Math 8246 Group Theory

Peter Webb

August 4, 2020

Contents

Chapter 1

Introduction

1.1 Some history

The cohomology of groups arose from three different sources during the first half of the 20th century. The earliest appearance of the low degree homology and cohomology groups took place before cohomology had been defined, and came as group-theoretic constructions that were important in understanding groups. The first of these to be considered is the *abelianization* G/G' of a group G, essential to the work of Galois on solving polynomial equations in terms of radicals. This group was later seen to be the first homology group $H_1(G, \mathbb{Z})$. In 1904 I. Schur studied a group, now known as the *Schur multiplier* of G, that plays a role in central extensions of G, and it turns out to be isomorphic to the second homology group $H_2(G, \mathbb{Z})$. In 1934 R. Baer studied a group of equivalence classes of group extensions of G by a representation M. This group was later seen to be the second cohomology group $H^2(G, M)$.

Mention Hopf's 1941 formula?

At a similar time during the 20th century the importance of groups in topology was emerging, as was the fact that topological methods can be used to derive information about groups. A significant theorem in this development was the following.

Theorem 1.1.1 (Hurewicz 1936)**.** *Let X be a path-connected space with base point x_0 and $\pi_n(X, x_0) = 0$ for all $n \geq 2$. Then X is determined up to homotopy by $\pi_1(X, x_0)$.*

A space X satisfying the conditions of the theorem is called *aspherical*. In honor of later work of Eilenberg and MacLane in constructing such spaces, if $G = \pi_1(X)$ for some aspherical space X that is also a CW-complex we call X an *Eilenberg-MacLane space*, and write it $K(G, 1)$. If G is regarded as a topological group with the discrete topology, this space is also denoted BG, and is termed the *classifying space* of G.

If X is an aspherical CW-complex, its homology depends only on its fundamental group. A possible definition of group homology and cohomology when $G = \pi_1(X)$ is

$$H_n(G, \mathbb{Z}) = H_n(X) \quad \text{and} \quad H^n(G, \mathbb{Z}) = H^n(X),$$

these groups being determined up to isomorphism.

Example 1.1.2. Take X to be d loops joined together at a point x_0. Then $\pi_1(X, x_0) = F_d$ is a free group on d generators and $\pi_n(X, x_0) = 0$ for $n \geq 2$, so that X is a classifying space for the free group. According to the above definition

$$H_n(F_d, \mathbb{Z}) = \begin{cases} \mathbb{Z} & \text{if } n = 0 \\ \mathbb{Z}^d & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Note that the universal cover of X is a tree on which F_d acts freely, which is a contractible space. For most groups G the $K(G, 1)$ is more complicated than this. It is not immediately apparent, but if G is a non-identity finite group then a $K(G, 1)$ must be infinite-dimensional.

In papers of 1945, Eilenberg and MacLane and, independently, Eckmann, introduced an algebraic approach that both defines the homology and cohomology groups, and also allows them to be computed. The algebraic definition is

E-M was submitted 1943. Check Eckmann's date.

$$H_n(G, M) = \mathrm{Tor}_n^{\mathbb{Z}G}(\mathbb{Z}, M) \quad \text{and} \quad H^n(G, M) = \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, M).$$

Thus, for each group G and representation M of G there are abelian groups $H_n(G, M)$ and $H^n(G, M)$ where $n = 0, 1, 2, 3, \ldots$, called the nth homology and cohomology of G with coefficients in M. To understand this we need to know what a *representation* of G is, and we also need to know what the *group ring* $\mathbb{Z}G$ is. These things will be explained in the next sections. Eilenberg and MacLane also realized at this time that the Schur multiplier and Baer's group of extensions appear among their infinite list of groups.

Is this true?

We may see the connection between the topological and algebraic definitions of group cohomology using the theory of covering spaces. If X is an aspherical CW-complex its universal cover $\tilde{X}$ has trivial homotopy groups, and so is contractible by a theorem of Whitehead. Furthermore its fundamental group $G = \pi_1(X, x_0)$ acts freely on $\tilde{X}$ by deck transformations and $X = \tilde{X}/G$. The cellular chain complex $C_\bullet(\tilde{X})$ of $\tilde{X}$ is thus an acyclic complex of $\mathbb{Z}G$-modules (apart from homology $\mathbb{Z}$ in degree 0), and (provided a suitable subdivision of X has been taken) they are free. The homotopy lifting property of the universal cover shows that this complex of $\mathbb{Z}G$-modules is determined up to equivariant chain homotopy. The homology of X may be computed by taking the homology of the largest quotient of $C_\bullet(\tilde{X})$ on which G acts trivially. We will study these technicalities in the future sections.

Explain. Reference?

The theorem of Hurewicz tells us what the group cohomology is if there happens to be an aspherical space with the right fundamental group, but it does not say that there always is such a space. That assertion is the next theorem.

Theorem 1.1.3 (Eilenberg and MacLane 1953)**.** *Given any group G there exists an aspherical CW complex X with $\pi_1(X, x_0) = G$.*

One way to construct an Eilenberg-MacLane space for a group G is to take a presentation of the group, start with a set of loops corresponding to the generators of

G, glue in 1-cells corresponding to the relators of G, and then glue in higher dimensional cells to kill higher homotopy. This approach is rudimentary, and there are other more systematic approaches. One is to regard the group as a category and form the nerve of the category.

Example 1.1.4. We construct Baer's group of extensions: it can be done without knowing the definition of group cohomology, although some terms are defined in later sections. A *group extension* is defined to be a short exact sequence of groups

When did Baer do this?

$$1 \to A \to E \to G \to 1,$$

which is equivalent to requiring that the image of A in E is a normal subgroup of E, and the quotient is isomorphic to G. If A is abelian, such an extension determines a module action of G on A via conjugation within E: given $g \in G$, $a \in A$ let $\bar{g} \in E$ be an element that maps on to g. Then $a \mapsto {}^{\bar{g}}a = \bar{g}a\bar{g}^{-1}$ is the action of g on a. We check this action is well defined, giving a homomorphism $G \to \mathrm{Aut}(A)$, i.e. A is a representation of G.

Given a representation A of G, an *extension of G by A* will mean an exact sequence of groups

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

such that the action of G on A induced by conjugation within E is the same as the given action.

Here are some examples of extensions. Let $D_8 = \langle x, y \mid x^4, y^2, yxy^{-1} = y^3 \rangle$ and $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. Consider

$$\begin{aligned} &1 \to \langle x^2 \rangle \to D_8 \to C_2 \times C_2 \to 1 \\ &1 \to \langle y, x^2 \rangle \to D_8 \to C_2 \to 1 \\ &1 \to \{\pm 1\} \to Q_8 \to C_2 \times C_2 \to 1 \end{aligned}$$

Class Activity. Is the action given by conjugation of the quotient group on the normal subgroup trivial or not, in these examples? (*Trivial* means that every group element acts as the identity automorphism.)

Two extensions of G by A are said to be equivalent if and only if they can appear in a commutative diagram

$$\begin{array}{ccccc} A & \longrightarrow & E_1 & \longrightarrow & G \\ \| & & \downarrow \phi & & \| \\ A & \longrightarrow & E_2 & \longrightarrow & G \end{array}$$

for some homomorphism $\phi : E_1 \to E_2$. Such a homomorphism is necessarily an isomorphism (as may be verified as an exercise). Therefore 'equivalence' is an equivalence relation on the set of extensions of G by A. Equivalent extensions necessarily have isomorphic middle groups; it is possible to have non-equivalent extensions whose middle groups are isomorphic.

We put $H^2(G,A) := \{\text{equivalence classes of extensions of } G \text{ by } A\}$, and define an addition on $H^2(G,A)$ as follows. Given extensions

$$1 \to A \to E_i \xrightarrow{\pi_i} G \to 1$$

where $i = 1, 2$, form the commutative diagram with exact rows

$$\begin{array}{ccccccccc}
1 & \longrightarrow & A\times A & \longrightarrow & E_1\times E_2 & \longrightarrow & G\times G & \longrightarrow & 1 \\
 & & \| & & \uparrow & & \uparrow{\scriptstyle \text{diagonal}} & & \\
1 & \longrightarrow & A\times A & \longrightarrow & X & \longrightarrow & G & \longrightarrow & 1 \\
 & & {\scriptstyle \text{add}}\downarrow & & \downarrow & & \| & & \\
1 & \longrightarrow & A & \longrightarrow & Y & \longrightarrow & G & \longrightarrow & 1
\end{array}$$

where

$$X = \{(e_1, e_2) \in E_1 \times E_2 \mid \pi_1 e_1 = \pi_2 e_2\}$$
$$Y = X/\{(a, -a) \mid a \in A\}$$

The bottom row is an extension of G by A called the *Baer sum* of the two extensions. We define the sum of the equivalence classes of the two extensions to be the equivalence class of their Baer sum. Under this operation $H^2(G,A)$ becomes an abelian group in which the zero element is the semidirect product. At this point these facts and the background justification that the Baer sum is well defined on equivalence classes, could be taken as an exercise. We will establish the group structure on $H^2(G,A)$ in a later section.

The calculation of the structure of Baer's group is not straightforward, and it is best done using the technical machinery we will develop in later sections. For example, we will see that when $G = C_2 \times C_2$ and $A = C_2$ there are eight equivalence classes of extensions: one is the direct product $E \cong C_2 \times C_2 \times C_2$, there are three equivalence classes where $E \cong C_4 \times C_2$, three where $E \cong D_8$, and one where $E \cong Q_8$.

Insert a picture.

The calculation of these groups of extensions is useful when Baer's group turns out to be the identity, in which case all extensions of the prescribed type are split. It is also useful in constructing p-groups for the purposes of classification, since all finite p-groups of order larger than p can be realized as extensions of smaller groups. We will use Baer's group in a later section in classifying crystallographic groups.

Exercise: show that the three extensions $C_2 \to C_4 \times C_2 \to C_2 \times C_2$ are inequivalent.

Possibly mention Dummit and Foote 17.4, the Brauer group $Br(K/F) \cong H^2(G, K^\times)$ of central simple F-algebras that split over K, $G = Gal(K/F)$

Chapter 2

Appendix: Basic Homological Algebra

All rings we consider will have a 1, and modules will generally be left unital modules. In this section R may denote any ring. We will need to know about tensor products, and these are described in the books by Dummit and Foote (section 10.4) and Rotman (section 8.4).

Introduce: commutative diagram, category?, monomorphism = injection = mono = 1-1 map

2.1 Tensor products

See Dummit and Foote section 10.4.

Definition 2.1.1. See Dummit and Foote before Theorem 10. If R is a ring, M is a right R-module and N is a left R-module we let X be the free abelian group with basis the elements of $M \times N$ and Y the subgroup generated by all elements of the form $(m_1+m_2, n)-(m_1, n)-(m_2, n)$, $(m, n_1+n_2)-(m, n_1)-(m, n_2)$ and $(mr, n)-(m, rn)$. We define $M \otimes_R N := X/Y$.

Elements of $M \otimes_R N$ are called *tensors*. We write $m \otimes n$ for the image of (m, n) in $M \otimes_R N$, and such tensors are called *simple tensors* or *basic tensors*. Every tensor can be written as a linear combination of simple tensors. In $M \otimes_R N$ the following relations hold:

$$(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$$
$$m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$$
$$mr \otimes n = m \otimes rn$$

We deduce, for example, that $m \otimes 0 = 0 = 0 \otimes n$ for all m and n. From the definition we have that $M \otimes_R N$ has the structure of an abelian group. It does not, in general, have the structure of an R-module.

Definition 2.1.2. Let M be a right R-module, N a left R-module and L an abelian

group. A mapping $\phi : M \times N \to L$ is said to be *R-balanced* if and only if

$$\begin{aligned} \phi(m_1 + m_2, n) &= \phi(m_1, n) + \phi(m_2, n) \\ \phi(m, n_1 + n_2) &= \phi(m, n_1) + \phi(m, n_2) \\ \phi(mr, n) &= \phi(m, rn) \end{aligned}$$

always. For example, the mapping $M \times N \to M \otimes_R N$ given by $\phi(m, n) = m \otimes n$ is balanced.

Class Activity. Discuss the difference between the notion of being balanced and some concept of being R-bilinear. We could try to formulate a notion of being R-bilinear using axioms such as the following. Given left R-modules L, M, N, a mapping $\phi : M \times N \to L$ is R-bilinear if and only if

$$\begin{aligned} \phi(r_1 m_1 + r_2 m_2, n) &= r_1 \phi(m_1, n) + r_2 \phi(m_2, n) \\ \phi(m, s_1 n_1 + s_2 n_2) &= s_1 \phi(m, n_1) + s_2 \phi(m, n_2) \\ \phi(mr, n) &= \phi(m, rn) = r\phi(m, n). \end{aligned}$$

How much of that makes sense? Is it a problem that $\phi(rm, sn) = r\phi(m, sn) = rs\phi(m, n) = sr\phi(m, n)$?

Theorem 2.1.3 (Dummit and Foote Corollary 11)**.** *The balanced map $M \times N \to M \otimes_R N$ is universal with respect to balanced maps. This means: given a balanced map $M \times N \to L$ there exists a unique group homomorphism $M \otimes_R N \to L$ so that the given balanced map is the composite $M \times N \to M \otimes_R N \to L$. The tensor product $M \otimes_R N$ is defined up to isomorphism by this property.*

Theorem 2.1.4 (Dummit and Foote Theorem 10)**.** *Balanced maps $M \times N \to L$ biject with group homomorphisms $M \otimes_R N \to L$.*

Example 2.1.5. If $f : R \to S$ is a ring homomorphism with $f(1_R) = 1_S$ then $S \otimes_R R \cong S$ as left S-modules via an isomorphism $s \otimes r \mapsto sf(r)$. The left S-module structure comes from multiplication on the left side. Thus, for example, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Q}$.

Example 2.1.6. Let I be a right ideal of R. Then $(I \backslash R) \otimes_R M \cong M/IM$. As a proof, we construct inverse maps $(I + r) \otimes m \mapsto rm + IM$ and $(I + 1) \otimes m \leftarrow m + IM$.

Example 2.1.7. $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/\text{g.c.d.}(m, n)\mathbb{Z}$.

Theorem 2.1.8. *Tensor product distributes over direct sums:*

$$(M \oplus M') \otimes_R N \cong (M \otimes_R N) \oplus (M' \otimes_R N),$$

with a similar formula on the other side.

Proof. This follows from the universal property. □

Example 2.1.9. For example, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^n \cong \mathbb{Q}^n$.

Example 2.1.10. Let U and V be vector spaces over a field K with bases $u_1, \ldots, u_r$ and $v_1, \ldots, v_s$. Then the tensors $u_i \otimes v_j$ where $1 \leq i \leq r$ and $1 \leq j \leq s$ form a basis for $U \otimes_K V$.

Sometimes people regard a rank n tensor as an array of numbers $(a_{i,j,k,\ldots})$ with n suffices $i, j, k, \ldots$. Such numbers are the coordinates of the element $\sum a_{i,j,k,\ldots} u_i \otimes v_j \otimes w_k \otimes \cdots$ of the vector space $U \otimes V \otimes W \otimes \cdots$.

Definition 2.1.11. Let $\phi : M \to M'$ and $\psi : N \to N'$ be homomorphisms of right and left R-modules, respectively. We define $\phi \otimes \psi : M \otimes_R N \to M' \otimes_R N'$ to be the group homomorphism determined by the balanced map $M \times N \to M' \otimes_R N'$ given by $(m, n) \mapsto \phi(m) \otimes \psi(n)$.

Example 2.1.12. Let $\phi : \mathbb{Z}^2 \to \mathbb{Z}^2$ have matrix $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ and let $\psi : \mathbb{Z}^2 \to \mathbb{Z}^2$ have matrix $\begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix}$, with respect to given bases of $\mathbb{Z}^2$. Then on taking the basis of $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathbb{Z}^2$ in a certain order the matrix of $\phi \otimes \psi$ is

$$\begin{bmatrix} 1\begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix} & 2\begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix} \\ 3\begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix} & 4\begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix} \end{bmatrix}$$

Class Activity. Put the basis vectors $u_i \otimes v_j$ in the correct order so that the above matrix is the matrix of $\phi \otimes \psi$. What is the trace of $\phi \otimes \psi$?

Is base change for rank 2 tensors $B^T aB$ or BAB^{-1}?

Definition 2.1.13. If A and B are rings there is a multiplication on the group $A \otimes B$ defined on basic tensors by $(a_1 \otimes b_1)(a_2 \otimes b_2) := a_1 a_2 \otimes b_1 b_2$, making $A \otimes B$ into a ring.

Examples 2.1.14. Consider exercises 3, 4, 25 of Dummit and Foote. Are any of $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$, $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{C}$ isomorphic as rings?

Definition 2.1.15. Let R and S be rings. An (S, R)-bimodule is a left S-module A that is also a right R-module, in such a way that the actions of R and S commute: $(ra)s = r(as)$ for all $r \in R$, $a \in A$ and $s \in S$.

If R is a commutative ring then every left R-module A can also be regarded as a right R-module, and so A is automatically an (R, R)-bimodule. The definition of a bimodule has more serious impact when the rings R and S are not commutative.

If A is an (S, R)-bimodule, B is a left S-module and C is a left R-module then $A \otimes_R C$ is a left S-module with action given by $s(a \otimes c) := sa \otimes c$, $\mathrm{Hom}_S(A, B)$ is a left R-module with action given by $(r\phi)(a) := \phi(ar)$, and $\mathrm{Hom}_S(B, A)$ is a right R-module with action given by $(\phi r)(b) := \phi(rb)$. The operation of tensor product on bimodules is associative.

Theorem 2.1.16 (Dummit and Foote Theorem 43 from 10.5)**.** *Let A be an (S, R)-bimodule, B a left S-module and C a left R-module. Then*

$$\mathrm{Hom}_S(A \otimes_R C, B) \cong \mathrm{Hom}_R(C, \mathrm{Hom}_S(A, B))$$

via an isomorphism that is natural in B and C.

Proof. We define inverse isomorphisms

$$\phi \mapsto (b \mapsto (a \mapsto \phi(a \otimes b)))$$
$$(a \otimes b \mapsto \psi(b)(a)) \leftarrow \psi$$

With the first mapping we check that the image is an R-module homomorphism and that the inner mapping is an S-module homomorphism. With the second mapping we check that it is an S-module homomorphism and that the mapping $(a, b) \to \psi(b)(a)$ is R-balanced.

The two mappings are mutually inverse, and so we have an isomorphism. □

In categorical language, we say that the functor $A \otimes_R - : R\text{-mod} \to S\text{-mod}$ is *left adjoint* to the functor $\mathrm{Hom}_S(A, -) : S\text{-mod} \to R\text{-mod}$, which is *right adjoint* to $A \otimes_R -$.

Corollary 2.1.17. *Let $f : R \to S$ be a ring homomorphism, let B be a left R-module and let C be a left S-module. We regard S as an (S, R)-bimodule where the left action of S is multiplication and the right action of R is multiplication after first applying f. Then $\mathrm{Hom}_S(S \otimes_R B, C) \cong \mathrm{Hom}_R(B, C)$, where C is regarded as a left R-module via the homomorphism f.*

Proof. This is an instance of the previous theorem, because $\mathrm{Hom}_S(S, C) \cong C$ as R-modules via a correspondence $g \leftrightarrow g(1)$. This is an isomorphism of R-modules because if $r \in R$ then $rg \leftrightarrow (rg)(1) = g(r) = r \cdot g(1)$. Note that the action of R on $\mathrm{Hom}_S(S, C)$ is $(rg)(s) = g(sr)$. □

2.2 Splitting and exactness; projective and injective modules

Definition 2.2.1. Let $\alpha : A \to B$ be a homomorphism. We say that α is a *split monomorphism* if there exists a morphism $\beta : B \to A$ so that $\beta\alpha = 1_A$; and we say that α is a *split epimorphism* if there exists a morphism $\beta : B \to A$ so that $\alpha\beta = 1_B$.

Define exact, and short exact sequence.

It is an exercise to see that a split monomorphism is a monomorphism, and a split epimorphism is a epimorphism. From the algebraic point of view of manipulation of symbols, it is a question of identifying whether an element α has a right or left inverse which, in the context of rings, is a natural thing to do. We are also familiar with equivalent conditions for a matrix with entries in a field to have a left or right inverse. Over more general rings the issue is a little more subtle.

Lemma 2.2.2. *Given a short exact sequence of R-modules*

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

the following are equivalent:

1. *the monomorphism α is split;*
2. *the epimorphism β is split;*
3. *there is a commutative diagram*

$$\begin{array}{ccccccccc} 0 & \to & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \to & 0 \\ & & & \searrow^{i_1} & \cong\uparrow & \nearrow_{\pi_2} & & & \\ & & & & A\oplus C & & & & \end{array}$$

where i_1 is inclusion and π_2 is projection.

Exercise? Is it equivalent to replace π_2 in the diagram by i_2 going in the opposite direction?

Definition 2.2.3. If any of 1, 2, or 3 of Lemma 2.2.2 is satisfied we say the sequence $0 \to A \to B \to C \to 0$ is *split.*

The next result puts together Theorem 28, Corollary 32, Theorem 33, Proposition 34, Theorem 39 and Corollary 41 from section 10.5 of Dummit and Foote.

Lemma 2.2.4. *Let A, B, C and M be left R-modules, N a right R-module.*

1. *The sequence $A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is exact if and only if*
   $0 \to \mathrm{Hom}_R(C, M) \xrightarrow{\beta^*} \mathrm{Hom}_R(B, M) \xrightarrow{\alpha^*} \mathrm{Hom}_R(A, M)$ *is exact for all M, if and only if*
   $N \otimes_R A \xrightarrow{\alpha_*} N \otimes_R B \xrightarrow{\beta_*} N \otimes_R C \to 0$ *is exact for all N.*
2. *The sequence $0 \to A \to B \to C$ is exact if and only if*
   $0 \to \mathrm{Hom}_R(M, A) \xrightarrow{\alpha_*} \mathrm{Hom}_R(M, B) \xrightarrow{\beta_*} \mathrm{Hom}_R(M, C)$ *is exact for all M.*

Proof. Outline. We first show that if $A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is exact then

$$0 \to \mathrm{Hom}_R(C, M) \xrightarrow{\beta^*} \mathrm{Hom}_R(B, M) \xrightarrow{\alpha^*} \mathrm{Hom}_R(A, M)$$

is exact. For the converse, assume that

$$0 \to \mathrm{Hom}_R(C, M) \xrightarrow{\beta^*} \mathrm{Hom}_R(B, M) \xrightarrow{\alpha^*} \mathrm{Hom}_R(A, M)$$

is exact. We show that $B \to C$ is onto: let $B \to C \to C' \to 0$ be exact. Then $0 \to \mathrm{Hom}_R(C', M) \to \mathrm{Hom}_R(c, M) \to \mathrm{Hom}_R(B, M)$ is exact. Therefore $\mathrm{Hom}(C'M) = 0$ for all M, so that $C' = 0$. Next, we show that $\alpha A \subseteq \mathrm{Ker}\,\beta$. If $\beta\alpha \neq 0$ then $\mathrm{Hom}(C, C) to \mathrm{Hom}(A, C)$ maps $1 \to \beta\alpha$ is nonzero. Next we show $\alpha A = \mathrm{Ker}\,\beta$. Take $p : B \to M = B/\alpha A$ in

$$0 \to \mathrm{Hom}_R(C, M) \xrightarrow{\beta^*} \mathrm{Hom}_R(B, M) \xrightarrow{\alpha^*} \mathrm{Hom}_R(A, M),$$

which has $\alpha^* p = 0$, and $\mathrm{Im}\,\beta^*$ is contained in maps that are zero on $\mathrm{Ker}\,\beta$. Now p is not such unless etc. Use an adjoint property for the $\otimes$? Also, take $N = R$ in one direction. □ This needs some work.

Definition 2.2.5. We say that the functors $\mathrm{Hom}_R(\quad, M)$ and $\mathrm{Hom}_R(M, \quad)$ are *left exact*, while $N \otimes \_\_$ is *right exact*. A covariant functor F is *exact* if and only if whenever $0 \to A \to B \to C \to 0$ is exact then $0 \to F(A) \to F(B) \to F(C) \to 0$ is exact, i.e. F is both right and left exact.

Definition 2.2.6. The R-module P is said to be *projective* if and only if given any diagram

$$\begin{array}{ccc} & & P \\ & & \downarrow \beta \\ A & \xrightarrow{\alpha} & B \end{array}$$

with α epi there exists $\gamma : P \to A$ such that $\beta = \alpha\gamma$.

Lemma 2.2.7. *The following are equivalent for an R-module P:*

1. *P is projective,*
2. *every epimorphism $M \to P$ splits,*
3. *there is a module Q such that $P \oplus Q$ is free,*
4. *$\mathrm{Hom}_R(P, \quad)$ is an exact functor.*

Definition 2.2.8. There is a similar (dual) definition of an *injective* module. An equivalent condition is that an R-module I is injective if and only if $\mathrm{Hom}_R(\quad, I)$ is an exact functor. Also, an R module N is *flat* if and only if $N \otimes \_\_$ is an exact functor.

Proposition 2.2.9. *Projective modules are flat.*

Proof. Free modules are flat and hence so are projective modules, because they are direct summands of free modules. □

2.3 Chain complexes

Definition 2.3.1. A *chain complex* of R-modules is a sequence of R-modules

$$\mathcal{M} = \cdots \xrightarrow{d_3} M_2 \xrightarrow{d_2} M_1 \xrightarrow{d_1} M_0 \xrightarrow{d_0} \cdots$$

such that $d_i d_{i+1} = 0$ always. This condition is equivalent to the requirement that $\mathrm{Im}(d_{i+1}) \subseteq \mathrm{Ker}(d_i)$ always. We define the *homology group* of $\mathcal{M}$ in degree i to be $H_i(\mathcal{M}) = \mathrm{Ker}(d_i)/\mathrm{Im}(d_{i+1})$. The maps in the family $d = (d_i)$ send modules in given degrees to modules in degree lower by 1, and so we say d has degree -1. We also consider sequences of modules with a family of mappings d of degree $+1$ and in that case we term the sequence a *cochain complex*. The group $H^i(\mathcal{M}) = \mathrm{Ker}(d_i)/\mathrm{Im}(d_{i-1})$ is the *cohomology group* of $\mathcal{M}$ in degree i in this case.

A morphism of complexes $\phi : \mathcal{M} \to \mathcal{N}$ is a sequence of morphisms $\phi_i : M_i \to N_i$ such that

$$\begin{array}{ccccccccc} \cdots & \xrightarrow{d_3} & M_2 & \xrightarrow{d_2} & M_1 & \xrightarrow{d_1} & M_0 & \xrightarrow{d_0} & \cdots \\ & & \downarrow{\scriptstyle \phi_2} & & \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_0} & & \\ \cdots & \xrightarrow{e_3} & N_2 & \xrightarrow{e_2} & N_1 & \xrightarrow{e_1} & N_0 & \xrightarrow{e_0} & \cdots \end{array}$$

commutes. Such a ϕ induces a map $H_n(\phi) : H_n(\mathcal{M}) \to H_n(\mathcal{N})$.

Class Activity. The diagram

I'm not sure whether this is a good example. See also the next example

$$\begin{array}{ccccccc} \mathbb{Z}^2 & \xrightarrow{\left[\begin{smallmatrix}1 & 1\\ 1 & 1\end{smallmatrix}\right]} & \mathbb{Z}^2 & \xrightarrow{\left[\begin{smallmatrix}1 & -1\\ -1 & 1\end{smallmatrix}\right]} & \mathbb{Z}^2 \\ \downarrow{\scriptstyle [1\ 1]} & & \downarrow{\scriptstyle [1\ 1]} & & \downarrow{\scriptstyle [1\ 1]} \\ \mathbb{Z} & \xrightarrow{[2]} & \mathbb{Z} & \xrightarrow{[0]} & \mathbb{Z} \end{array}$$

is a morphism of chain complexes. We may compute the homology of a chain complex in general using the Smith normal form for integer matrices. In this example the top complex has homology groups $\mathbb{Z}, 0, \mathbb{Z}$ and the bottom complex has homology groups $0, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}$.

In different language, a chain complex is a graded R-module $\mathcal{M} = (M_i)_{i\in\mathbb{Z}}$ equipped with a graded endomorphism $d : \mathcal{M} \to \mathcal{M}$ of degree -1 satisfying $d^2 = 0$. This means that d is a module homomorphism and $d(M_i) \subseteq d(M_{i-1})$ for all i. The homology of $\mathcal{M}$ is the graded group $H(\mathcal{M}) = \mathrm{Ker}(d)/\,\mathrm{Im}(d)$. If the map d had degree $+1$ we would have a *cochain complex* instead.

Definition 2.3.2. A *(chain) homotopy* between two morphisms $\phi, \theta : \mathcal{M} \to \mathcal{N}$ is a graded module morphism $h : \mathcal{M} \to \mathcal{N}$ of degree $+1$ such that $eh + hd = \phi - \theta$. In this case we say that ϕ and θ are homotopic and write $\phi \simeq \theta$.

Proposition 2.3.3. *1. If ϕ and θ are homotopic then the two mappings $H_n(\phi) = H_n(\theta) : H_n(\mathcal{M}) \to H_n(\mathcal{N})$ are the same.*

2. If there are chain maps $\phi : \mathcal{M} \to \mathcal{N}$ and $\psi : \mathcal{N} \to \mathcal{M}$ with $\phi\psi \simeq 1_{\mathcal{N}}$ and $\psi\phi \simeq 1_{\mathcal{M}}$ then $H_n(\phi)$ and $H_n(\psi)$ are inverse isomorphisms on homology.

See Exercise 3 of section 17.1 of Dummit and Foote for the following.

Lemma 2.3.4 (The Snake Lemma)**.** *Let the following commutative diagram of R-modules have exact rows:*

$$\begin{array}{ccccccccc} & & A & \xrightarrow{\phi} & B & \xrightarrow{\theta} & C & \to & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \to & A' & \xrightarrow{\phi'} & B' & \xrightarrow{\theta'} & C' & & \end{array}$$

Then there is an exact sequence

$$\mathrm{Ker}\,\alpha \to \mathrm{Ker}\,\beta \to \mathrm{Ker}\,\gamma \xrightarrow{\omega} \mathrm{Coker}\,\alpha \to \mathrm{Coker}\,\beta \to \mathrm{Coker}\,\gamma$$

where the mappings between the kernels are the restrictions of ϕ and θ, and the mappings between the cokernels are induced by ϕ' and θ'. Furthermore, if ϕ is mono so is $\operatorname{Ker}\alpha \to \operatorname{Ker}\beta$*, and if θ' is epi so is* $\operatorname{Coker}\beta \to \operatorname{Coker}\gamma$.

Proof. The map ω is defined as follows: let $c \in \operatorname{Ker}\gamma$, choose $b \in B$ with $\theta(b) = c$. Then $\theta'\beta(b) = \gamma\theta(b) = 0$ so $\beta(b) = \phi'(a)$ for some $a \in A'$. Define $\omega(c) = a + \alpha(A) \in \operatorname{Coker}(\alpha)$. This is well-defined (see Mr Cooperman's objections in 'It's My Turn'). We now check exactness (see Hilton and Stammbach p.99).

For example, to check exactness at $\operatorname{Ker}\gamma$, we observe first that $\theta(\operatorname{Ker}\beta) \subseteq \operatorname{Ker}\omega$. This is because if $\beta(b) = 0$ then in the construction of $\omega\theta(b)$ we can use the elements $b \in B$, $\beta(b) = 0 \in B'$ and $0 \in A'$, so that $\omega\theta(b) = 0$.

To show that $\theta(\operatorname{Ker}\beta) \supseteq \operatorname{Ker}\omega$ let $c \in \operatorname{Ker}\gamma \cap \operatorname{Ker}\omega$. In constructing $\omega(c)$ we find elements $b \in B$ and $a \in A'$ as above. The element a lies in $\alpha(A)$ because $\omega(c) = 0$. Write $a = \alpha(a_0)$ for some $a_0 \in A$. Now $\beta\phi(a_0) = \phi'\alpha(a_0) = \beta(b)$. Thus $b - \phi(a_0) \in \operatorname{Ker}\beta$ and $\theta(b - \phi(a_0)) = \theta(b) - \theta\phi(a_0) = \theta(b) = c$. Therefore $c \in \theta(\operatorname{Ker}\beta)$.

The remaining arguments are similar. □

Class Activity. Is the morphism of chain complexes given earlier a chain homotopy equivalence? Is the morphism below a chain homotopy equivalence?

$$\begin{array}{ccccc} \mathbb{Z}^2 & \xrightarrow{\left[\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right]} & \mathbb{Z}^2 & \xrightarrow{\left[\begin{smallmatrix}1&-1\\-1&1\end{smallmatrix}\right]} & \mathbb{Z}^2 \\ \downarrow{\scriptstyle [1\ 0]} & & \downarrow{\scriptstyle 0} & & \downarrow{\scriptstyle [1\ 1]} \\ \mathbb{Z} & \xrightarrow{0} & 0 & \xrightarrow{0} & \mathbb{Z} \end{array}$$

Try upward morphisms $\begin{bmatrix}1\\0\end{bmatrix}$.

Definition 2.3.5. The mapping ω in the Snake Lemma is called the *connecting homomorphism.* A sequence of complexes $\mathcal{L} \xrightarrow{\phi} \mathcal{M} \xrightarrow{\theta} \mathcal{N}$ is said to be *exact at* $\mathcal{M}$ if and only if each for all i, the sequence $L_i \xrightarrow{\phi_i} M_i \xrightarrow{\theta_i} N_i$ of modules in degree i is exact at M_i.

Theorem 2.3.6. *A short exact sequence* $0 \to \mathcal{L} \xrightarrow{\phi} \mathcal{M} \xrightarrow{\theta} \mathcal{N} \to 0$ *of chain complexes gives rise to a long exact sequence in homology:*

$$\cdots \to H_n(\mathcal{L}) \xrightarrow{H_n(\phi)} H_n(\mathcal{M}) \xrightarrow{H_n(\theta)} H_n(\mathcal{N}) \xrightarrow{\omega_n} H_{n-1}(\mathcal{L}) \to \cdots .$$

The connecting homomorphism ω is natural, in the sense that a commutative diagram of chain complexes

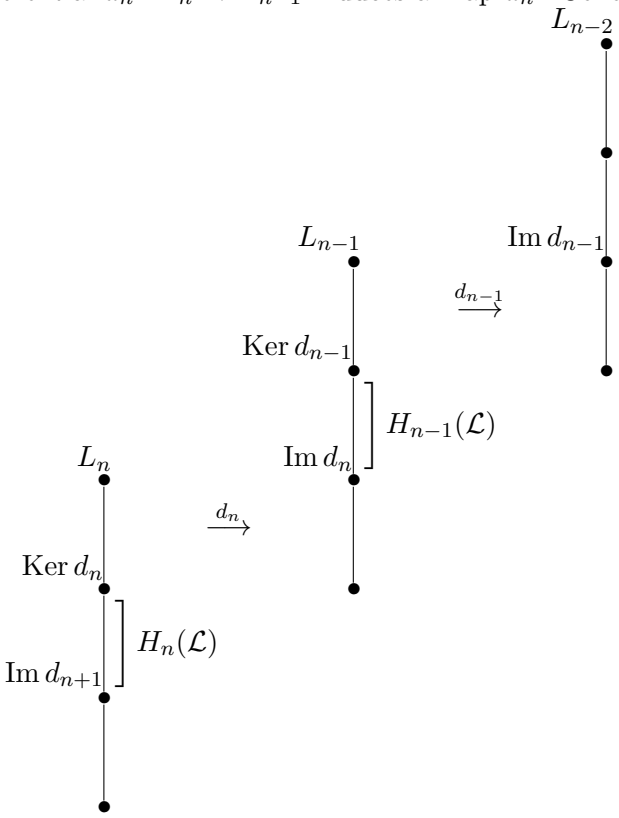
$$\begin{array}{ccccccccc} 0 & \to & \mathcal{L} & \to & \mathcal{M} & \to & \mathcal{N} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \mathcal{L}' & \to & \mathcal{M}' & \to & \mathcal{N}' & \to & 0 \end{array}$$

with exact rows yields a commutative square

$$\begin{array}{ccc} H_n(\mathcal{N}) & \to & H_{n-1}(\mathcal{L}) \\ \downarrow & & \downarrow \\ H_n(\mathcal{N}') & \to & H_{n-1}(\mathcal{L}'). \end{array}$$

Proof. The differential $d_n : L_n \to L_{n-1}$ induces a map $d_n : \operatorname{Coker} d_{n+1} \to \operatorname{Ker} d_{n-1}$:

Label the top two edges of the left term as $\operatorname{Coker} d_{n+1}$.



Similarly with the M's and N's. Apply the snake lemma to the following diagram, all

rows and columns of which are exact:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & H_n(\mathcal{L}) & & H_n(\mathcal{M}) & & H_n(\mathcal{N}) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \operatorname{Coker} d_{n+1} & \longrightarrow & \operatorname{Coker} e_{n+1} & \longrightarrow & \operatorname{Coker} f_{n+1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \operatorname{Ker} d_{n-1} & \longrightarrow & \operatorname{Ker} e_{n-1} & \longrightarrow & \operatorname{Ker} f_{n-1} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & H_{n-1}(\mathcal{L}) & & H_{n-1}(\mathcal{M}) & & H_{n-1}(\mathcal{N}) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

The naturality is an exercise. □

Class Activity. Why are the middle rows of the last big diagram exact? (We use the snake lemma with

$$\begin{array}{ccccccccc}
0 & \to & L_{n+1} & \to & M_{n+1} & \to & N_{n+1} & \to & 0 \\
 & & {\scriptstyle d_{n+1}}\downarrow & & {\scriptstyle e_{n+1}}\downarrow & & {\scriptstyle f_{n+1}}\downarrow & & \\
0 & \to & L_n & \to & M_n & \to & N_n & \to & 0.)
\end{array}$$

Class Activity. Calculate the homology of the kernel complex of the morphism of chain complexes given earlier. Noting that the morphism was surjective in each degree, apply the last theorem with the long exact sequence.

There is a similar result that applies when we have a short exact sequence of cochain complexes $0 \to \mathcal{L} \to \mathcal{M} \to \mathcal{N} \to 0$. In that case the connecting homomorphism has degree $+1$, giving a long exact sequence

$$\cdots \to H^n(\mathcal{L}) \to H^n(\mathcal{M}) \to H^n(\mathcal{N}) \xrightarrow{\omega_n} H^{n+1}(\mathcal{L}) \to \cdots .$$

2.4 Projective resolutions, Ext and Tor

Let R be a ring and M an R-module. A *projective resolution* of M is an exact sequence

$$\cdots \to P_2 \to P_1 \to P_0 \to M \to 0$$

in which the P_i are projective modules. Let $\mathcal{P}$ be the complex obtained by replacing M by 0 in the above, so $H_n(\mathcal{P}) = 0$ if $n > 0$ and $H_0(\mathcal{P}) \cong M$ is a given isomorphism. It is useful to write $\mathcal{P} \to M$ to denote this projective resolution.

Example at this point? Maybe $\mathbb{Z}C_2$?

We may always construct resolutions of a module M as follows. Given M, choose a free module P_0 with surjective mapping $P_0 \to M$ and form the kernel K_0. Repeat this process with K_0 instead of M. Depending on the context, other constructions of resolutions may be available: we may have a *bar resolution*, and resolutions constructed from other structures such as a presentation or an action on a space.

Given a second module N we may form the cochain complex

$$\mathrm{Hom}_R(\mathcal{P}, N) = [0 \to \mathrm{Hom}_R(P_0, N) \xrightarrow{d_0} \mathrm{Hom}_R(P_1, N) \xrightarrow{d_1} \mathrm{Hom}_R(P_2, N) \xrightarrow{d_2} \cdots]$$

obtained by applying $\mathrm{Hom}_R(-, N)$ to $\mathcal{P}$. We now define the degree n Ext group of M and N by

$$\mathrm{Ext}^n_R(M, N) = H^n(\mathrm{Hom}_R(\mathcal{P}, N)),$$

the nth cohomology group of this complex.

The above definition depends on the choice of resolution $\mathcal{P}$. It is the case that if we change the resolution we obtain Ext groups that are naturally isomorphic to those just constructed. More of this later!

Example 2.4.1. Let $R = \mathbb{Z}$, so that R-modules are the same thing as abelian groups. For each integer m, the cyclic group $\mathbb{Z}/m\mathbb{Z}$ has a projective resolution as follows:

$$0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \to 0$$

where $\mathcal{P}$ is the chain complex $0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \to 0$. Taking another abelian group N we compute $\mathrm{Ext}^i(\mathbb{Z}/m\mathbb{Z}, N)$ as the degree i cohomology of the cochain complex

$$\mathrm{Hom}(\mathcal{P}, N) = [\mathrm{Hom}(\mathbb{Z}, N) \xrightarrow{m} \mathrm{Hom}(\mathbb{Z}, N)] = [N \xrightarrow{m} N].$$

Thus

$$\mathrm{Ext}^0_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, N) \cong \{x \in N \mid mx = 0\}$$

and

$$\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, N) \cong N/mN$$

where $mN = \{mx \mid x \in N\}$. Thus if $N = \mathbb{Z}/p\mathbb{Z}$, where p is prime dividing m, these groups are both $\mathbb{Z}/p\mathbb{Z}$; and if p does not divide m then both groups are 0

Proposition 2.4.2. $\mathrm{Ext}^0_R(M, N) \cong \mathrm{Hom}_R(M, N)$.

Proof. From the definition, $\mathrm{Ext}^0_R(M, N) = \mathrm{Ker}\, d_0$. Now $P_1 \to P_0 \to M \to 0$ is exact, so

$$0 \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(P_o, N) \xrightarrow{d_0} \mathrm{Hom}_R(P_1, N)$$

is exact by Lemma 2.2.4, and the result follows. □

Theorem 2.4.3. *Let $0 \to A \to B \to C \to 0$ be an exact sequence of R-modules and let M be another R-module. There are exact sequences of abelian groups*

$$(1) \qquad \begin{aligned} 0 \to \mathrm{Hom}_R(M,A) \to \mathrm{Hom}_R(M,B) \to \mathrm{Hom}_R(M,C) \\ \xrightarrow{\omega} \mathrm{Ext}^1(M,A) \to \mathrm{Ext}^1(M,B) \to \cdots \end{aligned}$$

$$(2) \qquad \begin{aligned} 0 \to \mathrm{Hom}_R(C,M) \to \mathrm{Hom}_R(B,M) \to \mathrm{Hom}_R(A,M) \\ \to \mathrm{Ext}^1(C,M) \to \mathrm{Ext}^1(B,M) \to \cdots \end{aligned}$$

Proof. (1) We calculate our Ext groups with a resolution $\mathcal{P} \to M$. The sequence $0 \to A \to B \to C \to 0$ gives a sequence of cochain complexes

$$(*) \qquad 0 \to \mathrm{Hom}_R(\mathcal{P},A) \to \mathrm{Hom}_R(\mathcal{P},B) \to \mathrm{Hom}_R(\mathcal{P},C) \to 0.$$

where, at each level in the grading, this sequence is

$$0 \to \mathrm{Hom}_R(P_n,A) \to \mathrm{Hom}_R(P_n,B) \to \mathrm{Hom}_R(P_n,C) \to 0$$

obtained by applying $\mathrm{Hom}_R(P_n,-)$. Because each P_n is projective, $\mathrm{Hom}_R(P_n,-)$ is exact, and so $(*)$ is a short exact sequence of cochain complexes. We now apply Theorem 2.3.6 and Proposition 2.4.2.

(2) We construct resolutions $\mathcal{P} \to B$, $\mathcal{P}' \to A$ and $\mathcal{P}'' \to C$ appearing in a commutative diagram

$$\begin{array}{ccc} \mathcal{P}' & \longrightarrow & A \\ \downarrow & & \downarrow \\ \mathcal{P} & \longrightarrow & B \\ \downarrow & & \downarrow \\ \mathcal{P}'' & \longrightarrow & C \end{array}$$

with exact columns. To do this, let $\mathcal{P}', \mathcal{P}''$ be any resolutions of A and C and construct $\mathcal{P}$ as follows. The start is pictured in a diagram:

$$\begin{array}{ccccc} P_0' & \xrightarrow{\epsilon'} & A & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \\ P_0' \oplus P_0'' & \xrightarrow{\epsilon} & B & & \\ \downarrow & & \downarrow & & \\ P_0'' & \xrightarrow{\epsilon''} & C & \longrightarrow & 0. \end{array}$$

Lift ϵ'' to a map $P_0'' \to B$ and use this and ϵ' as the components of ϵ, so that the diagram commutes. By the snake lemma, $\operatorname{Ker}\epsilon' \to \operatorname{Ker}\epsilon \to \operatorname{Ker}\epsilon''$ is exact and ϵ is

epi. Now repeat this procedure with the terms $\operatorname{Ker}\epsilon' \to \operatorname{Ker}\epsilon \to \operatorname{Ker}\epsilon''$ instead of with $A \to B \to C$, and then with subsequent kernels, to construct $\mathcal{P}''$.

This could be explained better!

Apply $\operatorname{Hom}_R(-, M)$ to this diagram of resolutions and use the fact that

$$0 \to P'_n \to P'_n \oplus P''_n \to P''_n \to 0$$

splits in each degree to get a short exact sequence of cochain complexes

$$0 \to \operatorname{Hom}_R(\mathcal{P}'', M) \to \operatorname{Hom}_R(\mathcal{P}, M) \to \operatorname{Hom}_R(\mathcal{P}', M) \to 0.$$

The long exact sequence in cohomology is the one we are trying to construct. □

Here is an immediate deduction:

Corollary 2.4.4. *1. An R-module P is projective if and only if for all $n \geq 1$ and for all modules M we have $\operatorname{Ext}^n_R(P, M) = 0$.*

2. An R-module I is injective if and only if for all $n \geq 1$ and for all modules M we have $\operatorname{Ext}^n_R(M, I) = 0$.

Proof. (1) If P is projective then $\cdots \to 0 \to P \to P \to 0$ is a projective resolution of P, so that the complex $\operatorname{Hom}_R(\mathcal{P}, M)$ is zero above degree 0 and hence so is its cohomology. Conversely, if $\operatorname{Ext}^n_R(P, M) = 0$ for all $n \geq 1$ then whenever we have a short exact sequence $0 \to A \to B \to C \to 0$ the long exact sequence becomes

$$0 \to \operatorname{Hom}_R(P, A) \to \operatorname{Hom}_R(P, B) \to \operatorname{Hom}_R(P, C) \to \operatorname{Ext}^1_R(P, A) = 0$$

so that $\operatorname{Hom}_R(P, -)$ is an exact functor. It follows that P is projective.

(2) If I is injective then $\operatorname{Hom}_R(-, I)$ is an exact functor so $\operatorname{Hom}_R(\mathcal{P}, I)$ has zero cohomology except in degree 0, and hence the Ext groups are zero above degree 0. Conversely if these Ext groups are zero we deduce as in part (1) from the long exact sequence that $\operatorname{Hom}_R(-, I)$ is an exact functor, so the I is injective. □

We see in the above that we only need the groups $\operatorname{Ext}^1_R(P, M)$ to vanish for all modules M to deduce that P is projective, and similarly only $\operatorname{Ext}^1_R(M, I)$ needs to vanish for all modules M to deduce that I is injective.

Corollary 2.4.5. *Let $0 \to A \to B \to C \to 0$ be a short exact sequence of R-modules.*

1. If B is projective then $\operatorname{Ext}^n_R(C, M) \cong \operatorname{Ext}^{n-1}_R(A, M)$ for all modules M, provided $n \geq 2$.

2. If B is injective then $\operatorname{Ext}^{n-1}_R(C, M) \cong \operatorname{Ext}^n_R(A, M)$ for all modules M, provided $n \geq 2$.

Proof. For the proof of 1, part of the long exact sequence becomes

$$0 = \operatorname{Ext}^{n-1}_R(B, M) \to \operatorname{Ext}^{n-1}_R(A, M) \to \operatorname{Ext}^n_R(C, M) \to \operatorname{Ext}^n_R(B, M) = 0$$

giving the claimed isomorphism. The proof of 2 is similar using the long exact sequence in the second variable. □

The process of changing the degree of an Ext group at the expense of changing the module as indicated in the above corollary is known as *dimension shifting*. It is useful in showing that Ext groups are well-defined up to isomorphism, and also in defining operations on the Ext groups, as well as obtaining different identifications of specific Ext groups that arise.

The next result provides a useful way to compute Ext groups.

Proposition 2.4.6. *Let A and M be R-modules, let $\cdots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to M \to 0$ be a projective resolution of M, and put $K_i = \operatorname{Ker} d_i$. There is an exact sequence*

$$0 \to \operatorname{Hom}_R(K_{n-2}, A) \to \operatorname{Hom}_R(P_{n-1}, A) \to \operatorname{Hom}_R(K_{n-1}, A) \to \operatorname{Ext}^n_R(M, A) \to 0.$$

This result shows that every element of $\operatorname{Ext}^n_R(M, N)$ is represented by a homomorphism $K_{n-1} \to N$.

Proof. First proof: The long exact sequence associated to $0 \to K_{n-1} \to P_{n-1} \to K_{n-2} \to 0$ starts

$$0 \to \operatorname{Hom}_R(K_{n-2}, A) \to \operatorname{Hom}_R(P_{n-1}, A) \to \operatorname{Hom}_R(K_{n-1}, A) \to \operatorname{Ext}^1_R(K_{n-2}, A) \to 0.$$

By dimension shifting we have

$$\operatorname{Ext}^1_R(K_{n-2}, A) \cong \operatorname{Ext}^2_R(K_{n-3}, A) \cong \cdots \cong \operatorname{Ext}^{n-1}_R(K_0, A) \cong \operatorname{Ext}^n_R(M, A).$$

Second proof: From the definition, $\operatorname{Ext}^n_R = \operatorname{Ker} d_n / \operatorname{Im} d_{n-1}$ where the differentials d_j appear in the cochain complex

$$\begin{array}{ccccccc}
\operatorname{Hom}(P_{n-1}, N) & & \xrightarrow{d_{n-1}} & & \operatorname{Hom}(P_n, N) & \to & \operatorname{Hom}(P_{n+1}, N) \\
& \searrow & & \nearrow & & \searrow \quad \nearrow & \\
& & \operatorname{Hom}(K_{n-1}, N) & & & \operatorname{Hom}(K_n, N) & \\
& \nearrow & & & \nearrow & & \\
0 & & & & 0 & &
\end{array}.$$

Left exactness of Hom gives $\operatorname{Hom}(K_{n-1}, N) = \operatorname{Ker} d_n$. This produces an exact sequence $\operatorname{Hom}(P_{n-1}, N) \to \operatorname{Hom}(K_{n-1}, N) \to \operatorname{Ext}^n(M, N) \to 0$. We supply the kernel of the map at the left using the left exactness of Hom. □

We now show that Ext groups are well-defined by proving a uniqueness result for projective resolutions.

Theorem 2.4.7. *Let $\mathcal{P} \to M$ and $\mathcal{Q} \to N$ be complexes of R-modules, where the modules in $\mathcal{P}$ are projective and $\mathcal{Q} \to N \to 0$ is an acyclic complex. Every homomorphism $\phi : M \to N$ lifts to a map of chain complexes*

$$\begin{array}{ccc}
\mathcal{P} & \longrightarrow & M \\
\big\downarrow & & \big\downarrow \phi \\
\mathcal{Q} & \longrightarrow & N
\end{array}$$

and any two such mappings of complexes $\mathcal{P} \to \mathcal{Q}$ that lift ϕ are chain homotopic.

Proof. We construct by induction on n a commutative diagram of the following form, for each n:

$$\begin{array}{ccccccccccccc}
P_n & \xrightarrow{d_n} & P_{n-1} & \xrightarrow{d_{n-1}} & P_{n-2} & \xrightarrow{d_{n-2}} & \cdots & \to & P_0 & \to & M & \to & 0 \\
 & & \downarrow{\scriptstyle \phi_{n-1}} & & \downarrow{\scriptstyle \phi_{n-2}} & & & & \downarrow{\scriptstyle \phi_0} & & \downarrow{\scriptstyle \phi} & & \\
Q_n & \xrightarrow{e_n} & Q_{n-1} & \xrightarrow{e_{n-1}} & Q_{n-2} & \xrightarrow{e_{n-2}} & \cdots & \to & Q_0 & \to & M & \to & 0
\end{array}$$

We start the induction at $n = 0$ using projectivity of P_0 and the fact that $Q_0 \to M$ is an epimorphism. For the induction step, suppose that $\phi_0, \ldots, \phi_{n-1}$ have been defined. Now $e_{n-1}\phi_{n-1}d_n = \phi_{n-2}d_{n-1}d_n = 0$, so $\operatorname{Im}\phi_{n-1}d_n \subseteq \operatorname{Ker} e_{n-1} = \operatorname{Im} e_n$. We may now define ϕ_n by the projectivity of P_n.

To show that any two families of maps (ϕ_n) and (ψ_n) lifting ϕ are chain homotopic, we construct mappings $T_n : P_n \to Q_{n+1}$ so that $\phi_n - \psi_n = e_{n+1}T_n + T_{n-1}d_n$ for all $n \geq 0$, with the understanding that $T_{-1} = 0$. We define $\phi_{-1} = \psi_{-1} = \phi$. Suppose that T_{n-1} has been constructed. We calculate

$$\begin{aligned}
e_n(\phi_n - \psi_n - T_{n-1}d_n) &= \phi_{n-1}d_n - \psi_{n-1}d_n - e_nT_{n-1}d_n \\
&= (\phi_{n-1} - \psi_{n-1} - e_nT_{n-1})d_n \\
&= T_{n-2}d_{n-1}d_n \\
&= 0.
\end{aligned}$$

Therefore $\operatorname{Im}(\phi_n - \psi_n - T_{n-1}d_n) \subseteq \operatorname{Im} e_{n+1}$ and so there exists T_n with

$$(\phi_n - \psi_n - T_{n-1}d_n) = e_{n+1}T_n,$$

by projectivity of P_n. Rearranging this equation, it is $\phi_n - \psi_n = e_{n+1}T_n + T_{n-1}d_n$, as required. □

Corollary 2.4.8. *Let $\mathcal{P}_1 \to M$ and $\mathcal{P}_2 \to M$ be two projective resolutions of M.*
(1) $\mathcal{P}_1 \to M$ and $\mathcal{P}_2 \to M$ are chain homotopy equivalent.
(2) If F is any R-linear functor from R-modules to abelian groups, then

$$H_*(F(\mathcal{P}_1) \cong H_*(F(\mathcal{P}_2)$$

by a canonical isomorphism.
(3) $\operatorname{Ext}^n_R(M, N)$ is functorial in both variables.

We remark also that $Ext^n_R(M, N)$ can also be defined by taking an injective resolution $N \to \mathcal{I}$ of N and forming $H_n(\operatorname{Hom}_R(M, \mathcal{I}))$. It is a theorem that we get a group that is naturally isomorphic to the group defined by a projective resolution of M. We say that Ext is *balanced* to indicate that it has this property.

Definition 2.4.9. Let M be a left R-module, N a right R-module, and $\mathcal{P} \to N$ a resolution of N by projective right modules. We put

$$\operatorname{Tor}^R_n(N, M) = H_n(\mathcal{P} \otimes_R M),$$

which is the nth homology of the complex

$$\cdots \to P_2 \otimes_R M \to P_1 \otimes_R M \to P_0 \otimes_R M \to 0.$$

Tor has properties analogous to those of Ext and we list them below. They are proved in a similar manner to the corresponding results for Ext, using that $\_\_ \otimes_R M$ is right exact instead of left exact.

Proposition 2.4.10. $\mathrm{Tor}_0^R(N, M) \cong N \otimes_R M$.

Theorem 2.4.11. *If $0 \to A \to B \to C \to 0$ and $0 \to L \to M \to N \to 0$ are short exact sequences of right and left modules respectively there are long exact sequences*

(i)
$$\begin{aligned}\cdots &\to \mathrm{Tor}_2^R(C, L) \to \mathrm{Tor}_1^R(A, L) \to \mathrm{Tor}_1^R(B, L) \to \mathrm{Tor}_1^R(C, L)\\ &\to A \otimes_R L \to B \otimes_R L \to C \otimes_R L \to 0\end{aligned}$$

and

(ii)
$$\begin{aligned}\cdots &\to \mathrm{Tor}_2^R(A, N) \to \mathrm{Tor}_1^R(A, L) \to \mathrm{Tor}_1^R(A, M) \to \mathrm{Tor}_1^R(A, N)\\ &\to A \otimes_R L \to A \otimes_R M \to A \otimes_R N \to 0.\end{aligned}$$

Remark 2.4.12. One can view Tor as a measure of the failure of $\otimes$ to be left exact.

Proposition 2.4.13. $\mathrm{Tor}_n^R(N, M) = 0$ *if either of M or N is flat and $n > 0$.*

It follows that $\mathrm{Tor}_n^R(N, M) = 0$ if M or N is projective, because projective modules are flat. This allows a process of 'dimension shifting' analogous to that for Ext.

In the next result we let

$$\begin{array}{ccccccccccccc}\cdots & \to & P_2 & & \xrightarrow{d_2} & & P_1 & & \xrightarrow{d_1} & & P_0 & \to & N & \to & 0\\ & & & \searrow & & \nearrow & & \searrow & & \nearrow & & & & & \\ & & & & K_1 & & & & K_0 & & & & & & \end{array}$$

be the resolution of N, so that $K_n = d_{n+1}(P_{n+1})$.

Proposition 2.4.14. *There is an exact sequence*

$$0 \to \mathrm{Tor}_n^R(N, M) \to K_{n-1} \otimes_R M \to P_{n-1} \otimes_R M \to K_{n-2} \otimes_R M \to 0$$

for $n \geq 1$. (Here we take $K_{-1} = N$.)

Remark 2.4.15. We can also calculate $\mathrm{Tor}_n^R(N, M)$ by taking a projective resolution of M by left modules, applying $N \otimes_R -$ and taking homology of the resulting complex. In this way one obtains a sequence of functors that turn out to be naturally isomorphic to the functors we have defined.

2.5 Pushouts, pullbacks and Schanuel's lemma

For this see section 10.5 of Dummit and Foote, Exercises 27 and 28.

Include pages 19-23 of my original notes about the correspondence of $\mathrm{Ext}^1(M, N)$ with module extensions, and properties of pushouts.

Chapter 3

Group cohomology

3.1 Group representations

This section is extracted from P.J. Webb, A course in finite group representation theory, Cambridge 2016.

Let G denote a finite group, and let R be a commutative ring with a 1. If V is an R-module we denote by $GL(V)$ the group of all invertible R-module homomorphisms $V \to V$. In case $V \cong R^n$ is a free module of rank n this group is isomorphic to the group of all non-singular $n \times n$ matrices over R, and we denote it by $GL(n, R)$ or $GL_n(R)$, or in case $R = \mathbb{F}_q$ is the finite field with q elements by $GL(n, q)$ or $GL_n(q)$. We point out also that unless otherwise stated, modules will be left modules and morphisms will be composed reading from right to left, so that matrices in $GL(n, R)$ are thought of as acting from the left on column vectors.

A *(linear) representation* of G (over R) is a group homomorphism

$$\rho : G \to GL(V).$$

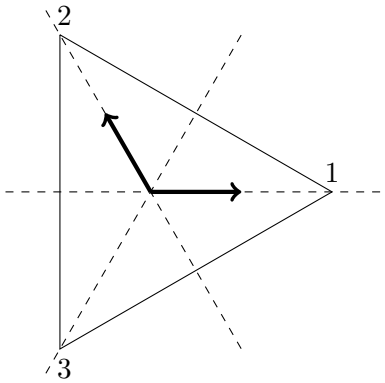
In a situation where V is free as an R-module, on taking a basis for V we may write each element of $GL(V)$ as a matrix with entries in R and we obtain for each $g \in G$ a matrix $\rho(g)$. These matrices multiply together in the manner of the group and we have a *matrix representation* of G. In this situation the rank of the free R-module V is called the *degree* of the representation. Sometimes by abuse of terminology the module V is also called the representation, but it should more properly be called the *representation module* or *representation space* (if R is a field).

To illustrate some of the possibilities that may arise we consider some examples.

Example 3.1.1. For any group G and commutative ring R we can take $V = R$ and $\rho(g) = 1$ for all $g \in G$, where 1 denotes the identify map $R \to R$. This representation is called the *trivial representation*, and it is often denoted simply by its representation module R. Although this representation turns out to be extremely important in the theory, it does not at this point give much insight into the nature of a representation.

Example 3.1.2. A representation on a space $V = R$ of rank 1 is in general determined by specifying a homomorphism $G \to R^\times$. Here $R^\times$ is the group of units of R, and it is isomorphic to $GL(V)$. For example, if $G = \langle g \rangle$ is cyclic of order n and $k = \mathbb{C}$ is the field of complex numbers, there are n possible such homomorphisms, determined by $g \mapsto e^{\frac{2r\pi i}{n}}$ where $0 \leq r \leq n-1$. Another important example of a degree 1 representation is the *sign representation* of the symmetric group S_n on n symbols, given by the group homomorphism which assigns to each permutation its sign, regarded as an element of the arbitrary ring R.

Example 3.1.3. Let $R = \mathbb{R}$, $V = \mathbb{R}^2$ and $G = S_3$. This group G is isomorphic to the group of symmetries of an equilateral triangle. The symmetries are the three reflections in the lines that bisect the equilateral triangle, together with three rotations.



Positioning the center of the triangle at the origin of V and labeling the three vertices of the triangle as 1, 2 and 3 we get a representation

$$
\begin{aligned}
() &\mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
(1,2) &\mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\
(1,3) &\mapsto \begin{bmatrix} -1 & 0 \\ -1 & 1 \end{bmatrix} \\
(2,3) &\mapsto \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix} \\
(1,2,3) &\mapsto \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \\
(1,3,2) &\mapsto \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}
\end{aligned}
$$

where we have taken basis vectors in the directions of vertices 1 and 2, making an angle of $\frac{2\pi}{3}$ to each other. In fact these matrices define a representation of degree 2 over any ring R, because although the representation was initially constructed over

$\mathbb{R}$ the matrices have integer entries, and these may be interpreted in every ring. No matter what the ring is, the matrices always multiply together to give a copy of S_3.

At this point we have constructed three representations of S_3: the trivial representation, the sign representation and one of dimension 2.

Example 3.1.4. Let $R = \mathbb{F}_p$, $V = R^2$ and let $G = C_p = \langle g \rangle$ be cyclic of order p generated by an element g. We see that the assignment

$$\rho(g^r) = \begin{bmatrix} 1 & 0 \\ r & 1 \end{bmatrix}$$

is a representation. In this case the fact that we have a representation is very much dependent on the choice of R as the field $\mathbb{F}_p$: in any other characteristic it would not work, because the matrix shown would no longer have order p.

We can think of representations in various ways. One of them is that a representation is the specification of an action of a group on an R-module, as we now explain. Given a representation $\rho : G \to GL(V)$, an element $v \in V$ and a group element $g \in G$ we get another module element $\rho(g)(v)$. Sometimes we write just $g \cdot v$ or gv for this element. This rule for multiplication satisfies

$$\begin{aligned} g \cdot (\lambda v + \mu w) &= \lambda g \cdot v + \mu g \cdot w \\ (gh) \cdot v &= g \cdot (h \cdot v) \\ 1 \cdot v &= v \end{aligned}$$

for all $g \in G$, $v, w \in V$ and $\lambda, \mu \in R$. A rule for multiplication $G \times V \to V$ satisfying these conditions is called a *linear action* of G on V. To specify a linear action of G on V is the same thing as specifying a representation of G on V, since given a representation we obtain a linear action as indicated above, and evidently given a linear action we may recover the representation.

Another way to define a representation of a group is in terms of the group algebra. We define the *group algebra* RG (or $R[G]$) of G over R to be the free R-module with the elements of G as an R-basis, and with multiplication given on the basis elements by group multiplication. The elements of RG are the (formal) R-linear combinations of group elements, and the multiplication of the basis elements is extended to arbitrary elements using bilinearity of the operation. What this means is that a typical element of RG is an expression $\sum_{g \in G} a_g g$ where $a_g \in R$, and the multiplication of these elements is given symbolically by

$$(\sum_{g \in G} a_g g)(\sum_{h \in G} b_h h) = \sum_{k \in G} (\sum_{gh=k} a_g b_h) k.$$

More concretely, we exemplify this definition by listing some elements of the group algebra $\mathbb{Q}S_3$. We write elements of S_3 in cycle notation, such as $(1, 2)$. This group element gives rise to a basis element of the group algebra which we write either as $1 \cdot (1, 2)$, or simply as $(1, 2)$ again. The group identity element $()$ also serves as the

identity element of $\mathbb{Q}S_3$. In general, elements of $\mathbb{Q}S_3$ may look like $(1,2)-(2,3)$ or $\frac{1}{5}(1,2,3)+6(1,2)-\frac{1}{7}(2,3)$. Here is a computation:

$$\begin{aligned}(3(1,2,3)+(1,2))(()-2(2,3)) &= 3(1,2,3)+(1,2)-6(1,2)-2(1,2,3)\\ &= (1,2,3)-5(1,2).\end{aligned}$$

An (associative) *R-algebra* is defined to be a (not necessarily commutative) ring A with a 1, equipped with a (unital) ring homomorphism $R \to A$ whose image lies in the center of A. The group algebra RG is indeed an example of an R-algebra.

Example 3.1.5. If $G = \langle x \rangle$ is an infinite cyclic group then $\mathbb{Z}G = \mathbb{Z}[x, x^{-1}]$ is the ring of Laurent polynomials in x.

Example 3.1.6. If p is a prime number it follows from some algebraic number theory that the ring of integers $\mathbb{Z}[e^{2\pi i/p}]$ has rank $p-1$ as a free abelian group. If $G = \rangle x \langle$ is cyclic of order p, there is a surjective ring homomorphism $\mathbb{Z}G \to \mathbb{Z}[e^{2\pi i/p}]$ specified by $x \mapsto e^{2\pi i/p}]$. Its kernel is $\mathbb{Z}N$, where $N = \sum_{g\in G} g$. Notice that $N^2 = |G|N$. This relationship shows that $\mathbb{Z}[e^{2\pi i/p}]$-modules may be regarded as $\mathbb{Z}G$ modules.

Having defined the group algebra, we may now define a representation of G over R to be a unital RG-module. The fact that this definition coincides with the previous ones is the content of the next proposition. Throughout this text we may refer to group representations as modules (for the group algebra).

Proposition 3.1.7. *A representation of G over R has the structure of a unital RG-module. Conversely, every unital RG-module provides a representation of G over R.*

Proof. Given a representation $\rho : G \to GL(V)$ we define a module action of RG on V by $(\sum a_g g)v = \sum a_g \rho(g)(v)$.

Given an RG-module V, the linear map $\rho(g) : v \mapsto gv$ is an automorphism of V and $\rho(g_1)\rho(g_2) = \rho(g_1 g_2)$ so $\rho : G \to GL(V)$ is a representation. □

The group algebra gives another example of a representation, called the *regular representation*. In fact for any ring A we may regard A itself as a left A-module with the action of A on itself given by multiplication of the elements. We denote this left A-module by ${}_AA$ when we wish to emphasize the module structure, and this is the (left) regular representation of A. When $A = RG$ we may describe the action on ${}_{RG}RG$ by observing that each element $g \in G$ acts on ${}_{RG}RG$ by permuting the basis elements in the fashion $g \cdot h = gh$. Thus each g acts by a *permutation matrix*, namely a matrix in which in every row and column there is precisely one non-zero entry, and that non-zero entry is 1. The regular representation is an example of a *permutation representation*, namely one in which every group element acts by a permutation matrix.

Regarding representations of G as RG-modules has the advantage that many definitions we wish to make may be borrowed from module theory. Thus we may study RG-submodules of an RG-module V, and if we wish we may call them *subrepresentations* of the representation afforded by V. To specify an RG-submodule of V it is

necessary to specify an R-submodule W of V that is closed under the action of RG. This is equivalent to requiring that $\rho(g)w \in W$ for all $g \in G$ and $w \in W$. We say that a submodule W satisfying this condition is *stable* under G, or that it is an *invariant submodule* or *invariant subspace* (if R happens to be a field). Such an invariant submodule W gives rise to a homomorphism $\rho_W : G \to GL(W)$ that is the subrepresentation afforded by W.

Example 3.1.8. 1. Let $C_2 = \{1, -1\}$ be cyclic of order 2 and consider the representation

$$\begin{aligned} \rho : C_2 &\to GL(\mathbb{R}^2) \\ 1 &\mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ -1 &\mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \end{aligned}$$

There are just four invariant subspaces, namely $\{0\}$, $\langle \binom{1}{0} \rangle$, $\langle \binom{0}{1} \rangle$, $\mathbb{R}^2$ and no others. The representation space $\mathbb{R}^2 = \langle \binom{1}{0} \rangle \oplus \langle \binom{0}{1} \rangle$ is the direct sum of two invariant subspaces.

Example 3.1.9. In Example 3.1.4 above, an elementary calculation shows that $\langle \binom{0}{1} \rangle$ is the only 1-dimensional invariant subspace, and so it is not possible to write the representation space V as the direct sum of two non-zero invariant subspaces.

We make use of the notions of a *homomorphism* and an *isomorphism* of RG-modules. Since RG has as a basis the elements of G, to check that an R-linear homomorphism $f : V \to W$ is in fact a homomorphism of RG-modules, it suffices to check that $f(gv) = gf(v)$ for all $g \in G$ — we do not need to check for every $x \in RG$. By means of the identification of RG-modules with representations of G (in the first definition given here) we may refer to homomorphisms and isomorphisms of group representations. In many books the algebraic condition on the representations that these notions entail is written out explicitly, and two representations that are isomorphic are also said to be *equivalent*.

If V and W are RG-modules then we may form their (external) *direct sum* $V \oplus W$, which is the same as the direct sum of V and W as R-modules together with an action of G given by $g(v, w) = (gv, gw)$. We also have the notion of the internal direct sum of RG-modules and write $U = V \oplus W$ to mean that U has RG-submodules V and W satisfying $U = V + W$ and $V \cap W = 0$. In this situation we also say that V and W are *direct summands* of U. We just met this property in Example 3.1.8, which gives a representation that is a direct sum of two non-zero subspaces; by contrast, Example 3.1.9 provides an example of a subrepresentation that is not a direct summand.

3.2 Fixed points, fixed quotients, and the augmentation ideal

When M is a left $\mathbb{Z}G$-module the algebraic definition of group (co)homology of G with coefficients in M, in degree n, is $H^n(G, M) := \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, M)$ and $H_n(G, M) :=$

$\mathrm{Tor}_n^{\mathbb{Z}G}(\mathbb{Z}, M)$. If M is a right $\mathbb{Z}G$-module we also put $H_n(G, M) := \mathrm{Tor}_n^{\mathbb{Z}G}(M, \mathbb{Z})$.

In general we have to deal with left and right modules in describing tensor products and Tor, but in the case of group rings there is a way round this that allows us to get by with considering only left modules. The group ring $\mathbb{Z}G$ has an antiautomorphism $a : \mathbb{Z}G \to \mathbb{Z}G$ specified on the basis elements by $g \mapsto g^{-1}$. Thus a is an isomorphism of abelian groups and $a(xy) = a(y)a(x)$. Given a right module N we may make it into a left module N^ℓ by $x \cdot n = na(x)$ for $x \in \mathbb{Z}G$ and $n \in N$. We check that $(xy) \cdot n = na(xy) = na(y)a(x) = x \cdot (na(y)) = x \cdot (y \cdot n)$. Intuitively, because we can turn left modules M back into right modules M^r by a similar procedure, reversing the previous construction, we lose no information in this process. As a matter of notation we may now refer to right modules N and resolutions $\mathcal{P} \to N$ by writing down the corresponding left modules N^ℓ and $\mathcal{P}^\ell \to N^\ell$. Thus if we have two left $\mathbb{Z}G$-modules A and B, the tensor product $A \otimes_{\mathbb{Z}G} B$ really means $A^r \otimes_{\mathbb{Z}G} B$ and $\mathrm{Tor}_n^{\mathbb{Z}G}(A, B)$ really means $\mathrm{Tor}_n^{\mathbb{Z}G}(A^r, B)$. The outcome is that we only write down left modules, which is a simplification of notation. Note that we do not define the tensor product of two left modules by this, it is just notation.

At a deeper level, it is the case that P is a projective right $\mathbb{Z}G$-module if and only if P^ℓ is a projective left $\mathbb{Z}G$-module. This follows from the facts that projective modules are the summands of free modules, and that $\mathbb{Z}G^\ell \cong \mathbb{Z}G$ as left $\mathbb{Z}G$-modules (the first copy of $\mathbb{Z}G$ being a right module). The isomorphism is $g \mapsto g^{-1}$. Thus if $\mathcal{P} \to N$ is a projective resolution of right modules, $\mathcal{P}^\ell \to N^\ell$ will be a projective resolution of left modules. Finally, the trivial module has the property that $\mathbb{Z}^\ell = \mathbb{Z}$.

We now start to explore these cohomology groups by identifying them in low degrees and by construction of some particular resolutions of $\mathbb{Z}$. We define a mapping $\epsilon : \mathbb{Z}G \to \mathbb{Z}$ by the assignment $g \mapsto 1$ for every $g \in G$, extended by linearity to the whole of $\mathbb{Z}G$. Thus the effect of ϵ on a general element of $\mathbb{Z}G$ is

$$\epsilon(\sum_{g \in G} \lambda_g g) = \sum_{g \in G} \lambda_g.$$

This is the *augmentation map* and it is a ring homomorphism, and also a homomorphism of $\mathbb{Z}G$-modules. We write $IG := \mathrm{Ker}\, \epsilon$ and this 2-sided ideal is called the *augmentation ideal* of $\mathbb{Z}G$. Because ϵ is surjective we may always use it to start a projective $\mathbb{Z}G$-resolution of $\mathbb{Z}$, and evidently $\mathbb{Z} \cong \mathbb{Z}G/IG$. If G is finite we will also consider the element $N = \sum_{g \in G} g \in \mathbb{Z}G$, which is sometimes called the *norm element*.

If M is a $\mathbb{Z}G$-module we write $M^G := \{m \in M \mid gm = m \text{ for all } g \in G\}$ for the *fixed points* of G on M and $M_G := M/\langle gm - m \mid m \in M,\, g \in G\rangle$ for the *fixed quotient* or *cofixed points* of G on M, where the submodule being factored out is the span of all elements $gm - m$, $m \in M$, $g \in G$.

Proposition 3.2.1. *Let M be a $\mathbb{Z}G$-module.*

1. *The set $\{g - 1 \mid 1 \neq g \in G\}$ is a $\mathbb{Z}$-basis for IG.*
2. *$H^0(G, M) = \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M) \cong M^G$. The fixed point set M^G coincides with the set of elements of M annihilated by IG.*

3. *$H_0(G, M) = \mathbb{Z} \otimes_{\mathbb{Z}G} M \cong M/(IG \cdot M) = M_G$ is the largest quotient of M on which G acts trivially.*

4. *$(\mathbb{Z}G)_G = \mathbb{Z}G/IG \cong \mathbb{Z}$. If G is finite then $(\mathbb{Z}G)^G = \mathbb{Z} \cdot N \cong \mathbb{Z}$, while if G is infinite then $(\mathbb{Z}G)^G = 0$.*

5. *If $G = \langle g_1, \ldots, g_n \rangle$ then $g_1 - 1, \ldots, g_n - 1$ generate IG as a $\mathbb{Z}G$-module.*

Proof. (1) The set is independent and is contained in $\operatorname{Ker} \epsilon$. To show that it spans $\operatorname{Ker} \epsilon$, suppose that $\sum_{g \in G} \lambda_g g \in \operatorname{Ker} \epsilon$ where $\lambda_g \in \mathbb{Z}$. This means that $\sum_{g \in G} \lambda_g = 0$. Thus $\sum_{g \in G} \lambda_g g = \sum_{g \in G} \lambda_g g - \sum_{g \in G} \lambda_g = \sum_{g \in G} \lambda_g (g-1)$, showing that $\{g - 1 \mid 1 \neq g \in G\}$ spans $\operatorname{Ker} \epsilon$.

(2) The first equality is a standard result about Ext groups. The map that sends a $\mathbb{Z}G$-module homomorphism $\phi : \mathbb{Z} \to M$ to $\phi(1)$ is an isomorphism $\operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M) \to M^G$. An element $m \in M$ is fixed by G if and only if $(g-1)m = 0$ for all $g \in G$, which happens if and only if $IGm = 0$, by part (1).

(3) The first equality is a standard result about Tor groups. Since $\mathbb{Z} \cong \mathbb{Z}G/IG$ and tensor product with a quotient of a ring is the same as factoring out the action of the quotienting ideal, the next isomorphism follows. From part (1) we have that $IG \cdot M$ is the span of elements $(g-1)m$ with $g \in G$ and $m \in M$ and this gives the identification with M_G. If N is a submodule of M then G acts trivially on M/N if and only if $(g-1)m \in N$ for all $g \in G$, and this shows that M_G is the largest quotient of M on which G acts trivially.

What about the symbol N? It is used for a submodule and also the group element sum.

(4) The first statement is a particular case of (3). If $\sum_{x \in G} \lambda_x x \in \mathbb{Z}G$ is fixed by G it equals $g \sum_{x \in G} \lambda_x x$ for all $g \in G$. The coefficients of gx in these two expressions are λ_{gx} in the first and λ_x in the second, so $\lambda_{gx} = \lambda_x$ for all g in G since the group elements form a basis of $\mathbb{Z}G$. If G is infinite and some λ_x is non-zero this group ring element must have infinite support on the basis, which is not possible, so in this case $(\mathbb{Z}G)^G = 0$. If G is finite all the coefficients of group elements must be equal, so the fixed element is a scalar multiple of N.

(5) Any group element can be expressed as a product $u_1 u_2 \cdots u_t$ where each u_i is either one of the given generators or its inverse. Now

$$u_1 u_2 \cdots u_t - 1 = u_1 u_2 \cdots u_{t-1}(u_t - 1) + u_1 u_2 \cdots u_{t-2}(u_{t-1} - 1) + \cdots + (u_1 - 1)$$

and also $g_i^{-1} - 1 = -g_i^{-1}(g_i - 1)$. Applying these two formulas allows us to express any basis element $g - 1$ of IG as an element of the $\mathbb{Z}G$-submodule generated by the $g_i - 1$. We deduce that the elements $g_i - 1$ generate IG as a $\mathbb{Z}G$-module. □

Class Activity. Let $G = \{1, x\} = C_2$ be a cyclic group of order 2.

1. What is $\operatorname{rank}_{\mathbb{Z}}(IG)$?

2. Is $IG \cong \mathbb{Z}$, the trivial $\mathbb{Z}G$-module, as abelian groups?

3. Is $IG \cong \mathbb{Z}$, the trivial $\mathbb{Z}G$-module, as $\mathbb{Z}G$-modules?

4. Is $N \in IG$?

5. Is $\mathbb{Z}G/(N) \cong \mathbb{Z}$ as $\mathbb{Z}G$-modules? Is $\mathbb{Z}G/(N) \cong IG$ as $\mathbb{Z}G$-modules? (Warning: one of these is true for cyclic groups. In general neither of them is true.)

3.3 Resolutions for group rings and first (co)homology

Insert something!

Proposition 3.3.1. *$H_1(G, \mathbb{Z}) \cong IG/(IG)^2 \cong G/G'$, the abelianization of G.*

Proof. We compute $H_1(G, \mathbb{Z})$ by applying $\mathbb{Z} \otimes_{\mathbb{Z}G} -$ to the sequence

$$0 \to IG \to \mathbb{Z}G \to \mathbb{Z} \to 0,$$

getting an exact sequence

$$0 = H_1(G, \mathbb{Z}G) \to H_1(G, \mathbb{Z}) \to \mathbb{Z} \otimes_{\mathbb{Z}G} IG \to \mathbb{Z} \otimes_{\mathbb{Z}G} \mathbb{Z}G \to \mathbb{Z} \otimes_{\mathbb{Z}G} \mathbb{Z} \to 0.$$

The left term is zero since $\mathbb{Z}G$ is projective and hence flat. The two right terms identify as $\mathbb{Z} \to \mathbb{Z}$ via the identity map, so we deduce that $H_1(G, \mathbb{Z}) \cong \mathbb{Z} \otimes_{\mathbb{Z}G} IG \cong IG/(IG)^2$.

We now construct an isomorphism $G/G' \to IG/(IG)^2$. We will write elements of G/G' multiplicatively as cosets gG' and elements of $IG/(IG)^2$ additively as cosets $x + IG^2$. Consider the mapping $G \to IG/(IG)^2$ specified by $g \mapsto (g-1) + IG^2$. It sends a product gh to

$$\begin{aligned} gh - 1 + IG^2 &= (g-1)(h-1) + (g-1) + (h-1) + IG^2 \\ &= (g-1) + (h-1) + IG^2, \end{aligned}$$

so that it is a group homomorphism. Because the target group is abelian it vanishes on the commutator subgroup G'. We therefore obtain a homomorphism $G/G' \to IG/(IG^2)$. An inverse homomorphism is constructed as follows. First consider the homomorphism of abelian groups $IG \to G/G'$ specified on the basis elements of IG by $(g-1) \mapsto gG'$. It sends a product $(g-1)(h-1) = (gh-1) - (g-1) - (h-1)$ to $(gh)(g^{-1})(h^{-1})G' = G'$ and hence induces a homomorphism $IG/(IG^2) \to G/G'$. Evidently these two mappings are mutually inverse. □

3.3.1 Resolutions for free groups and for cyclic groups

Example 3.3.2. We now consider some examples of resolutions for group rings. Let G be a free group of rank d. Then G acts freely on its Cayley graph Γ with respect to a set of free generators, which we know to be a tree. Its vertices are in a single regular orbit, and its edges lie in d regular orbits, one for each generator. We see from this that the augmented simplicial chain complex of this tree is an acyclic complex

$$0 \to \mathbb{Z}G^d \to \mathbb{Z}G \to \mathbb{Z} \to 0$$

so that this is a projective resolution of $\mathbb{Z}$. Apart from $\mathbb{Z}$, these are free abelian groups of infinite rank. If we apply either $\mathbb{Z} \otimes_{\mathbb{Z}G} -$ or $\mathrm{Hom}_{\mathbb{Z}G}(-, \mathbb{Z})$ we get either the augmented

cellular chain complex $0 \to \mathbb{Z}^d \to \mathbb{Z} \to \mathbb{Z} \to 0$ or the augmented cellular cochain complex $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}^d \to 0$ of the quotient graph $G\backslash\Gamma$. This quotient consists of d loops joined at a single vertex, and it is an Eilenberg-MacLane space for G. Its homology and cohomology is the same as that computed algebraically:

$$H^0(G,\mathbb{Z}) \cong H_0(G,\mathbb{Z}) \cong \mathbb{Z}$$
$$H^1(G,\mathbb{Z}) \cong H_1(G,\mathbb{Z}) \cong \mathbb{Z}^d$$
$$H^i(G,\mathbb{Z}) \cong H_i(G,\mathbb{Z}) = 0 \text{ otherwise.}$$

We see various things from this:

Proposition 3.3.3. *When G is a free group of rank d, $H_n(G,M) = H^n(G,M) = 0$ if $n > 1$. Also, $IG \cong (\mathbb{Z}G)^d$ is a free $\mathbb{Z}G$-module of rank d.*

Notice that when $G = \mathbb{Z}$ is free of rank 1 we have $\mathbb{Z}G \cong \mathbb{Z}[x, x^{-1}]$, the ring of Laurent polynomials in the generator x of G. A group is said to have *cohomological dimension* d if there is a projective resolution

$$0 \to P_d \to P_{d-1} \to \cdots \to P_0 \to \mathbb{Z} \to 0$$

and d is the smallest integer for which this happens. It is equivalent to require that $H^n(G,M) = 0$ for all modules M and for all $n \geq d+1$. We see (as an exercise) that the identity group is the only group of cohomological dimension 0, and that free groups have cohomological dimension 1. The converse, that groups of cohomological dimension 1 are free, is a theorem of Stallings (1968) in the case of finitely generated groups and Swan (1969) in general.

In the above example we see the connection between the topological approach to group (co)homology as the (co)homology of an aspherical space with fundamental group G, and the algebraic approach that is computed via a projective resolution. Given such an aspherical space its universal cover is a contractible space on which G acts freely. It follows that G acts on the chain complex of the universal cover (for example, the simplicial chain complex if the space is a simplicial complex) and the free action means that the chain complex is an acyclic complex of free $\mathbb{Z}G$-modules, or in other words a projective resolution of $\mathbb{Z}$. Applying $\mathbb{Z} \otimes_{\mathbb{Z}G} -$ to this resolution converts each copy of $\mathbb{Z}G$ spanned by a regular orbit of simplices into a single copy of $\mathbb{Z}$ and produces a complex that may be identified with the chain complex of the aspherical space. Its homology is $H_*(G,\mathbb{Z})$. From this viewpoint we see that the interpretation of $H_1(G,\mathbb{Z})$ as the abelianization of G exemplifies the theorem of Hurewicz that the first homology is the abelianization of the fundamental group.

We present another example: finite cyclic groups.

Theorem 3.3.4. *Let $G = \langle g \rangle$ be a finite cyclic group. There is a periodic resolution*

$$\cdots \to \mathbb{Z}G \xrightarrow{d_2} \mathbb{Z}G \xrightarrow{d_1} \mathbb{Z}G \to \mathbb{Z} \to 0$$

$$\nearrow \quad \searrow \quad \nearrow \quad \searrow \quad \nearrow$$

$$IG \qquad \mathbb{Z}\cdot N \qquad IG$$

in which $d_1(1) = g - 1$ *and* $d_2(1) = N$.

Proof. Since G is generated by the single element g, so IG is generated as a $\mathbb{Z}G$-module by $g - 1$ and so d_1 maps surjectively to IG. An element $x \in \mathbb{Z}G$ lies in the kernel of d_1 if and only if $x \cdot (g - 1) = 0$, which happens if and only if $x \in \mathbb{Z}G^G$, if and only if $x = \lambda N$ for some $\lambda \in \mathbb{Z}$. Thus $\operatorname{Ker} d_1 = \mathbb{Z} \cdot N \cong \mathbb{Z}$. We now iterate this start of the resolution. □

Corollary 3.3.5. *Let* $G = \langle g \rangle$ *be a finite cyclic group and* M *a* $\mathbb{Z}G$*-module. Then for all* $n \geq 1$ *we have*

$$H^{2n-1}(G, M) \cong H^1(G, M) \cong \operatorname{Ker}(M \xrightarrow{N} M)/(IG \cdot M)$$

and

$$H^{2n}(G, M) \cong H^2(G, M) \cong M^G/(N \cdot M).$$

Proof. We apply $\operatorname{Hom}_{\mathbb{Z}G}(-M)$ to the resolution in Theorem 3.3.4 to get a complex

$$0 \longrightarrow M \xrightarrow{g-1} M \xrightarrow{N} M \xrightarrow{g-1} M \xrightarrow{N} M \longrightarrow \cdots$$

where N and $g - 1$ denote the maps that are multiplication by these elements. We take homology to obtain the result, using the fact that the kernel of $g - 1$ is the fixed points, by Proposition 3.2.1(2). □

Example 3.3.6. If G is cyclic of order r and $M = \mathbb{Z}$ then for every $n \geq 1$ we have $H^{2n-1}(G, \mathbb{Z}) = 0$ and $H^{2n}(G, \mathbb{Z}) = \mathbb{Z}/r\mathbb{Z}$.

Maybe include here the bar resolution?

Class Activity. If G is cyclic of order r and $M = \mathbb{Z}/r\mathbb{Z}$ find $H^i(G, M)$. Answers: A: for all $i \geq 1$, $H^{2i-1}(G, \mathbb{Z}/r\mathbb{Z}) = \mathbb{Z}/r\mathbb{Z}$ and $H^{2i}(G, \mathbb{Z}/r\mathbb{Z}) = 0$; B: for all $i \geq 1$, $H^{2i-1}(G, \mathbb{Z}/r\mathbb{Z}) = 0$ and $H^{2i}(G, \mathbb{Z}/r\mathbb{Z}) = \mathbb{Z}/r\mathbb{Z}$; C: $H^i(G, \mathbb{Z}/r\mathbb{Z}) = \mathbb{Z}/r\mathbb{Z}$ for all $i \geq 1$; D: None of the above.

Proposition 3.3.7. *Let* H *be a subgroup of* G.

1. *If the cohomological dimension* $\operatorname{cd}(G) = d$ *then* $cd(H) \leq d$, *and*
2. *groups of finite cohomological dimension are torsion free.*

Proof. (1) A finite resolution of $\mathbb{Z}$ by projective $\mathbb{Z}G$-modules is also, by restriction, a finite resolution of $\mathbb{Z}$ by projective $\mathbb{Z}H$-modules, because projective $\mathbb{Z}G$-modules restrict to projective $\mathbb{Z}H$-modules. If there is a resolution over $\mathbb{Z}G$ of length d, then there is a resolution over $\mathbb{Z}H$ of length at most d.

(2) If $\operatorname{cd}(G) = d$ and G has an element g of finite order, then $\operatorname{cd}\langle g \rangle \leq d$. However, we have seen in Example 3.3.6 that cyclic groups of order bigger than 1 have non-zero cohomology groups in arbitrarily high degrees, so cannot have finite resolutions of $\mathbb{Z}$. □

As a partial converse to the above result, Serre has shown that if G is a torsion-free group with a subgroup H of finite index, then $\operatorname{cd}(G) = \operatorname{cd}(H)$.

Exercise: Show that G is a torsion free group with a cyclic subgroup of finite index then G is cyclic.

3.3.2 Derivations and first cohomology

We next examine the first degree cohomology and for this we introduce derivations.

Definition 3.3.8. Let M be a $\mathbb{Z}G$-module. A mapping $d : G \to M$ is a *derivation* if and only if $d(gh) = gd(h) + d(g)$. We write $\mathrm{Der}(G, M) := \{\text{derivations } G \to M\}$ for the set of derivations of G into M. It is a group with respect to the addition $(d_1 + d_2)(g) = d_1(g) + d_2(g)$. Observe that the defining equation for a derivation looks more symmetric if we regard M as having the trivial G-action from the right, in which case $d(gh) = gd(h) + d(g)h$. We can always construct a derivation from G to M for any element $M \in M$ by putting $d(g) = (g - 1)m$ for each $g \in G$. We check that such map is indeed a derivation. A derivation arising in this way is called *principal*, and we write $P(G, M)$ for the set of all principal derivations from G into M. It is a subgroup of $\mathrm{Der}(G, M)$.

We will use the facts that if d is a derivation then $d(1) = 0$ and $d(g^{-1}) = -g^{-1}d(g)$, and we may take these as an exercise.

Lemma 3.3.9. *Given any mapping $d : G \to M$ we may define an abelian group homomorphism $\delta : IG \to M$ by specifying $\delta(g-1) = d(g)$ for each non-identity element $g \in G$, using the fact that the $g - 1$ with $1 \neq g \in G$ form a basis for the free abelian group IG. Then d is a derivation if and only if δ is a module homomorphism. Thus* $\mathrm{Der}(G, M) \cong \mathrm{Hom}_{\mathbb{Z}G}(IG, M)$.

Proof. In the calculation that follows we will use the fact that $h(g-1) = (hg-1)-(h-1)$ We check that δ is a module homomorphism $\Leftrightarrow \delta h(g - 1) = h\delta(g - 1)$ for all $g, h \in G$ $\Leftrightarrow d(gh) - d(h) = hd(g)$ for all $g, h \in G \Leftrightarrow d(hg) = hd(g) + d(h)$ for all $g, h \in G$. Thus every derivation determines a module homomorphism $IG \to M$ and, conversely, every module homomorphism gives a derivation, by the same formula. □

Given a short exact sequence of groups $1 \to M \to E \xrightarrow{p} G \to 1$ we say that a mapping of sets $s : G \to E$ is a *section* if $ps = \mathrm{id}_G$. If the section is a group homomorphism we call it a *splitting*. We will consider the semidirect product $E = M \rtimes G$ which we take to be the set $M \times G$ with multiplication $(m_1, g_1)(m_2, g_2) = (m_1 + (g_1 m_2), g_1 g_2)$.

Lemma 3.3.10. *Let $s : G \to E = M \rtimes G$ be a section, so that $s(g) = (d(g), g)$ for some mapping $d : G \to M$. Then s is a group homomorphism if and only if d is a derivation. Thus* $\mathrm{Der}(G, M)$ *is in bijection with the set of splittings $G \to E$.*

Proof. We know that s is a homomorphism if and only if $s(gh) = s(g)s(h)$ for all $g, h \in G$, which happens if and only if $(d(gh), gh) = (d(g) + gd(h), gh)$ for all $g, h \in G$. This, in turn, happens if and only if $d(gh) = d(g) + gd(h)$ for all $g, h \in G$, which is the condition that d should be a derivation. □

As a consequence of this we obtain an algebraic proof that the augmentation ideal of a free group is a free module.

Corollary 3.3.11. *Let F be a free group, freely generated by a set of generators X. Then the augmentation ideal IF is freely generated as a $\mathbb{Z}F$-module by the elements $\{x-1 \mid x \in X\}$.*

Proof. Let M be any $\mathbb{Z}F$-module. We first claim that any mapping $f : X \to M$ extends uniquely to a derivation $d : F \to M$. This is because the mapping $X \to M \rtimes F$ given by $x \mapsto (f(x), x)$ extends uniquely to a group homomorphism $F \to M \rtimes F$ of the form $g \mapsto (d(g), g)$ for some uniquely specified derivation d. We deduce that the mapping $(x-1) \mapsto f(x)$ where $x \in X$ extends uniquely to a $\mathbb{Z}F$-module homomorphism $IF \to M$, by Lemma 3.3.9. It follows that IF satisfies the universal property of a free $\mathbb{Z}F$-module with generating set as claimed. □

We will compute $H^1(G, M)$ using the following exact sequence that comes by applying $\mathrm{Hom}_{\mathbb{Z}G}(-, M)$ to the short exact sequence $0 \to IG \to \mathbb{Z}G \to \mathbb{Z} \to 0$:

$$\begin{array}{ccccccccc} \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M) & \to & \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M) & \to & \mathrm{Hom}_{\mathbb{Z}G}(IG, M) & \to & H^1(G, M) & \to & 0 \\ \| & & \| & & \| & & & & \\ M^G & & M & & \mathrm{Der}(G, M) & & & & \end{array}$$

This is a special case of Proposition 2.4.6.

Lemma 3.3.12. *A derivation $d \in \mathrm{Der}(G, M)$ is principal if and only if the corresponding map $\delta : IG \to M$ lies in the image of $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M) \to \mathrm{Hom}_{\mathbb{Z}G}(IG, M)$. Hence $H^1(G, M) \cong \mathrm{Der}(G, M)/P(G, M)$.*

Proof. Any $\phi : \mathbb{Z}G \to M$ has the form $\phi(g) = g \cdot \phi(1) = gm$ where $m = \phi(1) \in M$. Its restriction to IG is $\phi(g-1) = (g-1)m$ and such maps are exactly the maps in the image of $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M) \to \mathrm{Hom}_{\mathbb{Z}G}(IG, M)$. The corresponding derivations are $P(G, M)$. □

We define two splittings $s_1, s_2 : G \to E = M \rtimes G$ to be M-conjugate if there is an element $m \in M$ so that $(m, 1)s_1(g)(m, 1)^{-1} = s_2(g)$ for all $g \in G$.

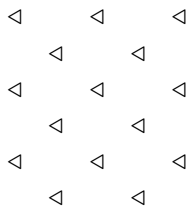
Theorem 3.3.13. *Let M be a $\mathbb{Z}G$-module. The M-conjugacy classes of splittings of $1 \to M \to M \rtimes G \to G \to 1$ biject with $H^1(G, M)$.*

Proof. Splittings $s_i(g) = (d_i(g), g),\ i = 1, 2$ are M-conjugate if and only if $(m + d_1(g) - gm, g) = (d_2(g), g)$ for all $g \in G$, if and only if $m + d_1(g) - gm = d_2(g)$ for all $g \in G$, if and only if $(d_1 - d_2)(g) = (g-1)m$ for all $g \in G$, if and only if $d_1 - d_2 \in P(G, M)$. □

Example 3.3.14. Let $G = \{1, g\}$ be cyclic of order 2 and let $\tilde{\mathbb{Z}}$ be the $\mathbb{Z}G$-module that is an infinite cyclic group on which g acts as multiplication by -1. We have already seen that $IG \cong \tilde{\mathbb{Z}}$ as $\mathbb{Z}G$-modules, so that $\mathrm{Der}(G, \tilde{\mathbb{Z}}) \cong \mathrm{Hom}_{\mathbb{Z}G}(IG, \tilde{\mathbb{Z}}) \cong \mathbb{Z}$ as abelian groups, generated by the derivation $d(g) = 1 \in \tilde{\mathbb{Z}}$. The semidirect product $\tilde{\mathbb{Z}} \rtimes G$ is the infinite dihedral group, and every element of it outside the normal infinite cyclic subgroup $\tilde{\mathbb{Z}}$ has order 2, providing a splitting. The principal derivations $G \to \tilde{Z}$

have the form $d(g) = (g-1)m = -2m$ for each $m \in \tilde{\mathbb{Z}}$, so that $P(G, M) = 2\mathbb{Z}$ and $H^1(G, \tilde{\mathbb{Z}}) \cong \mathbb{Z}/2\mathbb{Z}$. We see that the infinite dihedral group has two conjugacy classes of splittings (conjugate under the normal infinite cyclic group).

Example 3.3.15. Let $G = \{1, g\}$ be cyclic of order 2. Then $H^1(C_2, \mathbb{Z}C_2) = 0$. The semidirect product $\mathbb{Z}C_2 \rtimes C_2$ is isomorphic to the wreath product $\mathbb{Z} \wr C_2$, and can be realized as the group of rigid motions of $\mathbb{R}^2$ that preserve the pattern



All subgroups of order 2 of this group are conjugate by a translation.

Example 3.3.16. Both $H^1(C_2, \mathbb{Z}) = 0$ and $H^1(C_2, \tilde{\mathbb{Z}}/3\tilde{\mathbb{Z}}) = 0$ and the semidirect products are $\mathbb{Z} \times C_2$ in the first case and the symmetric group S_3 in the second case. In the first case, there is a unique element of order 2, and with S_3 all subgroups of order 2 are conjugate by the Sylow 3-subgroup.

3.4 Second homology and cohomology

3.4.1 Extending a resolution to degree 2

Having identified the first homology and cohomology in terms of group theoretical properties we now do the same in degree 2. For this we need to extend the resolution of $\mathbb{Z}$, and we will do this using the information in a presentation of the group G.

Proposition 3.4.1. *Let $1 \to K \to E \to G \to 1$ be an exact sequence of groups, where K is a normal subgroup of E. Then $\mathrm{Ker}(\mathbb{Z}E \to \mathbb{Z}G) = \mathbb{Z}E \cdot IK$, the left ideal of $\mathbb{Z}E$ generated by IK. This kernel is in fact a 2-sided ideal also equal to $IK \cdot \mathbb{Z}E$, and we will denote it by $\overline{IK}$. If $[E/K]$ is a set of representatives for the cosets of K in E then $\overline{IK} = \bigoplus_{t \in [E/K]} tIK$ as abelian groups.*

Proof. Taking a set of left coset representatives for K in E we can write $E = \bigsqcup_{t \in [E/K]} tK$, so that a typical element of $\mathbb{Z}E$ may be written $x = \sum_{t \in [E/K]} \sum_{k \in K} \lambda_{tk} tk$. Let us write π for both the homomorphism $E \to G$ and the corresponding ring homomorphism $\mathbb{Z}E \to \mathbb{Z}G$ and observe that the elements $\pi(t)$ where $t \in [E/K]$ are independent in $\mathbb{Z}G$. We have $\pi(x) = \sum_{t \in [E/K]} \sum_{k \in K} \lambda_{tk} \pi(t)$, so if $\pi(x) = 0$ then $\sum_{k \in K} \lambda_{tk} = 0$ for all t. This means that the element $y_t := \sum_{k \in K} \lambda_{tk} k$ lies in IK. We also have that $x = \sum_{t \in [E/K]} t y_t$ which shows that $\mathrm{Ker}(\mathbb{Z}E \to \mathbb{Z}K) = \bigoplus_{t \in [E/K]} t \cdot IK = \mathbb{Z}E \cdot IK$. Being the kernel of a ring homomorphism, this kernel is a 2-sided ideal. We could have argued with right coset representatives in the above, and this would have given us that the kernel also equals $IK \cdot \mathbb{Z}E$. □

With the notation of the proposition, there is an action of G on the abelianization K/K' determined by conjugation within E as follows. First E acts on K by conjugation, and hence on K/K'. Now K is contained in the kernel of this action, so we obtain an action of G on K/K'.

Example? Class activity? This construction is so fundamental I should express it that way.

Proposition 3.4.2. *Let $1 \to K \to E \to G \to 1$ be an exact sequence of groups, where K is a normal subgroup of E. Then there is an exact sequence of $\mathbb{Z}G$-modules*

$$0 \to \overline{IK}/(\overline{IK} \cdot IE) \to IE/(\overline{IK} \cdot IE) \to IG \to 0$$

in which $\overline{IK}/(\overline{IK} \cdot IE) \cong K/K'$ as $\mathbb{Z}G$-modules.

Observe that the isomorphism $IG/IG^2 \cong G/G'$ is a special case of this on considering the exact sequence $1 \to G \to G \to 1 \to 1$.

Proof. We note that $IK \cdot IE = IK \cdot \mathbb{Z}E \cdot IE = \overline{IK} \cdot IE$ and we can also write $IK \cdot IE$ for the term we are factoring out. The exact sequence arises from the sequences in the diagram

$$\begin{array}{ccccccccc} 0 & \to & \overline{IK} & \to & \mathbb{Z}E & \to & \mathbb{Z}G & \to & 0 \\ & & \| & & \uparrow & & \uparrow & & \\ 0 & \to & \overline{IK} & \to & IE & \to & IG & \to & 0, \end{array}$$

where the lower sequence is exact by the snake lemma. Since $\overline{IK} \cdot IE \subseteq \overline{IK}$, we can factor it out from the two left terms to get our exact sequence, using the third isomorphism theorem.

If M is a $\mathbb{Z}E$-module then

$$\mathbb{Z}G \otimes_{\mathbb{Z}E} M \cong (\mathbb{Z}E/\overline{IK} \otimes_{\mathbb{Z}E} M \cong M/(\overline{IK} \cdot M)$$

is a $\mathbb{Z}G$-module, so that all the terms in the claimed exact sequence are $\mathbb{Z}G$-modules. We construct inverse isomorphisms

$$\begin{array}{rccl} & \overline{IK}/(\overline{IK} \cdot IE) & \cong & K/K' \\ \phi: & (k-1)t + \overline{IK} \cdot IE & \to & kK' \\ & (k-1) + \overline{IK} \cdot IE & \leftarrow & kK' \quad : \psi \end{array}$$

We have to check this assignments are well defined and that they preserve the $\mathbb{Z}G$-module action. They are evidently mutually inverse. □

Corollary 3.4.3. *Let $1 \to R \to F \to G \to 1$ be a presentation of G, i.e. a short exact sequence of groups in which F is free. There is an exact sequence of $\mathbb{Z}G$-modules*

$$0 \to R/R' \to \mathbb{Z}G^{d(F)} \to IG \to 0$$

where $d(F)$ is the minimum number of generators of F. Hence there is a resolution of $\mathbb{Z}$ by free $\mathbb{Z}G$-modules that starts

$$\xrightarrow{d_2} \quad \mathbb{Z}G^{d(F)} \quad \xrightarrow{d_1} \quad \mathbb{Z}G \quad \to \quad \mathbb{Z} \quad \to \quad 0.$$

$$\nearrow \qquad \searrow \qquad \nearrow$$

$$R/R' \qquad\qquad IG$$

Proof. We identify the left term in the short exact sequence

$$0 \to \overline{IR}/(\overline{IR} \cdot IF) \to IF/(\overline{IR} \cdot IF) \to IG \to 0$$

as R/R' by Proposition 3.4.2. The middle term is isomorphic to $\mathbb{Z}G \otimes_{\mathbb{Z}F} \mathbb{Z}F^{d(F)} \cong \mathbb{Z}G^{d(F)}$. □

We recover the rank formula for subgroups of free groups of finite index in the case that the subgroup is normal.

Corollary 3.4.4. *Let $1 \to R \to F \to G \to 1$ be a presentation of a finite group G. Assuming that R is a free group, its rank $d(R)$ satisfies $d(R) = |G|(d(F) - 1) + 1$.*

Proof. The short exact sequence $0 \to R/R' \to \mathbb{Z}G^{d(F)} \to IG \to 0$ splits as a sequence of abelian groups because IG is a free abelian group. Furthermore the rank of R/R' is $d(R)$. Thus the ranks satisfy $d(R) + |G| - 1 = |G|d(F)$, which rearranges to give the claimed rank formula. □

Definition 3.4.5. The $\mathbb{Z}G$-module R/R' arising from the presentation of G is called the *relation module* associated to the presentation.

If the presentation is determined by generators $G = \langle g_1, \ldots, g_n \rangle$ with free generators $x_1, \ldots, x_n$ of F mapping to them, we have already seen that IF is a free $\mathbb{Z}F$-module, freely generated by the $x_i - 1$. In the construction of the short exact sequence, $x_i - 1$ maps to $g_i - 1$, and so the mapping $\mathbb{Z}G^{d(F)} \to IG$ sends the ith free generator to $g_i - 1$. We deduce again that the elements $g_i - 1$ generate IG, as already shown in Proposition 3.2.1.

Example 3.4.6. If G is itself a free group and the presentation has $R = 1$ we deduce that $R/R' = 0$ and $\mathbb{Z}F^{d(F)} \to IF$ is an isomorphism, thereby confirming Corollary 3.3.11.

Example 3.4.7. Let $G = \langle g \rangle$ be cyclic of order n, and let $1 \to R \to F \to G \to 1$ be the presentation where $F = \langle x \rangle$ and $R = \langle x^n \rangle$ with x mapping to g. Here $R' = 1$ and the generator x^n of the relation module R/R' maps to $x^n - 1 + \overline{IR} \cdot IF$ in $IF/(\overline{IR} \cdot IF)$, which is a free $\mathbb{Z}G$-module with basis $\{x - 1) + \overline{IR} \cdot IF$. Now

$$x^n - 1 = (1 + x + x^2 + \cdots + x^{n-1})(x - 1),$$

so that identifying $IF/(\overline{IR} \cdot IF)$ with $\mathbb{Z}G$, the generator x^n of the relation module maps via the differential d_2 to the norm element $1 + x + \cdots + x^{n-1}$. We have already observed that d_1 maps the generator of $\mathbb{Z}G$ to $g - 1$, so we obtain the start of the resolution described in Theorem 3.3.4.

3.4.2 Second cohomology and extensions

We use the start of the resolution we have just constructed to interpret the second cohomology and homology in group theoretic terms. Second cohomology may be computed using the next proposition.

Proposition 3.4.8. *Let $1 \to R \to F \to G \to 1$ be a presentation of G and M a $\mathbb{Z}G$-module. There is an exact sequence*

$$\mathrm{Der}(F, M) \to \mathrm{Hom}_{\mathbb{Z}G}(R/R', M) \to H^2(G, M) \to 0.$$

The map on the left is given by restriction of derivations to R.

Proof. We use the start of the resolution given in Corollary 3.4.3 together with the sequence of Proposition 2.4.6 that computes Ext groups. We also use the identification of the term $\mathbb{Z}G^{d(F)}$ that appears in 3.4.3 as the module $IF/(\overline{IR} \cdot IF)$. Thus we have an exact sequece

$$\mathrm{Hom}_{\mathbb{Z}G}(IF/(\overline{IR} \cdot IF), M) \to \mathrm{Hom}_{\mathbb{Z}G}(R/R', M) \to H^2(G, M) \to 0.$$

It remains to observe that $\mathrm{Hom}_{\mathbb{Z}G}(IF/(\overline{IR} \cdot IF), M) = \mathrm{Hom}_{\mathbb{Z}F}(IF, M) = \mathrm{Der}(F, M)$ if M is a $\mathbb{Z}G$-module (by Proposition 3.2.1 and because $\overline{IR}$ acts as zero on M), and also that under this identification the first map in the sequence is given by restriction. □

Theorem 3.4.9. *Let M be a $\mathbb{Z}G$-module. There is a bijection*

$$\psi : H^2(G, M) \to \{\textit{equivalence classes of extensions of } G \textit{ by } M\}.$$

Proof. We use the short exact sequence of Proposition 3.4.8 to compute $H^2(G, M)$. Thus any element $\bar{\theta} \in H^2(G, M)$ may be represented by a $\mathbb{Z}G$-module homomorphism $\theta : R/R' \to M$. Two homomorphisms $\theta, \theta' : R/R' \to M$ represent the same element of $H^2(G, M)$ if and only if they differ by the restriction of a derivation from F to M.

Put this construction separately, before this theorem. Comment that it describes the functoriality of H^2.

We construct an extension $\psi(\bar{\theta})$ that appears as the lower sequence in the following diagram:

$$(*) \qquad \begin{array}{ccccccccc} 1 & \to & R/R' & \to & F/R' & \to & G & \to & 1 \\ & & \theta\downarrow & & \eta\downarrow & & \| & & \\ 1 & \to & M & \to & E & \to & G & \to & 1 \end{array}$$

where $E = M \rtimes (F/R')/\{(-\theta(rR'), rR') \mid r \in R\}$. The map η is determined by $x \mapsto (0, x)$ and the map $M \to E$ is determined by $m \mapsto (m, 1)$. We check that the left hand square commutes. We now exploit the fact that in any two such commutative diagrams with the same map θ and the same top row, the bottom row is determined up to equivalence.

This sentence is strange.

We must also check that ψ is well defined on cohomology classes. Let $d \in \mathrm{Der}(F, M)$. We show that $\psi(\bar{\theta})$ and $\psi(\overline{\theta + d})$ are the same. This is so because the mapping $F/R' \to$

$M \rtimes F/R'$ given by $x \mapsto (dx, x)$ is a homomorphism (by Lemma 3.8) and it induces a homomorphism $\tilde{\eta} : F/R' \to E$. We check that the diagram

$$\begin{array}{ccccccccc} 1 & \to & R/R' & \to & F/R' & \to & G & \to & 1 \\ & & {\scriptstyle \theta+d}\downarrow & & {\scriptstyle \tilde{\eta}}\downarrow & & \| & & \\ 1 & \to & M & \to & E & \to & G & \to & 1 \end{array}$$

commutes.

We next define a mapping

$$\phi : \{\text{equivalence classes of extensions of } G \text{ by } M\} \to H^2(G, M)$$

as follows. Given an extension $\mathcal{E} : 1 \to M \to E \to G \to 1$ lift the identity map on G to a commutative diagram

$$\begin{array}{ccccccccc} 1 & \to & R & \to & F & \to & G & \to & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \to & M & \to & E & \to & G & \to & 1 \end{array}$$

using that fact that F is free. Since M is abelian we have $R' \subseteq \mathrm{Ker}(R \to M)$, so we get a diagram of the form (*) whose left hand vertical arrow represents $\phi(\mathcal{E})$. We check that the left hand vertical arrow is indeed a $\mathbb{Z}G$-module homomorphism.

We must also check that ϕ is well-defined, independently of the lifting of homomorphisms. Suppose we lift the identity on G in two ways

$$\begin{array}{ccccccccc} 1 & \to & R & \to & F & \to & G & \to & 1 \\ & & {\scriptstyle \alpha_i}\downarrow & & {\scriptstyle \beta_i}\downarrow & & \| & & \qquad i = 1, 2. \\ 1 & \to & M & \to & E & \to & G & \to & 1 \end{array}$$

For each $x \in F$ let $d(x) \in M$ be defined by $\beta_2(x) = d(x)\beta_1(x)$. We check that $d \in \mathrm{Der}(F, M)$, so that $\alpha_2 = \alpha_1 + d$ and these two liftings give rise to the same element in cohomology.

Evidently ϕ and ψ are mutually inverse. □

Remark 3.4.10. (1) We leave it as an exercise to verify that $\psi(0)$ is the split extension and that the group operation in cohomology corresponds to the Baer sum of extensions.

(2) Theorem 3.15 can also be done for non-abelian groups M, replacing the module action of G on M by a 'coupling' - a homomorphism from G to the outer automorphism group of M. Now $H^2(G, Z(M))$ classifies extensions (provided there are any, which there might not be), where $Z(M)$ denotes the center.

(3) We might expect H^1 to classify extensions, since this is what happens for extensions of modules. In fact by dimension shifting we have $H^2(G, M) \cong \mathrm{Ext}^1_{\mathbb{Z}G}(IG, M)$, so that group extensions of G correspond to module extensions of IG. This correspondence is the one we have already seen in Proposition 3.4.2.

(4) The construction of a commutative diagram such as (*) above is analogous to the construction of a pushout for modules, but it is not the pushout in the category of groups (the pushout is the free product with amalgamation). The construction of (*) is the one that is relevant in this situation and we may call it the *explicit pushout*.

Example 3.4.11. We compute $H^2(C_2 \times C_2, \mathbb{F}_2)$ and identify the extensions. In this case there are several ways to compute the cohomology, one of the fastest being to use the Künneth theorem (which is not available to us at this stage). We will do the computation using a presentation, to illustrate the theory just developed. The method we shall describe may be programmed on a computer — it is really just linear algebra — and it yields presentations of the group extensions corresponding to the cohomology classes.

We start with the presentation $G = \langle a, b \mid a^2,\ b^2,\ [a,b]\rangle$, which we also write as an extension $1 \to R \to F \to G \to 1$, and we use the exact sequence of Proposition 3.16:

$$\mathrm{Der}(F, \mathbb{F}_2) \to \mathrm{Hom}_{\mathbb{Z}G}(R/R', \mathbb{F}_2) \to H^2(G, \mathbb{F}_2) \to 0.$$

Let us write $\bar{a}$, $\bar{b}$ for the images of a and b in G.

We show that $\mathrm{Der}(F, \mathbb{F}_2)$ has zero image in $\mathrm{Hom}_{\mathbb{Z}G}(R/R', \mathbb{F}_2)$. If $d \in \mathrm{Der}(F, \mathbb{F}_2)$ then

$$\begin{aligned} d(a^2) &= ad(a) + d(a) = 2d(a) = 0, \\ d(b^2) &= 0 \quad \text{similarly, and} \\ d(aba^{-1}b^{-1}) &= aba^{-1}d(b^{-1}) + abd(a^{-1}) + ad(b) + d(a) \\ &= -d(b) - d(a) + d(b) + d(a) = 0 \end{aligned}$$

using the fact that $\mathbb{F}_2$ has the trivial action and $d(b^{-1}) = -b^{-1}d(b)$. We conclude that $H^2(G, \mathbb{F}_2) \cong \mathrm{Hom}_{\mathbb{Z}G}(R/R', \mathbb{F}_2)$. Furthermore we have

$$\mathrm{Hom}_{\mathbb{Z}G}(R/R', \mathbb{F}_2) \cong \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{F}_2 \otimes_{\mathbb{Z}} (R/R')/(IG \cdot R/R'), \mathbb{F}_2) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{F}_2 \otimes_{\mathbb{Z}G} R/R', \mathbb{F}_2)$$

since we are now dealing with modules with trivial action.

At this point we need a good description of R/R' in order to compute $\mathbb{F}_2 \otimes_{\mathbb{Z}G} R/R'$. One approach to finding such a description is to obtain a set of free generators of R using Schreier's method, from which we can get matrices for the action of G on R/R'. We will follow a different approach.

As a $\mathbb{Z}G$-module, R/R' is generated by a^2R', b^2R', $[a,b]R'$. This is because R is generated as a normal subgroup of F by a^2, b^2 and $[a,b]$, so that R is generated by these elements and their F-conjugates. From this it follows that R/R' is generated by $a^2R', b^2R', [a,b]R'$ and their conjugates, which are the images under G in the module action on R/R'.

From the exact sequence $0 \to R/R' \to \mathbb{Z}G^2 \to IG \to 0$ we may identify R/R' as a submodule of the free module $\mathbb{Z}G^2$, and we express its generators in terms of coordinates with respect to the basis

$$\{a - 1 + \overline{IR} \cdot IF,\ b - 1 + \overline{IR} \cdot IF\}$$

of $IF/(\overline{IR} \cdot IF) \cong \mathbb{Z}G^2$. We have

$$\begin{aligned} a^2 - 1 &= (a+1)(a-1) \\ b^2 - 1 &= (b+1)(b-1) \\ aba^{-1}b^{-1} - 1 &= aba^{-1}(b^{-1}-1) + ab(a^{-1}-1) + a(b-1) + a - 1 \\ &= (1 - aba^{-1})(a-1) + (a - aba^{-1}b^{-1})(b-1). \end{aligned}$$

So

$$\begin{aligned} a^2R' &\leftrightarrow (\bar{a}+1, 0) \\ b^2R' &\leftrightarrow (0, \bar{b}+1) \\ [a,b]R' &\leftrightarrow (1 - \bar{a}\bar{b}\bar{a}^{-1}, \bar{a} - \bar{a}\bar{b}\bar{a}^{-1}\bar{b}^{-1}) = (1-\bar{b}, \bar{a}-1) \end{aligned}$$

gives the correspondence with elements of $\mathbb{Z}G^2$. Thus R/R' is isomorphic to the $\mathbb{Z}G$-submodule of $\mathbb{Z}G^2$ generated by these last three elements on the right.

We will now compute $\mathbb{F}_2 \otimes_{\mathbb{Z}G} R/R'$, and so we will work with coefficients mod 2. We write $+1$ instead of -1. Now $IG \cdot (\mathbb{F}_2 \otimes_{\mathbb{Z}} R/R')$ is the $\mathbb{F}_2G$-submodule of $(\mathbb{F}_2G)^2$ generated by the multiples $\bar{a}+1$ and $\bar{b}+1$ of the generators of $\mathbb{F}_2 \otimes_{\mathbb{Z}} R/R'$. Since $(\bar{a}+1)^2 = 0 = (\bar{b}+1)^2$ and $(\bar{a}+1)(\bar{b}+1) = \sum_{g\in G} g$ we obtain that

$$\begin{aligned} IG \cdot (\mathbb{F}_2 \otimes_{\mathbb{Z}} R/R') &= \langle (\sum_{g\in G} g, 0), (0, \sum_{g\in G} g) \rangle \\ &= (\mathbb{F}_2 G^2)^G \end{aligned}$$

which has dimension 2. From the rank formula in Corollary 3.4.4 we have that $\dim \mathbb{F}_2 \otimes R/R' = 5$. Therefore $\dim(\mathbb{F}_2 \otimes R/R')/(IG \cdot (\mathbb{F}_2 \otimes R/R')) = 5 - 2 = 3$. Thus $H^2(G, \mathbb{F}_2)$ is a 3-dimensional vector space over $\mathbb{F}_2$. We conclude that the images of the three generators a^2R', b^2R' and $[a,b]R'$ form a basis for this space, since they span it.

We now construct extensions corresponding to the elements of $H^2(G, \mathbb{F}_2)$. Any cohomology class is represented by a homomorphism $\phi : R/R' \to \mathbb{F}_2$, and there are 8 possibilities given by the values of ϕ on the generators. Given such a ϕ the corresponding extension is $1 \to \mathbb{F}_2 \to F/R' \,/\, \operatorname{Ker}\phi \to G \to 1$. This is because this extension appears in a commutative diagram

$$\begin{array}{ccccccccc} 1 & \to & R/R' & \to & F/R' & \to & G & \to & 1 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow & & \| & & \\ 1 & \to & \mathbb{F}_2 & \to & F/R' \,/\, \operatorname{Ker}\phi & \to & G & \to & 1 \end{array}$$

and the bottom row of such a diagram is determined up to equivalence by the rest of the diagram. We give examples of homomorphisms ϕ and presentations for the corresponding extension groups:

$$\phi : \begin{cases} a^2R' \mapsto 1 \\ b^2R' \mapsto 1 \\ [a,b]R' \mapsto 1 \end{cases} \qquad E = \langle a, b \mid a^2 = b^2 = [a,b],\, a^4 = 1 \rangle \cong Q_8$$

$$\phi : \begin{cases} a^2R' \mapsto 1 \\ b^2R' \mapsto 0 \\ [a,b]R' \mapsto 1 \end{cases} \qquad E = \langle a, b \mid b^2 = 1,\, a^2 = [a,b],\, a^4 = 1,\, [a^2, b] = 1 \rangle \cong D_8.$$

In general a presentation for an extension $1 \to M \to E \to G \to 1$ is obtained by taking a presentation of M as a group, adjoining generators for G and imposing relations that define the module action of G on M, and finally adjoining relators that set the relators of G equal to the elements of M to which they are mapped by ϕ. In the above examples we have suppressed some of the generators and relations that arise in this general procedure, because there are many of them. To see that the mappings ϕ give extensions with the claimed presentations we observe that the relations given are satisfied in the extension group, and we then prove that the presentation defines a group of order 8, so must be the extension group.

Insert picture.

Continuing with these calculations we find that the zero element of $H^2(C_2 \times C_2, \mathbb{F}_2)$ is an extension with middle group $C_2 \times C_2 \times C_2$, there are three elements with groups $C_2 \times C_4$ forming a 2-dimensional subspace, three extensions have middle group D_8 and the remaining one has middle group Q_8. This describes the structure of the group considered by Baer with the operation of Baer sum, described in the introduction.

3.4.3 The Schur multiplier

We turn our attention to the *Schur multiplier* of G, which we may define to be $H_2(G, \mathbb{Z})$. In other sources we find a number of different definitions of the Schur multiplier. When G is finite there are isomorphisms (that we have not yet encountered):

$$H_2(G, \mathbb{Z}) \cong H^3(G, \mathbb{Z}) \cong H^2(G, \mathbb{Q}/\mathbb{Z}) \cong H^2(G, \mathbb{C}^\times).$$

Sometimes one of these other groups is taken as the definition. Neither Schur nor Hopf had group cohomology available to them to define the multiplier. It is also possible to define it in group theoretic terms using the next theorem (although we would then have to deal with the question that the isomorphism type of the group defined is independent of the choices made). After this next result we give an account of the role of the Schur multiplier in purely group theoretic terms.

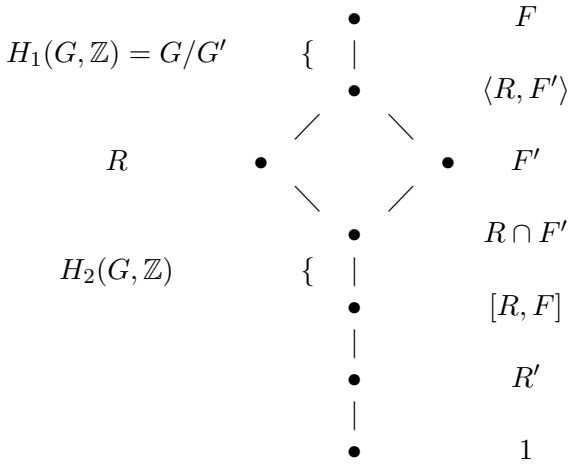
When H and K are subgroups of a group G we write $[H, K]$ for the subgroup generated by all commutators $[h, k]$ where $h \in H$ and $k \in K$.

Theorem 3.4.12 (Hopf formula)**.** *Let* $1 \to R \to F \to G \to 1$ *be a presentation of* G*. Then* $H_2(G, \mathbb{Z}) \cong (R \cap F')/[R, F]$.

Write something about the history and what it was that Hopf proved.

The quotient group in the statement of the theorem is illustrated in the following

diagram.



We see two homology groups identified as quotients of subgroups of F. In fact all integral homology groups may be interpreted in this way, as has been observed by Gruenberg (insert reference).

Proof. We use the short exact sequence $0 \to \overline{IR}/(\overline{IR} \cdot IF) \to IF/(\overline{IR} \cdot IF) \to IG \to 0$ to compute $H_2(G, \mathbb{Z})$. By Corollary 3.4.3 this sequence identifies as $0 \to R/R' \to \mathbb{Z}G^{d(F)} \to IG \to 0$. After applying $\mathbb{Z} \otimes_{\mathbb{Z}G} -$ to it we obtain

$$H_2(G, \mathbb{Z}) = \mathrm{Ker}(\mathbb{Z} \otimes_{\mathbb{Z}G} (\overline{IR}/(\overline{IR} \cdot IF)) \to \mathbb{Z} \otimes_{\mathbb{Z}G} (IF/(\overline{IR} \cdot IF))).$$

This map is induced by inclusion $\overline{IR} \to IF$. In identifying these groups we observe that $\otimes_{\mathbb{Z}G}$ is the same as $\otimes_{\mathbb{Z}F}$ because the action of $\overline{IR}$ has been factored out, and also that $\mathbb{Z} \cong \mathbb{Z}F/IF$, so that

$$\mathbb{Z} \otimes_{\mathbb{Z}G} IF/(\overline{IR} \cdot IF) = \mathbb{Z} \otimes_{\mathbb{Z}F} IF/(\overline{IR} \cdot IF) \cong IF/(IF^2 + \overline{IR} \cdot IF) = IF/IF^2 \cong F/F'.$$

Also

$$\mathbb{Z} \otimes_{\mathbb{Z}G} \overline{IR}/(\overline{IR} \cdot IF) \cong \mathbb{Z} \otimes_{\mathbb{Z}G} R/R' \cong R/[R, F]$$

since this is the largest quotient of R/R' on which G (or F) acts trivially. From this we obtain that

$$H_2(G, \mathbb{Z}) = \mathrm{Ker}(R/[R, F] \to F/F')$$

where the map is induced by inclusion of R in F. Evidently this kernel is $R \cap F'/[R, F]$. □

Corollary 3.4.13. *The isomorphism type of $(R \cap F')/[R, F]$ is independent of the choice of presentation of G.*

Proof. This comes from the fact that homology groups are well defined. □

A *central extension* $1 \to M \to E \to G \to 1$ is a group extension in which M is contained in the center $Z(E)$. Equivalently, $[M, E] = 1$.

Lemma 3.4.14. *Let $1 \to M \to E \to G \to 1$ be a central group extension and consider a commutative diagram of groups*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & L & \longrightarrow & J & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \psi} & & \| & & \\ 1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1. \end{array}$$

Then

1. *the restricted vertical maps $J' \to E'$ and $L \cap J' \to M \cap E'$ are surjective, and*
2. *the group $M \cap E'$ is a homomorphic image of $H_2(G, \mathbb{Z})$.*

Proof. (1) We show that every commutator $[e, f] \in E'$ is in the image of J'. We can write these elements of E as $e = \psi(\hat{e})m_e$ and $f = \psi(\hat{f})m_f$ for some elements $m_e, m_f \in M$ and $\hat{e}, \hat{f} \in J$. Then

$$\begin{aligned} &= [\psi(\hat{e})m_e, \psi(\hat{f})m_f] \\ &= [\psi(\hat{e}), \psi(\hat{f})] \\ &= \psi([\hat{e}, \hat{f}]) \end{aligned}$$

and this shows surjectivity $J' \to E'$. By considering the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & L \cap J' & \longrightarrow & J' & \longrightarrow & G' & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \psi} & & \| & & \\ 1 & \longrightarrow & M \cap E' & \longrightarrow & E' & \longrightarrow & G' & \longrightarrow & 1 \end{array}$$

a similar argument to that used to prove the snake lemma shows that $L \cap J' \to M \cap E'$ is surjective. Specifically, if $g \in M \cap E'$ then $g = \psi(h)$ for some $h \in J'$. The image of h in G' equals the image of g in G', which is 1, so h lies in $L \cap J'$ and so the restriction of ϕ to $L \cap J'$ is surjective.

(2) There is a diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & R/[R,F] & \longrightarrow & F/[R,F] & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \psi} & & \| & & \\ 1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1. \end{array}$$

This comes from first producing a similar diagram without the terms $[R, F]$ factored out, using the free property of F, and then observing that $[R, F]$ lies in the kernel of the vertical maps because M is central in E. From part (1) we have that $M \cap E'$ is a homomorphic image of $(R/[R,F]) \cap (F/[R,F])' = (R \cap F')/[R,F]$. □

We say that a central extension $1 \to M \to E \to G \to 1$ is a *stem extension* if $M \subseteq E'$ (or, equivalently, if the induced map $E/E' \to G/G'$ is an isomorphism).

Class Activity. How many times was the central property used in the last proof? Is the equivalence with $E/E' \to G/G'$ being an isomorphism easy to see, or difficult? Which of the group extensions $1 \to C_2 \to E \to C_2 \times C_2 \to 1$ that we considered before are stem extensions? What can we deduce about $H_2(C_2 \times C_2, \mathbb{Z})$?

A group G is said to be *perfect* if and only if $G = G'$. For example, simple non-abelian groups are perfect, and so are other groups such as $SL(2,5)$ of order 120, which has a unique element of order 2 with quotient A_5. The theory of central extensions is most easily described for perfect groups, which is why we focus on them.

Proposition 3.4.15. *Let G be a perfect group. A central extension $1 \to M \to E \to G \to 1$ is stem if and only if E is perfect.*

Proof. In one direction, if E is perfect then certainly $M \subseteq E'$. Conversely, suppose that $M \subseteq E'$. The commutator subgroup E' maps surjectively to $G' = G$, so by the correspondence between subgroups of G and subgroups of E that contain M, we deduce that $E' = E$. □

The next result describes all central stem extensions of a given perfect group.

Theorem 3.4.16. *Suppose that G is a perfect group. There exists a central stem extension $1 \to A \to \hat{G} \to G \to 1$ with the property that whenever $1 \to M \to E \to G \to 1$ is a central stem extension there exists a unique commutative diagram*

$$\begin{array}{ccccccccc} 1 & \to & A & \to & \hat{G} & \to & G & \to & 1 \\ & & \downarrow & & \downarrow \phi & & \| & & \\ 1 & \to & M & \to & E & \to & G & \to & 1 \end{array}$$

Moreover $A \cong H_2(G, \mathbb{Z})$ and all group extensions $1 \to A \to \hat{G} \to G \to 1$ satisfying the above property are isomorphic.

The notion of isomorphism of extensions just used is as follows. We may form a category whose objects are extensions of G and in which the morphisms are commutative diagrams of the kind in this theorem, with the identity map on G as the right hand vertical morphism. An isomorphism of extensions of G is an invertible such morphism, and is characterized by the fact that all its vertical morphisms are isomorphisms.

Proof. Let $1 \to R \to F \to G \to 1$ be a presentation of G. The extension with the special property we seek is $1 \to (R \cap F')/[R,F] \to F'/[R,F] \to G' = G \to 1$. We saw in the proof of Lemma 3.4.14 also that there is always a commutative diagram of extensions with this sequence as the top row and with bottom row $1 \to M \cap E' \to E' \to G' \to 1$, but in this case both G and E are perfect and $M \cap E' = M$, so there is a commutative diagram as claimed. We must show that $\hat{G} := F'/[R,F]$ is perfect. Since $G = G' = F'R/R$ we have $F'R = F$ so $F' = [F'R, F'R] \subseteq [F'R, F'R][R,F] \subseteq [F', F'][R,F] = F''[R,F] \subseteq F'$ because R is central modulo $[R,F]$. Thus

$$(F'/[R,F])' = F''[R,F]/[R,F] = F'/[R,F]$$

and $F'/[R,F]$ is perfect. It follows from Proposition 3.4.15 that this extension is stem.

We show that in any commutative diagram as in the statement of the theorem where the bottom row is prescribed, the vertical homomorphisms are uniquely determined. If there were two homomorphisms ϕ, say ϕ_1 and ϕ_2, then for all $x \in \hat{G}$ we would have $\phi_2(x) = m_x\phi_1(x)$ for some $m_x \in M$. Now

$$\phi_2([x,y]) = [m_x\phi_1(x), m_y\phi_1(y)] = [\phi_1(x), \phi_1(y)] = \phi_1([x,y])$$

since m_x and m_y are central. Since $\hat{G} = \hat{G}'$ is generated by commutators, $\phi_1 = \phi_2$.

It follows that any two extensions satisfying the property of the theorem are isomorphic, since we would have two commutative diagrams

$$\begin{array}{ccccccccc} 1 & \to & A_1 & \to & \hat{G}_1 & \to & G & \to & 1 \\ & & \uparrow\downarrow & & {\scriptstyle\phi_2}\uparrow\downarrow{\scriptstyle\phi_1} & & \| & & \\ 1 & \to & A_2 & \to & \hat{G}_2 & \to & G & \to & 1 \end{array}$$

and the composites must be the identity by uniqueness of the lift of the identity. □

The group $\hat{G}$ is called the *universal cover* or *stem cover* of the perfect group G. It is a maximal stem extension of G, in the sense that all others are images of it, and $\hat{G}$ is a perfect group. When G is not perfect there may be several maximal stem extensions of G. They are all central extensions of G by $H_2(G,\mathbb{Z})$ and are constructed by factoring out from $F/[R,F]$ the various complements to $(R\cap F')/[R,F]$ in $R/[R,F]$ obtained by splitting the surjection $R/[R,F] \to R/(R\cap F')$.

We continue with the theory for perfect groups. The next result will be useful in a subsequent example.

Proposition 3.4.17. *Let G be a perfect group and $1 \to M \to E \to G \to 1$ a central stem extension of G. Then E is the universal cover of G if and only if $H_2(E,\mathbb{Z}) = 0$.*

Proof. We will use Witt's identity (analogous to the Jacobi identity for Lie algebras)

$${}^b[a,[b^{-1},c]] \cdot {}^c[b,[c^{-1},a]] \cdot {}^a[c,[a^{-1},b]] = 1,$$

which holds in all groups. We prove this by expanding the terms and cancelling.

"⇒" Let E be the universal cover of G and $\hat{E}$ the universal cover of E (noting that E is perfect). Let K be the kernel of the composite $\hat{E} \to E \to G$. An argument similar

in spirit to the snake lemma applied to the diagram

$$\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & & \downarrow & & & & \\
 & & & & H_2(E,\mathbb{Z}) & & & & \\
 & & & & \downarrow & & & & \\
1 & \longrightarrow & K & \longrightarrow & \hat{E} & \longrightarrow & G & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle \alpha} & & \| & & \\
1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\
 & & \| & & \downarrow & & & & \\
 & & H_2(G,\mathbb{Z}) & & 1 & & & &
\end{array}$$

shows that K is an extension $1 \to H_2(E,\mathbb{Z}) \to K \to M \to 1$ where $M = H_2(G,\mathbb{Z})$.

We show that $K \leq Z(\hat{E})$. Let $k \in K$, $g, h \in \hat{E}$. Then $[g^{-1}, k] \in H_2(E,\mathbb{Z})$ since $M \leq Z(E)$, and now $[h, [g^{-1}, k]] = 1$ in $\hat{E}$ since $H_2(E,\mathbb{Z}) \leq Z(\hat{E})$. Similarly $[g, [k^{-1}, h]] = 1$. Therefore by Witt's identity $[k, [h^{-1}, g]] = 1$ for all $g, h \in \hat{E}$ and $k \in K$. But $\hat{E}$ is generated by commutators $[h^{-1}, g]$, so $[k, \hat{E}] = 1$ and $k \in Z(\hat{E})$. We conclude that $1 \to K \to \hat{E} \to G \to 1$ is a central stem extension of G.

Now by universality of E we have a commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle \beta} & & \| & & \\
1 & \longrightarrow & K & \longrightarrow & \hat{E} & \longrightarrow & G & \longrightarrow & 1
\end{array}$$

in which the vertical homomorphisms are surjections. We have seen before that the composite $\alpha\beta = 1_E$ so β is also a monomorphism. Therefore α is an isomorphism, and its kernel $H_2(E,\mathbb{Z})$ must be trivial.

"$\Leftarrow$" Suppose that $H_2(E,\mathbb{Z}) = 0$ and let $1 \to H_2(G,\mathbb{Z}) \to \tilde{E} \to G \to 1$ be the universal cover of G. Then there is a commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & H_2(G,\mathbb{Z}) & \longrightarrow & \tilde{E} & \longrightarrow & G & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle \beta} & & \| & & \\
1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1
\end{array}$$

with surjective vertical maps, and $1 \to \operatorname{Ker}\beta \to \tilde{E} \to E \to 1$ is a stem central extension, because E is perfect and $\operatorname{Ker}\beta$ is contained in the central subgroup $H_2(G,\mathbb{Z})$ of $\tilde{E}$. Now $\operatorname{Ker}\beta$ is a homomorphic image of $H_2(E,\mathbb{Z})$, so it is the identity group, and β is an isomorphism. □

We conclude this treatment of the Schur multiplier with a connection with presentations of groups, providing a way to calculate it, and also giving an application of the theory.

Proposition 3.4.18. *Let G be a finite group with a presentation using d generators and r relators. Then the minimum number of generators of the Schur multiplier satisfies $d(H_2(G,\mathbb{Z})) \leq r - d$.*

Proof. Because $R/[R,F]$ is a homomorphic image of R and the action of F on it induced by conjugation is trivial, it can be generated by generated by the images of the r relators, so that $d(R/[R,F]) \leq r$. It has as a quotient $R/(R \cap F')$, which is isomorphic to RF'/F' by the second isomorphism theorem. This group is free abelian, because it is a subgroup of the free abelian group F/F'. Thus the extension of abelian groups

$$1 \to (R \cap F')/[R,F] \to R/[R,F] \to R/(R \cap F') \to 1$$

is split. This means

$$R/[R,F] \cong (R \cap F')/[R,F] \oplus R/(R \cap F')$$

and

$$d(R/[R,F]) = d((R \cap F')/[R,F]) + d(R/(R \cap F'))$$

because the last group on the right is free abelian. In fact, $d(R/(R \cap F')) = d(RF'/F') = d(F)$ because $R/(R \cap F') = RF'/F'$ is a subgroup of finite index in the free abelian group F/F' of rank d. Recall that $(R \cap F')/[R,F] \cong H_2(G,\mathbb{Z})$ is Hopf's formula. Putting this together gives the result. □

Example 3.4.19. There are presentations

Put the first two presentations earlier?

$$\begin{aligned} S_3 &= \langle x, y \mid x^2 = 1,\ xyx^{-1} = y^2 \rangle, \\ Q_8 &= \langle x, y \mid x^2 = y^2,\ xyx = y \rangle, \\ SL(2,5) &= \langle x, y \mid x^2 = y^3 = (xy)^5 \rangle. \end{aligned}$$

In the first presentation we deduce that $y = x^2yx^{-2} = x(xyx^{-1})x^{-1} = xy^2x^{-1} = y^4$, so $y^3 = 1$, giving a familiar presentation of S_3. In the second presentation we deduce that $xyx^{-1} = yx^{-2} = y^{-1}$ and also $yxy^{-1} = x^{-1}$, so that $yx^{-1}y^{-1} = x$. From this we may deduce that the commutator $xyx^{-1}y^{-1} = x^2 = y^{-2} = x^{-2}$, so that $x^4 = 1$, and this gives a familiar presentation of Q_8. For the third presentation we may deduce from a computer algebra system that the presentation is of a group of order 120 with a unique element of order 2.

Because these presentations have the same number of relators as generators, we conclude that the Schur mulitpliers of these groups are 0, by Proposition 3.4.18. Furthermore, we may compute from the presentation that the group labeled $SL(2,5)$ is perfect. To do this, impose the relators on a free abelian group of rank 2 and put them

into Smith normal form to compute the abelianization. We can find generators of A_5 satisfying those relations, so there is a short exact sequence

$$1 \to C_2 \to SL(2,5) \to A_5 \to 1.$$

We deduce that $H_2(A_5, \mathbb{Z}) = C_2$ by Proposition 3.4.17. It follows from this that in any presentation of A_5 the number of relators must exceed the number of generators by at least 1, by Proposition 3.4.18.

The extension $1 \to C_2 \to Q_8 \to C_2 \times C_2 \to 1$ is stem, and so we deduce that $H_2(C_2 \times C_2, \mathbb{Z})$ has C_2 as an image. Furthermore, Q_8 admits no further stem extension, because its multiplier is trivial. A refinement of the argument for perfect groups shows that, in fact, $H_2(C_2 \times C_2, \mathbb{Z})$ is a group of order 2. There is also a maximal stem extension $1 \to C_2 \to D_8 \to C_2 \times C_2 \to 1$, but in this case $H_2(D_8, \mathbb{Z}) \neq 0$ because there is a further stem extension $1 \to C_2 \to D_{16} \to D_8 \to 1$, applying Lemma 3.4.14. Thus, without the hypothesis that a group be perfect, it need not be the case that its maximal stem extensions are characterized by having trivial multiplier, in the manner of Proposition 3.4.17.

Refinement? Draw a picture of the stem extensions, including SD_{2^n} etc.

We have seen that if a finite group G has a presentation with the same number of generators as relators then the Schur multiplier must be 0. In 1955 B.H. Neumann asked the converse question: whether $H_2(G, \mathbb{Z}) = 0$ for a finite group G implies that G has a presentation with the same number of generators and relations. This was answered in the negative by Swan in 1965 (Topology 4, pages 193-208), who showed that for the groups $(C_7 \times \cdots \times C_7) \rtimes C_3$ with an arbitrary number of cyclic factors C_7 and where C_3 acts on each C_7 factor by squaring, the Schur multiplier is 0, but $r - d$ increases without bound.

3.5 Special properties of the cohomology of finite groups

We collect some special properties of homology and cohomology that only hold when G is finite.

Proposition 3.5.1. *If G is a finite group and M is a finitely generated $\mathbb{Z}G$-module then $H^n(G, M)$ and $H_n(G, M)$ are finitely generated for all n.*

Proof. The arguments we shall give all depend on the fact that subgroups (and quotient groups) of finitely generated abelian groups are finitely generated; in other words, $\mathbb{Z}$ is Noetherian. Observe that a $\mathbb{Z}G$-module is finitely generated as a $\mathbb{Z}G$-module if and only if it is finitely generated as an abelian group, because G is finite. We start by constructing a $\mathbb{Z}G$-projective resolution of $\mathbb{Z}$ in which all the modules and kernels are finitely generated as abelian groups (or as $\mathbb{Z}G$-modules). Assuming that the kernel at some stage in the resolution is finitely generated, we map a finitely generated $\mathbb{Z}G$-projective module onto it and the kernel is again finitely generated as an abelian group, hence as a $\mathbb{Z}G$-module. We repeat the process.

We next apply the functors $\mathrm{Hom}_{\mathbb{Z}G}(-,M)$ and $M\otimes_{\mathbb{Z}G}-$ to this projective resolution and again obtain complexes of finitely generated abelian groups because $\mathrm{Hom}_{\mathbb{Z}G}(P,M)\subseteq \mathrm{Hom}_{\mathbb{Z}}(P,M)$, which is a finitely generated abelian group if P and M are, and $M\otimes_{\mathbb{Z}G}P$ is an image of $M\otimes_{\mathbb{Z}}P$ which is finitely generated. The homology groups of these complexes are again finitely generated by the structure of finitely generated abelian groups. □

Proposition 3.5.2. *Suppose that G is a finite group. Let A and B be left $\mathbb{Z}G$-module, C a right $\mathbb{Z}G$-module and suppose that A is free as an abelian group. Then $|G|\cdot \mathrm{Ext}^n_{\mathbb{Z}G}(A,B)=0$ and $|G|\cdot \mathrm{Tor}^{\mathbb{Z}G}_n(C,A)=0$ for all $n\geq 1$.*

Proof. Let

$$\begin{array}{ccccccccccccc} \cdots & \to & P_2 & & \xrightarrow{d_2} & & P_1 & & \xrightarrow{d_1} & & P_0 & \to & A & \to & 0 \\ & & & \searrow & & \nearrow & & \searrow & & \nearrow & & & & & \\ & & & & K_1 & & & & K_0 & & & & & & \end{array}$$

be a projective resolution of A, so that

$$\mathrm{Hom}_{\mathbb{Z}G}(P_{n-1},B)\to \mathrm{Hom}_{\mathbb{Z}G}(K_{n-1},B)\to \mathrm{Ext}^n_{\mathbb{Z}G}(A,B)\to 0$$

is exact if $n\geq 1$. Given a $\mathbb{Z}G$-module homomorphism $\theta: K_{n-1}\to B$ we show that $|G|\cdot\theta$ lies in the image of $\mathrm{Hom}_{\mathbb{Z}G}(P_{n-1},B)$. Since the kernels K_n are submodules of free modules they are free abelian groups, so that the exact sequence $0\to K_{n-1}\to P_{n-1}\to K_{n-2}\to 0$ is split as a sequence of abelian groups, and $P_{n-1}\cong K_{n-1}\oplus K_{n-2}$ as abelian groups. We extend θ to a map $\eta: P_{n-1}\to B$ of abelian groups in any way we choose, for example, $\eta=(\theta,0): K_{n-1}\oplus K_{n-2}\to B$. Then $\tilde{\eta}=\sum_{g\in G} g\eta g^{-1}: P_{n-1}\to B$ is a $\mathbb{Z}G$-module homomorphism by a familiar argument in representation theory, and with $\tilde{\eta}|_{K_{n-1}}=|G|\theta$ because η commutes with the action of G on K_{n-1}.

The argument for Tor is similar. □

The argument we have just given works without the hypothesis that A is free as an abelian group, provided $n\geq 2$. It is not always true that $|G|\cdot\mathrm{Ext}^1_{\mathbb{Z}G}(A,B)=0$ for arbitrary modules A and B. For example, if we take $A=B=\mathbb{Z}/m\mathbb{Z}$ with the trivial $\mathbb{Z}G$-action we have $\mathrm{Ext}^1_{\mathbb{Z}G}(A,B)\cong Z/m\mathbb{Z}$, and in fact $0\to\mathbb{Z}/m\mathbb{Z}\to\mathbb{Z}/m^2\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}\to 0$ is a non-split extension of order m in the Ext group. There is no restriction on m here, and it does not have to be a divisor of $|G|$. Also, if k is a field and A and B are kG-modules then $|G|\cdot\mathrm{Ext}^n_{kG}(A,B)=0$ for all $n\geq 1$.

The special case that $|G|$ annihilates $H^n(G,M)$ and $H_n(G,M)$ when $n\geq 1$ is often proved using the properties of the restriction and corestriction maps (which we have not yet defined). It is a quick proof, but so is the one we have given. The proof here is more elementary because there is no need to define restriction and corestriction, and it applies more generally.

Corollary 3.5.3. *If G is a finite group and M is a finitely generated $\mathbb{Z}G$-module then for all $n \geq 1$, $H^n(G, M)$ and $H_n(G, M)$ are finite abelian groups of exponent dividing $|G|$.*

We say that the abelian group A is *uniquely divisible by an integer* n if for all $a \in A$ there exists a unique $b \in A$ with $a = nb$. This happens if and only if the homomorphism $n : A \to A$ is an isomorphism. We say that A is *uniquely divisible* if it is uniquely divisible by every positive integer n. For example, $\mathbb{Q}$ and $\mathbb{R}$ are uniquely divisible; $\mathbb{Q}/\mathbb{Z}$ is divisible, but not uniquely. If A is finite and $g.c.d(|A|, n) = 1$ then A is uniquely divisible by n.

Corollary 3.5.4. *If G is a finite group and M is a $\mathbb{Z}G$-module that is uniquely divisible by $|G|$ as an abelian group, then $H^n(G, M) = 0$ and $H_n(G, M) = 0$ for all $n \geq 1$.*

Proof. Since multiplication $|G| : M \to M$ is an isomorphism, so is $|G| : H^n(G, M) \to H^n(G, M)$ by functoriality of cohomology. This map is zero if $n \geq 1$, by Proposition 3.5.2, so it follows that $H^n(G, M) = 0$ if $n \geq 1$. The argument with $H_n(G, M)$ is similar. □

The vanishing of homology and cohomology on a class of modules allows us to do 'dimension shifting' in the same way as we have seen using projective and injective modules.

Corollary 3.5.5. *Let G be a finite group. Then*

$$H^n(G, \mathbb{Z}) \cong H^{n-1}(G, \mathbb{Q}/\mathbb{Z}) \cong H^{n-1}(G, \mathbb{C}^\times)$$

for all $n \geq 2$, with similar isomorphisms in homology.

Proof. For the first isomorphism we use the long exact sequence in cohomology associated to the short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. Because $\mathbb{Q}$ is uniquely divisible, the terms $H^n(G, \mathbb{Q})$ are all zero when $n \geq 1$, and this gives the result.

In the second isomorphism $\mathbb{C}^\times$ denotes the multiplicative group of nonzero complex numbers, which is isomorphic to $\mathbb{R}^\times_{>0} \times S^1$ via the correspondence $z \leftrightarrow (|z|, \arg(z))$. We thus have a short exact sequence $1 \to \mathbb{Z} \to \mathbb{R}^\times_{>0} \times \mathbb{R}^+ \to \mathbb{C}^\times \to 1$. Because $\mathbb{R}^\times_{>0} \cong \mathbb{R}^+$ via the natural logarithm, the term in the middle of this sequence is uniquely divisible and now the long exact sequence associated to the exact sequence gives the result. □

Example 3.5.6. Several apparently different definitions of the Schur multiplier can be found in the literature, and we now explain how they are connected. We need a result that we have not yet considered, known as the integral duality theorem. This states, for a finite group G, that $H^{n+1}(G, \mathbb{Z}) \cong H_n(G, \mathbb{Z})$ when $n \geq 1$. Putting this together with Corollary 3.5.5, we have $H_2(G, \mathbb{Z}) \cong H^3(G, \mathbb{Z}) \cong H^2(G, \mathbb{C}^\times) \cong H^2(G, \mathbb{Q}/\mathbb{Z})$. These groups are all isomorphic to the Schur multiplier when G is finite. When G is not finite we need to use the definition $H_2(G, \mathbb{Z})$.

Do integral duality somewhere.

The following theorem was introduced by Zassenhaus in his book of 1937, where he attributes the result to Schur. We will give the first step in the proof

Theorem 3.5.7 (Schur-Zassenhaus)**.** *Let $1 \to M \to E \to G \to 1$ be a short exact sequence of finite groups where g.c.d.$(|M|, |G|) = 1$. Then the extension is split, so that $E \cong M \rtimes G$. Under the further assumption that one of M or G is solvable, all subgroups of E of order $|G|$ are conjugate.*

The last statement is still correct without the assumption that one of M or G is solvable, because one of these groups must have odd order and so be solvable by the Feit-Thompson theorem, but this is a much harder result.

Proof. We only give the proof in the case where M is abelian. Here $H^2(G, M) = H^1(G, M) = 0$ by Corollary 3.5.4, so the result follows from our interpretation of second and first cohomology. □

Let C be an abelian group. We will call any module of the form $\mathbb{Z}G \otimes_{\mathbb{Z}} C$ an *induced* module, and any module of the form $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, C)$ a *coinduced* module. The latter is made into a left $\mathbb{Z}G$-module using the right action on $\mathbb{Z}G$. Thus if $\phi : \mathbb{Z}G \to C$ and $g, x \in \mathbb{Z}G$ then $(g\phi)(x) := \phi(xg)$.

Lemma 3.5.8. *If M is coinduced then $H^n(G, M) = 0$ for all $n \geq 1$. If M is induced then $H_n(G, M) = 0$ for all $n \geq 1$.*

There is no restriction on G for this result.

Proof. Let $M = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, C)$ for some abelian group C. We compute cohomology with coefficients in M by applying the functor $\mathrm{Hom}_{\mathbb{Z}G}(-, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, C))$ to a projective resolution and taking cohomology of the resulting cochain complex. For any module P we have a natural isomorphism $\mathrm{Hom}_{\mathbb{Z}G}(P, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, C)) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G \otimes_{\mathbb{Z}G} P, C) \cong \mathrm{Hom}_{\mathbb{Z}}(P, C)$. Applying the functor $\mathrm{Hom}_{\mathbb{Z}}(-, C)$ to a projective resolution of $\mathbb{Z}$, we get an acyclic complex (meaning that it has zero homology) because, as abelian groups, the projective resolution splits. This means that each term in the resolution is the direct sum of the image of one differential and the kernel of the next, so that the complex obtained by applying $\mathrm{Hom}_{\mathbb{Z}}(-, C)$ has the same property, so is acyclic. Thus $H^n(G, M) = 0$ for $n \geq 1$. Similarly to compute homology we consider terms $P \otimes_{\mathbb{Z}G} \mathbb{Z}G \otimes_{\mathbb{Z}} C \cong P \otimes_{\mathbb{Z}} C$, and again applying $- \otimes_{\mathbb{Z}} C$ to the projective resolution gives an acyclic complex for the same reason. □

Make sure this adjoint isomorphism is somewhere in the text.

Proposition 3.5.9. *If G is finite then induced and coinduced modules coincide. Hence cohomology vanishes on induced modules in degrees ≥ 1, as does homology. If P is a projective RG-module for some commutative ring R then $H^n(G, P) = 0$ for all $n \geq 1$.*

Proof. For any abelian group C we define a mapping $\mathbb{Z}G \otimes_{\mathbb{Z}} C \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, C)$ by $g \otimes c \mapsto \phi_{(g,c)}$ where $\phi_{(g,c)} : \mathbb{Z}G \to C$ is the homomorphism determined by

$$\phi_{(g,c)}(h) = \begin{cases} c & \text{if } g = h^{-1}, \\ 0 & \text{otherwise.} \end{cases}$$

We check that this is a homomorphism of $\mathbb{Z}G$-modules that is always injective, and is

Write out the check? Class activity? Write something about using R.

surjective if G is finite.

For the final statement about projective RG-modules, observe that $RG = \mathbb{Z}G \otimes_{\mathbb{Z}} R$ is an induced module left $\mathbb{Z}G$-module, so that cohomology vanishes on it when $n \geq 1$. Projective modules are direct summands of sums of such modules, so cohomology also vanishes on them. □

Remark 3.5.10. There is another left action of G on $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, C)$ that is often seen where, for each element $g \in G$, we use the left action of g^{-1} on $\mathbb{Z}G$. Thus for a homomorphism ϕ we take $(g\phi)(x) = \phi(g^{-1}x)$, as distinct from $g\phi(x) = \phi(xg)$. The two $\mathbb{Z}G$-modules $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, C)$ obtained in this way are isomorphic, with an isomorphism being given on morphisms ϕ by composing with the anti-automorphism of $\mathbb{Z}G$ that inverts the group elements. We chose to use the right action on $\mathbb{Z}G$ in the definition of the left action on a coinduced module because this is available for every ring and because it fits well with the adjunction of Hom and tensor product.

Corollary 3.5.11. *Let C be an abelian group. Any group extension*

$$1 \to \mathbb{Z}G \otimes_{\mathbb{Z}} C \to E \to G \to 1$$

with G finite must split, giving a wreath product $E \cong C \wr G$. Furthermore, all complements in E to the base group $C^{|G|}$ are conjugate.

Proof. The group $C \wr G$ is the wreath product with G permuting copies of C in the regular action, and we simply observe that the base group in this wreath product is the induced module $\mathbb{Z}G \otimes_{\mathbb{Z}} C$. The vanishing of first and second cohomology proves all the statements. □

Chapter 4

Crystallography

4.1 Groups associated to $\mathbb{R}^n$

We start by introducing notation for groups associated to the vector space $\mathbb{R}^n$, which we take to be the set of column vectors of length n with entries in $\mathbb{R}$. We will also put the standard inner product on $\mathbb{R}^n$, so that it has a notion of distance, and it becomes *Euclidean space* $\mathbb{E}^n$. The only difference between $\mathbb{R}^n$ and $\mathbb{E}^n$ is that the latter comes equipped with the inner product.

Definition 4.1.1.

- The *general linear group* $GL(n)$ is the group of invertible linear transformations $\mathbb{R}^n \to \mathbb{R}^n$. It can be identified as the group of invertible $n \times n$-matrices.
- We write $T(n)$ for the group of all mappings $t_w : \mathbb{R}^n \to \mathbb{R}^n$ of the form $t_w(v) = v+w$, for some vector $w \in \mathbb{R}^n$. This mapping t_w is *translation* through the vector w.
- The set of all distance-preserving linear maps $\mathbb{E}^n \to \mathbb{E}^n$ is the group $O(n)$ of *orthogonal transformations*. It can be identified as the group of all $n \times n$-matrices A with the property that $A^T A = I$ is the identity matrix, and its elements have determinant ± 1. When $n = 2$ the elements of determinant $+1$ are rotations, and those with determinant -1 are reflections.
- Given $\alpha \in GL(n)$ and $w \in \mathbb{R}^n$, let $\phi_{w,\alpha} : \mathbb{R}^n \to \mathbb{R}^n$ be the mapping specified by $\phi_{w,\alpha}(v) = \alpha(v) + w$. Such a mapping is called an *affine transformation* of $\mathbb{R}^n$. The translations t_w are the special case that arises when α is the identity. The set
$$\mathrm{Aff}(n, \mathbb{R}) = \{\phi_{w,\alpha} \mid w \in \mathbb{R}^n,\ \alpha \in GL(n)\}$$
is the *affine group* in dimension n.
- Let $R(n)$ be the group of distance preserving transformations, or *rigid motions* of $\mathbb{E}^n$.

Rigid motions of $\mathbb{E}^n$ are also called *isometries* of $\mathbb{E}^n$.

Example 4.1.2. We describe all the rigid motions of $\mathbb{E}^2$. A rigid motions of $\mathbb{E}^2$ is one of the following:

- a translation t_w,
- a rotation about some point in $\mathbb{E}^2$,
- a reflection in some (affine) line of $\mathbb{E}^2$, or
- a glide reflection.

Glide reflections are transformations $\phi_{w,\alpha}(v) = \alpha(v) + w$ where w is a nonzero vector in $\mathbb{E}^2$ and α is reflection in the line determined by w. To see that this is a complete list of rigid motions, take an arbitrary rigid motion θ of $\mathbb{E}^2$ and consider the composite $\eta = t_{-\theta(0)}\theta$. This is a rigid motion that fixes 0, so it is an orthogonal transformation of $\mathbb{E}^2$, hence a reflection or a rotation. Now $\theta = t_{\theta(0)}\eta$ and by examining the possible maps that can arise in this way we see that it is one of the four kinds of rigid motion listed.

Proposition 4.1.3. *1. The sets $GL(n)$, $T(n)$, $O(n)$, $\mathrm{Aff}(n)$ and $R(n)$ are all groups under composition of mappings.*

2. $T(n) \cong \mathbb{R}^n$.

3. $\mathrm{Aff}(n) = T(n) \rtimes GL(n)$. This group is isomorphic to the group of $(n+1)\times(n+1)$ block matrices of the form $\begin{bmatrix}\alpha & w\\ 0 & 1\end{bmatrix}$ where $w \in \mathbb{R}^n$ and $\alpha \in GL(n)$.

4. $R(n) = T(n) \rtimes O(n)$. This group is a subgroup of $\mathrm{Aff}(n)$, isomorphic to the group of $(n+1)\times(n+1)$ block matrices of the form $\begin{bmatrix}\alpha & w\\ 0 & 1\end{bmatrix}$ where $w \in \mathbb{R}^n$ and $\alpha \in O(n)$.

Proof. To see that $\mathrm{Aff}(n)$ is closed under composition and taking inverses, we compute that $\phi_{u,\beta}\phi_{w,\alpha} = \phi_{u+\beta(w),\beta\alpha}$ and $\phi_{w,\alpha}^{-1} = \phi_{-\alpha^{-1}(w),\alpha^{-1}}$. We see that $R(n) \cong T(n) \rtimes O(n)$, because any rigid transformation is the product of a translation and an element of $O(n)$, clearly $T(n) \lhd R(n)$ and $O(n) \cap T(n) = 1$. □

To be completed. Is it obvious that every rigid transformation is a product of a translation and an orthogonal transformation?

The set of $(n+1)\times(n+1)$-matrices is a metric space, with the distance between two matrices being the usual distance between vectors in $\mathbb{R}^{(n+1)^2}$. Thus $\mathrm{Aff}(n,\mathbb{R})$ becomes a metric space by restriction of the distance function in its realization as a set of $(n+1)\times(n+1)$-matrices, as do all of the groups $GL(n)$, $T(n)$, $O(n)$, and $R(n)$, which are subgroups of $\mathrm{Aff}(n)$. Notice that the distance function this defines on the translation group $T(n)$, which identifies with $(n+1)\times(n+1)$ matrices of the form $\begin{bmatrix}I & w\\ 0 & 1\end{bmatrix}$, is the same as the distance function obtained by identifying $T(n)$ with $\mathbb{E}^n$: the

length of a translation t_w is the same as the length of the vector w. We will use the fact that $O(n)$ is compact: it consists of matrices A with $A^T A = I$ so it is closed and bounded.

Theorem 4.1.4. *Let H be a subgroup of $R(n)$. The following are equivalent.*

1. *H is discrete in the induced topology as a subset of $R(n)$,*
2. *$H \cap T(n)$ is discrete in the induced topology as a subset of $R(n)$,*
3. *there exists a number $d > 0$ such that every non-identity element of $H \cap T(n)$ has length at least d.*
4. *there exists a number $d > 0$ such that, for every vector $w \in \mathbb{E}^n$ and every non-identity element of $t \in H \cap T(n)$, the distance from w to tw at least d.*
5. *there exists a number $d > 0$ such that, for every vector $w \in \mathbb{E}^n$ and every non-identity element of $g \in H$, either $w = gw$ or the distance from w to tw at least d.*

Proof missing. Part of it is in Prop 4.3.1

Definition 4.1.5. We say that a subgroup H of $\mathrm{Aff}(n, \mathbb{R})$ is *discrete* if its induced topology is discrete. Equivalently, this means that, for all $h \in H$, there exists $d > 0$ so that the ball $B_d(h)$ of radius d has $B_d(h) \cap H = \{h\}$.

Proposition 4.1.6. *Let H be a subgroup of the group $T(n)$ of all translations of $\mathbb{R}^n$. The following are equivalent.*

1. *H is discrete.*
2. *H is generated by r independent translations for some $r \leq n$. Thus $H \cong \mathbb{Z}^r$.*

Proof. The implication (2) implies (1) is immediate.

To prove that (1) implies (2), assume condition (1). We show that $H \cong \mathbb{Z}^r$ for some $r \leq n$ by induction on n. When $n = 0$ evidently H must be the trivial group, so the result holds, and this starts the induction.

Now suppose that $n > 0$ and the result is true for smaller values of n. It is convenient for the notation to let $X := H \cdot 0$ be the set of translates of the zero vector under the action of H, so that a translation $t_w \in H$ corresponds to the vector $w \in X$, and X is a discrete subset of $\mathbb{R}^n$.

We can find a non-zero vector $v \in X$ that cannot be expressed as $v = \lambda w$ for any $w \in X$ with $\lambda > 1$. To do this, start with any non-zero vector $u \in X$. By discreteness of X, the closed ball center 0 with $\|u\|$ as radius only contains finitely many elements of X, and we may let v be such an non-zero element of minimal length. We see that the subgroup generated by v is $\langle v \rangle = X \cap \mathbb{R}v$, because if $X \cap \mathbb{R}v$ were larger than this we could find a vector w in it with $v = \lambda w$ and $\lambda > 1$. We claim that $X/\langle v \rangle \cong (X + \mathbb{R}v)/\mathbb{R}v$ is a discrete subgroup of $\mathbb{R}^{n-1}$. To see this, we show that if $w \in X - \mathbb{R}v$ then the distance from w to any point on $\mathbb{R}v$ is greater than some fixed

$\epsilon > 0$. The justification for this is that the possible distances from points in X to the line segment between 0 and v are the same as the possible distances from points in X to the line segment between nv and $(n+1)v$ for every n, since addition of v preserves these distances. Since this line segment is compact, there is a closest point w to it, and we can take ϵ to be smaller than the distance between w and the line segment.

Now, by induction, $(X + \mathbb{R}v)/\mathbb{R}v$ is isomorphic to $\mathbb{Z}^{r-1}$ for some $r \leq n$, generated by certain vectors $v_1 + \langle v \rangle, \ldots, v_{r-1} + \langle v \rangle$. We see that $v_1, \ldots, v_{r-1}, v$ generate X, which is a torsion free abelian group, so it is isomorphic to $\mathbb{Z}^r$. □

We remark that finitely generated subgroups of $T(n)$ are always free abelian, being torsion free, but there are many of these subgroups that are not discrete and their rank may be larger than n. For instance, if we take non-zero real numbers a and b for which a/b is not rational then the subgroup generated by a and b is dense in $\mathbb{R}$.

There is an action of $GL(n)$ on $T(n)$ given by conjugation within $\mathrm{Aff}(n)$, which restricts to an action of $O(n)$ on $T(n)$ given by conjugation within $R(n)$. After identifying $T(n)$ with $\mathbb{E}^n$, these are the same as the usual action of $GL(n)$ on $\mathbb{R}^n$, and of $O(n)$ on $\mathbb{E}^n$. That is to say, if $\alpha \in GL(n)$ and $t_w \in R(n)$ is translation by the vector $w \in \mathbb{R}^n$ then $\alpha t_w \alpha^{-1} = t_{\alpha w} \in \mathrm{Aff}(n)$. In the case of the action of $O(n)$, the action is by orthogonal transformations of $T(n)$, after it is identified with $\mathbb{E}^n$. Put this somewhere else.

4.2 Crystal structures and their space groups

One notion of a crystalline substance in the real (3-dimensional) world is that it is a substance whose molecules are positioned in a pattern that repeats itself, in each of three independent directions. This is suggested by the property that a crystal will break cleanly along certain planes of cleavage when struck by a blow from a sharp edge parallel to that plane, and that the normal vectors to such planes of cleavage can be chosen to be in three independent directions. Such a property is not shared by glass, for example, which tends to be amorphous, and will shatter into unorganized pieces no matter how it is struck.

The symmetry properties of such a crystal are the most important part of the information obtained in examining the crystal by means of X-ray crystallography. For these practical applications a classification of the possible crystals that can arise, in terms of their symmetry, is crucial. This is a mathematical problem, and it starts with an abstract formulation of what we mean by a crystal. We give it a different name to make the distinction between the object seen in real life and its mathematical model.

Definition 4.2.1. A *crystal structure* in dimension n is a subset $\mathcal{C}$ of n-dimensional real Euclidean space $\mathbb{E}^n$ such that

- Among the rigid motions of $\mathbb{E}^n$ that send $\mathcal{C} \to \mathcal{C}$, there exist n linearly independent translations, and
- there exists a number $d > 0$ such that every non-identity translation preserving $\mathcal{C}$ has magnitude at least d.

We let $S(\mathcal{C})$ denote the group of rigid motions $\mathbb{E}^n \to \mathbb{E}^n$ that preserve $\mathcal{C}$. This is the *space group* corresponding to $\mathcal{C}$. We will say that a group G is a *space group in dimension* n if it is the space group of some crystal structure in dimension n.

The subgroup

$$T = \{t \in S(\mathcal{C}) \mid t \text{ is a translation}\} = S(\mathcal{C}) \cap T(n)$$

is called the *translation subgroup*. It is a normal subgroup of $S(\mathcal{C})$, and the quotient $P = S(\mathcal{C})/T$ is called the *point group*.

Class Activity. At this point some examples are presented where point groups are calculated. Insert examples.

It is tempting to think that in the action of $S(\mathcal{C})$ on $\mathbb{E}^n$, the point group is a group of orthogonal transformations fixing some point, but this need not be the case. In fact it will happen precisely when the extension $1 \to T \to S(\mathcal{C}) \to P \to 1$ is split, because then the realization of P as a subgroup of $S(\mathcal{C})$ provides a splitting. In general this subtle point means that one genuinely has to work with quotient groups in the definition and calculation of the point group.

There is, however, a module action of P on T given by conjugation within $S(\mathcal{C})$. This comes about because conjugation T by of elements of $S(\mathcal{C})$ make T into a module for $S(\mathcal{C})$. Because T acts trivially in this action, it gives rise to an action of the quotient group P. By considering the embedding

$$P = S(\mathcal{C})/(S(\mathcal{C}) \cap T(n)) \cong (T(n) \cdot S(\mathcal{C}))/T(n) \hookrightarrow R(n)/T(n) = O(n)$$

we see that the conjugation action on T is by orthogonal transformations. We reiterate that this action does not come from the initial action of $S(\mathcal{C})$ on $\mathbb{E}^n$.

Lemma 4.2.2. *Let $S(\mathcal{C})$ be a space group in dimension n. Then $T \cong \mathbb{Z}^n$, P acts faithfully on T in the action given by conjugation, and P is finite.*

Proof. By Theorem 4.1.4, T is a discrete subgroup of $T(n)$, and it contains n independent elements. It follows by Proposition 4.1.6 that $T \cong \mathbb{Z}^n$.

Because P embeds in $O(n)$, which acts faithfully on $T(n)$, P also acts faithfully on $T(n)$. But now $T(n) \cong \mathbb{R} \otimes_{\mathbb{Z}} T$ and so P must act faithfully on T by conjugation. since any element that acted trivially would also act trivially on $T(n)$.

Let $T = \langle t_1, \ldots, t_n \rangle$. Consider the set $P\{t_1, \ldots, t_n\}$ of all images of these generators under the conjugation action of P. This is a subset of T, which is discrete. This set is permuted faithfully by P and its elements lie inside a closed ball of finite radius, because P acts as a subgroup of $O(n)$, preserving lengths of vectors. Since the closed ball is compact, the set is finite, and so P is finite. □

4.3 Characterizations of space groups

In this section we present two further equivalent characterizations of space groups. One reason for doing this is that in consulting the literature on these groups different

definitions are encountered and the theory is developed from that standpoint, without showing that it is the equivalent to theory developed from a different standpoint. The main reason, for our purposes, is that we will use the algebraic characterization that we obtain as part of the approach to classifying space groups.

Theorem 4.3.1. *Let G be a subgroup of $R(n)$. Then G is a space group in dimension n if and only if G is a discrete subgroup of $R(n)$ that contains n linearly independent translations.*

Proof. If G is a space group then we know it is a discrete subgroup of $R(n)$ by Theorem 4.1.4, and it contains n linearly independent translations.

Conversely, suppose that G is a discrete subgroup of $R(n)$ that contains n linearly independent translations. Then $G \cap T(n)$ is a discrete subgroup of $T(n)$ and it contains n independent translations, so $G \cap T(n) \cong \mathbb{Z}^n$ is a lattice, generated by n independent translations, by Proposition 4.1.6. Furthermore, $G/(G \cap T(n))$ embeds as a discrete subgroup of $O(n)$ under the mapping $R(n) \to O(n)$, which is projection onto the second factor under the identification $R(n) = T(n) \rtimes O(n)$. The image of G under this map is discrete because the projection is an open map, and the cosets in G of $G \cap T(n)$ are all open sets, so their images in $O(n)$ are all open. It follows that $G/(G \cap T(n))$ is finite because $O(n)$ is compact.

This argument is nonsense. The cosets are open in G, but not in $R(n)$. Projection need not send a discrete subgroup to a discrete subgroup, e.g. $\mathbb{Z}^2$ to a line with slope $\sqrt{2}$ has kernel 1 (discrete) and the image is not discrete.

We now produce a crystal structure $\mathcal{C}$ for G. To do this, we show that there is an open subset U of $\mathbb{E}^n$ for which $U \cap gU = \emptyset$ for all non-identity $g \in G$. We examine the fixed points of elements of G. For elements in a coset $(G \cap T(n))g$ the fixed points are the translates under the translation subgroup of the fixed points of g, which are an affine subspace of dimension less than n. There are finitely many such cosets, so the union of all these affine subspaces is a proper closed subset of $\mathbb{E}^n$. Choose a vector w not in this union, so it is fixed by no non-identity element of G. There exists $d > 0$ so that for all $h \in G$, the distance from w to hw is $\geq x$. This is because we can find such d for the elements in each coset of $G \cap T(n)$, because these differ by translations, and we can take the minimum d that arises with the finitely many cosets. Taking U to be the open ball center w, radius $d/2$, this open set has the desired property.

Take an unsymmetric pattern contained in U, and let $\mathcal{C}$ be the orbit of the pattern under G. Then $\mathcal{C}$ is a crystal structure. We show that its space group $S(\mathcal{C})$ is G. Certainly $S(\mathcal{C})$ contains G; it can be no larger than G because any element $s \in S(\mathcal{C})$ sends the unsymmetric pattern to the same place as some $g \in G$, and now $g^{-1}s$ stabilizes the pattern, so equals 1 by its asymmetry. Hence $s = g \in G$. □

Theorem 4.3.2. *Let G be an abstract group with a normal subgroup $T \cong \mathbb{Z}^n$ such that the quotient $P = G/T$ is finite and acts faithfully on T by conjugation. Then G is isomorphic to a space group of dimension n.*

Proof. Embed T in $T(n)$ by a homomorphism ϕ in any way as a discrete subgroup

containing n independent translations, and form the explicit pushout

$$\begin{array}{ccccccccc} 1 & \longrightarrow & T & \xrightarrow{\theta} & G & \longrightarrow & P & \longrightarrow & 1 \\ & & {\scriptstyle\phi}\downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & T(n) & \longrightarrow & E & \longrightarrow & P & \longrightarrow & 1 \end{array}$$

where $E = T(n) \rtimes G/\{(-\phi t, \theta t) \mid t \in T\}$. Since $T(n) \cong \mathbb{R}^n$ is uniquely divisible by $|P|$ we have $H^2(P, T(n)) = 0$ and the lower extension splits.

Because P is finite we may put an inner product on $\mathbb{R}^n$ that is preserved by P. This may be done by taking any inner product $\langle \quad , \quad \rangle_1$ and defining

$$\langle u, v \rangle = \sum_{g \in P} \langle gu, gv \rangle_1.$$

Now P acts orthogonally, so there exists a map $\tau : P \to O(n)$ expressing the orthogonal action of P using this inner product. The diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & T(n) & \longrightarrow & T(n) \rtimes P & \longrightarrow & P & \longrightarrow & 1 \\ & & \| & & & & {\scriptstyle\tau}\downarrow & & \\ 1 & \longrightarrow & T(n) & \longrightarrow & T(n) \rtimes O(n) & \longrightarrow & O(n) & \longrightarrow & 1 \\ & & & & \| & & & & \\ & & & & R(n) & & & & \end{array}$$

may thus be completed to a commutative diagram by a map $T(n) \rtimes P \to R(n)$, which must necessarily be a monomorphism. Then the composite $G \hookrightarrow T(n) \rtimes P \hookrightarrow R(n)$ embeds G as a discrete subgroup of $R(n)$ with $G \cap T(n) \cong \mathbb{Z}^n$, by Proposition 4.1.4. □

Lemma 4.3.3. *Let G be any group that is an extension $1 \to T \to G \to P \to 1$ where $T \cong \mathbb{Z}^n$, $|P| < \infty$ and P acts faithfully on T, Then T is a maximal abelian subgroup of G, and is the unique such subgroup isomorphic to $\mathbb{Z}^n$.*

Proof. If $T < H \leq G$ and $h \in H - T$ then h acts non-trivially on T, so H is non-abelian. Thus T is a maximal abelian subgroup of G.

Suppose $X \cong \mathbb{Z}^n$ is any subgroup isomorphic to $\mathbb{Z}^n$. Then

$$1 \to X \cap T \to X \to X/(X \cap T) \cong XT/T \to 1$$

is exact and XT/T is a subgroup of the finite group P, so $X/(X \cap T)$ is finite and hence $X \cap T \cong \mathbb{Z}^n$ so $X \cap T \cong \mathbb{Z}^n$ has finite index in T. If there were $x \in X - T$ then x would act non-trivially on T and hence on $X \cap T$, so X would be non-abelian – a contradiction. Therefore $X = X \cap T \subseteq T$. This shows that T is the unique maximal subgroup isomorphic to $\mathbb{Z}^n$. □

We will show how to classify crystal structures in terms of their symmetries, and before doing this we introduce an equivalence relation so that crystal structures are regarded as the same under certain circumstances. One way to describe the equivalence of crystal structures is to say that the space group of one may be identified with the space group of the other after applying an affine transformation. Such transformations are composites of linear (vector space) transformations and translations and form the *affine group*, which has the structure $\mathbb{E}^n \rtimes GL(n, \mathbb{R})$. Thus we will not distinguish crystal structures if one is scaled up from the other, or is a skewed version of the other, or is translated, provided they have the same symmetries. Since we are only interested in the symmetries a crystal structure has, we work with its space group.

Definition 4.3.4. Two space groups are *equivalent* if they are conjugate as subgroups of the affine group. Sometimes the term *affinely equivalent* is also used. We also say that two crystal structures are equivalent if their space groups are equivalent.

Proposition 4.3.5. *Let* $1 \to T_1 \to G_1 \to P_1 \to 1$ *and* $1 \to T_2 \to G_2 \to P_2 \to 1$ *be space groups acting on* $\mathbb{E}^n$ *with translation subgroups* T_1 *and* T_2*. The following are equivalent.*

1. *The space groups are equivalent.*
2. *There exists a commutative diagram*

$$\begin{array}{ccccccccc} 1 & \to & T_1 & \to & G_1 & \to & P_1 & \to & 1 \\ & & \cong\downarrow & & \cong\downarrow & & \cong\downarrow & & \\ 1 & \to & T_2 & \to & G_2 & \to & P_2 & \to & 1 \end{array}$$

   in which the vertical arrows are isomorphisms.

3. $G_1 \cong G_2$ *as abstract groups.*

Proof. 1. $\Rightarrow$ 3. is clear.

3. $\Rightarrow$ 2: If $\phi : G_1 \to G_2$ is an isomorphism then $\phi(T_1)$ must be the unique maximal abelian subgroup of G_2 isomorphic to $\mathbb{Z}^n$. Hence $\phi(T_1) = T_2$ by Lemma 4.3.3, and ϕ provides a commutative diagram as in condition 2.

2. $\Rightarrow$ 1: Suppose we are given a commutative diagram in which the vertical arrows are isomorphisms

$$\begin{array}{ccccccccc} 1 & \to & T_1 & \to & G_1 & \to & P_1 & \to & 1 \\ & & {\scriptstyle\alpha}\downarrow & & {\scriptstyle\beta}\downarrow & & {\scriptstyle\gamma}\downarrow & & \\ 1 & \to & T_2 & \to & G_2 & \to & P_2 & \to & 1. \end{array}$$

These extensions are both embedded in $R(n) = \mathbb{R}^n \rtimes O(n)$ because they are assumed to be space groups, so we have containments for $i = 1, 2$:

$$\begin{array}{ccccccccc} 1 & \to & T_i & \to & G_i & \to & P_i & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & \mathbb{R}^n & \to & \mathbb{R}^n \rtimes GL(n,\mathbb{R}) & \to & GL(n,\mathbb{R}) & \to & 1. \end{array}$$

In this manner we may assume that $T_i \leq \mathbb{R}^n$ and $P_i \leq GL(n,\mathbb{R})$ for $i = 1, 2$. Since both T_1 and T_2 contain bases of $\mathbb{R}^n$ they are conjugate by an element $x \in GL(n,\mathbb{R})$, so that ${}^xT_1 = T_2$. After conjugating the whole group G_1 by x we may assume $T_1 = T_2 = T$, say. Now $\gamma : P_1 \to P_2$ must be the identity, because for any element $g \in P_1$, $g^{-1}\gamma(g)$ must act as the identity on T, and hence also on $\mathbb{R}^n$. This cannot happen unless $g = \gamma(g)$ because $GL(n,\mathbb{R})$ acts faithfully on $\mathbb{R}^n$. We write P for the group $P_1 = P_2$. Let E denote the preimage of P in $\mathbb{R}^n \rtimes GL(n,\mathbb{R})$, so that β extends to an automorphism $\tilde{\beta} : E \to E$ as follows:

$$\begin{array}{ccccccccc} & & & & & & E & & & \\ & & & & & \nearrow & & \searrow & & \\ 1 & \to & \mathbb{R}^n & & & & \tilde{\beta}\downarrow & & P & \to & 1 \\ & & & & & \searrow & & \nearrow & & \\ & & & & & & E & & & \end{array}$$

We show that $\tilde{\beta}$ is conjugation by some translation in $\mathbb{R}^n$. Firstly, both extensions here split, because $H^2(P,\mathbb{R}^n) = 0$; and now $\tilde{\beta}$ is conjugation by an element of $\mathbb{R}^n$ since $H^1(P,\mathbb{R}^n) = 0$. Since β is the restriction of $\tilde{\beta}$ it is also given by conjugation by an element of $\mathbb{R}^n$. Earlier, when we assumed that T_1 and T_2 contain a common basis, we modified β by conjugation by a an element of $GL(n,\mathbb{R})$. Putting this together, we have shown that G_1 and G_2 are conjugate in the affine group $\mathbb{R}^n \rtimes GL(n,\mathbb{R})$, so this completes the proof that 2. $\Rightarrow$ 1. □

Remark 4.3.6. It is possible to give a geometric argument for the conjugation by an element of $\mathbb{R}^n$ in the last paragraph, assuming splitting of the extensions. If C is a complement to $\mathbb{R}^n$ in E then $\tilde{\beta}(C)$ is another complement, and both may be regarded as groups of orthogonal transformations with different vectors $u, v \in \mathbb{E}^n$ taken to be the origin. Now conjugation by the translation from u to v induces $\tilde{\beta}$, and hence β.

As a summary of the results so far, we have now shown that to classify space groups of dimension n up to affine equivalence it is equivalent to classify extensions $1 \to T \to G \to P \to 1$ where $T \cong \mathbb{Z}^n$ and P is a finite group acting faithfully on T, up to equivalence by diagrams as in Proposition 4.3.5 part 2.

Theorem 4.3.7. *The following are equivalent.*

1. *G is (isomorphic to) a space group in dimension n.*
2. *G is a discrete subgroup of $R(n)$ containing n independent translations.*
3. *G has a normal subgroup T isomorphic to $\mathbb{Z}^n$ so that $P := G/T$ is finite and acts faithfully on T by conjugation.*

4.4 Classification of 2-dimensional spacegroups

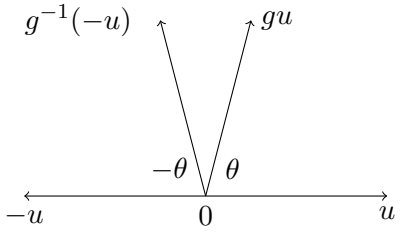
We go through this classification explicitly in dimension 2, but the same approach works in every dimension. We must determine:

- the finite groups P with a faithful action on $\mathbb{Z}^2$, i.e. the finite subgroups of $GL(2,\mathbb{Z})$,
- for each such P the different faithful $\mathbb{Z}P$-modules T with $T \cong \mathbb{Z}^2$ as abelian groups. We need only determine T up to $\mathbb{Z}P$-isomorphism since if $T \cong T'$ we obtain isomorphic extensions using either T or T',
- the possible extensions for each P and T. We calculate $H^2(P,T)$.
- the equivalence of extensions given by diagrams as in Proposition 4.3.5

As in Theorem 4.3.2 we may assume that T is a subgroup of $\mathbb{E}^2$ and that P acts as a group of orthogonal transformations of $\mathbb{E}^2$ preserving T. The next result may be proved in various ways: one approach is to use a description of the structure of $SL(2,\mathbb{Z})$ as a free product with amalgamation. We give a proof that is elementary and geometric.

Lemma 4.4.1. *Let $T \cong \mathbb{Z}^2$ be a 2-dimensional lattice. Any automorphism of T (i.e. an element of $GL(2,\mathbb{Z})$) of finite order has order 1, 2, 3, 4, or 6.*

Proof. Let g be an automorphism of T. We may assume that T is embedded in $\mathbb{E}^2$ and that g acts orthogonally on $\mathbb{E}^2$, preserving T. Now g is either a rotation or a reflection. If it is a reflection, it has order 2. Suppose instead that g is a rotation and choose a non-zero translation $u \in T$ of minimal length. If g is rotation through an angle θ consider the vector $g^{-1}(-u)$. Now the vector $gu - g^{-1}(-u)$ lies in T and is parallel to u. By minimality of u, $gu - g^{-1}(-u)$ is an integer multiple of u. That integer can only be $0, 1$ or 2 and so $\theta = 0, \frac{\pi}{3}, \frac{\pi}{2}, \frac{2\pi}{3}$, or π.



□

Corollary 4.4.2. *Every element of finite order in $GL(3,\mathbb{Z})$ has order 1, 2, 3, 4, or 6. There is no crystal structure in $\mathbb{E}^3$ having a point group with 5-fold symmetry and, in particular, there is no crystal structure in $\mathbb{E}^3$ having a point group with icosahedral symmetry.*

Proof. As we have done before, we let g be an element of finite order in $GL(3,\mathbb{Z})$. We may assume that it acts orthogonally on $\mathbb{E}^3$ preserving a lattice $T \cong \mathbb{Z}^3$. Because the eigenvalues of g are either real or occur in complex conjugate pairs a basis can be chosen so that the matrix of g has the form $\begin{bmatrix} \pm 1 & 0 \\ 0 & A \end{bmatrix}$ where A a 2×2-matrix that is either a Explain why.

rotation matrix or a diagonal matrix with entries ± 1 having order 1 or 2. Matrices of this form have order 2 unless A is a rotation matrix, so we assume that A is a rotation matrix, so that g either has an axis X of rotation, or an axis X that it reverses. We claim that there are nonzero elements of T lying on X. To see this, take any point of T not perpendicular to X. Then the sum of the images of this point under the powers of g is a point $0 \neq v \in X \cap T$. It now follows that the projection of T to $X^\perp$ is a discrete subgroup of $X^\perp$. To see this, suppose to the contrary that, for each n, we can find a point $a_n \neq 0$ in the projection of T to $X^\perp$ with $\|a_n\| < \frac{1}{n}$. We can find $\lambda_n \in \mathbb{R}$ so that $a_n + \lambda_n v$ lies in T and also lies in the compact region that is the product of an interval of length $\|v\|$ in X with a closed unit disc in $X^\perp$. This gives infinitely many distinct points of T lying in that compact region, which is a contradiction. Therefore the projection of T to $X^\perp$ is discrete and so it is isomorphic to $\mathbb{Z}^2$ by 5.1. Now g preserves this 2-dimensional lattice in $\mathbb{E}^2$, so acts on it as a rotation of order 1, 2, 3, 4, or 6 by Lemma 5.6. It follows that the order of g is also one of these numbers. We see that 5-fold symmetry is not possible, hence neither is the group of the icosahedron, since it contains elements of order 5. □

Why is there such?

As a stepping stone in the determination of all possible faithful actions of a finite group on a n-dimensional lattice we introduce the notion of a Bravais lattice. We define a *Bravais lattice* in dimension n to be a subgroup $\mathbb{Z}^n \cong T \leq \mathbb{E}^n$ together with its full orthogonal automorphism group $Q = \{g \in O(n) \mid gT = T\}$ acting on it. Thus a Bravais lattice really consists of a pair (T, Q), but we may refer to just T as the lattice. We will refer to Q as the *Bravais point group*. We consider two of these pairs (T_i, Q_i), $i = 1, 2$ equivalent if there is an automorphism $\alpha \in GL(n, \mathbb{R})$ so that $T_2 = gT_1$ and $Q_2 = {}^gQ_1$. Since every finite group subgroup of $GL(n, \mathbb{R})$ is conjugate to a subgroup of $O(n)$ we have immediately the following result.

Expand on the argument about a discrete subgroup quoted from 5.1, or maybe state separately that a discrete group of translations is $\mathbb{Z}^r$.

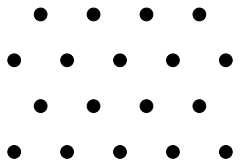
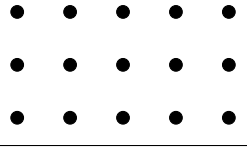
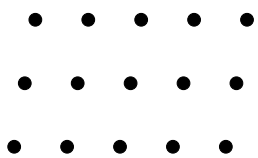
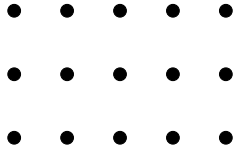
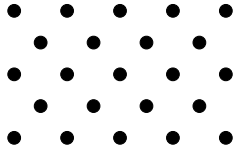
Proposition 4.4.3. *Any faithful $\mathbb{Z}P$-module T with $T \cong \mathbb{Z}^n$ and P finite is $\mathbb{Z}P$-isomorphic to one of the Bravais lattices with P acting as a subgroup of the Bravais point group.*

It follows from this that to obtain all finite groups acting faithfully on lattices $\mathbb{Z}^n$ up to module isomorphism of the lattices, we get a complete list by enumerating the Bravais lattices (T, Q) and listing all subgroups of Q. We only need list these subgroups up to conjugacy, since conjugate subgroups will give isomorphic lattices. Even then we may obtain more than once the same group with an isomorphic lattice, so we should inspect our list to make sure such repetitions do not occur.

Why? Give an isomorphism of such.

Proposition 4.4.4. *The Bravais lattices in dimension 2 are given in the accompanying list.*

Center the words.

P contains	T embeds in $\mathbb{E}^2$ as:	Maximum P
rotation $\frac{\pi}{3}$ or $\frac{2\pi}{3}$		D_{12}
rotation $\frac{\pi}{2}$		D_8
rotation π		C_2
reflection	 generators of T can be chosen along reflection lines	$C_2 \times C_2$
reflection	 generators of T cannot be chosen along reflection lines	$C_2 \times C_2$

The Bravais Lattices in 2 dimensions.

Proof. We let P be a Bravais point group, assume that P contains either a certain rotation or a reflection and reconstruct the embedding of T in $\mathbb{E}^n$. We start with rotations. Every lattice is preserved by rotation through π, so all lattices will be accounted for by this approach. Choose a non-zero element of T that is closest to the origin. After base change, we can assume this is the first standard basis vector. Now if P contains a rotation through $\frac{\pi}{3}$ or $\frac{2\pi}{3}$ we recover a triangular lattice, and if P contains a rotation through $\frac{\pi}{2}$ we recover a square lattice. We continue the argument in this way, assuming P contains a rotation through π, and finally that P contains a reflection. With these last possibilities an inappropriate choice of embedding for T would allow a larger automorphism group than that shown in the list, but then this Bravais lattice would have to be one of the earlier ones given on the list. Note that the two lattices with automorphism group $C_2 \times C_2$ are non-isomorphic for the reason that on one of them generators of T may be chosen along the reflection lines, and in the other this is not possible. □

The argument for the last case of $C_2 \times C_2$ is tricky. Write something.

The only possible point groups of Bravais lattices in dimension 2 are cyclic and dihedral, and this is no surprise in view of the following result, attributed by Weyl in his book 'Symmetry' to Leonardo da Vinci.

Theorem 4.4.5 (Leonardo da Vinci)**.** *Any finite group of real* 2×2 *matrices is either cyclic or dihedral.*

Proof. Every finite group of matrices preserves a positive definite bilinear form and so may be regarded as a subgroup of the orthogonal group. Elements of $O(2)$ are rotations or reflections. In any group of these operations, the rotations form a normal subgroup that must be cyclic if it is finite, and it is of index 1 or 2. If there is a reflection in the group, it inverts the rotations under conjugation. From this we see that they only possibilities are cyclic and dihedral. □

Theorem 4.4.6. *The possible faithful actions of a finite group* P *on* $\mathbb{Z}^2$ *up to* $\mathbb{Z}P$*-isomorphism and up to equivalence under* $\mathrm{Aut}(P)$ *are given in the accompanying table.*

Put in vertical space.

P	Matrices giving action	non-isomorphic extensions
1	$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$	p1
C_2	$\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix} = T_1$	p2
	$\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix} = T_2$	pm,pg
	$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} = T_3$	cm
C_3	$\begin{bmatrix}-1 & 1\\ -1 & 0\end{bmatrix}$	p3
C_4	$\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$	p4
C_6	$\begin{bmatrix}0 & 1\\ -1 & 1\end{bmatrix}$	p6
$C_2 \times C_2$	$\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}$ $\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} = T_1$	p2mm, p2mg, p2gg
	$\begin{bmatrix}-1 & 0\\ -1 & 1\end{bmatrix}$ $\begin{bmatrix}1 & 0\\ 1 & -1\end{bmatrix} = T_2$	c2mm
D_6	$\begin{bmatrix}-1 & 1\\ -1 & 0\end{bmatrix}$ $\begin{bmatrix}1 & 0\\ 1 & -1\end{bmatrix} = T_1$	p31m
	$\begin{bmatrix}-1 & 1\\ -1 & 0\end{bmatrix}$ $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} = T_2$	c2mm
D_8	$\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$ $\begin{bmatrix}-1 & 0\\ 0 & 11\end{bmatrix}$	p4mm, p4gm
D_{12}	$\begin{bmatrix}0 & 1\\ -1 & 1\end{bmatrix}$ $\begin{bmatrix}1 & 0\\ 1 & -1\end{bmatrix}$	p6mm

Proof. We examine all the subgroups of the Bravais point groups. If P acts faithfully on T then the image of P in $\mathrm{Aut}(T)$ is a subgroup of the Bravais point group of T. If we take such an embedding of P up to equivalence under $\mathrm{Aut}(P)$, we obtain all actions of P by listing subgroups of the Bravais point groups. The possible subgroups are cyclic of orders 1, 2, 3, 4 or 6, and dihedral of orders 4, 6, 8 or 12. Isomorphism of the module action on T is the same thing as conjugacy of the action in $GL_n(\mathbb{Z})$ □

At this point we mention a further piece of terminology, that we shall not have occasion to use. For each point group P and each $\mathbb{Z}P$-isomorphism class of lattices T there may be several space groups that are extensions of P by T. We call the collection of such space groups an *arithmetic crystal class.* There is a weaker equivalence relation on space groups that arises by grouping together all those space groups with the same point group P and such that the $\mathbb{Q}P$-modules $\mathbb{Q} \otimes_{\mathbb{Z}} T$ are isomorphic. We obtain in this way a *geometric crystal class* of space groups. For example in dimension 2, pm and pg constitute an arithmetic crystal class, and cm is also in the same geometric crystal class, because the lattice on which P acts has the same character in each of these three cases.

4.5 Computation of $H^2(P, T)$

We turn now to the final ingredient in the classification of crystal structures. Having determined the possibilities for the point group and the translation lattice, we compute the possible extensions that there may be.

In the case of wallpaper patterns we have seen that the point group is either cyclic or dihedral, and as far as the cyclic groups are concerned we may quote a formula for the cohomology: $H^2(P, T) = T^P / \sum_{g \in P} g \cdot T$. In case P is C_3, C_4 or C_6 it is clear that there are no non-zero fixed points on T , so $T^P = 0$, and the only extension of P by T is split. In case $P = C_2$ there are three possible actions, giving lattices T_1, T_2 and T_3 listed in the table of possible actions. These lattices have the structure

$$T_1 = \tilde{\mathbb{Z}} \oplus \tilde{\mathbb{Z}}, \quad T_2 = \mathbb{Z} \oplus \tilde{\mathbb{Z}}, \quad T_3 = \mathbb{Z}C_2$$

as $\mathbb{Z}C_2$-modules, where $\tilde{\mathbb{Z}}$ denotes a copy of $\mathbb{Z}$ with the generator of C_2 acting as -1. Since $T_1^P = 0$ and T_3 is the regular representation we get zero cohomology in these cases. By direct calculation $H^2(C_2, T_2) = \mathbb{Z}/2\mathbb{Z}$. We conclude that for all the cyclic point groups in two dimensions $H^2(P, T) = 0$, except $H^2(C_2, T_2) = \mathbb{Z}/2\mathbb{Z}$, and there is one non-split extension in this case.

Class Activity. Give a reason why $T_3 \ncong T_2$.

For the remaining point groups we apply an algorithm due to Zassenhaus. The algorithm computes $H^2(G, M)$ when M is a $\mathbb{Z}G$-module that is free abelian of finite rank as a group. As a preliminary, we recall the following theorem of H.J.S. Smith from 1861, that is equivalent to the structure theorem for finitely generated abelian groups.

Put Smith Normal Form somewhere else.

Theorem 4.5.1 (Smith normal form)**.** *Let $A \in M_{m,n}(\mathbb{Z})$. There exist matrices $P \in GL(m,\mathbb{Z})$ and $Q \in GL(n,\mathbb{Z})$ such that PAQ is a diagonal matrix*

$$\begin{bmatrix} b_1 & & & & & & \\ & b_2 & & & & & \\ & & \ddots & & & & \\ & & & b_u & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}$$

with $b_1 \mid b_2 \mid \cdots \mid b_u \neq 0$. The b_i are called the invariant factors of A.

Theorem 4.5.2. *Let P be a finite group given by a presentation*

$$P = \langle g_1, \ldots, g_d \mid r_1, \ldots, r_t \rangle.$$

This presentation corresponds to an exact sequence $1 \to R \to F \to P \to 1$ where F is the free group on $g_1, \ldots, g_d$ and R is generated as a normal subgroup by $r_1, \ldots, r_t$. Let T be a $\mathbb{Z}P$-module such that $T \cong \mathbb{Z}^n$ as an abelian group, and let $\rho : P \to GL(n,\mathbb{Z})$ be the corresponding representation of P. Form the $nd \times nt$ matrix given in block form by

In Cor 3.4.3 the matrix with Fox derivatives was not explicitly given. Refer to the exercise that does this?

$$\Lambda = (\rho\left(\frac{\partial r_j}{\partial g_i}\right)) \in M_{nd,nt}(\mathbb{Z})$$

where the elements $\frac{\partial r_j}{\partial g_i} \in \mathbb{Z}F$ are defined by

$$r_j - 1 = \sum_{i=1}^{d} \frac{\partial r_j}{\partial g_i}(g_i - 1), \quad j = 1, \ldots, t.$$

Then $H^2(P,T) \cong \mathbb{Z}/b_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/b_u\mathbb{Z}$ where $b_1, \ldots, b_u$ are the non-zero invariant factors of Λ.

Proof. We compute second cohomology using the resolution of Corollary 3.4.3, obtained from the presentation. It looks as follows.

$$\begin{array}{ccccccccccc} \mathbb{Z}P^t & & \xrightarrow{\left(\frac{\partial r_j}{\partial g_i}\right)} & & \mathbb{Z}P^d & & \to & & \mathbb{Z}P & \to & \mathbb{Z} & \to & 0 \\ & \searrow & & \nearrow & & \searrow & & \nearrow & & & & & \\ & & R/R' & & & & IP & & & & & & \end{array}$$

We embed T in the n-dimensional real vector space $T(n) = \mathbb{R} \otimes_{\mathbb{Z}} T$, which becomes a $\mathbb{Z}P$-module through the action on T. Because $\mathbb{R}$ is uniquely divisible, we have $H^2(P, T(n)) = 0$. From this we obtain the following commutative diagram. The

rows are the sequences used to calculate $H^2(P,T)$ and $H^2(P,T(n)) = 0$ in the manner of Proposition 3.4.8.

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 \to & \mathrm{Hom}(IP,T) & \to & \mathrm{Hom}(\mathbb{Z}P^d,T) & \to & \mathrm{Hom}(R/R',T) & \to H^2(P,T) \to 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 \to & \mathrm{Hom}(IP,T(n)) & \xrightarrow{\beta} & \mathrm{Hom}(\mathbb{Z}P^d,T(n)) & \xrightarrow{\alpha} & \mathrm{Hom}(R/R',T(n)) & \to & 0. \end{array}$$

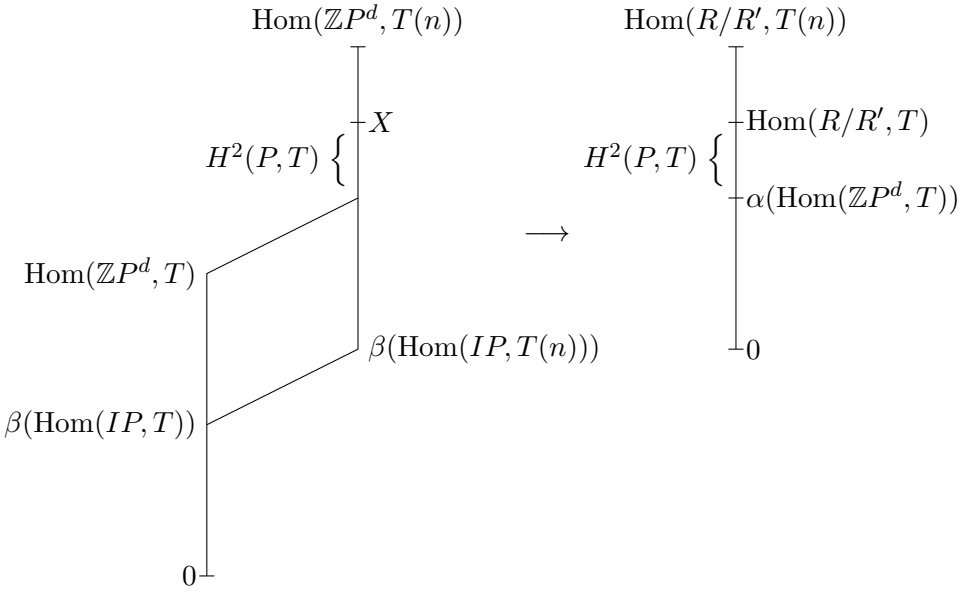
All the rows and columns here are exact, so β is injective and α is surjective. Let

$$X = \{\phi : \mathbb{Z}P^d \to T(n) \mid \phi(R/R') \subseteq T\}.$$

Then

$$0 \to \mathrm{Hom}(IP,T(n)) \to X \to \mathrm{Hom}(R/R',T) \to 0$$

is exact, and so the composite surjection $X \to \mathrm{Hom}(R/R',T) \to H^2(P,T)$ has kernel $\beta(\mathrm{Hom}(IP,T(n))) + \mathrm{Hom}(\mathbb{Z}P^d,T)$. These constructions are shown in the following picture of sections of $\mathrm{Hom}(\mathbb{Z}P^d,T(n))$ and $\mathrm{Hom}(R/R',T(n))$. All the modules mentioned are quotients of submodules of $\mathrm{Hom}(\mathbb{Z}P^d,T(n))$.



Now $\mathbb{Z}P^d$ is a free module, so homomorphisms $\phi : \mathbb{Z}P^d \to T(n)$ biject with d-tuples $[v_1, \ldots, v_d]$ of elements of $T(n)$, where v_i is the image of the ith basis vector of $\mathbb{Z}P^d$, and we regard the d-tuple as a $1 \times d$-matrix. The generators of R/R' have coordinates in $\mathbb{Z}P^d$ that are the columns of the matrix $\left(\frac{\partial r_j}{\partial g_i}\right)$, and so the images of the generators

of R/R' under such a homomorphism ϕ form a t-tuple of vectors in $T(n)$ that are the columns of

$$[v_1, \ldots, v_d]\Lambda \in T(n)^t.$$

From this we see that

$$X \cong \{[v_1, \ldots, v_d] \in T(n)^d \mid [v_1, \ldots, v_d]\Lambda \in T^t\}.$$

In a similar way

$$\begin{aligned}\mathrm{Hom}(IP, T(n)) &\cong \{\phi : \mathbb{Z}P^d \to T(n) \mid \phi(R/R') = 0\} \\ &= \{[v_1, \ldots, v_d] \in T(n)^d \mid [v_1, \ldots, v_d]\Lambda = 0\} \\ &= \mathrm{Ker}\,\Lambda\end{aligned}$$

where this means the left kernel. With these identifications, $\mathrm{Hom}(\mathbb{Z}P^d, T) \cong T^d$ is the integer lattices of row vectors with entries in T. We conclude that

$$H^2(P, T) \cong \{[v_1, \ldots, v_d] \in T(n)^d \mid [v_1, \ldots, v_d]\Lambda \in T^t\}/(\mathrm{Ker}\,\Lambda + T^d).$$

At this stage we observe that our calculation will be independent of the choice of basis for the domain T^d and codomain T^t of Λ, so we will choose bases such that Λ is in Smith normal form. The result is now immediate because, for a diagonal matrix $\mathrm{diag}(b_1, \ldots, b_q)$, we have

$$\{\underline{x} \in \mathbb{Z}^q \mid b_i x_i \in \mathbb{Z} \text{ for all } i\}/\mathbb{Z}^q = (\bigoplus \frac{1}{b_i}\mathbb{Z})/\mathbb{Z}^q \cong \bigoplus \mathbb{Z}/b_i\mathbb{Z}$$

and the zeros on the diagonal of Λ simply contribute to the kernel. □

Example. Let $P = \langle x, y \mid x^2 = y^2 = (xy)^2 = 1\rangle$ acting on $T = \mathbb{Z}^2$ via $A = \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}$ and $B = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$. We have

$$\begin{aligned}x^2 - 1 &= (x+1)(x-1) \\ y^2 - 1 &= (y+1)(y-1) \\ (xy)^2 - 1 &= (xy+1)(xy-1) \\ &= (xy+1)x(y-1) + (xy+1)(x-1).\end{aligned}$$

So

$$\begin{aligned}\Lambda &= \begin{bmatrix}x+1 & 0 & xy+1\\ 0 & y+1 & (xy+1)x\end{bmatrix}_{\substack{x\mapsto A\\ y\mapsto B}} \\ &= \begin{bmatrix}0 & 0 & & \\ 0 & 2 & 0 & 0\\ & & 0 & 0\\ 0 & & 0 & 2 & 0\end{bmatrix}\end{aligned}$$

and $H^2(C_2 \times C_2, T) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. The following are homomorphisms $R/R' \to T$ that represent the elements of this group:

$$\begin{array}{rcccc} x^2 & \mapsto & \left\{\begin{matrix}[0,0]\\[0,0]\\[0,0]\end{matrix}\right. & \underbrace{\left\{\begin{matrix}[0,1]\\[0,0]\\[0,0]\end{matrix}\right.}_{\text{isomorphic extensions}} & \left\{\begin{matrix}[0,0]\\[1,0]\\[0,0]\end{matrix}\right. & \left\{\begin{matrix}[0,1]\\[1,0]\\[0,0]\end{matrix}\right. \\ y^2 & \mapsto & & & & \\ (xy)^2 & \mapsto & & & & \end{array}$$

where the vectors are shown as row vectors. For example, the second extension has a presentation

$$\langle x, y, e_1, e_2 \mid x^2 = e_2,\ y^2 = (xy)^2 = [e_1, e_2] = 1,\ {}^x e_1 = e_1^{-1},\ {}^x e_2 = e_2,\ {}^y e_1 = e_1,\ {}^y e_2 = e_2^{-1} \rangle$$

and the third has the same presentation but with x and y interchanged and e_1 and e_2 interchanged, so is isomorphic.

When do two elements of $H^2(P, T)$ give extensions that are equivalent as space groups? It happens if and only if there is a commutative diagram

$$\begin{array}{rccccc} \mathcal{E}: & T & \longrightarrow & G_1 & \longrightarrow & P \\ & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle \beta} \\ \alpha\mathcal{E}: & T & \longrightarrow & G_2 & \longrightarrow & P \end{array}$$

where $\alpha \in GL(T)$. Since T is the same P-module in the top and bottom extension we have, for all $g \in P$, for all $t \in T$, ${}^{\beta(g)}(\alpha t) = \alpha({}^g t)$ so that ${}^{\beta(g)}(t) = \alpha^g(\alpha^{-1}t)$. We see from this that β has the same effect as conjugation by α within $GL(T)$, and since $\beta P = P$ we have $\alpha \in N_{GL(T)}(P)$. We may formalize this by observing that $N_{GL(T)}(P)$ acts on equivalence classes of extensions, and hence on $H^2(P, T)$ in the following way. Given $\alpha \in N_{GL(T)}(P)$ and an extension $\mathcal{E} : T \xrightarrow{\phi} G_1 \xrightarrow{\theta} P$ we obtain an extension $\alpha\mathcal{E} : T \xrightarrow{\phi\alpha^{-1}} G_1 \xrightarrow{\beta\theta} P$ where β denotes conjugation by α within $GL(T)$. Using this action we may now state the following result, which we have already proved.

I must sort out what is really going on with the conjugation action: it should send an extension by T to an extension by ${}^\alpha T$. Also, in listing the $\mathbb{Z}P$-lattices I have ignored non-isomorphic lattices that differ by an automorphism of P.

Proposition 4.5.3. *Two space groups that are extensions of P by T are affine equivalent if and only if their cohomology classes in $H^2(P, T)$ belong to the same orbit in the action of $N_{GL(T)}(P)$.*

We now express this in a fashion that is compatible with our previous description of $H^2(P, T)$ in terms of the relation module. Let $\alpha \in N_{GL(T)}(P)$ and let $\beta : P \to P$ be conjugation by α. Let $1 \to R \to F \to P \to 1$ be a presentation of P and suppose the extension $\mathcal{E}$ is represented by a homomorphism $f : R/R' \to T$, continuing with the previous notation. Lift β^{-1} to a homomorphism $F \to F$, and hence to a homomorphism γ as shown:

$$\begin{array}{ccccc} R & \longrightarrow & F & \longrightarrow & P \\ \downarrow{\scriptstyle \gamma} & & \downarrow & & \downarrow{\scriptstyle \beta^{-1}} \\ R & \longrightarrow & F & \longrightarrow & P. \end{array}$$

Define ${}^\alpha f : R/R' \to T$ by ${}^\alpha f(rR') = f(\gamma(r)R')$. Then we have

Proposition 4.5.4. *If $\mathcal{E}$ is an extension represented by $f : R/R' \to T$ then the extension $\alpha\mathcal{E}$ is represented by ${}^{\alpha}f$.*

Check on whether $\alpha\mathcal{E}$ is defined.

Proof. Consider the diagram

$$\begin{array}{rccccc}
 & R/R' & \longrightarrow & F/R' & \longrightarrow & P \\
 & \downarrow{\scriptstyle \gamma} & & \downarrow & & \downarrow{\scriptstyle \beta^{-1}} \\
 & R/R' & \longrightarrow & F/R' & \longrightarrow & P \\
 & \downarrow{\scriptstyle f} & & \downarrow & & \| \\
\mathcal{E}: & T & \longrightarrow & G & \longrightarrow & P \\
 & \downarrow{\scriptstyle \alpha} & & \| & & \downarrow{\scriptstyle \beta} \\
\alpha\mathcal{E}: & T & \longrightarrow & G & \longrightarrow & P.
\end{array}$$

The morphism of extensions between the middle rows of the diagram shows that $\mathcal{E}$ is represented by f, and the composite morphism from the top row to the bottom row shows that $\alpha\mathcal{E}$ is represented by ${}^{\alpha}f$. □

This last result enables us to determine the action of $N_{GL(T)}(P)$ on $H^2(P,T)$ by computer. It completes the description of the method of determining the equivalence classes of space groups in a given dimension n, known as the Zassenhaus algorithm. In summary, its steps are:

- Determine the isomorphism classes of finite subgroups P of $GL_n(\mathbb{Z})$ and obtain presentations for them.
- For each such P determine all $\mathbb{Z}P$-lattices T of rank n up to $\mathbb{Z}P$-isomorphism. For each T determine $N_{GL(T)}(P)$.
- Compute $H^2(P,T)$.
- Compute the orbits of $N_{GL(T)}(P)$ on $H^2(P,T)$.

The 18th problem in Hilbert's list of problems presented to the International Congress of Mathmaticians in 1900 was to show that there are only finitely many space groups in any given dimension. His problem was stated in German, and it translates as follows: "Is there in n-dimensional Euclidean space ... only a finite number of essentially different kinds of groups of motions with a [compact] fundamental region?"

The fact that this is so was proved by Bieberbach between 1910 and 1912. We could prove it now by showing that each of the sets indicated as the first three of the four items above is finite. There are only finitely many isomorphism types of subgroups of $GL(n,\mathbb{Z})$ as a consequence of a result of Minkowski, stating that if p is an odd prime then $\mathrm{Ker}(GL(n,\mathbb{Z}) \to GL(n,\mathbb{Z}/p\mathbb{Z})$ is torsion free. This deals with the first set. For the second set, The Jordan-Zassenhaus theorem states that if P is a finite group, there

are only finitely isomorphism types of $\mathbb{Z}P$-lattices T of any given rank n. This deals with the second set. Finally, if P is finite and T is finitely generated then $H^2(P,T)$ is finite, by Corollary 3.5.3.

Insert numbers of space groups in different dimensions, page 6/19 of the original notes.

Chapter 5

An application of the Burnside ring

5.1 The Burnside ring

We start by following the treatment in volume 1 of Benson's book.

Let G be a finite group.

Definition 5.1.1. The *Burnside ring* of G is the quotient $b(G) = A/B$ where A is the free abelian group with symbols Ω in bijection with a set of representatives of the finite G-sets as a basis, and B is the subgroup generated by expressions $\Theta - \Omega - \Psi$ whenever $\Theta \cong \Omega \sqcup \Psi$ as G-sets. We write $[\Omega]$ for the image of Ω in $b(G)$. Thus $[\Omega \sqcup \Psi] = [\Omega] + [\Psi]$ and $[\Omega] = [\Psi]$ if $\Omega \cong \Psi$. There is a multiplication defined on $b(G)$ by $[\Omega] \cdot [\Psi] = [\Omega \times \Psi]$ where $\Omega \times \Psi$ is made into a G-set using the diagonal action: $g(\omega, \psi) := (g\omega, g\psi)$.

Proposition 5.1.2. *Let G be a finite group. As an abelian group, $b(G)$ is a free abelian group with basis the symbols $[G/H]$ where H ranges over subgroups of G taken up to conjugacy. As a ring, $b(G)$ has multiplicative identity the one-point set $[G/G]$.*

Definition 5.1.3. Let $\mathrm{cc}(G)$ denote the set of conjugacy classes of subgroups of G. We define the *marks homomorphism* $m : b(G) \to \mathbb{Z}^{\mathrm{cc}(G)}$ by $m([\Omega]) = (|\Omega^H|)_{H \in \mathrm{cc}(G)}$. The matrix with entries $(|(G/K)^H|)_{(K,H)}$ is known as the *table of marks*. The rows and columns of the table of marks are usually placed in non-decreasing order of size of subgroups.

Proposition 5.1.4 (Burnside)**.** *1. m is a ring homomorphism.*

2. m is one-to-one.

3. The table of marks is the transpose of the matrix of m with respect to the standard bases of $b(G)$ and $\mathbb{Z}^{\mathrm{cc}(G)}$. When subgroups are placed in non-decreasing order, it is lower triangular, with diagonal entries $|N_G(H)/H|$.

Proof. 1. For each subgroup H we have $(\Omega \times \Psi)^H = \Omega^H \times \Psi^H$ because, in the diagonal action, an element (ω, ψ) is fixed by H if and only if each of ω and ψ is. Thus $m(\Omega \times \Psi) = m(\Omega) \cdot m(\Psi)$.

2. Suppose that $m(\sum_i n_i[G/H_i]) = 0$. Then $m(\bigsqcup_i (G/H_i)^{a_i}) = m(\bigsqcup_i (G/H_i)^{b_i})$ for some integers a_i, b_i. Pick a subgroup H_i that is maximal among all the stabilizers that appear. Then $(G/J)^{H_i} \neq \emptyset$ if and only if $H_i \subseteq_G J$ so we deduce that G/H_i occurs with the same multiplicity on both sides. Canceling this term, we repeat with the shorter expression.

3. The triangular property follows because $m_H(G/K) = |(G/K)^H| = 0$ unless H is conjugate to a subgroup of K. □

Corollary 5.1.5. *Let K be a field of characteristic 0. Then $K \otimes_{\mathbb{Z}} b(G) \cong K^{\mathrm{cc}(G)}$ as rings, which is semisimple.*

Definition 5.1.6. For each subgroup H of G let $\epsilon_H \in \mathbb{Q}^{\mathrm{cc}(G)}$ be the primitive idempotent that is 1 in the position of the conjugacy class of H and 0 elsewhere. We define e_H to be the primitive idempotent of $B(G) := \mathbb{Q} \otimes_{\mathbb{Z}} b(G)$ that is the preimage of ϵ_H. Thus, writing m for the extension of the marks homomorphism to $B(G)$ we have $e_H = m^{-1}(\epsilon_H$.

Corollary 5.1.7. *The elements e_H of $B(G)$ are characterized by the properties*

1. *$e_H^2 = e_H$ is a primitive idempotent,*
2. *$e_H = e_K$ if and only if H and K are conjugate,*
3. *$e_H e_K = 0$ if H and K are not conjugate,*
4. *$1 = \sum_{H \in \mathrm{cc}(G)} e_H$,*
5. *e_H lies in the span of the $[G/K]$ with K conjugate to a subgroup of H.*

Proof. The first properties come about because the ϵ_H are a complete system of primitive idempotents of $\mathbb{Q}^{\mathrm{cc}(G)}$. The last property arises because the matrix of the marks homomorphism is triangular. We leave it as an exercise that these properties characterize the idempotents. □

Definition 5.1.8. If H and K are subgroups of G we define the *transporter* of H into K to be

$$N_G(H, K) := \{g \in G \mid {}^gH \subseteq K\}.$$

When $H = K$ this is the normalizer of H.

Proposition 5.1.9. *1. $N_G(H, K)$ is a union of left cosets $gN_G(H)$ and also a union of right cosets $N_G(K)g$.*

2.

$$\begin{aligned} |N_G(H, K)| &= |\{G\text{-conjugates of } H \text{ contained in } K\}| \cdot |N_G(H)| \\ &= |\{G\text{-conjugates of } K \text{ containing } H\}| \cdot |N_G(K)|. \end{aligned}$$

Draw a picture to illustrate the bipartite graph given by containment of conjugates of H in conjugates of K. The total number of edges is the number in part 2.

Proof. 1. Exercise.

2. We define a mapping $N_G(H,K) \to \{{}^gH \mid g \in G,\ {}^gH \subseteq K\}$ by $g \mapsto {}^gH$ and examine the fibers. And so on. □

Definition 5.1.10. The *Möbius function* on a poset $\mathcal{P}$ is the function $\mu : \mathcal{P} \times \mathcal{P} \to \mathbb{Z}$ satisfying equations

$$\sum_{a \le x \le b} \mu(x,b) = \delta_{a,b}$$

for all $a, b \in \mathcal{P}$. Here $\delta_{a,b}$ is the Kronecker delta. We are only interested in the values of $\mu(u,v)$ when u, v are comparable, so if they are not comparable we might as well set $\mu(u,v) = 0$.

The Möbius function also satisfies (and is defined by) the equations

$$\sum_{a \le x \le b} \mu(a,x) = \delta_{a,b}.$$

Example 5.1.11. The lattice of subgroups of the symmetric group S_3 and its Möbius function.

Theorem 5.1.12 (Gluck, Yoshida (1981))**.** *Let μ be the Möbius function on the poset of subgroups of the finite group G. Then*

$$e_H = \frac{1}{|N_G(H)|} \sum_{K \le H} \mu(K,H) \cdot |K| \cdot [G/K].$$

Proof. We verify that, applying the marks homomorphism m to the right hand side of this equation, we get the function that is 1 on H and 0 on other subgroups not conjugate to H. That is, for each subgroup L we verify

$$\frac{1}{|N_G(H)|} \sum_{K \le H} \mu(K,H) \cdot |K| \cdot |(G/K)^L| = \begin{cases} 1 & \text{if } L \sim_G H \\ 0 & \text{otherwise.} \end{cases}$$

Now

$$\begin{aligned} (G/K)^L &= \{gK \mid L \subseteq {}^gK\} \quad \text{because the stabilizer of } gK \text{ is } {}^gK \\ &= \{g^{-1}K \mid {}^gL \subseteq K\} \end{aligned}$$

and, under the map that sends g to g^{-1}, this bijects with the set of cosets

$$\{Kg \mid {}^gL \subseteq K\} = K \backslash N_G(L,K).$$

This has size

$$\frac{|N_G(L,K)|}{|K|} = \frac{|\{G\text{-conjugates of } L \text{ contained in } K\}| \cdot |N_G(L)|}{|K|}.$$

The sum is

$$\begin{aligned}
&\frac{1}{|N_G(H)|}\sum_{K\le H}\mu(K,H)\cdot|K|\cdot\frac{|\{G\text{-conjugates of } L \text{ contained in } K\}|\cdot|N_G(L)|}{|K|}\\
&\qquad=\frac{|N_G(L)|}{|N_G(H)|}\sum_{L\sim_G L_1\le K\le H}\mu(K,H)\quad\text{summing over } L_1 \text{ and } K\\
&\qquad=\frac{|N_G(L)|}{|N_G(H)|}\sum_{L\sim_G L_1}\sum_{L_1\le K\le H}\mu(K,H)\quad\text{where the second sum is over } K\\
&\qquad=\frac{|N_G(L)|}{|N_G(H)|}\sum_{L_1\sim_G L}\delta_{L_1,H}\\
&\qquad=\begin{cases}1 & \text{if } L\sim_G H\\ 0 & \text{if } L\not\sim_G H.\end{cases}
\end{aligned}$$

□

Example 5.1.13. When $G=S_3$ is the symmetric group of degree 3,

$$\begin{aligned}
e_1&=\frac{1}{6}[S_3/1],\\
e_{C_2}&=[S_3/C_2]-\frac{1}{2}[S_3/1]\\
e_{C_3}&=\frac{1}{6}(3[S_3/C_3]-[S_3/1])\\
&=\frac{1}{2}[S_3/C_3]-\frac{1}{6}[S_3/1]\\
e_{S_3}&=\frac{1}{6}(6[S_3/S_3]-3[S_3/C_3]-6[S_3/C_2]+3[S_3/1])\\
&=[S_3/S_3]-\frac{1}{2}[S_3/C_3]-[S_3/C_2]+\frac{1}{2}[S_3/1].
\end{aligned}$$

5.2 The Green ring

Definition 5.2.1. Let R be a field or a complete discrete valuation ring. The *Green ring* $a(RG)$ is the quotient A/B where A is the free abelian group with symbols M as a basis whenever M is a finitely generated RG-module, and B is the subgroup generated by expressions $M-M_1-M_2$ whenever $M\cong M_1\oplus M_2$ as RG-modules. We write $[M]$ for the image of M in $a(G)$. Thus $[M_1\oplus M_2]=[M_1]+[M_2]$ and $[M]=[N]$ if $M\cong N$. There is a multiplication defined on $a(G)$ by $[M]\cdot[N]=[M\otimes N]$ where $M\otimes N$ is made into an RG-module using the diagonal action: $g(m\otimes n):=(gm\otimes gn)$. We put $A(RG)=\mathbb{Q}\otimes_{\mathbb{Z}}a(RG)$.

We have ring homomorphisms $\phi:b(G)\to a(G)$ and $\phi:B(G)\to A(G)$, both given by $[\Omega]\mapsto[R\Omega]$ where $R\Omega$ is the permutation module determined by Ω. Under such a

ring homomorphism, idempotents are sent to idempotents or zero, and the one point G-set $[G/G]$ is sent to the trivial module $[R]$. Linear combinations of G-sets are sent to the same linear combination of permutations modules. We may use this idea to obtain expressions in $A(RG)$ for the trivial module as a linear combination of induced modules. We will see that this is useful in computing cohomology. The following theorem is a key ingredient.

Theorem 5.2.2 (Conlon)**.** *Let R be a field of characteristic p or a complete discrete valuation ring with residue field of characteristic p. If $\phi(e_H) \neq 0$ then H has a normal p-subgroup with cyclic quotient.*

We do not prove this theorem for the moment.

Definition 5.2.3. If a group H has a normal p-subgroup with cyclic quotient we call H *cyclic mod p.*

Corollary 5.2.4. *In $A(RG)$ we have the following expression for the trivial module:*

$$[R] = \sum_{H \text{ cyclic mod } p} \phi(e_H).$$

Substituting the explicit expressions for the Burnside ring idempotents, we get an explicit expression for the trivial module as a linear combination of induced modules from subgroups that are cyclic mod p. If G is not cyclic mod p the equation $\phi(e_G) = 0$ also gives an expression for the trivial module as a linear combination of properly induced modules.

We will see also that linear combinations of permutation modules in the Green ring provide isomorphisms between direct sums of permutation modules.

Example 5.2.5. Let $G = S_3$ and $p = 2$. We take R to be the field $\mathbb{F}_2$ with 2 elements. The subgroups of S_3 that are cyclic mod 2 are $1, C_2$ and C_3 and there is one conjugacy class of each of these. The image of a coset space $[S_3/H]$ in $A(\mathbb{F}_2 S_3)$ is the induced (permutation) module $\mathbb{F}_2 \uparrow_H^{S_3}$. These modules decompose into indecomposable modules as follows:

$$\begin{aligned}
\mathbb{F}_2 \uparrow_1^{S_3} &= P_1 \oplus P_2 \oplus P_2 \\
\mathbb{F}_2 \uparrow_{C_2}^{S_3} &= \mathbb{F}_2 \oplus P_2 \\
\mathbb{F}_2 \uparrow_{C_3}^{S_3} &= P_1 \\
\mathbb{F}_2 \uparrow_{S_3}^{S_3} &= \mathbb{F}_2
\end{aligned}$$

where $\mathbb{F}_2$ denotes the trivial module, P_1 is the projective module with 2 trival composition factors, and P_2 is the 2-dimensional simple projective module. From the calculation

in Example 5.1.13 we see that

$$\begin{aligned}
\phi(e_1) &= \frac{1}{6}\mathbb{F}_2\uparrow_1^{S_3} = \frac{1}{6}P_1 + \frac{1}{3}P_2,\\
\phi(e_{C_2}) &= \mathbb{F}_2\uparrow_{C_2}^{S_3} - \frac{1}{2}\mathbb{F}_2\uparrow_1^{S_3} = \mathbb{F}_2 - \frac{1}{2}P_1\\
\phi(e_{C_3}) &= \frac{1}{2}\mathbb{F}_2\uparrow_{C_3}^{S_3} - \frac{1}{6}\mathbb{F}_2\uparrow_1^{S_3} = \frac{1}{3}P_1 - \frac{1}{3}P_2\\
\phi(e_{S_3}) &= \mathbb{F}_2 - \frac{1}{2}\mathbb{F}_2\uparrow_{C_3}^{S_3} - \mathbb{F}_2\uparrow_{C_2}^{S_3} + \frac{1}{2}\mathbb{F}_2\uparrow_1^{S_3}\\
&= \mathbb{F}_2 - \frac{1}{2}P_1 - \mathbb{F}_2 - P_2 + \frac{1}{2}P_1 + P_2 = 0.
\end{aligned}$$

We verify that

$$\mathbb{F}_2 = \phi(e_1) + \phi(e_{C_2}) + \phi(e_{C_3}) = \mathbb{F}_2\uparrow_{C_2}^{S_3} + \frac{1}{2}\mathbb{F}_2\uparrow_{C_3}^{S_3} - \frac{1}{2}\mathbb{F}_2\uparrow_1^{S_3}$$

and this is an expression for $\mathbb{F}_2$ in terms of properly induced modules. The same expression is obtained by rearranging the terms in the equation $\phi(e_{S_3}) = 0$. The equation holds in the Green ring. After multiplying by 2 to clear denominators and taking the negative term on the right over to the left with a + sign, it is equivalent to stating that we have an $\mathbb{F}_2S_3$-module isomorphism

$$\mathbb{F}_2 \oplus \mathbb{F}_2 \oplus \mathbb{F}_2\uparrow_1^{S_3} \cong \mathbb{F}_2\uparrow_{C_2}^{S_3} \oplus \mathbb{F}_2\uparrow_{C_2}^{S_3} \oplus \mathbb{F}_2\uparrow_{C_3}^{S_3}.$$

We used the coefficient ring $R = \mathbb{F}_2$ to obtain the explicit descriptions of the induced modules, but the expressions such as

$$\phi(e_{S_3}) = R - \frac{1}{2}R\uparrow_{C_3}^{S_3} - R\uparrow_{C_2}^{S_3} + \frac{1}{2}R\uparrow_1^{S_3}$$

hold over any coefficient ring R. Taking, for instance, the 2-adic integers $R = \mathbb{Z}_2$, we obtain again that $\phi(e_{S_3}) = 0$ by Conlon's theorem, and a corresponding isomorphism of permutations modules over $\mathbb{Z}_2$.

Example 5.2.6. This time let $G = S_4$ with $p = 2$ and $R = \mathbb{F}_2$. We may do similar computations with the Möbius function on the poset of subgroups of S_4, computing the Burnside ring idempotents, and so on. To get the concluding expression for the trivial module in terms of induced modules from subgroups that are cyclic mod p, we may take the expression over S_3 and inflate it to an isomorphism of S_4-modules, via the surjective homomorphism $S_4 \to S_3$ with kernel the Klein 4-group $V = \langle (1,2)(3,4), (1,3)(2,4)\rangle$. We obtain

$$\mathbb{F}_2 = \mathbb{F}_2\uparrow_{D_8}^{S_4} + \frac{1}{2}\mathbb{F}_2\uparrow_{A_4}^{S_4} - \frac{1}{2}\mathbb{F}_2\uparrow_V^{S_4}.$$

We also get such an expression by computing e_{S_4} and rearranging the equations $\phi(e_{S_4}) = 0$. For this we need the values of $\mu(H, S_4)$, and it helps to use the fact about the Möbius function that these are non-zero only on intersections of maximal subgroups of S_4.

Picture needed of subgroups of S_4 with values of the Möbius function.

5.3 Computation of cohomology using cyclic mod p subgroups

To make the notation easier, let us write u_H for the permutation module $R\uparrow_H^G$, using the same notation for this module as an element of the Green ring. Thus at the end of the last section we established an identity for $\mathbb{F}_2S_4$-modules

$$u_{S_4} = u_{D_8} + \frac{1}{2}u_{A_4} - \frac{1}{2}u_V.$$

Such identities give rise to isomorphisms between direct sums of cohomology groups

Theorem 5.3.1. *Let R be a field or a complete discrete valuation ring, and let G be a finite group. Suppose that $u_G = \sum_{K\leq G}\lambda_K u_K$ is an equation in the Green ring $A(RG)$. Then for each finitely generated RG-module M we have*

$$H^n(G,M) = \sum_{K\leq G}\lambda_K H^n(K, M\downarrow_K^G).$$

for each n, this equation holding in the Green ring of finitely generated abelian groups. A similar result holds for homology.

Proof. We start by tensoring the equation $u_G = \sum_{K\leq G}\lambda_K u_K$ by M to get

$$M = M\cdot u_G = \sum_{K\leq G}\lambda_K M\cdot u_K = \sum_{K\leq G}\lambda_K M\downarrow_K^G\uparrow_K^G$$

in $A(RG)$. The additive functor $H^n(G,-)$ gives rise to a homomorphism $A(RG)\to A(\mathbb{Z})$. We apply it to both sides of the equation and use the Eckmann-Schapiro lemma. This implies that $H^n(G, M\downarrow_K^G\uparrow_K^G) \cong H^n(K, M\downarrow_K^G)$. □

Equations such as this are sufficient to determine the additive structure of cohomology.

Example 5.3.2. Let $G = S_4$ with $p = 2$ and $R = \mathbb{F}_2$ or $\mathbb{Z}_2$. From the equation

$$u_{S_4} = u_{D_8} + \frac{1}{2}u_{A_4} - \frac{1}{2}u_V.$$

in $A(RS_4)$ we obtain

$$H^n(S_4,R) = H^n(D_8,R) + \frac{1}{2}H^n(A_4,R) - \frac{1}{2}H^n(V,R).$$

In case $R = \mathbb{Z}_2$ it is a fact that $H^n(G,\mathbb{Z}_2) \cong H^n(G,\mathbb{Z})_2$ is the Sylow 2-subgroup of $H^n(G,\mathbb{Z})$, and similarly with homology. Applying this to the abelianization $H_1(S_4,\mathbb{Z})$ we obtain

Include something up extending through a flat coefficient ring in the homological algebra section.

$$H_1(S_4,\mathbb{Z})_2 = H_1(D_8,\mathbb{Z})_2 + \frac{1}{2}H_1(A_4,\mathbb{Z})_2 - \frac{1}{2}H_1(V,\mathbb{Z})_2 = C_2\oplus C_2 + 0 - C_2 = C_2$$

in $A(\mathbb{Z})$, which is the correct answer. We may compute the Sylow 2-subgroup of the Schur multiplier of S_4, using the fact that the Schur multipliers of $D_8, A_4, C_2\times C_2$ are all C_2. We get

$$H_2(G,\mathbb{Z})_2 = H_2(D_8,\mathbb{Z})_2 + \frac{1}{2}H_2(A_4,\mathbb{Z})_2 - \frac{1}{2}H_2(V,\mathbb{Z})_2 = C_2 + \frac{1}{2}(C_2 - C_2) = C_2.$$

5.4 Euler characteristics and the Möbius function

We now introduce topological ideas into the combinatorics we have been using. From each poset we obtain a topological space, and we make the connection between the Möbius function on the poset and the Euler characteristic of this space.

Definition 5.4.1. A *chain of length* n in $\mathcal{P}$ is a list of comparable elements $x_0 < x_1 < \cdots < x_n$, no two of which are equal.

Example 5.4.2. When $a = b$ there is only one chain: $a = x_0 = b$ starting at a and ending at b. Also $\mu(a, a) = 1$. When $a < b$ with no elements between them, there is one chain $a = x_0 < x_1 = b$ between a and b. In this case $\mu(a, b) = -1$.

Proposition 5.4.3 (Hall)**.** *Let a, b be elements of a poset $\mathcal{P}$. Then*

$$\mu(a,b) = \sum_{n=0}^{\infty} (-1)^n |\{\textit{chains } a = x_0 < x_1 < \cdots < x_n = b\}|.$$

Proof. Define

$$g(a,b) := \sum_{n=0}^{\infty} (-1)^n |\{\text{chains } a = x_0 < x_1 < \cdots < x_n = b\}|.$$

We check that g satisfies the defining property of the Möbius function as follows. We have $\sum_{a \le c \le b} g(c, b) = 0$ if $a < b$ because each chain $a = x_0 < x_1 < \cdots < x_n = b$ determines a chain $x_1 < \cdots < x_n = b$ contributing to $g(x_1, b)$ with opposite sign. □

Corollary 5.4.4 (Hall)**.** $\sum_{a \le c \le b} \mu(a, c) = \delta_{a,b}$

Proof. The function defined by these equations also satisfies the equation with chains. □

Definition 5.4.5. Given a poset $\mathcal{P}$ there is a simplicial complex $|\mathcal{P}|$ (also written $\Delta(\mathcal{P})$) where the n-simplices are the strictly increasing chains $x_0 < x_1 < \cdots < x_n$. The faces of such a chain are the subchains. This simplicial complex is called the *order complex* or *nerve* of the poset.

The definition tells us how to fasten simplices together in abstract without relying on an embedding in space, and this approach is analogous to defining a graph by specifying abstractly the sets of vertices and edges, as well as which vertices are at the ends of which edge.

Examples 5.4.6. Some pictures of posets.

Some pictures of posets.

Definition 5.4.7. The *Euler characteristic* of a finite simplicial complex Δ is

$$\chi(\Delta) := \sum_{n=0}^{\infty} (-1)^n |\Delta_n|$$

where Δ_n is the set of n-simplices of Δ. This time the lines $|X|$ mean the size of the set X. The *reduced Euler characteristic* is $\tilde{\chi}(\Delta) := \chi(\Delta) - 1$. When we apply this to a poset $\mathcal{P}$ we may write $\chi(\mathcal{P})$ instead of $\chi(|\mathcal{P}|)$.

Given a poset $\mathcal{P}$ we will write $]a, b[$ to denote the open interval $]a, b[= \{x \in \mathcal{P} \mid a < x < b\}$.

Proposition 5.4.8. *In a poset, if $a < b$ then $\mu(a, b) = \tilde{\chi}(]a, b[)$.*

Is it also true when $a = b$?

Proof. The chains in the expression for $\mu(a, b)$ biject with chains in $]a, b[$, except for the chain $a < b$. □

We now apply these ideas to idempotents of the Burnside ring using the geometry of the poset of subgroups.

Proposition 5.4.9. *Let $\mathcal{H}$ be a set of subgroups of G, closed under conjugation and under taking subgroups. Regarding $\mathcal{H}$ as a poset, adjoin an artificial element $*$ larger than everything else. Then in $B(G)$ the idempotent $\sum_{H \in [G\backslash\mathcal{H}]} e_H$ has the expression*

$$\sum_{K \in \mathcal{H}} \frac{1}{|G : K|}(-\tilde{\chi}(]K, *[)) \cdot [G/K].$$

Notice that this expression also equals

$$\sum_{K \in [G\backslash\mathcal{H}]} \frac{1}{|N_G(K) : K|}(-\tilde{\chi}(]K, *[)) \cdot [G/K]$$

where the sum is over a set of representatives for the orbits of G on $\mathcal{H}$ (the conjugacy classes).

Proof.

$$\begin{aligned}
\sum_{H \in [G\backslash\mathcal{H}]} e_H &= \sum_{H \in [G\backslash\mathcal{H}]} \frac{1}{|N_G(H)|} \sum_{K \leq H} \mu(K, H) \cdot |K| \cdot [G/K] \\
&= \sum_{H \in \mathcal{H}} \frac{1}{|G|} \sum_{K \leq H} \mu(K, H) \cdot |K| \cdot [G/K] \\
&= \sum_{K \in \mathcal{H}} \frac{1}{|G : K|} \sum_{K \leq H} \mu(K, H) \cdot |K| \cdot [G/K] \\
&= \sum_{K \in \mathcal{H}} \frac{1}{|G : K|}(-\mu(K, *)) \cdot [G/K] \\
&= \sum_{K \in \mathcal{H}} \frac{1}{|G : K|}(-\tilde{\chi}(]K, *[)) \cdot [G/K].
\end{aligned}$$

□

As a corollary we obtain a theorem of K.S. Brown. For a subgroup K of a finite group G and a prime p we define

$$\mathcal{S}_p^{>K} := \{H \leq G \mid p \mid |H|,\ H >_G K\}.$$

Theorem 5.4.10. *Let G be a finite group and p a prime. Let K be a p-subgroup of G. Then $\chi(\mathcal{S}_p^{>K}) \equiv 1 \pmod{|N_G(K) : K|_p}$.*

Proof. Take $\mathcal{H}$ to be the set of all p-subgroups of G. Then $\sum_{H \in [G\backslash\mathcal{H}]} e_H \in b(G)_{(p)}$ so the denominators in the coefficients of the G-sets $[G/K]$ are prime to p. The coefficient of $[G/K]$ is $-\tilde{\chi}(]K, *[)/|N_G(K) : K|$ from which the result follows. □

We obtain a set of congruences from this result, one of which is the numerical part of Sylow's theorem. To show how this arises, we include it in the next theorem, assuming a proof of the rest of Sylow's theorem.

Theorem 5.4.11. *Let G be a finite group and p a prime.*

1. *If $p \mid |G|$ then the number of Sylow p-subgroups is congruent to 1 modulo p.*
2. *(Brown) $\chi(\mathcal{S}_p^{>1}(G)) \equiv 1 \pmod{|G|_p}$*

Proof. 1. Let K be a maximal subgroup of a Sylow p-subgroup and assume that all Sylow p-subgroups are conjugate. Then $\mathcal{S}_p^{>K}(G)$ consists of the Sylow p-subgroups of G, and its Euler characteristic is the number of such subgroups, which is congruent to 1 modulo $|N_G(K) : K|_p = p$.

2. We take $K = 1$ in Theorem 5.4.10 and note that $N_G(K) = G$. □

Example 5.4.12.

Group	A_5	S_5	S_6	$GL(3,2)$
$\tilde{\chi}(\mathcal{S}_2^{>1}(G))$	4	16	16	8

We obtain formulas in group cohomology every time we get identities in the Green ring between permutation modules, and Proposition 5.4.9 provides such an identity.

Corollary 5.4.13. *Let p be a prime, and let $\mathcal{H}$ be a set of subgroups of G, closed under conjugation and under taking subgroups. Let R be a field or complete discrete valuation ring with residue field of characteristic p. Suppose that $\mathcal{H}$ contains all subgroups that are cyclic mod p. Regarding $\mathcal{H}$ as a poset, adjoin an artificial element $*$ larger than everything else.*

1. *In the Green ring of RG-modules we have an expression for the trivial module*

$$[R] = \sum_{K \in \mathcal{H}} \frac{1}{|G : K|}(-\tilde{\chi}(]K, *[)) \cdot [R \uparrow_K^G].$$

2. *For each $n \geq 0$ and finitely generated $\mathbb{Z}G$-module M we have an expression in the Green ring of finitely generated abelian groups*

$$H^n(G, M)_p = \sum_{K \in \mathcal{H}} \frac{1}{|G : K|}(-\tilde{\chi}(]K, *[)) \cdot H^n(K, M)_p.$$

Proof. (1) Because $\mathcal{H}$ contains all subgroups that are cyclic mod p, the expression in Proposition 5.4.9 provides a similar expression for the trivial module in the Green ring as a sum of induced modules.

(2) Taking $R = \mathbb{Z}_p$ and applying $\mathrm{Ext}^n_{\mathbb{Z}_pG}(-, \mathbb{Z}_p \otimes_{\mathbb{Z}} M)$ to the expression in (1) gives the result. □

5.5 Computation of cohomology using topology of the subgroup poset

The origin of this material is Theorems A and A$'$ of [17]. We describe a result slightly weaker than Theorem A$'$.

What we describe fits into the context of using a group action on a topological space to get information about the cohomology of the group, and the main construction from these ingredients is often the *equivariant cohomology* of the group acting on the space. We do not need to do this here, but point out that there is a connection. We will consider a finite group G acting simplicially on a simplicial complex Δ. This means that G permutes the simplices of Δ, preserving dimensions of simplices, and preserving incidence between the simplices.

When considering such an action it is usual to impose the condition that, for each simplex $\sigma \in \Delta$, the stabilizer G_σ fixes σ pointwise. The sort of example excluded by this condition is that of a group of order 2 acting on a graph with two vertices joined by a single edge, fixing the edge but interchanging the two vertex. This example is also excluded in the Bass-Serre theory of groups acting on trees, where a group acting on a graph with this condition is said to act 'without inversions'. The stabilizer condition we impose is the higher dimensional version of acting without inversions. The technical consequence of this condition (using terms that have not yet been introduced) is that with it, if two G-simplicial complexes are G-equivariantly homotopy equivalent, then their chain complexes are homotopy equivalent as complexes of $\mathbb{Z}G$-modules. Much of the time the kind of simplicial complex we will work with will be the nerve $|\mathcal{P}|$ of a poset $\mathcal{P}$, acted on by a group G of poset automorphisms. In this case G acts on the chains giving a simplicial action on $|\mathcal{P}|$ and the stabilizer condition is necessarily satisfied.

We fix a prime p and let R be either a field of characteristic p, or a complete discrete valuation ring with residue field of characteristic p. We call such a ring R a *complete p-local ring*. From group theory, we use the notation $O_p(G)$ for the largest normal p-subgroup of G. The next result include a congruence in the Green ring, and it is helpful to know that the sum of images of induction from p'-subgroups is exactly the span of the projective modules.

Theorem 5.5.1. *Let the finite group G act simplicially on a simplicial complex Δ, so that for all simplices $\sigma \in \Delta$ the stabilizer G_σ fixes σ pointwise. Let p be a prime and R a complete p-local ring. Suppose that for all subgroups $H \leq G$ with $O_p(H) \neq 1$ the*

Euler characteristic $\chi(\Delta^H) = 1$. *Then in the Green ring of* RG*-modules,*

$$[R] \equiv \sum_{\sigma \in [G\backslash\Delta]} (-1)^{\dim \sigma} [R \uparrow_{G_\sigma}^G] \text{ modulo the image of induction from } p'\text{-groups.}$$

It follows that, for all $n \geq 1$ *and finitely generated* $\mathbb{Z}G$*-modules* M*,*

$$H^n(G, M)_p = \sum_{\sigma \in [G\backslash\Delta]} (-1)^{\dim \sigma} H^n(G_\sigma, M)_p$$

in the Green ring of finitely generated abelian groups.

Proof. We prove the congruence in the Green ring by expressing both sides in terms of induced modules $R \uparrow_H^G$ where H is cyclic mod p, using Corollary 5.4.13, which depends on Conlon's theorem, and show that the coefficient of $[R \uparrow_H^G]$ is the same on both sides when $p \mid |H|$. For each subgroup K of G let $\mathcal{C}(K)$ denote the set of subgroups of K that are cyclic mod p, and let μ_K be the Möbius function on $\mathcal{C}(K) \cup \infty$. In the Green ring of RK-modules,

$$[R] = \sum_{H \in \mathcal{C}(K)} \frac{-\mu_K(H, \infty)}{|K : H|} [R \uparrow_H^K]$$

so on inducing to G we get

$$[R \uparrow_K^G] = \sum_{H \in \mathcal{C}(K)} \frac{-\mu_K(H, \infty)}{|K : H|} [R \uparrow_H^G]$$

in the Green ring of RG-modules. Noting that there are $|G : G_\sigma|$ simplices in each orbit of G on Δ, the right hand side of the expression to be proved becomes

Put dots under the active symbols in the summation.

$$\begin{aligned} \sum_{\sigma \in \Delta} \frac{(-1)^{\dim \sigma}}{|G : G_\sigma|} [R \uparrow_{G_\sigma}^G] &= \sum_{\sigma \in \Delta} \frac{(-1)^{\dim \sigma}}{|G : G_\sigma|} \sum_{H \in \mathcal{C}(G_\sigma)} \frac{-\mu_{G_\sigma}(H, \infty)}{|G_\sigma : H|} [R \uparrow_H^G] \\ &= \sum_{H \in \mathcal{C}(G_\sigma)} \frac{[R \uparrow_H^G]}{|G : H|} \sum_{\sigma \in \Delta,\, G_\sigma \supseteq H} (-1)^{\dim \sigma} (-\mu_{G_\sigma}(H, \infty)). \end{aligned}$$

The left hand side of the expression to be proved is

$$\sum_{H \in \mathcal{C}(G)} \frac{[R \uparrow_H^G]}{|G : H|} - \mu_G(H, \infty).$$

We show that if $p \mid |H|$ where $H \in \mathcal{C}(G)$, then

$$-\mu_G(H, \infty) = \sum_{\sigma \in \Delta^H} (-1)^{\dim \sigma} (-\mu_{G_\sigma}(H, \infty)).$$

The left side is defined by $\sum_{J \leq H \in \mathcal{C}(G)} -\mu_G(H, \infty) = 1$ for all $J \in \mathcal{C}(G)$. We show that the right hand side satisfies this:

$$\begin{aligned}\sum_{J \leq H \in \mathcal{C}(G)} \sum_{\sigma \in \Delta^H} (-1)^{\dim \sigma}(-\mu_{G_\sigma}(H, \infty)) &= \sum_{\sigma \in \Delta^J} (-1)^{\dim \sigma} \sum_{J \leq H \leq G_\sigma,\, H \in \mathcal{C}(G)} (-\mu_{G_\sigma}(H, \infty)) \\ &= \sum_{\sigma \in \Delta^J} (-1)^{\dim \sigma} \\ &= \chi(\Delta^J) \\ &= 1 \text{ if } O_p(J) \neq 1,\end{aligned}$$

and because $J \in \mathcal{C}(G)$ the last condition happens if and only if $p \,\big|\, |J|$. This shows that the two sides of the equation in the Green ring are equal. The consequence for group cohomology follows from the Eckmann-Schapiro lemma, and because the p-torsion part of cohomology vanishes on subgroups of order prime to p □

In looking for examples of how Theorem 5.5.1 applies, the main thing is to find simplicial complexes Δ for which the fixed point condition $\chi(\Delta^H) = 1$ for all subgroups H with $O_p(G) \neq 1$ is satisfied. It is the case that the order complex $|\mathcal{S}_p^{>1}|$ satisfies this condition, but before proving this we will develop some tools in combinatorial homotopy theory. In the meantime we can verify that it holds in particular cases.

Example 5.5.2. Let p be a prime and G a finite group with cyclic Sylow p-subgroups of order p. Let $\Delta = \mathcal{S}_p^{>1}$ be the set of these subgroups, with G-action given by conjugation of the subgroups. The subgroups H of G with $O_p(H) \neq 1$ are the subgroups lying between a Sylow p-subgroup and its normalizer in this example, and the fixed points Δ^H is the single Sylow p-subgroup of H. This single point is contractible, with Euler characteristic 1, so the hypotheses of of Theorem 5.5.1 are satisfied.

By Sylow's theorem, G has a single orbit on Δ, and if $\sigma = H$ is a Sylow p-subgroup then the stabilizer $G_\sigma = N_G(H)$. The theorem says that $[R] \equiv [R \uparrow^G_{N_G(H)}]$ in the Green ring, and that $H^n(G, M) \cong H^n(N_G(H), M)_p$ when $n \geq 1$. This result for cohomology is a special case of a result in the book of Cartan and Eilenberg [7].

In the particular case when $G = S_3$ and $p = 2$ the Sylow 2-subgroup $H = \langle (1, 2) \rangle$ also has normalizer equal to H, and $R \uparrow^{S_3}_H \cong R \oplus V$ where V is projective, and induced from the subgroup of order 3. We have $H^n(S_3, M)_2 \cong H^n(\langle (1, 2) \rangle, M)$ for all $n \geq 1$.

5.6 Homotopy equivalences of posets and categories

Chapter 6

Bibliography

[1] E. Ascher and A. Janner, *Algebraic aspects of crystallography I and II,* Helv. Phys. Acta 38 (1965), 551-572, Commun. Math. Phys. 11 (1968/9), 138-167.

AJ is not listed in MathSciNet.

[2] D.J. Benson and P. Kropholler, *Cohomology of groups,* pp. 917–950 in ed: I.M. James, Handbook of Algebraic Topology, North-Holland (1995).

[3] H. Brown, R. Bülow, J. Neubüser, H. Wondratschek and H. Zassenhaus, *Crystallographic groups of four-dimensional space,* Wiley 1978.

[4] J. Burkhardt, *Die Bewegungsgruppen der Kristallographie,* 2nd ed. Birkhäuser, Basel 1966.

[5] J.F. Carlson, *The cohomology of groups,* pp. 581–610 in: ed. M. Hazewinkel, Handbook of Algebra vol 1, Elsevier 1996.

[6] J.F.Carlson, L. Townsley, L. Valero-Elizondo and M. Zhang, *Cohomology rings of finite groups,* Springer 2003.

[7] H. Cartan and S. Eilenberg, *Homological algebra,* Princeton University Press 1956.

[8] D.R. Farkas, *Crystallographic groups and their mathematics,* Rocky Mountain J. Math. 11 (1981), 511-551.

[9] P.J. Hilton and U. Stammbach, *A course in homological algebra,* Springer 1971.

[10] R. Lyndon, *Groups and geometry,* LMS lecture notes in math. 101, Cambridge University Press 1985.

[11] C.H. MacGillavry, *Symmetry aspects of M.C. Escher's periodic drawings,* Bohn, Scheltema and Holkema, Utrecht 1976.

[12] S. MacLane, *Origins of the cohomology of groups,* Enseign. Math. 24 (1978), 1–29.

[13] D. Schattschneider, *The plane symmetry groups: their recognition and notation,* Amer. Math. Monthly 85 (1978), 439-450.

[14] R.L.E. Schwartzenberger, *N-dimensional crystallography*, Pitman 1980.

[15] C.A.Weibel, *An introduction to homological algebra,* Cambridge 1997.

[16] J.A. Wolf, *Spaces of constant curvature,* 4th ed. Publish or Perish 1977.

[17] P.J. Webb, *A local method in group cohomology,* Commentarii Math. Helv. 62 (1987), 135–167.