Group cohomology, Steenrod operations and Massey higher products

Béatrice I. Chetard

December 9, 2016

Abstract

We present detailed calculations of the cohomology ring of several small 2-groups, together with the action of the Steenrod algebra on said cohomology.

Introduction

The cohomology of a group $G$ was first defined sometime during World War II, independently by Eilenberg and Mac Lane in Columbia and Chicago, Freudenthal in Amsterdam, and Hopf in Switzerland. Communication was difficult then, and the fact that four mathematicians in three different countries came up with the same idea at the same time shows how pressing the need for the concept had become. A few years after the end of the war, in 1950, Hochschild used the term Galois cohomology for the first time in a paper where he studied local class field theory. Since then, Galois cohomology has become a prevalent part of abstract algebra and an active area of research.

One of the great challenges of Galois theory is that of determining absolute Galois groups, and group cohomology provides us with tools to understand these. For example, let $F$ be an arbitrary field and $F_{\text{sep}}$ its separable closure. The absolute Galois group $G_F := \text{Gal}(F_{\text{sep}}|F)$ of $F$ can be written as the limit of the Galois groups of the finite subextensions $K|F$ of $F_{\text{sep}}$, and its cohomology groups can be calculated as the colimits of the cohomology groups of the (finite) Gal($K|F$). From an infinite problem, we reduce to a finite one.

The first step towards understanding absolute Galois groups is therefore to understand how to compute finite group cohomology, and our aim was to achieve this by exploring as wide an array of tools as possible, while keeping the complexity of the computations manageable. This paper presents a variety of hand computations of the cohomology of small 2-groups, with coefficients in $\mathbb{F}_2$, together with the ring structure and the action of the Steenrod squares.

The cohomology of the smallest nontrivial group, $C_2$, is computed directly, using a projective resolution and the definition of the cup product. This is the corner stone of our computations, as the result will be heavily used in the sequel. We then move on to the finite product $C_n^2$, whose cohomology can be deduced directly from that of $C_2$ by the Künneth formula. The cohomology of $C_4$ is computed via the Lyndon-Hochschild-Serre spectral sequence associated to its normal subgroup $C_2$, and the result is then generalised to $C_2^n$ via the use of the universal coefficient theorem, and, once again, the subgroup $C_2$. The last approach we chose is somewhat different, and is adapted from a method presented by Jon Carlson in Modules and group algebras ([Car96]): the cohomology is computed using the correspondence between elements of the $n$-th Ext group Ext^n_{kG}(k,k) and homotopy classes of chain maps of degree $-n$ from a projective resolution of $k$ to itself.

The action of the Steenrod squares on the cohomology rings is straightforward combinatorics for $C_2$ and $C_2^n$, because these are generated by classes of degree 1 and have no nilpotent elements. The computation for $C_4$ is more interesting, as it involves the definition of $Sq^1$ as the Bockstein homomorphism. Finally, the
case $D_8$ will require heavy use of the characterisation of the second cohomology groups $H^2(G, A)$ as classes of abelian extensions of $G$ by $A$.

The main source I learned group cohomology from is [Wei94], with some occasional browsing of [NSW00] and [Bro82] for an additional point of view. The diagrammatic approach in section 2.5 is adapted from [Car96]. Historical facts come from [Wei99].

## Contents

1 Definitions 2
   1.1 Basic group cohomology 2
   1.2 Steenrod operations 4
   1.3 Massey higher products in low-dimensional group cohomology 5

2 Calculating cohomology rings 6
   2.1 Working directly from the definitions: the cyclic group $C_2$ 6
   2.2 The Künneth formula and the product of cyclic groups 7
   2.3 The Lyndon-Hochschild-Serre spectral sequence: the cyclic group $C_4$ 7
   2.4 The universal coefficient theorem applied to the group $C_{2^n}$ 9
   2.5 Cohomology with pictures: Jon Carlson’s diagrams 10

3 Steenrod operations 13
   3.1 Operations on $H^*(C_2, F_2)$ 13
   3.2 Operations on $H^*(C_4, F_2)$ 13
   3.3 Operations on $H^*(C_4, F_2)$ 13
   3.4 Operations on $H^*(D_8, F_2)$ 14

4 Towards Massey higher products 15

## 1 Definitions

### 1.1 Basic group cohomology

Let $G$ be a group, $k$ a commutative ring and $A$ a $kG$-module.

**Definition.** We define

$$H^i(G, A) := \text{Ext}^i_{kG}(k, A)$$

the $i$-th **cohomology group of $G$ with coefficients in $A$**, and

$$H_i(G, A) := \text{Tor}^i_{kG}(k, A)$$

the $i$-th **homology group of $G$ with coefficients in $A$**.

The definition of group cohomology is obviously valid for any action of $G$ on $A$. However, in the sequel, unless mentioned otherwise, $G$ will be understood to act trivially on $A$. If $P \rightarrow k$ is a projective resolution, an element $x \in \text{Ext}^i_{kG}(k, A)$ is an equivalence class of morphisms $P_i \rightarrow k$. In the sequel, we will often denote any representative of this equivalence class by $x$ as well.
$H^*(G; k)$ has the structure of a graded ring, with multiplication given as follows: let $P_i \to k$ be a projective resolution of $k$. A projective resolution of $k$ by $G \times G$-modules is given by the chain complex $P \otimes P$ defined by

$$(P \otimes_k P)_n := \bigoplus_{i+j=n} (P_i \otimes_k P_j)$$

together with the differentials

$$\partial(a \otimes b) = \partial a \otimes b + (-1)^{|a|} a \otimes \partial b$$

There is a natural homomorphism

$$\mu : \text{Hom}_{kG}(P, k) \otimes \text{Hom}_{kG}(P, k) \to \text{Hom}_{kG \times G}(P \otimes P, k)$$

$$\mu(f \otimes f')(a \otimes b) = f(a)f'(b)$$

where $a \in P_i$, $b \in P_j$ for some $i, j$. This homomorphism induces a homomorphism $\times : H^*(G, k) \to H^*(G \times G, k)$ on cohomology, the cross product. The cohomology product $\smile$, called the cup product\(^1\) is then defined as the composite of the cross product with the cohomology of the diagonal map

$$\Delta^* : H^*(G \times G; k) \to H^*(G; k)$$

This gives to $H^*(G, K)$ the structure of a graded commutative ring, that is

$$a \smile b = (-1)^{|a||b|} b \smile a$$

where $|a| = n$ whenever $a \in H^n(G, k)$.

**Low-dimensional homology and cohomology**

There are additional characterizations of low-dimensional cohomology groups, that we will make use of later.

**Proposition 1.1** ([Wei94, Prop. 6.1.11]). For any group $G$ and trivial $kG$-module $A$,

$$H^1(G, A) \cong \text{Hom}_{\text{Grp}}(G, A) \cong \text{Hom}_{\text{Ab}}\left(\frac{G}{[G, G]}, A\right)$$

**Theorem 1.2** ([Wei94, Th. 6.6.3]). Equivalence classes of extensions of $G$ by $A$

$$0 \to A \to E \to G \to 1$$

are in 1-1 correspondence with the cohomology group $H^2(G, A)$, where two extensions $E$ and $E'$ are equivalent if there is a homomorphism $E \to E'$ making the following diagram commute:

The correspondence is constructed as follows: for an extension

$$0 \to A \to E \to G \to 1$$

\(^1\)In the sequel, we will often omit the symbol $\smile$ and write $xy$ for $x \smile y$. 
choose a set-theoretic section \( s : G \to E \) of \( \pi \) such that \( s(1) = 1 \), and define the factor set determined by \( E \) and \( s \) as

\[
\begin{cases}
[ ]_s : G \times G \to A \\
[g,h]_s = s(g)s(h)s(gh)^{-1}
\end{cases}
\]

it can be shown that \([ ]_s\) corresponds uniquely to a 2-cocycle in the bar resolution of \( A \), a particular projective resolution\(^2\) of \( A \). This means, in particular, that a split extension corresponds to the element \( 0 \in H^2(G,A) \), since then \( s \) can be chosen to be a homomorphism and \([ ]_s = 0\).

### 1.2 Steenrod operations

Consider \( R, S \) as additive groups. A cohomology operation of type \((R, n; S, m)\) is a natural transformation

\[
\theta : H^n(\_; R) \to H^m(\_; S)
\]

**Bockstein homomorphism**

Consider the short exact sequence of abelian groups

\[
0 \to G \xrightarrow{i} H \xrightarrow{j} K \to 0
\]

This short exact sequence yields a long exact sequence

\[
\cdots \to H^n(X; G) \xrightarrow{\iota^*} H^n(X; H) \xrightarrow{j^*} H^n(X; K) \xrightarrow{\partial} H^{n+1}(X; G) \to \cdots
\]

The map \( \partial : H^n(X; K) \to H^{n+1}(X; G) \) is called the Bockstein homomorphism associated to the short exact sequence (1). In particular, the sequence

\[
0 \to \mathbb{Z}/p \xrightarrow{i} \mathbb{Z}/p^2 \xrightarrow{j} \mathbb{Z}/p \to 0
\]

yields a cohomology operation of type \((\mathbb{Z}/p, n ; \mathbb{Z}/p, n + 1)\), often denoted \( \beta \). This particular instance of the Bockstein homomorphism has two interesting properties:

- If \( p > 2 \) then \( \beta \beta = 0 \)
- If \( \cup \) denotes the cup product on \( H^*(X; \mathbb{Z}/p) \), \( \beta(a \cup b) = \beta(a) \cup b + (-1)^{\dim a} \cup \beta(b) \)

**Steenrod squares**

The Steenrod squares are a family of cohomology operations \( \{Sq^n\} \) of type \((\mathbb{Z}/2, m ; \mathbb{Z}/2, m + n)\), defined as the unique operations satisfying the following axioms:

- (i) \( Sq^n \) is a cohomology operation of type \((\mathbb{Z}/2, m ; \mathbb{Z}/2, m + n)\)
- (ii) \( Sq^0 \) is the identity homomorphism
- (iii) \( Sq^n \) is the cup square on classes of dimension \( n \) (that is, \( Sq^n(u) = u \cup u \))
- (iv) If \( |u| < n \) then \( Sq^n(u) = 0 \)
- (v) Cartan formula:

\[
Sq^n(u \cup v) = \sum_{i+j=n} (Sq^i u) \cup (Sq^j v)
\]

\(^2\)See [Wei94, §6.5].
If we try to fit the defining system into a matrix as follows:

\[
\begin{pmatrix}
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & 0 & \cdot & \cdot & \cdot \\
0 & 0 & 0 & 0 & \cdot & \cdot \\
0 & 0 & 0 & 0 & 0 & \cdot \\
\end{pmatrix}
\]

we obtain an element of \( \overline{H}_{n+1}(k) \), the quotient of the multiplicative group \( U_{n+1}(k) \) of matrices that agree with the identity on the diagonal, by the subgroup \( Z_{n+1}(k) \) of matrices that are zero everywhere except on the diagonal (where they agree on the identity) and in the top right corner. Note that \( Z_{n+1}(k) \) is a subgroup of the centre of \( U_{n+1}(k) \), so that the quotient \( \overline{H}_{n+1}(k) \) is well-defined.

There is actually a correspondence between these matrices and the defining systems for the Massey product:

**Theorem 1.3** ([Dwy75, Th. 2.4]). Let \( (u_1, \ldots, u_n) \) be elements of \( H^1(G, k) \). There is a one-to-one correspondence between defining systems \( M \) for the higher Massey product \( (u_1, \ldots, u_n) \) and group homomorphisms

\[ \phi : G \rightarrow U_{n+1}(k) \]

that have \(-u_1, \ldots, -u_n\) as near-diagonal components.

\(^3\)See [Kra66] for details of definitions and proofs, and [McC01, §8.2] for a discussion of the triple Massey product.
2 Calculating cohomology rings

2.1 Working directly from the definitions: the cyclic group $C_2$

Let $C_{2^n}$ be the cyclic group of order $2^n$, generated by $\sigma$. To calculate $H^*(C_{2^n}, \mathbb{F}_2)$, we need a projective resolution of $\mathbb{F}_2$ by $\mathbb{F}_2C_{2^n}$ modules. Consider the element of $\mathbb{F}_2C_{2^n}$:

$$N := 1 + \sigma + \sigma^2 + \ldots + \sigma^{n-1}$$

and note that $(\sigma + 1)N = 0$ in $\mathbb{F}_2C_{2^n}$. There is a projective resolution of $\mathbb{F}_2$ by $\mathbb{F}_2C_{2^n}$-modules given by:

$$\cdots \rightarrow \mathbb{F}_2C_{2^n} \xrightarrow{(\sigma+1)} \mathbb{F}_2C_{2^n} \rightarrow \mathbb{F}_2C_{2^n} \rightarrow \mathbb{F}_2 \rightarrow 0$$

We then apply the functor $\text{Hom}_{\mathbb{F}_2}(\mathbb{F}_2C_{2^n}, -)$ to this sequence and chop off the last term to obtain

$$\cdots \rightarrow \text{Hom}_{\mathbb{F}_2}(\mathbb{F}_2C_{2^n}, \mathbb{F}_2) \rightarrow \text{Hom}_{\mathbb{F}_2}(\mathbb{F}_2C_{2^n}, \mathbb{F}_2) \rightarrow 0$$

that is,

$$\cdots \rightarrow \mathbb{F}_2 \rightarrow \mathbb{F}_2 \rightarrow \mathbb{F}_2 \rightarrow \mathbb{F}_2 \rightarrow 0$$

Since the differentials are all 0, we have

$$H^i(C_{2^n}; \mathbb{F}_2) \cong \mathbb{F}_2, \ i \geq 0$$

We now restrict to the case $n = 1$, that is, we determine the cohomology ring $H^*(C_2, \mathbb{F}_2)$. Note that in the projective resolution above, all boundary maps are multiplication by $(\sigma + 1)$. Let $x \in H^1(C_2, \mathbb{F}_2)$ be a generator (that is, any nonzero homomorphism $\mathbb{F}_2C_2 \rightarrow \mathbb{F}_2$). We want to show that the cup power $x^n$ generates $H^n(C_2, \mathbb{F}_2)$, which boils down to showing that the morphism $- \cup x : H^i(C_2, \mathbb{F}_2) \rightarrow H^{i+1}(C_2, \mathbb{F}_2)$ is injective.

Now let $y : C_2 \mathbb{F}_2 \rightarrow \mathbb{F}_2$ be a cocycle of degree $n$. By definition of the cup product, we have

$$y \cup x = \Delta^*(y \times x)$$

that is, $yx$ is the composition

$$H^n(C_2, \mathbb{F}_2) \otimes H^1(C_2, \mathbb{F}_2) \xrightarrow{x} H^{n+1}(C_2 \times C_2, \mathbb{F}_2) \xrightarrow{\Delta^*} H^{n+1}(C_2, \mathbb{F}_2)$$

The cocycle $y \times x$ is the class of a homomorphism $\bigoplus_{i \leq n} \mathbb{F}_2C_2 \otimes \mathbb{F}_2C_2 \rightarrow \mathbb{F}_2$, whose values on the generators of $\bigoplus_{i \leq n} \mathbb{F}_2C_2 \otimes \mathbb{F}_2C_2$ are given by

$$y \times x(a \otimes b) = y(a)x(b)$$

So, in particular, $y \cup x(1) = y \times x(1 \otimes 1) = y(1)$ (since $x$ is a nonzero homomorphism one must have $x(1) = 1$). To determine whether $y \cup x$ is zero in the cohomology, we consider an arbitrary homomorphism $z : \bigoplus \mathbb{F}_2C_2 \otimes \mathbb{F}_2C_2 \rightarrow \mathbb{F}_2$. Then

$$dz(a \otimes b) = z(da \otimes b) + z(a \otimes db)$$

$$= z((\sigma + 1)a \otimes b) + z(a \otimes (\sigma + 1)b)$$

$$= z(\sigma a \otimes b) + z(a \otimes \sigma b)$$

$$= z(a \otimes \sigma^{-1}b) + z(a \otimes \sigma b)$$

$$= 0$$
Thus there are no nonzero coboundaries, and since \( y \sim x(1) = y(1) \), the cup product \( yx \) is non zero whenever \( y \) is nonzero. So \( x^n \) generates \( H^n(C_2, \mathbb{F}_2) \). We have proven:

\[
H^*(C_2, \mathbb{F}_2) \cong \mathbb{F}_2[x]
\]

where \(|x| = 1\).

Remark. It is usually straightforward enough to find projective resolutions of \( \mathbb{F}_2 \) for the small groups that are discussed in this paper; however there are much more interesting methods that can be applied to determine the cohomology ring structure.

2.2 The Künneth formula and the product of cyclic groups

We now propose to calculate the cohomology ring of the product \( C_2 \times C_2 \). To do this, we can use the Künneth formula, a general homological algebra statement about the homology of tensor products of chain complexes. Applied to projective resolutions, it yields the following group cohomology statement:

**Proposition 2.1.** Let \( G \) and \( H \) be any two groups. Then for every \( n \geq 1 \) there is a split exact sequence:

\[
0 \to \bigoplus_{p+q=n} H^p(G, k) \otimes_k H^q(H, k) \xrightarrow{\times} H^*(G \times H, k) \to \bigoplus_{p+q=n+1} \text{Tor}_k^1(H^p(G, k), H^q(H, k)) \to 0
\]

where the first morphism is the cross product \( \times \).

Note that when \( k \) is a field, the torsion term vanishes and the cross product is actually an isomorphism of algebras.

The calculation can be done via a straightforward induction on \( N \). For \( N = 2 \), we have:

\[
H^*(C_2 \times C_2, \mathbb{F}_2) \cong \bigoplus_{i+j=n} \mathbb{F}_2 \cong \oplus \mathbb{F}_2
\]

The isomorphism is given by the cross product and so \( H^*(C_2 \times C_2, \mathbb{F}_2) \) is generated by classes of the form \( x^p \times y^n-y^p \), where \( x \in H^1(C_2 \times C_2, \mathbb{F}_2) \) is a projection on the first factor and \( y \in H^1(C_2 \times C_2, \mathbb{F}_2) \) on the second. This induces on \( H^*(C_2 \times C_2, \mathbb{F}_2) \) a graded ring structure, and:

\[
H^*(C_2 \times C_2, \mathbb{F}_2) = \mathbb{F}_2[x, y]
\]

with \(|x| = |y| = 1\). By induction we obtain:

\[
H^*(C_2^N, \mathbb{F}_2) \cong \mathbb{F}_2[x_1, \cdots, x_N]
\]

2.3 The Lyndon-Hochschild-Serre spectral sequence: the cyclic group \( C_4 \)

As seen in section 2.1, the group structure of the cohomology of \( C_4 \) is the following:

\[
H^*(C_4, \mathbb{F}_2) \cong \mathbb{F}_2, \ n \geq 0
\]

To compute the cohomology of \( C_4 \), we will make use of the Lyndon-Hochschild-Serre spectral sequence:

**Proposition 2.2 ([Wei94, Prop. 6.8.2]).** Let \( G \) be any group and \( H \) a normal subgroup of \( G \). Then there is a convergent first quadrant spectral sequence

\[
E_2^{p,q} = H^p(G/H, H^q(H, A)) \Rightarrow H^{p+q}(G, A)
\]
Where the abelian group $H^q(H, A)$ is made into a $G/H$-module by the action of conjugation by an element of $G/H$ (see [Wei94, Cor. 6.7.9]).

$C_4$ contains the normal subgroup $C_2$, so we can apply the Lyndon-Hochschild-Serre spectral sequence to the extension

$$0 \to C_2 \to C_4 \to C_2 \to 0$$

and obtain

$$E^0_{2q} \cong H^q(C_4/C_2, H^p(C_2, F_2)) \implies H^{p+q}(C_4, F_2)$$

Since $C_2$ is in the center of $C_4$, the conjugation action of $C_4/C_2$ on the cohomology of $C_2$ is trivial. Thus we have $E^0_{2q} = H^q(C_2, F_2)$ with $C_2$ acting trivially on $F_2$, that is, $E^0_{2q} = F_2$ for any $p, q$.

By definition, each group $E^0_{2q}$ is generated by $x^p \otimes y^q$. Observe the following:

- $d^2$ is a derivation, so for $y^{2n} \in H^{2n}(C_4/C_2, F_2)$
  $$d^2(y^{2n}) = 2d^2(y^n)y^n = 0$$

  So all the groups $E^0_{2q}$ survive on page 3.

- Since there are no nonzero differentials coming in or out of it, $E^1_{0,0}$ survives until $E_\infty$, and $H^1(C_4, F_2) = F_2$, so that $E^1_{0,0} = 0$. Thus the differential $d^2_{0,1}$ must be injective, whence an isomorphism. So $d^2(y) = x^2$.

- Repeating this reasoning and keeping in mind that the differential respects the multiplicative structure, that is, $d^2(a \otimes b) = d^2a \otimes b + a \otimes d^2b$, we obtain the following page 3:

  which allows us to conclude
  $$H^*(C_4, F_2) \cong F_2[x, y]/(x^2)$$

  with $|x| = 1, |y| = 2$.

**Remark.** The spectral sequence can also be used to calculate the multiplicative structure of $H^*(C^N_2, F_2)$: for $N = 2$, $E^0_{2q} \cong F_2$ and the sequence converges to

$$H^{p+q}(C^N_2, F_2) \cong \bigoplus_{i+j=p+q} F_2$$

so that all groups of page 2 survive until $E_\infty$. Thus the sequence collapses on page 2 and we obtain the desired multiplicative structure.
The result can be extended to any group of the form \( C_{2^n}, n \geq 2 \). Then we have \( H^n(C_{2^n}, \mathbb{F}_2) = \mathbb{F}_2 \) for \( n \geq 0 \) and the spectral sequence has exactly the same form as that of \( C_4 \). We obtain
\[
H^*(C_{2^n}, \mathbb{F}_2) \cong \frac{\mathbb{F}_2[x,y]}{(x^2)}
\]
with \(|x| = 1, |y| = 2\).

### 2.4 The universal coefficient theorem applied to the group \( C_{2^n} \)

Let \( G \) be an arbitrary group and consider the short exact sequence
\[
0 \rightarrow \mathbb{Z} \xrightarrow{\text{incl}} C \xrightarrow{\exp} C^* \rightarrow 1
\]
This induces a long exact sequence in cohomology:
\[
\cdots \rightarrow H^n(G, \mathbb{Z}) \rightarrow H^n(G, C) \rightarrow H^n(G, C^*) \rightarrow H^{n+1}(G, \mathbb{Z}) \rightarrow \cdots
\]
By [Wei94, Th. 6.1.10], if \( G \) is a finite group, then \( H^i(G, C) = 0 \) for all \( i \geq 1 \) since the order \(|G|\) of \( G \) is invertible in \( C \). Thus we have isomorphisms
\[
H^i(G, C^*) \cong H^{i+1}(G, \mathbb{Z})
\]
for all \( i \geq 1 \), and in particular, \( H^2(G, \mathbb{Z}) \cong H^3(G, C^*) \cong \text{Hom}(G, C^*) \).

To compute the cohomology of \( C_{2^n} \), we will use the **restriction homomorphism**: any group map \( \rho : G \rightarrow H \) induces an exact functor \( \rho^* : \mathbb{G} \rightarrow \text{mod} \rightarrow \text{mod} \), and there is a natural injection \( A^G \rightarrow (\rho^* A)^H \) extending to a ring homomorphism
\[
\text{res}_{ij}^G : H^*(G, A) \rightarrow H^*(H, A)
\]
In our case, \( \rho \) will be the inclusion of a subgroup \( H \) into \( G \). Then by the “restriction of an element to \( H \)” we mean the image of this element by the restriction homomorphism induced by the inclusion of \( H \) in \( G \).

Now let \( G = C_{2^n} \) with generator \( \sigma \). Then \( \text{Hom}(C_{2^n}, C^*) \cong \mathbb{Z}/2^n \) (generated by \( \sigma \mapsto e^{2i\pi/2^n} \)), so that the restriction \( \text{Hom}(C_{2^n}, C^*) \rightarrow \text{Hom}(C_2, C^*) \), which is the natural projection \( \mathbb{Z}/2^n \rightarrow \mathbb{Z}/2 \) is surjective. We now use the universal coefficient theorem:

**Proposition 2.3** (Universal coefficient theorem). There is a split exact sequence
\[
0 \rightarrow \text{Ext}^1_k(H_{n-1}(G, k), A) \rightarrow H^n(G, A) \rightarrow \text{Hom}_{Ab}(H_{n-1}(G, k), A) \rightarrow 0
\]
And conclude
\[ H^2(C_{2^n}, \mathbb{Z}/2) \cong \text{Hom}(C_{2^n}, \mathbb{C}^*) \otimes \mathbb{Z}/2 \]
The restriction is in fact an isomorphism
\[ H^2(C_{2^n}, \mathbb{F}_2) \cong H^2(C_2, \mathbb{F}_2) \]
But the restriction map is a ring homomorphism, and the even part \( H^{2*}(C_2, \mathbb{F}_2) \) is the polynomial ring \( \mathbb{F}_2[y] \) with \( y = x^2 \) a generator of degree 2. Thus
\[ H^{2*}(C_{2^n}, \mathbb{F}_2) \cong \mathbb{F}_2[y] \]
with \(|y| = 2\).

It remains to check the structure of the odd part. Consider the operation \( Sq^1 \):

- On the one hand, \( Sq^1 \) is the Bockstein homomorphism induced by the sequence \( 0 \rightarrow \mathbb{Z}/2 \rightarrow \mathbb{Z}/4 \rightarrow \mathbb{Z}/2 \rightarrow 0 \), so that \( Sq^1(x) = 0 \) if and only if \( x \) arises as the image of an element \( y \in H^1(C_{2^n}, \mathbb{F}_2) \) under the map induced by the quotient map \( \mathbb{Z}/4 \rightarrow \mathbb{Z}/2 \).
  In other words, using the identification \( H^1(C_{2^n}, A) \cong \text{Hom}(C_{2^n}, A) \), \( Sq^1(x) = 0 \) if, and only if the homomorphism \( x \) can be lifted to \( \mathbb{Z}/4 \). This is always the case when \( n \geq 2 \), so \( Sq^1(x) = 0 \)
- On the other hand, since \(|x| = 1\), \( Sq^1(x) = x^2 \), so \( x^2 = 0 \) in the cohomology of \( C_{2^n} \).

Finally, we investigate the products \( zy \), where \( z \in H^{k}(C_{2^n}, \mathbb{F}_2) \) is an arbitrary class of odd degree and \( y \) is the generator of degree 2. Let \( P \rightarrow \mathbb{F}_2 \) be the minimal resolution of \( \mathbb{F}_2 \) by \( \mathbb{F}_2C_{2^n} \)-modules, and define
\[ Q_k = \bigoplus_{i+j=k} P_i \otimes P_j \]
If \( zy = 0 \), then there is a \( t \in \text{Hom}(Q_{k+1}, \mathbb{F}_2) \) satisfying \( dt = zy \). Thus \( t \) has even degree, and:
\[
dt(1 \otimes 1) = t(N \otimes 1 + 1 \otimes N) \text{ where } N = \sum_{i=0}^{2^n-1} \sigma^i
\]
\[
= t(N \otimes 1) + t(1 \otimes N)
\]
\[
= \sum_{i=0}^{2^n-1} t(\sigma^i \otimes 1) + \sum_{i=0}^{2^n-1} t(1 \otimes \sigma^i)
\]
\[
= \sum_{i=0}^{2^n-1} t(1 \otimes \sigma^{-i}) + \sum_{i=0}^{2^n-1} t(1 \otimes \sigma^i)
\]
\[
= 0
\]
so there are no nonzero coboundaries in \( H^*(C_{2^n}, \mathbb{F}_2) \). By observing that, for example, \( z \times y(\sigma \otimes \sigma) = 1 \), we can conclude that \( zy \neq 0 \), and thus we obtain an isomorphism
\[ H^*(C_{2^n}, \mathbb{F}_2) \cong \mathbb{F}_2[y, x]/x^2 \]

### 2.5 Cohomology with pictures: Jon Carlson’s diagrams

In [Car96], Jon Carlson presents a very pictorial way to calculate group cohomology, which relies on the description of \( \text{Ext}^n_{RG}(k, A) \) as chain homotopy classes of chain maps of degree \( n \). Indeed, any element of \( \text{Ext}^n_{RG}(k, A) \) can be represented by a map \( \gamma : P_n \rightarrow k \), where \( P \rightarrow k \) is a projective resolution of \( k \), satisfying \( d\gamma = 0 \). Using this and the projectivity of \( P_i \), one can lift the map into a chain map \( \overline{\gamma} : P \rightarrow P \) of degree \(-n\),

```plaintext
10
```
and it can be shown that two maps represent the same element in \( \text{Ext}_{kG}^n(k, A) \) if and only if they are chain homotopic.

The cup product of two such classes \( \alpha, \beta \in \text{Ext}_{kG}^n(k, k) \) is then represented by the composition of the chain maps \( \alpha, \beta \). So computing the cohomology ring of a group \( G \) boils down to determining the chain maps \( P \to P \) of degree \(-n\), for each \( n \).

As an example, we consider the group \( D_8 \) with the following presentation:

\[
D_8 = \langle x, y | x^2 = y^2 = (xy)^4 = 1 \rangle
\]

Let \( A = x + 1 \) and \( B = y + 1 \) in \( \mathbb{F}_2 D_8 \). Then

\[
\mathbb{F}_2 D_8 = \frac{\mathbb{F}_2 \langle A, B \rangle}{(A^2, B^2, ABAB + BABA)}
\]

where \( \mathbb{F}_2 \langle A, B \rangle \) denotes the polynomial ring in noncommuting variables \( A, B \) over \( \mathbb{F}_2 \).

We can represent \( \mathbb{F}_2 D_8 \) by the following diagram:

![Diagram](image-url)

The point at the top is 1 and each arrows represents multiplication by either \( A \) or \( B \). Now, to form the projective resolution of \( \mathbb{F}_2 \) by \( \mathbb{F}_2 D_8 \)-modules, we splice the successive short exact sequences:

![Resolution Diagram](image-url)

Were, in the \( n \)-th sequence
• \( u_1 \mapsto Ax_1, u_2 \mapsto Bx_{n+1} \) and \( v_i \mapsto BABx_i + Ax_{i+1} \)

• \( x_1 \mapsto s_1, x_{n+1} \mapsto s_2 \) and \( x_i \mapsto v_{i-1} \) for \( 2 \leq i \leq n \)

We thus obtain a resolution \( P \to \mathbb{F}_2 \) with \( P_i = (\mathbb{F}_2D_8)^{i+1} \) (pictured below). Let \( b_1, b_2 \) be generators of \( P_1 \). The diagram below represents the chain map \( \bar{x} \) associated to the generator \( x \in H^1(D_8, \mathbb{F}_2) \) mapping \( b_1 \) to 1 and \( b_2 \) to 0.

By iterating the process, we can see that \( \bar{x}^n = \bar{x} \circ \cdots \circ \bar{x} \) sends the leftmost generator of \( P_n \) to \( a \in P_0 \) and all other generators to 0. It can be shown, with some additional diagram chasing, that \( \bar{x}^n \) is not chain homotopic to zero. Thus \( \bar{x}^n \) represents a nonzero element of \( \text{Ext}^n_{\mathbb{F}_2D_8}(\mathbb{F}_2, \mathbb{F}_2) \). Repeating the same process with the map \( y \) sending \( b_2 \) to 1 and \( b_1 \) to 0, we obtain a map \( \bar{y} \) representing a non-nilpotent element of degree 1 in \( H^1(D_8, \mathbb{F}_2) \). It is then easy to see that \( xy = 0 \) in the cohomology.

Finally, if \( P_2 \) is generated by \( c_1, c_2, c_3 \), then \( \bar{x}^2 \) corresponds to the chain map sending \( c_1 \) to \( a \in P_0 \), and \( \bar{y}^2 \) sends \( c_3 \) to \( a \). The map \( \bar{z} \) sending the generator \( c_2 \) to \( a \) is not (chain homotopic to) zero, and not represented by any linear combination of \( \bar{x}^2 \) and \( \bar{y}^2 \) since both of these are 0 on \( c_2 \). Thus \( \bar{z} \) must be a third independent generator.

By playing a little more with the chain maps, we see that in degree \( n \), the map \( \bar{x}^n \) sends the leftmost generator of \( P_n = (\mathbb{F}_2D_8)^{n+1} \) to \( a \), and all other generators to 0. The map \( \bar{x}^{n-2} \bar{z} \) sends the next generator on the right to \( a \), and all others to 0, and so on. Similarly, \( \bar{y}^n \) sends the rightmost generator to \( a \) and the rest to 0, and \( \bar{y}^{n-2} \bar{z} \) the next generator on the left to \( a \). This way, we can generate the entire cohomology of \( D_8 \) with products of \( x, y \) and \( z \), and we obtain:

\[ H^n(D_8, \mathbb{F}_2) \cong \mathbb{F}_2[\bar{x}, \bar{y}, \bar{z}] / (\bar{x}\bar{y}) \]

where \( |x| = |y| = 1 \) and \( |z| = 2 \).
3 Steenrod operations

3.1 Operations on $H^*(C_2, \mathbb{F}_2)$
Recall that $H^*(C_2, \mathbb{F}_2) \cong \mathbb{F}_2[x]$ with $|x| = 1$. Here is a very straightforward, combinatorial approach to determining the Steenrod squares on a cohomology ring: consider the operator $Sq$ applied to the generator $x$:

$$Sq(x) = Sq^0(x) + Sq^1(x) + 0$$
$$= x + x^2$$
$$= x(x + 1)$$

thus for any $k \geq 1$,

$$Sq(x^k) = Sq^0(x^k) = (x + 1)^k x^k = \sum_{i=0}^{k} \binom{k}{i} x^{k+i}$$

whence

$$Sq^i(x^k) = \binom{k}{i} x^{k+i}$$

3.2 Operations on $H^*(C^n_2, \mathbb{F}_2)$
Write $H^*(C^n_2, \mathbb{F}_2) \cong \mathbb{F}_2[x_1, \ldots, x_n]$. Then, as computed above, $Sq(x_i) = x_i(x_i + 1)$ for each $i$. A similar calculation yields

$$Sq^i(x_1^{k_1} \cdots x_n^{k_n}) = \sum_{l_1, \ldots, l_n = 0} \left( \prod_{i=1}^{n} \binom{k_i}{l_i} x_1^{k_i+l_i} \right)$$

3.3 Operations on $H^*(C_4, \mathbb{F}_2)$
The ring $H^*(C_4, \mathbb{F}_2) \cong \mathbb{F}_2[x, y]/(x^2)$ presents the added interest of the generator $y$ of degree 2. We have:

- $Sq(x) = x$ since $x^2 = 0$. Thus $Sq(x^k) = x^k$ and $Sq^i(x^k) = 0$ for any $i \neq 0$.
- $Sq(y) = y + Sq^1(y) + y^2$

so we need to determine $Sq^1(y)$. For this, we use the alternative definition of $Sq^1$ as the Bockstein homomorphism associated to the sequence

$$0 \rightarrow \mathbb{Z}/2 \rightarrow \mathbb{Z}/4 \rightarrow \mathbb{Z}/2 \rightarrow 0$$

In our case, $Sq^1$ is the map denoted $\beta$ in the (exact) sequence below:

$$H^2(C_4, \mathbb{Z}/2) \rightarrow H^2(C_4, \mathbb{Z}/4) \xrightarrow{\alpha} H^2(C_4, \mathbb{Z}/2) \xrightarrow{\beta} H^3(C_4, \mathbb{Z}/2) \rightarrow \cdots$$

and so $Sq^1(y) = 0$ if and only if $y = \alpha(z)$ for some $z \in H^2(C_4, \mathbb{Z}/2)$. We know that the map $H^1(C_4, \mathbb{Z}/2) \rightarrow H^2(C_4, \mathbb{Z}/2)$ is zero, since it is $Sq^1$ on classes of degree 1. Using the fact that $H^2(C_4, \mathbb{Z}/4) = \mathbb{Z}/4$, (3) above becomes:

$$0 \rightarrow \mathbb{Z}/2 \rightarrow \mathbb{Z}/4 \xrightarrow{\alpha} \mathbb{Z}/2 \xrightarrow{\beta} \mathbb{Z}/2$$

See [Wei94, Th. 6.2.2] for the detailed computation.
thus $a$ must be surjective and $b = 0$. Hence $Sq^1(y) = 0$ and $Sq(y) = y + y^2 = y(y + 1)$, and we can apply the usual reasoning to get:

$$Sq(y^k) = \sum_{i=1}^{k} \binom{k}{i} y^{k+i}$$

so $Sq^2(y^k) = (\binom{k}{i})y^{k+i}$, $Sq^{2^1}(y^k) = 0$.

We can conclude:

$$Sq^{2^1+1}(xy^k) = 0$$

$$Sq^2(xy^k) = xSq^2(y^k) = x\binom{k}{i} y^{k+i}$$

### 3.4 Operations on $H^*(D_8, F_2)$

We showed that $H^*(D_8, F_2) \cong F_2[x, y, z]/(xy)$, where $x$ is the dual homomorphism to the generator $\sigma$ of $D_8$, $y$ is dual to $\tau$, and $z$ is a choice of a generator of degree 2 that we will make precise later. So there are three generators on which the Steenrod squares act.

Since $x$ is a non-nilpotent generator of degree 1, we have $Sq^1(x) = x + x^2$ so we apply the same reasoning as in section 3.1 and obtain $Sq^1(x^k) = \binom{k}{i} x^{k+i}$ and similarly for $y$.

To compute the action of the squares on $z$, we will use the restriction homomorphism. We first make a choice of generator: let $z \in H^2(D_8, F_2)$ be a non-trivial element such that its restrictions to the subgroups $\langle \sigma \rangle$ and $\langle \tau \rangle$ are both zero. Consider the extension:

$$0 \to C_2 \to D_{16} \to D_8 \to 1$$

any set-theoretic section of $D_{16} \to D_8$ sends the generating involutions $\sigma, \tau$ of $D_8$ to involutions, thus it is a homomorphism on the subgroups $\langle \sigma \rangle$ and $\langle \tau \rangle$. In other words, the restriction of this extension to the subgroups $\langle \sigma \rangle$ and $\langle \tau \rangle$ has a section, and is thus split, which means that it corresponds to 0 in the cohomology group $H^2(D_8, F_2)$. We just proved that $z$ corresponds to the extension above.

Now let us look at the restriction of $z$ on the subgroup $H = C_2 \times C_2$ generated by $\sigma$ and the commutator $[\sigma, \tau]$. Observe that the preimage of $H$ in $D_{16}$ is isomorphic to $D_8$, so that the restriction of $z$ to $H$ corresponds to the extension

$$0 \to C_2 \to D_8 \to C_2 \times C_2 \to 1$$

where one of the preimages of a generator of $C_2 \times C_2$ has order 4 in $D_8$ and the other has order 2.

The cohomology group $H^2(H, F_2)$ is generated by $a^2$ (where $a \in H^1(H, F_2)$ is dual to $\sigma$), $b^2$ ($b$ dual to $[\sigma, \tau]$) and $ab$. Write

$$\text{res}^G_H(z) = u.a^2 + v.b^2 + w.ab$$

with $u, v, w$ coefficients in $F_2$. We already established that the restriction of $z$ to $\langle \sigma \rangle$ is 0, so we must have $u = 0$. Now $b^2$ is the restriction of $z$ to $\langle [\sigma, \tau] \rangle$, which must be nontrivial since the preimage of $\langle [\sigma, \tau] \rangle$ in $D_{16}$ is not an involution (and thus the extension is non-split). Thus $v = 1$. Finally, since $\sigma$ and $[\sigma, \tau]$ do not commute in $D_{16}$, the restriction of $z$ to the subgroup $\langle \sigma \times [\sigma, \tau] \rangle$ is nontrivial as well. So $w = 1$ and

$$\text{res}^G_H(z) = a^2 + ab$$

Applying $Sq^1$, we obtain:

$$Sq^1(\text{res}(z)) = Sq^1(a^2 + ab) = a^2b + ab^2 = b(\text{res}^G_H(z))$$

Similarly, if $H' = \langle \tau, [\sigma, \tau] \rangle$, we have

$$Sq^1(\text{res}^G_{H'}(z)) = c(\text{res}^G_{H'}(z))$$
where \( c \) is dual to \( \tau \) in \( H^1(H', \mathbb{F}_2) \).

Since the Steenrod squares are natural transformations, they commute with the restriction, so that 
\[
Sq^1(\text{res}^G_H(z)) = \text{res}^G_H(Sq^1(z)).
\]
So \( Sq^1(z) \) is an element of \( H^3(D_8, \mathbb{F}_2) \) that restricts to both of these elements on \( H \) and \( H' \). Since restriction is a ring homomorphism, a straightforward inspection yields:

\[
Sq^1(z) = (x + y)z
\]

Thus \( Sq(z) = z + (x + y)z + z^2 \). Straightforward combinatorics then yield

\[
Sq^i(x^kz^l) = \sum_{s+t=i} \binom{k}{s} x^{k+s} \binom{l}{t} \sum_r z^{l+t-r}(x^r + y^r)
\]

and similarly for \( y^kz^l \).

### 4 Towards Massey higher products

A dual problem to that of computing \( G_F \) for an arbitrary field \( F \) is that of determining, for an arbitraty profinite group \( G \), whether \( G \) can be realised as the absolute Galois group of some field \( F \). Recent advances in this field have been made using Massey products. For example, it is shown in [MT13] that whenever \( G \) can be realised as the absolute Galois group of a field \( F \), the triple Massey product of any classes of degree 1 in the cohomology of \( G \) with coefficients in \( \mathbb{F}_2 \) must contain zero.

In [Kra66], after defining Massey higher products, Kraines shows how they can be linked to Steenrod operations and Bockstein homomorphisms: restricting the definition of the higher Massey product by adding conditions on defining systems turns the \( n \)-fold product of a class with itself into a well-defined cohomology operation. Cohomology operations are classified by the cohomology groups of Eilenberg-Mac Lane spaces, which are generated by Steenrod operations and Bockstein homomorphisms. Thus the Massey \( n \)-fold product can be shown to be the composition of a Bockstein homomorphism and a Steenrod power.

Unfortunately, this theorem is only true for coefficients in a finite field of odd order; even in these cases, the exact structure of general Massey products is not yet well determined. Understanding Massey products and how they relate to cohomology operations in a general setting would bring us one step closer to solving the inverse Galois problem.

### References


