

Math 8246 Group Theory

Peter Webb

January 7, 2019

Contents

1	Introduction	1
1.1	Some history	1
2	Appendix: Basic Homological Algebra	5
2.1	Tensor products	5
2.2	Splitting and exactness; projective and injective modules	8
2.3	Chain complexes	10
2.4	Projective resolutions, Ext and Tor	14
3	Group cohomology	20
3.1	Group representations	20
3.2	Fixed points, fixed quotients, and the augmentation ideal	24
3.3	Resolutions for group rings and first (co)homology	27
3.4	Second cohomology	33
3.5	The Schur multiplier	37
3.6	Special properties of the cohomology of finite groups	41
4	Crystallography	45
4.1	Definitions	45
4.2	Characterizations of space groups	46
4.3	Classification of 2-dimensional spacegroups	50
4.4	Computation of $H^2(P, T)$	54
5	Bibliography	59

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, 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 1932 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 $H^2(G, M)$.

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*, and it is interesting in that its homotopy type is an invariant of its fundamental group. 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 $K(G, 1)$. When any topology on G is ignored (so that if G has a topology, it is discrete), this space is also denoted BG , and is termed the *classifying space* of G .

It is a fact, for an aspherical CW-complex X , that its homology does not depend on its homotopy type. 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. Most groups have more complicated $K(G, 1)$ s 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.

It was in 1945 that Eilenberg and MacLane introduced an algebraic approach that computes these homology and cohomology groups, thus providing an algebraic definition. The definition is that

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

Thus, for each group G and representation M of G there are abelian groups $H_n(G, M)$ and $H^n(G, M)$ where $n = 0, 1, 2, 3, \dots$, called the n th 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.

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.

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, since this can be done without knowing the definition of group cohomology. A *group extension* is defined to be a short exact sequence of groups

$$1 \rightarrow A \rightarrow E \rightarrow G \rightarrow 1,$$

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 $G \rightarrow \text{Aut}(A)$, 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

$$1 \rightarrow A \rightarrow E \rightarrow G \rightarrow 1$$

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

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

Class Activity. Is the action given by conjugation of the quotient group on the normal subgroup trivial or not, in these examples?

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 $\phi : E_1 \rightarrow E_2$. Such a homomorphism is necessarily an isomorphism (by the 5-lemma, or the snake lemma, to be described). 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

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

where $i = 1, 2$, form

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

where

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

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 $E \cong Q_8$. 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.

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).

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:

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

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

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

group. A mapping $\phi : M \times N \rightarrow L$ 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 $M \times N \rightarrow M \otimes_R N$ 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. A mapping $\phi : M \times N \rightarrow L$ is *R*-bilinear if and only if

$$\begin{aligned}\phi(m_1r_1 + m_2r_2, n) &= r_1\phi(m_1, n) + r_2\phi(m_2, n) \\ \phi(m, s_1n_1 + s_2n_2) &= s_1\phi(m, n_1) + s_2\phi(m, n_2) \\ \phi(mr, n) &= \phi(m, rn) = r\phi(m, n).\end{aligned}$$

How much of that makes sense?

Theorem 2.1.3 (Dummit and Foote Corollary 11). *The balanced map $M \times N \rightarrow M \otimes_R N$ is universal with respect to balanced maps. This means: given a balanced map $M \times N \rightarrow L$ there exists a unique group homomorphism $M \otimes_R N \rightarrow L$ so that the given balanced map is the composite $M \times N \rightarrow M \otimes_R N \rightarrow L$. 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 $M \times N \rightarrow L$ biject with group homomorphisms $M \otimes_R N \rightarrow L$.*

Example 2.1.5. If $f : R \rightarrow S$ is a ring homomorphism with $f(1_R) = 1_S$ then $S \otimes_R R \cong S$ via an isomorphism $s \otimes r \mapsto sr$. 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 $(I \backslash R) \otimes_R M \cong M/IM$. Compare exercise 8. Is this true when I is a right ideal rather than a 2-sided ideal?

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, \dots, u_r and v_1, \dots, 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 $U \otimes_K V$.

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

Example 2.1.12. Let $\phi : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$ have matrix $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ and let $\psi : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$ 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

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

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 $\phi \otimes \psi$?

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, $\text{Hom}_S(A, B)$ is a left R -module and $\text{Hom}_S(B, A)$ is a right R -module. 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*

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

via an isomorphism that is natural in B and C .

Proof. We define inverse isomorphisms

$$\begin{aligned} \phi &\mapsto (b \mapsto (a \mapsto \phi(a \otimes b))) \\ (a \otimes b \mapsto \psi(b)(a)) &\leftarrow \psi \end{aligned}$$

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 $(a, b) \rightarrow \psi(b)(a)$ is R -balanced.

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

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

Corollary 2.1.17. *Let $f : R \rightarrow S$ 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 $\text{Hom}_S(S \otimes_R B, C) \cong \text{Hom}_R(B, C)$, where C is regarded as a left R -module via the homomorphism f .*

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

2.2 Splitting and exactness; projective and injective modules

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

It is an exercise to see that a split monomorphism is a monomorphism, and a split epimorphism is an 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*

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

the following are equivalent:

1. *the monomorphism α is split;*
2. *the epimorphism β is split;*

3. there is a commutative diagram

$$\begin{array}{ccccccc}
 0 & \rightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C \rightarrow 0 \\
 & & & & \downarrow i_1 & & \nearrow \pi_2 \\
 & & & & \cong \uparrow & & \\
 & & & & A \oplus C & &
 \end{array}$$

where i_1 is inclusion and π_2 is projection.

Definition 2.2.3. If any of 1, 2, or 3 of Lemma 2.2.2 is satisfied we say the sequence $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ 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. If $A \rightarrow B \rightarrow C \rightarrow 0$ is exact then $0 \rightarrow \text{Hom}_R(C, M) \rightarrow \text{Hom}_R(B, M) \rightarrow \text{Hom}_R(A, M)$ is exact and $N \otimes_R A \rightarrow N \otimes_R B \rightarrow N \otimes_R C \rightarrow 0$ is exact.
2. If $0 \rightarrow A \rightarrow B \rightarrow C$ is exact then $0 \rightarrow \text{Hom}_R(M, A) \rightarrow \text{Hom}_R(M, B) \rightarrow \text{Hom}_R(M, C)$ is exact.

Remark 2.2.5. If $0 \rightarrow \text{Hom}_R(C, M) \rightarrow \text{Hom}_R(B, M) \rightarrow \text{Hom}_R(A, M)$ is exact for all M then $A \rightarrow B \rightarrow C \rightarrow 0$ is exact. If $N \otimes_R A \rightarrow N \otimes_R B \rightarrow N \otimes_R C \rightarrow 0$ is exact for all N then $A \rightarrow B \rightarrow C \rightarrow 0$ is exact. If $0 \rightarrow \text{Hom}_R(M, A) \rightarrow \text{Hom}_R(M, B) \rightarrow \text{Hom}_R(M, C)$ is exact for all M then $0 \rightarrow A \rightarrow B \rightarrow C$ is exact.

Definition 2.2.6. We say that the functors $\text{Hom}_R(_, M)$ and $\text{Hom}_R(M, _)$ are *left exact*, while $N \otimes _$ is *right exact*. A covariant functor F is *exact* if and only if whenever $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ is exact then $0 \rightarrow F(A) \rightarrow F(B) \rightarrow F(C) \rightarrow 0$ is exact, i.e. F is both right and left exact.

Definition 2.2.7. 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 $\gamma : P \rightarrow A$ such that $\beta = \alpha\gamma$.

Lemma 2.2.8. The following are equivalent for an R -module P :

1. P is projective,
2. every epimorphism $M \rightarrow P$ splits,

- 3. there is a module Q such that $P \oplus Q$ is free,
- 4. $\text{Hom}_R(P, _)$ is an exact functor.

Definition 2.2.9. 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 $\text{Hom}_R(_, I)$ is an exact functor. Also, an R module N is *flat* if and only if $N \otimes _$ is an exact functor.

Proposition 2.2.10. *Projective modules are flat.*

Proof. Free modules are flat and hence so are projective modules, since 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

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

such that $d_i d_{i+1} = 0$ always. This condition is equivalent to the requirement that $\text{Im}(d_{i+1}) \subseteq \text{Ker}(d_i)$ always. We define the *homology group* of \mathcal{M} in degree i to be $H_i(\mathcal{M}) = \text{Ker}(d_i) / \text{Im}(d_{i+1})$. 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 $H^i(\mathcal{M}) = \text{Ker}(d_i) / \text{Im}(d_{i-1})$ is the *cohomology group* of \mathcal{M} in degree i in this case.

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

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

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

Class Activity. The diagram

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

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 $d : \mathcal{M} \rightarrow \mathcal{M}$ of degree -1 satisfying $d^2 = 0$. The homology of \mathcal{M} is the graded group $H(\mathcal{M}) = \text{Ker}(d)/\text{Im}(d)$. If the map d had degree $+1$ we would have a *cochain complex* instead.

Definition 2.3.2. A *(chain) homotopy* between two morphisms $\phi, \theta : \mathcal{M} \rightarrow \mathcal{N}$ is a graded module morphism $h : \mathcal{M} \rightarrow \mathcal{N}$ 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 $H_n(\phi) = H_n(\theta) : H_n(\mathcal{M}) \rightarrow H_n(\mathcal{N})$ are the same.

2. If there are chain maps $\phi : \mathcal{M} \rightarrow \mathcal{N}$ and $\psi : \mathcal{N} \rightarrow \mathcal{M}$ 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:*

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

Then there is an exact sequence

$$\text{Ker } \alpha \rightarrow \text{Ker } \beta \rightarrow \text{Ker } \gamma \xrightarrow{\omega} \text{Coker } \alpha \rightarrow \text{Coker } \beta \rightarrow \text{Coker } \gamma$$

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 $\text{Ker } \alpha \rightarrow \text{Ker } \beta$, and if θ' is epi so is $\text{Coker } \beta \rightarrow \text{Coker } \gamma$.

Proof. The map ω is defined as follows: let $c \in \text{Ker } \gamma$, 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 $\omega(c) = a + \alpha(A) \in \text{Coker } \alpha$. We now check exactness (see Hilton and Stammbach p.99).

For example, to check exactness at $\text{Ker } \gamma$, we observe first that $\theta(\text{Ker } \beta) \subseteq \text{Ker } \omega$. 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 $\theta(\text{Ker } \beta) \supseteq \text{Ker } \omega$ let $c \in \text{Ker } \gamma \cap \text{Ker } \omega$. 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 $b - \phi(a_0) \in \text{Ker } \beta$ and $\theta(b - \phi(a_0)) = \theta(b) - \theta\phi(a_0) = \theta(b) = c$. Therefore $c \in \theta(\text{Ker } \beta)$.

The remaining arguments are similar. □

Class Activity. • Is this morphism of chain complexes given earlier a chain homotopy equivalence?

- Calculate the homology of the kernel complex.

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 sequence $L_i \xrightarrow{\phi_i} M_i \xrightarrow{\theta_i} N_i$ is exact at M_i .

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

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

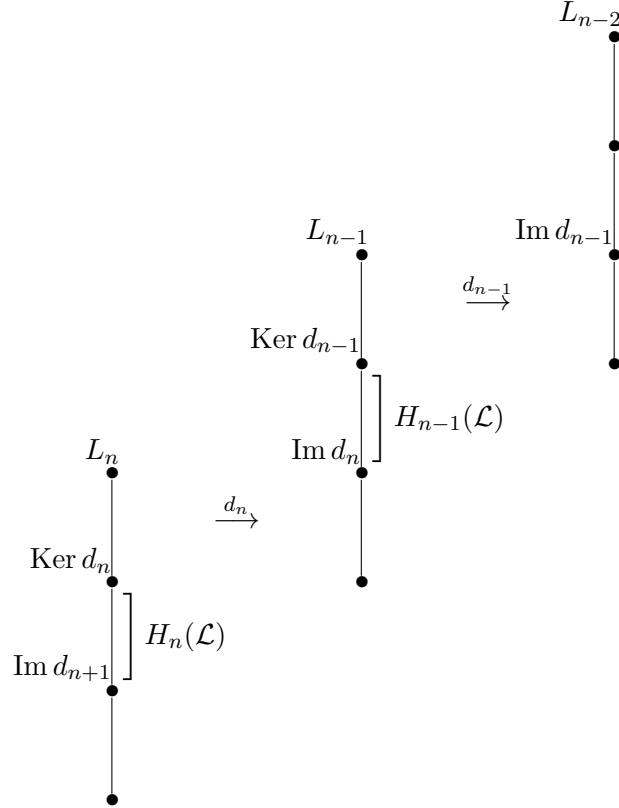
The connecting homomorphism ω is natural, in the sense that a commutative diagram of chain complexes

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

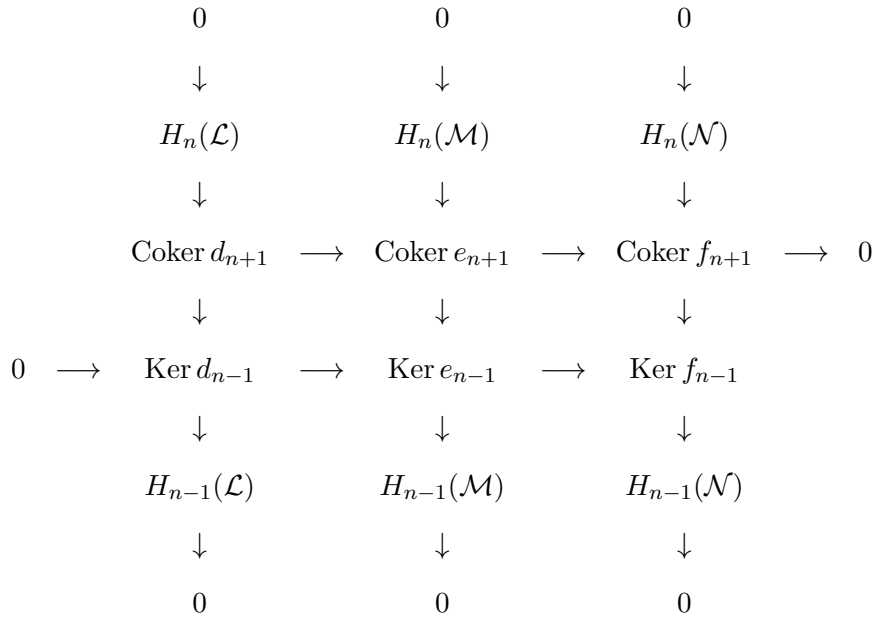
with exact rows yields a commutative square

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

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



Similarly with the M 's and N 's. Apply the snake lemma to the following diagram, all rows and columns of which are exact:



The naturality is an exercise. \square

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

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

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

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

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 $\mathcal{P} \rightarrow M$ to denote this projective resolution.

We may always construct resolutions of a module M as follows. Given M , choose a free module P_0 with surjective mapping $P_0 \rightarrow M$ 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

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

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

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

the n th 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:

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

where \mathcal{P} is the chain complex $0 \rightarrow \mathbb{Z} \xrightarrow{m} \mathbb{Z} \rightarrow 0$. 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

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

and

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

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

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

$$0 \rightarrow \text{Hom}_R(M, N) \rightarrow \text{Hom}_R(P_0, N) \xrightarrow{d_0} \text{Hom}_R(P_1, N)$$

is exact by Lemma 2.2.4, and the result follows. \square

Theorem 2.4.3. *Let $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ be exact and let M be another R -module. There are exact sequences*

$$(1) \quad \begin{array}{ccccccc} 0 & \rightarrow & \text{Hom}(M, A) & \rightarrow & \text{Hom}(M, B) & \rightarrow & \text{Hom}(M, C) \\ & & & & \xrightarrow{\omega} & \text{Ext}^1(M, A) & \rightarrow \text{Ext}^1(M, B) \rightarrow \dots \end{array}$$

$$(2) \quad \begin{array}{ccccccc} 0 & \rightarrow & \text{Hom}(C, M) & \rightarrow & \text{Hom}(B, M) & \rightarrow & \text{Hom}(A, M) \\ & & & & \rightarrow & \text{Ext}^1(C, M) & \rightarrow \text{Ext}^1(B, M) \rightarrow \dots \end{array}$$

Proof. We calculate our Ext groups with the resolution \mathcal{P} .

(1) The sequence $A \rightarrow B \rightarrow C$ gives a sequence of complexes

$$(*) \quad \text{Hom}(\mathcal{P}, A) \rightarrow \text{Hom}(\mathcal{P}, B) \rightarrow \text{Hom}(\mathcal{P}, C).$$

At each level in the grading this sequence is

$$\text{Hom}(P_n, A) \rightarrow \text{Hom}(P_n, B) \rightarrow \text{Hom}(P_n, C)$$

obtained by applying $\text{Hom}_R(P_n, _)$. We check that this gives a map of complexes. Since P_n is projective, $\text{Hom}_R(P_n, _)$ is exact and so $(*)$ is a short exact sequence of complexes. We now apply 1.5 and 2.1.

(2) We produce resolutions $\mathcal{P}, \mathcal{P}'$ and \mathcal{P}'' and 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. Let $\mathcal{P}', \mathcal{P}''$ be any resolutions of A and C and construct \mathcal{P} as follows:

$$\begin{array}{ccccccc}
 \mathcal{P}'_0 & & \xrightarrow{\epsilon'} & A & \longrightarrow & 0 & \\
 \downarrow & & & \downarrow & & & \\
 \mathcal{P}'_0 \oplus \mathcal{P}''_0 & & \xrightarrow{\epsilon} & B & & & \\
 \downarrow & & & \downarrow & & & \\
 \mathcal{P}''_0 & & \xrightarrow{\epsilon''} & C & \longrightarrow & 0. &
 \end{array}$$

Lift ϵ'' as shown and define ϵ so that the diagram commutes. By the snake lemma, $\text{Ker } \epsilon' \rightarrow \text{Ker } \epsilon \rightarrow \text{Ker } \epsilon''$ is exact and ϵ is epi. Now repeat with $\text{Ker } \epsilon' \rightarrow \text{Ker } \epsilon \rightarrow \text{Ker } \epsilon''$ to construct \mathcal{P}'' . \square

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 $\text{Ext}_R^n(P, M) = 0$.

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

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

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

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

(2) If I is injective then $\text{Hom}_R(-, I)$ is an exact functor so $\text{Hom}_R(\mathcal{P}, I)$ 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 $\text{Hom}_R(-, I)$ is an exact functor, so the I is injective. \square

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

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

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

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

$$0 = \text{Ext}_R^{n-1}(B, M) \rightarrow \text{Ext}_R^{n-1}(A, M) \rightarrow \text{Ext}_R^n(C, M) \rightarrow \text{Ext}_R^n(B, M) = 0$$

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

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 $\cdots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \rightarrow M \rightarrow 0$ be a projective resolution of M , and put $K_i = \text{Ker } d_i$. There is an exact sequence*

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

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

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

By dimension shifting we have

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

\square

One way to prove that Ext groups are well-defined is to prove a corresponding uniqueness statement for projective resolutions, which is what we do now.

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

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

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

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

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

We start the induction at $n = 0$ using projectivity of P_0 and the fact that $Q_0 \rightarrow M$ is an epimorphism. For the induction step, suppose that $\phi_0, \dots, \phi_{n-1}$ have been defined.

Now $e_{n-1}\phi_{n-1}d_n = \phi_{n-2}d_{n-1}d_n = 0$, so $\text{Im } \phi_{n-1}d_n \subseteq \text{Ker } e_{n-1} = \text{Im } e_n$. 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 $T_n : P_n \rightarrow Q_{n+1}$ 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 $\text{Im}(\phi_n - \psi_n - T_{n-1}d_n) \subseteq \text{Im } e_{n+1}$ 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. \square

Corollary 2.4.8. *Let $\mathcal{P}_1 \rightarrow M$ and $\mathcal{P}_2 \rightarrow M$ be two projective resolutions of M .*

(1) $\mathcal{P}_1 \rightarrow M$ and $\mathcal{P}_2 \rightarrow M$ 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) $\text{Ext}_R^n(M, N)$ is functorial in both variables.

We remark also that $\text{Ext}_R^n(M, N)$ can also be defined by taking an injective resolution $N \rightarrow \mathcal{I}$ of N and forming $H_n(\text{Hom}_R(M, \mathcal{I}))$. 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 $\mathcal{P} \rightarrow N$ a resolution of N by projective right modules. We put

$$\text{Tor}_n^R(N, M) = H_n(\mathcal{P} \otimes_R M),$$

which is the n th homology of the complex

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

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

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

$$(i) \quad \begin{array}{ccccccc} \cdots & \rightarrow & \text{Tor}_2^R(C, L) & \rightarrow & \text{Tor}_1^R(A, L) & \rightarrow & \text{Tor}_1^R(B, L) \rightarrow \text{Tor}_1^R(C, L) \\ & & \rightarrow & & A \otimes_R L & \rightarrow & B \otimes_R L \rightarrow C \otimes_R L \rightarrow 0 \end{array}$$

and

$$(ii) \quad \begin{array}{ccccccc} \cdots & \rightarrow & \text{Tor}_2^R(A, N) & \rightarrow & \text{Tor}_1^R(A, L) & \rightarrow & \text{Tor}_1^R(A, M) \rightarrow \text{Tor}_1^R(A, N) \\ & & \rightarrow & & A \otimes_R L & \rightarrow & A \otimes_R M \rightarrow A \otimes_R N \rightarrow 0. \end{array}$$

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

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

It follows that $\text{Tor}_n^R(N, M) = 0$ 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

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

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

Proposition 2.4.14. *There is an exact sequence*

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

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

Remark 2.4.15. We can also calculate $\text{Tor}_n^R(N, M)$ 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.

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 $V \rightarrow V$. 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

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

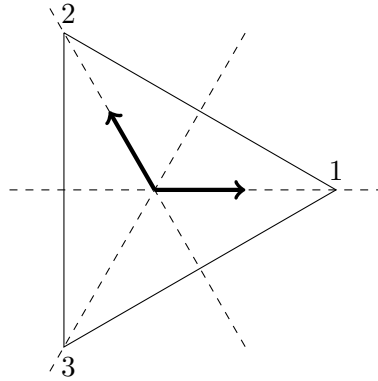
In a situation where V is free as an R -module, on taking a basis for V we may write each element of $GL(V)$ as a matrix with entries in R and we obtain for each $g \in G$ a matrix $\rho(g)$. These matrices multiply together in the manner of the group and we have a *matrix representation* of G . In this 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 $R \rightarrow R$. 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 $G \rightarrow R^\times$. 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 $\rho : G \rightarrow GL(V)$, 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 $G \times V \rightarrow V$ 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

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

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:

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

An (associative) *R-algebra* is defined to be a (not necessarily commutative) ring A with a 1, equipped with a (unital) ring homomorphism $R \rightarrow A$ 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 $G = \langle x \rangle$ is cyclic of order p , there is a surjective ring homomorphism $\mathbb{Z}G \rightarrow \mathbb{Z}[e^{2\pi i/p}]$ 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 $\rho : G \rightarrow GL(V)$ 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 $\rho(g_1)\rho(g_2) = \rho(g_1g_2)$ so $\rho : G \rightarrow GL(V)$ is a representation. \square

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 ${}_A A$ 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 ${}_R RG$ by observing that each element $g \in G$ acts on ${}_R RG$ 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 $\rho_W : G \rightarrow GL(W)$ 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

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

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

Example 3.1.9. In Example 3.1.4 above, an elementary calculation shows that $\langle \begin{pmatrix} 0 \\ 1 \end{pmatrix} \rangle$ 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 $f : V \rightarrow W$ 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 $H^n(G, M) := \text{Ext}_{\mathbb{Z}G}^n(\mathbb{Z}, M)$ and $H_n(G, M) :=$

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

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 $a : \mathbb{Z}G \rightarrow \mathbb{Z}G$ 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 $\mathcal{P} \rightarrow N$ by writing down the corresponding left modules N^ℓ and $\mathcal{P}^\ell \rightarrow N^\ell$. 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 $\text{Tor}_n^{\mathbb{Z}G}(A, B)$ really means $\text{Tor}_n^{\mathbb{Z}G}(A^r, B)$. 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 $\mathcal{P} \rightarrow N$ is a projective resolution of right modules, $\mathcal{P}^\ell \rightarrow N^\ell$ 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 $\epsilon : \mathbb{Z}G \rightarrow \mathbb{Z}$ 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

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

This is the *augmentation map* and it is a ring homomorphism, and also a homomorphism of $\mathbb{Z}G$ -modules. We write $IG := \text{Ker } \epsilon$ 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. *$H^0(G, M) = \text{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M) \cong M^G$. 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 $G = \langle g_1, \dots, g_n \rangle$ then $g_1 - 1, \dots, g_n - 1$ generate IG as a $\mathbb{Z}G$ -module.

Proof. (1) The set is independent and is contained in $\text{Ker } \epsilon$. To show that it spans $\text{Ker } \epsilon$, suppose that $\sum_{g \in G} \lambda_g g \in \text{Ker } \epsilon$ 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 $\text{Ker } \epsilon$.

(2) The first equality is a standard result about Ext groups. The map that sends a $\mathbb{Z}G$ -module homomorphism $\phi : \mathbb{Z} \rightarrow M$ to $\phi(1)$ is an isomorphism $\text{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M) \rightarrow M^G$. 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.

(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. \square

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

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

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

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

getting an exact sequence

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

The left term is zero since $\mathbb{Z}G$ is projective and hence flat. The two right terms identify as $\mathbb{Z} \rightarrow \mathbb{Z}$ 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 $G/G' \rightarrow IG/(IG)^2$. 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 $G \rightarrow IG/(IG)^2$ specified by $g \mapsto (g - 1) + IG^2$. It sends a product gh to $gh - 1 + IG^2 = (g - 1)(h - 1) + (g - 1) + (h - 1) + IG^2 = (g - 1) + (h - 1) + IG^2$, so that it is a group homomorphism. It thus sends a commutator $ghg^{-1}h^{-1}$ to $(g - 1) + (h - 1) - (g - 1) - (h - 1) + IG^2 = 0$, so vanishes on the commutator subgroup G' . We therefore obtain a homomorphism $G/G' \rightarrow IG/(IG)^2$. An inverse homomorphism is constructed as follows. First consider the homomorphism of abelian groups $IG \rightarrow G/G'$ 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 $IG/(IG)^2 \rightarrow G/G'$. Evidently these two mappings are mutually inverse. \square

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 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

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

so that this is a projective resolution of \mathbb{Z} . 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

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

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*

$$\begin{array}{ccccccccc} \cdots & \rightarrow & \mathbb{Z}G & \xrightarrow{d_2} & \mathbb{Z}G & \xrightarrow{d_1} & \mathbb{Z}G & \rightarrow & \mathbb{Z} & \rightarrow & 0 \\ & & \nearrow & & \searrow & & \nearrow & & \searrow & & \nearrow \\ & & IG & & \mathbb{Z} \cdot N & & IG & & & & \end{array}$$

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 $\text{Ker } d_1 = \mathbb{Z} \cdot N \cong \mathbb{Z}$. 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*

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

and

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

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

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

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 3.1(2). \square

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 $H^{2n}(G, \mathbb{Z}) = \mathbb{Z}/r\mathbb{Z}$.

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

We next examine the first degree cohomology and for this we introduce derivations. Let M be a $\mathbb{Z}G$ -module. A mapping $d : G \rightarrow M$ is a *derivation* if and only if $d(gh) = gd(h) + d(g)$. We write $\text{Der}(G, M) := \{\text{derivations } G \rightarrow M\}$ 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 $\text{Der}(G, M)$.

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 3.3.7. Let $d : G \rightarrow M$ be a mapping and define $\delta : IG \rightarrow M$ by $\delta(g-1) = d(g)$. Then d is a derivation if and only if δ is a module homomorphism. Thus $\text{Der}(G, M) \cong \text{Hom}_{\mathbb{Z}G}(IG, M)$.

Proof. 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 $g, h \in G$. \square

Given a short exact sequence of groups $1 \rightarrow M \rightarrow E \xrightarrow{p} G \rightarrow 1$ we say that a mapping of sets $s : G \rightarrow E$ is a *section* if $ps = \text{id}_G$. 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 3.3.8. Let $s : G \rightarrow E = M \rtimes G$ be a section, so that $s(g) = (dg, g)$ for some mapping $d : G \rightarrow M$. Then s is a group homomorphism if and only if d is a derivation. Thus $\text{Der}(G, M)$ is in bijection with the set of splittings $G \rightarrow E$.

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. \square

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

Corollary 3.3.9. *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 $\{x - 1 \mid x \in F\}$.*

Proof. Let M be any $\mathbb{Z}F$ -module. We first claim that any mapping $f : X \rightarrow M$ extends uniquely to a derivation $d : F \rightarrow M$. This is because the mapping $X \rightarrow M \rtimes F$ given by $x \mapsto (f(x), x)$ extends uniquely to a group homomorphism $F \rightarrow M \rtimes F$ 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 $IF \rightarrow M$, by the correspondence between derivations and such module homomorphisms. It follows that IF satisfies the universal property of a free $\mathbb{Z}F$ -module with generating set as claimed. \square

We will compute $H^1(G, M)$ using the exact sequence

$$\begin{array}{ccccccc} \text{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M) & \rightarrow & \text{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M) & \rightarrow & \text{Hom}_{\mathbb{Z}G}(IG, M) & \rightarrow & H^1(G, M) \rightarrow 0 \\ & & \parallel & & \parallel & & \\ & & M^G & & M & & \text{Der}(G, M) \end{array}$$

Lemma 3.3.10. *$d \in \text{Der}(G, M)$ is principal if and only if the corresponding map $\delta : IG \rightarrow M$ lies in the image of $\text{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M) \rightarrow \text{Hom}_{\mathbb{Z}G}(IG, M)$. Hence $H^1(G, M) \cong \text{Der}(G, M)/P(G, M)$.*

Proof. Any $\phi : \mathbb{Z}G \rightarrow M$ 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 $\text{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M) \rightarrow \text{Hom}_{\mathbb{Z}G}(IG, M)$. The corresponding derivations are $P(G, M)$. \square

We define two splittings $s_1, s_2 : G \rightarrow E = M \rtimes G$ 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 3.3.11. *Let M be a $\mathbb{Z}G$ -module. The M -conjugacy classes of splittings of $1 \rightarrow M \rightarrow M \rtimes G \rightarrow G \rightarrow 1$ 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 $d_1 - d_2 \in P(G, M)$. \square

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 3.3.12. *Let $1 \rightarrow K \rightarrow E \rightarrow G \rightarrow 1$ be an exact sequence of groups, where K is a normal subgroup of E . Then $\text{Ker}(\mathbb{Z}E \rightarrow \mathbb{Z}G) = \mathbb{Z}E \cdot IK$, 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 $\overline{IK} = \bigoplus_{t \in [E/K]} tIK$.*

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 $E \rightarrow G$ and the corresponding ring homomorphism $\mathbb{Z}E \rightarrow \mathbb{Z}G$ 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 $x = \sum_{t \in [E/K]} ty_t$ which shows that $\text{Ker}(\mathbb{Z}E \rightarrow \mathbb{Z}G) = \bigoplus_{t \in [E/K]} t \cdot IK = \mathbb{Z}E \cdot IK$. 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 $IK \cdot \mathbb{Z}E$. \square

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' .

Proposition 3.3.13. *Let $1 \rightarrow K \rightarrow E \rightarrow G \rightarrow 1$ 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*

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

in which $\overline{IK}/(IK \cdot IE) \cong K/K'$ 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 $1 \rightarrow G \rightarrow G \rightarrow 1 \rightarrow 1$.

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

$$\begin{array}{ccccccc} 0 & \rightarrow & \overline{IK} & \rightarrow & \mathbb{Z}E & \rightarrow & \mathbb{Z}G & \rightarrow & 0 \\ & & \parallel & & \uparrow & & \uparrow & & \\ 0 & \rightarrow & \overline{IK} & \rightarrow & IE & \rightarrow & IG & \rightarrow & 0, \end{array}$$

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

If M is a $\mathbb{Z}E$ -module then $M/IK \cdot M = M/\overline{IK} \cdot M$ 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

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

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

Corollary 3.3.14. *Let $1 \rightarrow R \rightarrow F \rightarrow G \rightarrow 1$ 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*

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

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

$$\begin{array}{ccccccc} \xrightarrow{d_2} & \mathbb{Z}G^{d(F)} & \xrightarrow{d_1} & \mathbb{Z}G & \rightarrow & \mathbb{Z} & \rightarrow 0. \\ & \nearrow & \searrow & \nearrow & & & \\ & R/R' & & IG & & & \end{array}$$

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

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

as R/R' by Proposition 3.13. The middle term is $\mathbb{Z}G \otimes_{\mathbb{Z}G} \mathbb{Z}F^{d(F)} \cong \mathbb{Z}G^{d(F)}$. \square

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 $G = \langle g_1, \dots, g_n \rangle$ then the mapping $\mathbb{Z}G^{d(F)} \rightarrow IG$ sends the i th free generator to $g_i - 1$. We have already seen that these elements generate IG in Lemma 3.1, and the above corollary confirms this. In case G is itself free and the presentation has $R = 1$ we deduce that $\mathbb{Z}F^{d(F)} \rightarrow IF$ is an isomorphism, thereby confirming Corollary 3.9.

Example 3.3.15. Let $G = \langle g \rangle$ be cyclic of order n , and let $1 \rightarrow R \rightarrow F \rightarrow G \rightarrow 1$ 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 $x^n - 1 + IR \cdot IF$ in $IF/(IR \cdot IF)$, which is a free $\mathbb{Z}G$ -module with basis $\{x - 1\} + IR \cdot IF$. Now

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

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

3.4 Second cohomology

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

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

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

Proof. We use the start of the resolution given in 3.14 together with the sequence of 2.5 that computes Ext groups. We also use the identification of the term $\mathbb{Z}G^{d(F)}$ that appears in 3.14 as the module $IF/(IR \cdot IF)$, as in the proof of 3.14. Thus we have an exact sequence

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

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

Theorem 3.4.2. *Let M be a $\mathbb{Z}G$ -module. There is a bijection*

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

Proof. We use the short exact sequence

$$0 \rightarrow R/R' \rightarrow IF/(IR \cdot IF) \rightarrow IG \rightarrow 0$$

to compute $H^2(G, M)$ by means of the exact sequence

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

Thus any element $\bar{\theta} \in H^2(G, M)$ may be represented by a homomorphism $\theta : R/R' \rightarrow M$. Notice that

$$\text{Hom}_{\mathbb{Z}G}(IF/(IR \cdot IF), M) \cong \text{Hom}_{\mathbb{Z}F}(IF/(IR \cdot IF), M) \cong \text{Hom}_{\mathbb{Z}F}(IF, M) \cong \text{Der}(F, M)$$

using the fact that IR acts as 0 on M , and by Lemma 3.7. Hence two homomorphisms $\theta, \theta' : R/R' \rightarrow M$ 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 .

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

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

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 $M \rightarrow E$ 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.

We must also check that ψ is well defined on cohomology classes. Let $d \in \text{Der}(F, M)$. We show that $\psi(\bar{\theta})$ and $\psi(\overline{\theta + d})$ are the same. This is so because the mapping $F/R' \rightarrow M \rtimes F/R'$ given by $x \mapsto (dx, x)$ is a homomorphism (by Lemma 3.8) and it induces a homomorphism $\tilde{\eta} : F/R' \rightarrow E$. We check that the diagram

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

commutes.

We next define a mapping

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

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

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

using that fact that F is free. Since M is abelian we have $R' \subseteq \text{Ker}(R \rightarrow M)$, 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

$$\begin{array}{ccccccccc} 1 & \rightarrow & R & \rightarrow & F & \rightarrow & G & \rightarrow & 1 \\ & & \alpha_i \downarrow & & \beta_i \downarrow & & \parallel & & \\ 1 & \rightarrow & M & \rightarrow & E & \rightarrow & G & \rightarrow & 1 \end{array} \quad i = 1, 2.$$

For each $x \in F$ let $d(x) \in M$ be defined by $\beta_2(x) = d(x)\beta_1(x)$. We check that $d \in \text{Der}(F, M)$, 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 3.4.3. (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 $H^2(G, \zeta(M))$ classifies extensions (provided there are any, which there might not be), where $\zeta(M)$ 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 $H^2(G, M) \cong \text{Ext}_{\mathbb{Z}G}^1(IG, M)$, so that group extensions of G correspond to module extensions of IG . This correspondence is the one we have already seen in Proposition 3.13.

(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 3.4.4. 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 $1 \rightarrow R \rightarrow F \rightarrow G \rightarrow 1$, and we use the exact sequence of Proposition 3.16:

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

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

We show that $\text{Der}(F, \mathbb{F}_2)$ has zero image in $\text{Hom}_{\mathbb{Z}G}(R/R', \mathbb{F}_2)$. If $d \in \text{Der}(F, \mathbb{F}_2)$ 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 $H^2(G, \mathbb{F}_2) \cong \text{Hom}_{\mathbb{Z}G}(R/R', \mathbb{F}_2)$. Furthermore we have

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

since we are now dealing with modules with trivial action.

As a $\mathbb{Z}G$ -module, R/R' is generated by $a^2R', b^2R', [a, b]R'$ (see the exercises) Because of the exact sequence $0 \rightarrow R/R' \rightarrow \mathbb{Z}G^2 \rightarrow IG \rightarrow 0$, R/R' is a submodule of a free module and we express its generators in terms of coordinates with respect to the basis

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

of $IF/IR \cdot IF$. 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.

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

$$\begin{aligned} IG \cdot (\mathbb{F}_2 \otimes_{\mathbb{Z}} R/R') &= \langle (\sum_{g \in G} g, 0), (0, \sum_{g \in G} g) \rangle \\ &= (\mathbb{F}_2G^2)^G \end{aligned}$$

which has dimension 2. Now counting dimensions in the sequence $0 \rightarrow \mathbb{F}_2 \otimes R/R' \rightarrow \mathbb{F}_2G^2 \rightarrow \mathbb{F}_2 \otimes IG \rightarrow 0$ we have $\dim \mathbb{F}_2 \otimes IG = 3$ and $\dim \mathbb{F}_2G^2 = 8$, so $\dim \mathbb{F}_2 \otimes R/R' = 5$. 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 $\phi : R/R' \rightarrow \mathbb{F}_2$, and there are 8 possibilities given by the values of ϕ on the generators. Given such a ϕ the corresponding extension is $1 \rightarrow \mathbb{F}_2 \rightarrow F/R' / \text{Ker } \phi \rightarrow G \rightarrow 1$. This is because this extension appears in a commutative diagram

$$\begin{array}{ccccccc} 1 & \rightarrow & R/R' & \rightarrow & F/R' & \rightarrow & G \rightarrow 1 \\ & & \downarrow \phi & & \downarrow & & \parallel \\ 1 & \rightarrow & \mathbb{F}_2 & \rightarrow & F/R' / \text{Ker } \phi & \rightarrow & G \rightarrow 1 \end{array}$$

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:

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

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

In general a presentation for an extension $1 \rightarrow M \rightarrow E \rightarrow G \rightarrow 1$ 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.

3.5 The Schur multiplier

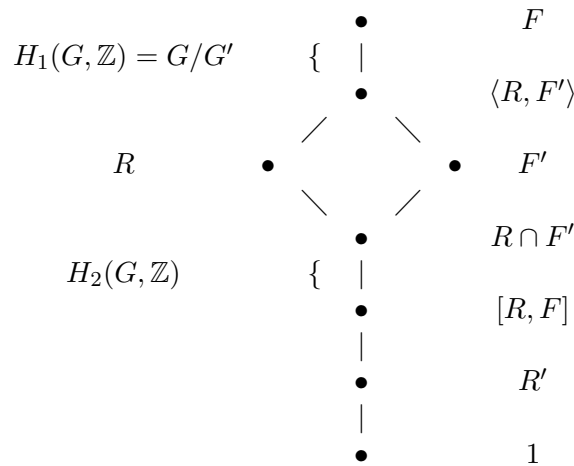
We turn attention to the *Schur multiplier* of G , which we may define to be $H_2(G, \mathbb{Z})$. When G is finite there are isomorphisms

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

and sometimes one of these other groups is taken to be the Schur multiplier. 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 3.5.1 (Hopf formula). *Let $1 \rightarrow R \rightarrow F \rightarrow G \rightarrow 1$ be a presentation of G . Then $H_2(G, \mathbb{Z}) \cong (R \cap F')/[R, F]$.*

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 was observed by Gruenberg.

Proof. We use the short exact sequence $0 \rightarrow \overline{IR}/(IR \cdot IF) \rightarrow IF/(IR \cdot IF) \rightarrow IG \rightarrow 0$ to compute $H_2(G, \mathbb{Z})$. After applying $\mathbb{Z} \otimes_{\mathbb{Z}G} -$ to it we obtain

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

This map is induced by inclusion $\overline{IR} \rightarrow IF$. 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

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

Also

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

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

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

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

Corollary 3.5.2. *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. \square

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

Proposition 3.5.3. *Let $1 \rightarrow M \rightarrow E \rightarrow G \rightarrow 1$ be a central group extension. Then*

1. *in any commutative diagram of groups*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & L & \longrightarrow & J & \longrightarrow & G & \longrightarrow & 1 \\ & & & & \downarrow & & \downarrow & & \parallel \\ & & & & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

the restricted vertical maps $L \cap J' \rightarrow M \cap E'$ and $J' \rightarrow E'$ are surjective, and

2. *$M \cap E'$ is a homomorphic image of $H_2(G, \mathbb{Z})$.*

We say that a central extension $1 \rightarrow M \rightarrow E \rightarrow G \rightarrow 1$ is a *stem extension* if $M \subseteq E'$ (or equivalently if $E/E' \rightarrow G/G'$ is an isomorphism). A group G is said to be *perfect* if and only if $G = G'$. The theory of central extensions is most easily described for perfect groups, and that is why we focus on them.

Proposition 3.5.4. *Let G be a perfect group. A central extension $1 \rightarrow M \rightarrow E \rightarrow G \rightarrow 1$ 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 $E' = E$. \square

Theorem 3.5.5. *Suppose that G is a perfect group. There exists a central stem extension $1 \rightarrow A \rightarrow \hat{G} \rightarrow G \rightarrow 1$ with the property that whenever $1 \rightarrow M \rightarrow E \rightarrow G \rightarrow 1$ is a central stem extension there exists a unique commutative diagram*

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

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

Proof. Let $1 \rightarrow R \rightarrow F \rightarrow G \rightarrow 1$ be a presentation of G . The extension with the special property we seek is in fact $1 \rightarrow R \cap F' / [R, F] \rightarrow F' / [R, F] \rightarrow G' = G \rightarrow 1$, which appeared in the proof of 3.20. We saw in the proof of 3.20 also that there is always a diagram of extensions as in the statement of the proposition, using the fact that here E must be perfect. We show that $\hat{G} := F' / [R, F]$ is perfect. Since $G = G' = F'R/R$ we have $F'R = F$ so $F' = [F'R, F'R] \subseteq [F'R, F'R][R, F] \subseteq [F', F'][R, F] = F''[R, F]$ since 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 3.21 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

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

and the composites must be the identity by uniqueness of the lift of the identity. \square

The group \hat{G} is 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. When G is not perfect there may be several maximal stem extensions of G . They are all central extensions of G by $H^2(G, \mathbb{Z})$.

Proposition 3.5.6. *Let G be a perfect group and $1 \rightarrow M \rightarrow E \rightarrow G \rightarrow 1$ a covering of G . Then E is the universal cover of G if and only if $H_2(E, \mathbb{Z}) = 0$.*

Proof. \Rightarrow We will use Witt's identity (analogous to the Jacobi identity)

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

which holds in all groups. One proves this by expanding the terms.

Let E be the universal cover of G , \hat{E} the universal cover of E . Let K be the kernel of the composite $\hat{E} \rightarrow E \rightarrow G$. An argument similar to the snake lemma applied to the diagram

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

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

We show that $K \leq \zeta(\hat{E})$. Let $k \in K$, $g, h \in \hat{E}$. Then $[g^{-1}, k] \in H_2(E, \mathbb{Z})$ since $M \leq \zeta(E)$, and now $[h, [g^{-1}, k]] = 1$ in \hat{E} since $H_2(E, \mathbb{Z}) \leq \zeta(\hat{E})$. 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 $k \in \zeta(\hat{E})$. We conclude that $1 \rightarrow K \rightarrow \hat{E} \rightarrow G \rightarrow 1$ is a covering of G .

Now by universality of E we have a commutative diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G \longrightarrow 1 \\ & & \downarrow & & \downarrow \beta & & \parallel \\ 1 & \longrightarrow & K & \longrightarrow & \hat{E} & \longrightarrow & G \longrightarrow 1 \end{array}$$

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. \square

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

Example 3.5.8. There are presentations $S_3 = \langle x, y \mid x^2 = 1, xyx^{-1} = y^2 \rangle$ and $SL(2, 5) = \langle x, y \mid x^2 = y^3 = (xy)^5 \rangle$. Since they have the same number of relators as generators, we conclude that their multipliers are 0. Furthermore $SL(2, 5)$ is perfect (the abelianization may be computed from the presentation), and since there is a short exact sequence $1 \rightarrow C_2 \rightarrow SL(2, 5) \rightarrow A_5 \rightarrow 1$ we deduce that $H_2(A_5, \mathbb{Z}) = C_2$ by 3.23. 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.

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.

3.6 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 3.6.1. *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. We may construct a projective resolution of \mathbb{Z} in which all the modules and kernels are finitely generated abelian groups, using the Noetherian property of $\mathbb{Z}G$. Now applying the functors $\text{Hom}_{\mathbb{Z}G}(-, M)$ and $M \otimes_{\mathbb{Z}G} -$ to this projective resolution we again obtain complexes of finitely generated abelian groups since $\text{Hom}_{\mathbb{Z}G}(P, M) \subseteq \text{Hom}_{\mathbb{Z}}(P, M)$, 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. \square

Proposition 3.6.2. *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 $|G| \cdot \text{Ext}_{\mathbb{Z}G}^n(A, B) = 0$ and $|G| \cdot \text{Tor}_n^{\mathbb{Z}G}(C, A) = 0$ for all $n \geq 1$.*

Proof. Let

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

be a projective resolution of A , so that

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

is exact. Given a homomorphism $\theta : K_{n-1} \rightarrow B$ we show that $|G| \cdot \theta$ lies in the image of $\mathrm{Hom}_{\mathbb{Z}G}(P_{n-1}, B)$. Since the K_n are submodules of a free module they are free abelian groups, so that $P_{n-1} \cong K_{n-1} \oplus K_{n-2}$ as abelian groups. We extend θ to a map $\eta : P_{n-1} \rightarrow B$ of abelian groups, for example, $\eta = (\theta, 0) : K_{n-1} \oplus K_{n-2} \rightarrow B$. Then $\tilde{\eta} = \sum_{g \in G} g\eta g^{-1} : P_{n-1} \rightarrow B$ is a $\mathbb{Z}G$ -module homomorphism with $\tilde{\eta}|_{K_{n-1}} = |G|\theta$.

The argument for Tor is similar. \square

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 $|G| \cdot \mathrm{Ext}_{\mathbb{Z}G}^1(A, B) = 0$ 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 $\mathrm{Ext}_{\mathbb{Z}G}^1(A, B) \cong \mathbb{Z}/m\mathbb{Z}$, and in fact $0 \rightarrow \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/m^2\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \rightarrow 0$ 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 $|G| \cdot \mathrm{Ext}_{kG}^n(A, B) = 0$ for all $n \geq 1$.

Corollary 3.6.3. *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 $n : A \rightarrow A$ 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 $\mathrm{g.c.d}(|A|, n) = 1$ then A is uniquely divisible by n .

Corollary 3.6.4. *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 $|G| : M \rightarrow M$ is an isomorphism, so is $|G| : H^n(G, M) \rightarrow H^n(G, M)$ by functoriality of cohomology. This map is zero if $n \geq 1$, by Proposition 4.2, so it follows that $H^n(G, M) = 0$ if $n \geq 1$. The argument with $H_n(G, M)$ is similar. \square

Corollary 3.6.5. (1) $H^n(G, \mathbb{Z}) \cong H^{n-1}(G, \mathbb{Q}/\mathbb{Z}) \cong H^{n-1}(G, \mathbb{C}^\times)$ for all $n \geq 2$, with similar isomorphisms in homology.

(2) If M is an RG -module in which $|G|$ is invertible then $H^n(G, M) = H_n(G, M) = 0$ for all $n \geq 1$.

Proof. Here \mathbb{C}^\times denotes the multiplicative group of nonzero complex numbers, which is isomorphic to $\mathbb{R}_{>0}^\times \times S^1$ via the correspondence $z \leftrightarrow (|z|, \arg(z))$. We thus have a short exact sequence $1 \rightarrow \mathbb{Z} \rightarrow \mathbb{R}_{>0}^\times \times \mathbb{R}^+ \rightarrow \mathbb{C}^\times \rightarrow 1$. Because $\mathbb{R}_{>0}^\times \cong \mathbb{R}^+$ 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. \square

We present an application of this and a result known as the integral duality theorem that states for a finite group that $H^{n+1}(G, \mathbb{Z}) \cong H_n(G, \mathbb{Z})$ when $n \geq 1$. Putting this together, 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.

Corollary 3.6.6 (Schur-Zassenhaus). *Let $1 \rightarrow M \rightarrow E \rightarrow G \rightarrow 1$ be a short exact sequence of finite groups where $\text{g.c.d.}(|M|, |G|) = 1$. Then the extension is split, $E \cong M \rtimes G$, and all subgroups of E of order $|G|$ are conjugate.*

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 4.4, so the result follows from our interpretation of second and first cohomology. \square

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 $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}G, C)$ a *coinduced* module. The latter is made into a $\mathbb{Z}G$ -module using the right action on $\mathbb{Z}G$.

Lemma 3.6.7. *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. If $M = \text{Hom}_{\mathbb{Z}}(\mathbb{Z}G, C)$ for some abelian group C we compute cohomology with coefficients in M by applying the functor $\text{Hom}_{\mathbb{Z}G}(-, \text{Hom}_{\mathbb{Z}}(\mathbb{Z}G, C))$ to a projective resolution and taking homology. Now for any module P we have a natural isomorphism $\text{Hom}_{\mathbb{Z}G}(P, \text{Hom}_{\mathbb{Z}}(\mathbb{Z}G, C)) \cong \text{Hom}_{\mathbb{Z}}(\mathbb{Z}G \otimes_{\mathbb{Z}G} P, C) \cong \text{Hom}_{\mathbb{Z}}(P, C)$ and when we apply the functor $\text{Hom}_{\mathbb{Z}}(-, C)$ to a projective resolution of \mathbb{Z} we get an acyclic complex because as abelian groups the projective resolution splits. 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. \square

Proposition 3.6.8. *If G is finite then induced and coinduced modules coincide. Hence cohomology vanishes on induced modules in degrees ≥ 1 . If P is a projective RG -module for some commutative ring R then $H^n(G, P) = 0$ for all $n \geq 1$.*

Proof. We define a mapping $\mathbb{Z}G \otimes_{\mathbb{Z}} C \rightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Z}G, C)$ by $g \otimes c \mapsto \phi_{(g,c)}$ where $\phi_{(g,c)} : \mathbb{Z}G \rightarrow C$ is the homomorphism determined by

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

We check that this is a homomorphism of $\mathbb{Z}G$ -modules that is always injective, and is surjective if G is finite. Since free modules are induced we deduce that cohomology vanishes on them, and hence also on projective modules since they are direct summands of free modules. \square

Corollary 3.6.9. *Let C be an abelian group. Any group extension*

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

with G finite must split, so that $E \cong C \wr G$. 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. \square

Chapter 4

Crystallography

4.1 Definitions

Let \mathbb{E}^n denote n -dimensional *Euclidean space* (that is, \mathbb{R}^n together with its usual notion of distance). By a *rigid motion* of \mathbb{E}^n we mean a distance-preserving mapping $\mathbb{E}^n \rightarrow \mathbb{E}^n$, also called an isometry of \mathbb{E}^n . Let $R(n)$ be the group of rigid motions of \mathbb{E}^n . We see that $R(n)$ contains the following elements:

- All translations. For each vector $v \in \mathbb{E}^n$ we will denote by t_v the translation through the vector v , and since these translations compose the same way as the vectors add we see that the group of all translations is isomorphic to \mathbb{E}^n .
- Orthogonal vector space transformations fixing the origin, i.e. the group $O(n, \mathbb{R})$, which we will abbreviate as $O(n)$.

In fact $R(n) \cong \mathbb{E}^n \rtimes O(n)$, since any rigid transformation is the product of a translation and an element of $O(n)$, clearly $\mathbb{E}^n \triangleleft R(n)$ and $O(n) \cap \mathbb{E}^n = 1$.

There is an action of $O(n)$ on \mathbb{E}^n given by conjugation within $R(n)$, and it is the same as the usual action of $O(n)$ on \mathbb{E}^n . That is to say, if $x \in O(n)$ and $t_v \in R(n)$ is translation by the vector $v \in \mathbb{E}^n$ then $xt_vx^{-1} = t_{xv} \in R(n)$. Furthermore, $R(n)$ inherits a topology as a subgroup of the affine group.

We define a *crystal structure* in dimension n to be 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 $\mathcal{C} \rightarrow \mathcal{C}$, there exist n linearly independent translations, and
- there exists a number $d > 0$ such that any translation preserving \mathcal{C} has magnitude at least d .

We let $S(\mathcal{C})$ denote the group of rigid motions $\mathbb{E}^n \rightarrow \mathbb{E}^n$ that preserve \mathcal{C} . This is the *space group* corresponding to \mathcal{C} . The subgroup

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

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*. There is a module action of P on T given by conjugation within $S(\mathcal{C})$, and by considering the embedding

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

we see that the action on T is orthogonal. In general we will say that G is a space group in dimension n if it is the space group of some crystal structure in dimension n .

At this point some examples are presented.

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 $1 \rightarrow T \rightarrow S(\mathcal{C}) \rightarrow P \rightarrow 1$ is split, since 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, and also that although we frequently identify T with a subgroup of \mathbb{E}^n , the conjugation action of P on T is not the same as an action of P on \mathbb{E}^n .

Lemma 4.1.1. *Let $S(\mathcal{C})$ be a space group. Then $T \cong \mathbb{Z}^n$, P acts faithfully on T and $|P| < \infty$.*

Proof. From the definition of a space group we may identify T with a discrete subgroup X of \mathbb{E}^n that contains n independent elements. We show that $X \cong \mathbb{Z}^n$ by induction on n . When $n = 0$ evidently X must be the trivial group, so the result holds. Now suppose that $n > 0$ and the result is true for smaller values of 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 $\lambda > 1$ (since the distance between any two distinct vectors in X must be at least d). Then $\langle v \rangle = X \cap \mathbb{R}v$ and $X/\langle v \rangle \cong (X + \mathbb{R}v)/\mathbb{R}v$ is a discrete subgroup of \mathbb{E}^{n-1} (since if $w \in X - \mathbb{R}v$ then the distance from w to any point on $\mathbb{R}v$ is greater than some fixed $\epsilon > 0$, by a compactness argument). It contains $n - 1$ independent elements, so by induction it is isomorphic to \mathbb{Z}^{n-1} , generated by vectors $v_1 + \langle v \rangle, \dots, v_{n-1} + \langle v \rangle$. Now v_1, \dots, v_{n-1}, v generate X , which is a torsion free abelian group, so it is isomorphic to \mathbb{Z}^n .

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

Let $T = \langle t_1, \dots, t_n \rangle$. We write the set of all images of these generators under the action of P as $P\{t_1, \dots, t_n\}$, which we regard as a subset of \mathbb{E}^n . P permutes this set of points faithfully. They lie inside a ball of finite radius, since P acts as a subgroup of $O(n)$. Since the distance between any two of them is at least d , there exist only finitely many of these points, and so $|P| < \infty$. \square

4.2 Characterizations of space groups

Proposition 4.2.1. *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 $T \leq \mathbb{E}^n$ is discrete and P is finite, so G is discrete.

Conversely, if G is discrete then $G \cap \mathbb{E}^n$ and $G/G \cap \mathbb{E}^n$ are discrete so $G \cap \mathbb{E}^n \cong \mathbb{Z}^n$ by the argument of the last lemma (since it contains n independent translations) and $G/G \cap \mathbb{E}^n$ is finite since it embeds in $O(n)$ which is compact. Now to produce a crystal structure \mathcal{C} for G , take an unsymmetric pattern so small and so positioned that it does not meet any of its images under non-identity elements of G . This can be done because in any bounded region of \mathbb{E}^n the points that have non-identity stabilizer are a finite union of proper subspaces, so it is possible to position the small pattern so that it does not meet any of these subspaces. Let \mathcal{C} be the orbit of the pattern. Then the space group $S(\mathcal{C})$ is G since it certainly contains G , and it can be no larger than this because any element $s \in S(\mathcal{C})$ sends the small 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 $s = g \in G$. \square

Theorem 4.2.2. *If G is 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 then G is (isomorphic to) a space group of dimension n .*

Proof. Embed T in \mathbb{R}^n in any way so that it contains n independent translations and form the extension pushout

$$\begin{array}{ccccccc} 1 & \longrightarrow & T & \xrightarrow{\theta} & G & \longrightarrow & P \longrightarrow 1 \\ & & \phi \downarrow & & \downarrow & & \parallel \\ 1 & \longrightarrow & \mathbb{R}^n & \longrightarrow & E & \longrightarrow & P \longrightarrow 1 \end{array}$$

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

Since $|P| < \infty$ we may put an inner product on \mathbb{R}^n that is preserved by P . This is done by taking any inner product $\langle \cdot, \cdot \rangle_1$ and defining

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

Now P acts orthogonally, so there exists an isomorphism $\sigma : \mathbb{R}^n \rightarrow \mathbb{E}^n$ and a map $\tau : P \rightarrow O(n)$ such that $\sigma(g \cdot v) = \tau(g) \cdot \sigma(v)$. The diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mathbb{R}^n & \longrightarrow & \mathbb{R}^n \rtimes P & \longrightarrow & P \longrightarrow 1 \\ & & \sigma \downarrow & & & & \tau \downarrow \\ 1 & \longrightarrow & \mathbb{E}^n & \longrightarrow & \mathbb{E}^n \rtimes O(n) & \longrightarrow & O(n) \longrightarrow 1 \\ & & & & \parallel & & \\ & & & & R(n) & & \end{array}$$

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

Lemma 4.2.3. *Let G be any group that is an extension $1 \rightarrow T \rightarrow G \rightarrow P \rightarrow 1$ 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 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.

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

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

is exact and XT/T is a subgroup of P that is finite, so $|X/(X \cap T)| < \infty$ and hence $X \cap T \cong \mathbb{Z}^n$. 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 . \square

We will show how to classify crystal structures in terms of their symmetries, but to do this we evidently need to introduce an equivalence relation so that two crystal structures are regarded as the same under certain circumstances. Informally, they will be equivalent if the space group of one may be identified with the space group of the other after space has been transformed by a combination of a linear (vector space) transformation and a translation. These transformations generate the *affine group*, which has the structure $\mathbb{E}^n \rtimes GL(n, \mathbb{R})$. Thus we do not distinguish crystal structures if one is bigger than the other, or one is a skewed version of the other, or 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. The definitions is that 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 4.2.4. *Let $1 \rightarrow T_1 \rightarrow G_1 \rightarrow P_1 \rightarrow 1$ and $1 \rightarrow T_2 \rightarrow G_2 \rightarrow P_2 \rightarrow 1$ 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*

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

in which the vertical arrows are isomorphisms.

3. *There exists a commutative diagram*

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

4. $G_1 \cong G_2$ as abstract groups.

Proof. (i) \Rightarrow (iv) is clear.

(iv) \Rightarrow (iii) \Rightarrow (ii): If $\phi : G_1 \rightarrow G_2$ is an isomorphism then $\phi(T_1)$ must be the unique maximal abelian subgroup of G_2 isomorphic to \mathbb{Z}^n . Hence $\phi(T_1) \subseteq T_2$ by 5.4, and ϕ provides a commutative diagram as in condition (iii). In fact 5.4 shows that $\phi(T_1) = T_2$ which establishes (ii).

(ii) \Rightarrow (i): Suppose we are given a commutative diagram in which the vertical arrows are isomorphisms

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

We will regard both of these extensions as being embedded in $\mathbb{R}^n \rtimes O(n)$ so we have containments

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

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 of $GL(n, \mathbb{R})$, and so after applying such a conjugation we may assume $T_1 = T_2 = T$, say. Now $\gamma : P_1 \rightarrow P_2$ must be the identity, since for any element $g \in P_1$, $g^{-1}\gamma(g)$ must act as the identity on T , and hence on \mathbb{R}^n . This cannot happen unless $g = \gamma(g)$ since $GL(n, \mathbb{R})$ 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 $\tilde{\beta} : E \rightarrow E$ as follows:

$$\begin{array}{ccccc} & & E & & \\ & \nearrow & & \searrow & \\ 1 & \rightarrow & \mathbb{R}^n & \rightarrow & P \rightarrow 1 \\ & \searrow & & \nearrow & \\ & & E & & \end{array}$$

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 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 (ii) \Rightarrow (i).

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 . \square

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 $1 \rightarrow T \rightarrow G \rightarrow P \rightarrow 1$ where $T \cong \mathbb{Z}^n$ and P is a finite group acting faithfully on T , up to equivalence by diagrams as in 5.5(ii).

Theorem 4.2.5. *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.

4.3 Classification of 2-dimensional spacegroups

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 . Thus we calculate $H^2(P, T)$.

As in 5.3 we may always assume that T is a subgroup of \mathbb{E}^n so that P acts as a group of orthogonal transformations of 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 4.3.1. *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 vector $u \in T$ of minimal length. If g is rotation through an angle θ then $t_u g^{-1} t_{-u}$ is rotation through $-\theta$ centered on u . Let $v = t_u g^{-1} t_{-u}(0)$. Now the vector $v - gu$ lies in T and points in the same direction as u . By minimality of u , $v - gu$ is an integer multiple of u and so $\theta = 0, \frac{\pi}{3}, \frac{\pi}{2}, \frac{2\pi}{3}$, or π .

\square

Draw picture, and do it with $g(u)$ and $g^{-1}(-u)$.

Corollary 4.3.2. *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 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. \square

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 $T_2 = \alpha T_1$ and $Q_2 = \alpha Q_1$. Since every finite group subgroup of $GL(n, \mathbb{R})$ is conjugate to a subgroup of $O(n)$ we have immediately the following result.

Proposition 4.3.3. *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

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 .

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.

Proposition 4.3.4. *The Bravais lattices in dimension 2 are given in the accompanying list.*

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. Choose a non-zero element of T that is closest to the origin. Clearly, up to linear transformation of \mathbb{E}^n , this could have been any non-zero 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. \square

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	$C_2 \times C_2$

TABLE: the Bravais Lattices in 2 dimensions.

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 4.3.5 (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. \square

Theorem 4.3.6. *The possible faithful actions of a finite group P on \mathbb{Z}^2 up to $\mathbb{Z}P$ -isomorphism are given on the accompanying table.*

Proof. We examine all the subgroups of the Bravais point groups. \square

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 g crystal class.

4.4 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.

For the remaining point groups we follow a general procedure that is due to Zassenhaus.

Theorem 4.4.1. *Let P be a finite group given by a presentation*

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

We will regard this presentation also as an exact sequence $1 \rightarrow R \rightarrow F \rightarrow P \rightarrow 1$ where F is the free group on g_1, \dots, g_d . Let T be a $\mathbb{Z}P$ -module such that $T \cong \mathbb{Z}^n$ as an abelian group, and let $\rho : P \rightarrow GL(n, \mathbb{Z})$ be the corresponding representation of P . Form the $nt \times nd$ matrix

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

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

$$r_i - 1 = \sum_{j=1}^d \frac{\partial r_i}{\partial g_j} (g_j - 1).$$

Now $\mathbb{Z}P^d$ is a free module, so homomorphisms $\phi : \mathbb{Z}P^d \rightarrow \mathbb{R}T$ biject with d -tuples (v_1, \dots, v_d) of elements of $\mathbb{R}T$, where v_i is the image of the i th basis vector of $\mathbb{Z}P^d$. The generators of R/R' have coordinates that are the rows of the matrix $\left(\frac{\partial r_i}{\partial g_j}\right)$, and so the images of the generators of R/R' form a t -tuple of vectors in $\mathbb{R}T$

$$\Lambda \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix} \in \mathbb{R}T^t.$$

From this we see that

$$X \cong \{\underline{x} \in \mathbb{R}T^d \mid \Lambda(\underline{x}) \in T^t\}.$$

In a similar way

$$\begin{aligned} \text{Hom}(IP, T) &\cong \{\phi : \mathbb{Z}P^d \rightarrow T \mid \phi(R/R') = 0\} \\ &= \{\underline{x} \in \mathbb{R}T^d \mid \Lambda(\underline{x}) = 0\} \\ &= \text{Ker } \Lambda \end{aligned}$$

and $\text{Hom}(\mathbb{Z}P^d, T) \cong T^d$. We conclude that

$$H^2(P, T) \cong \{\underline{x} \in \mathbb{R}T^d \mid \Lambda(\underline{x}) \in T^t\} / (\text{Ker } \Lambda + T^d).$$

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 since for a diagonal matrix $\text{diag}(b_1, \dots, b_q)$ we have

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

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

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

$$\Lambda = \begin{pmatrix} x+1 & 0 \\ 0 & y+1 \\ xy+1 & (xy+1)x \end{pmatrix} \begin{matrix} x \mapsto A \\ y \mapsto B \end{matrix}$$

$$= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

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

$$\begin{matrix} x^2 \mapsto \\ y^2 \mapsto \\ (xy)^2 \mapsto \end{matrix} \begin{matrix} \left\{ \begin{matrix} (0,0) \\ (0,0) \\ (0,0) \end{matrix} \right\} \\ \left\{ \begin{matrix} (0,1) \\ (0,0) \\ (0,0) \end{matrix} \right\} \\ \left\{ \begin{matrix} (0,0) \\ (1,0) \\ (0,0) \end{matrix} \right\} \\ \left\{ \begin{matrix} (0,1) \\ (1,0) \\ (0,0) \end{matrix} \right\} \end{matrix}$$

isomorphic extensions

where momentarily we represent vectors 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

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

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.

Proposition 4.4.3. *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 $N_{GL(T)}(P)$.*

I must sort out what is really going on with the conjugation action: it should send an extension by T to an extension by αT . Also, in listing the $\mathbb{Z}P$ -lattices I have ignored non-isomorphic lattices that differ by an automorphism of 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 $\beta : P \rightarrow P$ be conjugation by α . Let $1 \rightarrow R \rightarrow F \rightarrow P \rightarrow 1$ be a presentation of P and suppose the extension \mathcal{E} is represented by a homomorphism $f : R/R' \rightarrow T$, continuing with the previous notation. Lift β^{-1} to a homomorphism $F \rightarrow F$, and hence to a homomorphism γ as shown:

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

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

Proposition 4.4.4. *If \mathcal{E} is an extension represented by $f : R/R' \rightarrow T$ then the extension $\alpha\mathcal{E}$ is represented by ${}^\alpha f$.*

Proof. Consider the diagram

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

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 ${}^\alpha f$. \square

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 $H^2(P, T)$.

Chapter 5

Bibliography

- [1] E. Ascher & A. Janner, *Algebraic aspects of crystallography I & II*, Helv. Phys. Acta 38 (1965), 551-572, Commun. Math. Phys. 11 (1968/9), 138-167.
- [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 & 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] D.R. Farkas, *Crystallographic groups and their mathematics*, Rocky Mountain J. Math. 11 (1981), 511-551.
- [8] P.J. Hilton and U. Stambach, *A course in homological algebra*, Springer 1971.
- [9] R. Lyndon, *Groups and geometry*, LMS lecture notes in math. 101, Cambridge University Press 1985.
- [10] C.H. MacGillavry, *Symmetry aspects of M.C. Escher's periodic drawings*, Bohn, Scheltema & Holkema, Utrecht 1976.
- [11] S. MacLane, *Origins of the cohomology of groups*, Enseign. Math. 24 (1978), 1–29.
- [12] D. Schattschneider, *The plane symmetry groups: their recognition and notation*, Amer. Math. Monthly 85 (1978), 439-450.
- [13] R.L.E. Schwartzberger, *N-dimensional crystallography*, Pitman 1980.

- [14] C.A. Weibel, *An introduction to homological algebra*, Cambridge 1997.
- [15] J.A. Wolf, *Spaces of constant curvature*, 4th ed. Publish or Perish 1977.