the following basic result concerning the Krull dimension of polynomial rings. A proof can be found in [18, DIM4, Kor. 4.4].

Theorem A.10. *Let A be a Noetherian ring, $A \neq 0$. Then dim$A[x]$ = dim$A + 1$.*

Let $A_1, \ldots, A_n$ be rings and consider the product $A = \prod_{i=1}^n A_i$. A prime ideal in A must be of the form

$$A_1 \times \cdots \times A_{i-1} \times \mathfrak{p}_i \times A_{i+1} \times \cdots \times A_n,$$

for a prime ideal $\mathfrak{p}_\mathfrak{i} \subseteq A_i$, hence dim$A$ = max(dimA_i).

Theorem A.11. *Let $A \subseteq B$ be rings, B integral over A. Then dim$A$ =dim$B$.*

Proof. Let $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ be a chain of prime ideals in B. This gives rise to a chain of prime ideals in A, namely

$$\mathfrak{p}_1 \cap A \subseteq \cdots \subseteq \mathfrak{p}_n \cap A.$$

By Theorem A.6, the inclusions are still sharp, hence dim$A$ $\geq$dim$B$. Conversely, let $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_n$ be a chain of prime ideals in A. By Theorem A.7, there exists a prime ideal $\mathfrak{q}_1$ in B such that $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. Now it follows from Theorem A.8 that there exists a chain of prime ideals $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_n$ with $\mathfrak{q}_i \cap A = \mathfrak{p}_i$. Since the $\mathfrak{p}_i$'s are distinct, the inclusions in the chain must be sharp, hence dim$A$ $\leq$dim$B$. □

A.3 Graded Commutative Rings

Definition A.12. A graded ring is a ring R with a direct sum decomposition

$$R = \bigoplus_{i=0}^{\infty} R_i$$

of abelian subgroups such that $R_i R_j \subseteq R_{i+j}$ for all $i, j \geq 0$. A graded right R-module is a right R-module M with a direct sum decomposition

$$M = \bigoplus_{i=0}^{\infty} M_i$$

of abelian subgroups such that $R_i M_j \subseteq M_{i+j}$ for all $i, j \geq 0$. A graded R-algebra is an R-algebra A, which is both a graded ring and a graded R-module.

An element $r \in R$ is called homogeneous of degree i if $r \in R_i$, and we write $\deg(r) = i$. A ring homomorphism $\phi : R \to S$ of graded rings is called homogeneous if $\phi(R_i) \subseteq S_i$ for all $i \geq 0$. Note that R_0 is a subring of R, and each R_i is an R_0-module. Any ring S may trivially be considered as a graded ring with $S_0 = S$ and $S_i = 0$ for all other i. We have the following useful theorem about graded rings. A proof can be found in [1, Prop. 10.7]

Theorem A.13. *The following are equivalent for a graded ring R:*

1. *R is a Noetherian ring.*
2. *R_0 is a Noetherian ring and R is finitely generated as an R_0-algebra.*

Definition A.14. A graded ring R is called graded commutative if

$$xy = (-1)^{\deg(x)\deg(y)} yx$$

for all homogeneous elements $x, y \in R$.

Note that elements of even degree always commute, and if 2 is invertible in R, then the square of an element of odd degree is zero. Of course, a graded ring R may be commutative in the usual sense, in which case we say that it is commutative graded.

Let k be a field of characteristic p and let A be a graded commutative k-algebra. If $p = 2$ then A is commutative in the usual sense. If $p > 2$ we shall consider the following commutative subring. Let A^{ev} denote the subring of A consisting of elements in even degree, i.e.

$$A^{ev} = \bigoplus_{i=1}^{\infty} A_{2i}.$$

Remark A.15. If A is finitely generated as a k-algebra, then so is A^{ev}. The k-algebra generators of A of even degree and the products of pair of k-algebra generators of odd degree form a generating set of A^{ev}.

Theorem A.16. *Let $A \subseteq B$ be graded commutative k-algebras, both finitely generated over k. Suppose that B is finitely generated as a module over A and that $A_0 = k$. Then B^{ev} is finitely generated as a module over A^{ev}.*

Proof. By Theorem A.2, B is integral over A. Let $b \in B^{ev}$ and let

$$b^n + a_1 b^{n-1} + \cdots + a_{n-1} b + a_n = 0, \ a_i \in A$$

be an equation of integral dependence. We may assume without loss of generality that b is homogeneous, say $\deg(b) = m$. The sum of the terms in the above equation which live in dimension $m \cdot n$ equals zero and must have coefficients in A^{ev}, hence B^{ev} is integral over A^{ev}. Since B^{ev} is finitely generated as a k-algebra, it is in particular finitely generated as an A^{ev}-algebra, hence B^{ev} is a finite A^{ev}-module. □

B Finite p-Groups

Let p be a prime. This section contains some basic results regarding finite p-groups.

Definition B.1. A finite p-group is a group G of order p^a for some $a \geq 1$.

Theorem B.2. *Suppose G is a group of order p^a, $a \geq 1$. Then*

1. *The center of G is non trivial, $Z(G) \neq 1$.*
2. *If H is a non-trivial normal subgroup of G, then H meets the center non-trivially.*
3. *If H is a normal subgroup of G, then H contains a subgroup of order p^b that is normal in G for each divisor p^b of $|H|$*
4. *Every maximal subgroup of G is of index p and normal in G.*

A proof can be found in [4, Capter 6, Thm 1]. We will derive some easy consequences, which will be useful in the thesis.

Corollary B.3. *Suppose G is a group of order p^a, $a \geq 1$. Then there exists an increasing sequence of normal subgroups*

$$1 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_{a-1} \trianglelefteq G$$

so that $|N_i| = p^i$ for all i.

Proof. We proceed by induction. If $a = 1$ the statement is trivial. Let $a \geq 2$ and assume that the statement is true for groups of order p^{a-1}. Since $Z(G)$ is a non-trivial normal subgroup of G, it contains a subgroup N_1 of order p such that $N_1 \trianglelefteq G$. G/N_1 is a p-group of order p^{a-1}. By induction G/N_1 has a normal series as above. The preimage of this series in G together with N_1 form the desired normal series of G. □

Corollary B.4. *Suppose that G is a finite p-group. Then the following are equivalent for a subgroup $H \leq G$.*

1. *H is maximal and normal.*
2. *H is maximal.*
3. *$[G : H] = p$.*

Proof. Clearly 1. implies 2. By Theorem B.2, 2. implies 1. and 3. If H is of index p and $H \leq K \leq G$, then the equality $[G : H] = [G : K] \cdot [K : H]$ implies $K = G$, hence H is maximal, thus 3. implies 2. □

References

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[2] D. J. Benson. *Representations and cohomology. I*, volume 30 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, 1991. Basic representation theory of finite groups and associative algebras.

[3] D. J. Benson. *Representations and cohomology. II*, volume 31 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, 1991. Cohomology of groups and modules.

[4] D. S. Dummit and R. M. Foote. *Abstract Algebra.* John Wiley and Sons, Inc., 2004.

[5] Leonard Evens. The cohomology ring of a finite group. *Trans. Amer. Math. Soc.*, 101:224–239, 1961.

[6] Leonard Evens. A generalization of the transfer map in the cohomology of groups. *Trans. Amer. Math. Soc.*, 108:54–65, 1963.

[7] Leonard Evens. *The cohomology of groups.* Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1991. Oxford Science Publications.

[8] Allen Hatcher. *Algebraic topology.* Cambridge University Press, Cambridge, 2002.

[9] P. J. Hilton and U. Stammbach. *A course in homological algebra*, volume 4 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1997.

[10] B. Huppert. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, 1967.

[11] Dale Husemoller. *Fibre bundles*, volume 20 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, third edition, 1994.

[12] Paul J. McCarthy. *Algebraic extensions of fields.* Dover Publications Inc., New York, second edition, 1991.

[13] John McCleary. *A user's guide to spectral sequences*, volume 58 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, second edition, 2001.

[14] Stephen A. Mitchell. *Notes on principal bundles and classifying spaces.* Quillen Seminar, Spring 2006.

[15] D. Quillen and B. B. Venkov. Cohomology of finite groups and elementary abelian subgroups. *Topology*, 11:317–318, 1972.

[16] Daniel Quillen. The spectrum of an equivariant cohomology ring. I, II. *Ann. of Math. (2)*, 94:549–572; ibid. (2) 94 (1971), 573–602, 1971.

[17] Jean-Pierre Serre. Sur la dimension cohomologique des groupes profinis. *Topology*, 3:413–420, 1965.

[18] Anders Thorup. *Kommutativ Algbera.* Matematisk Afdeling, Københavns Universitet, 2005.

[19] B. B. Venkov. Cohomology algebras for some classifying spaces. *Dokl. Akad. Nauk SSSR*, 127:943–944, 1959.