An Introduction to the Cohomology of Groups

Peter J. Webb

0. What is group cohomology?

For each group G and representation M of G there are abelian groups $H_n(G, M)$ and $H^n(G, M)$ where $n = 0, 1, 2, 3, \ldots$, called the nth homology and cohomology of G with coefficients in M. To understand this we need to know what a *representation* of G is. It is the same thing as $\mathbb{Z}G$-module, but for this we need to know what the *group ring* $\mathbb{Z}G$ is, so some preparation is required. The homology and cohomology groups may be defined topologically and also algebraically.

We will not do much with the topological definition, but to say something about it consider the following result:

THEOREM (Hurewicz 1936). *Let X be a path-connected space with $\pi_n X = 0$ for all $n \geq 2$ (such X is called 'aspherical'). Then X is determined up to homotopy by $\pi_1(x)$.*

If $G = \pi_1(X)$ for some aspherical space X we call X an Eilenberg-MacLane space $K(G, 1)$, or (if the group is discrete) the classifying space BG. (It classifies principal G-bundles, whatever they are.)

If an aspherical space X is locally path connected the universal cover $\tilde{X}$ is contractible and $X = \tilde{X}/G$. Also $H_n(X)$ and $H^n(X)$ depend only on $\pi_1(X)$. If $G = \pi_1(X)$ we may thus define

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

and because X is determined up to homotopy equivalence the definition does not depend on X.

As an example we could take X to be d loops joined together at a point. Then $\pi_1(X) = F_d$ is free on d generators and $\pi_n(X) = 0$ for $n \geq 2$. Thus according to the above definition

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

Also, the universal cover of X is the tree on which F_d acts freely, and it is contractible.

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.

THEOREM (Eilenberg and MacLane 1953). *Given a group G there exists a connected CW complex X which is aspherical with $\pi_1(X) = G$.*

Algebraically, several of the low-dimensional homology and cohomology groups had been studied earlier than the topologically defined groups or the general definition of group cohomology. In 1904 Schur studied a group isomorphic to $H_2(G, \mathbb{Z})$, and this group is known as the *Schur multiplier* of G. In 1932 Baer studied $H^2(G, A)$ as a group of equivalence classes of extensions. It was in 1945 that Eilenberg and MacLane introduced an algebraic approach which included these groups as special cases. The definition is that

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

In order to deal with these definitions we need to know something about Ext and Tor.

Before studying these things, let us look at Baer's group of extensions. A *group extension* is a short exact sequence of groups

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

(so the image of A is normal in E, 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 which maps on to g. Then $a \mapsto {}^{\bar{g}}a = \bar{g}a\bar{g}^{-1}$ is the action of g on a. We check this action is well defined, giving a homomorphism $G \to \mathrm{Aut}(A)$, i.e. A is a representation of G.

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

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

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

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

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

for some homomorphism $\phi : E_1 \to E_2$. Such a homomorphism is necessarily an isomorphism (use 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. As a warning, it is possible to have non-equivalent extensions whose middle groups are isomorphic.

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

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

$i = 1, 2$, form

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

where

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

The bottom row is an extension of G by A called the *Baer sum* of the two extensions. We define the sum of the equivalence classes of the two extensions to be the equivalence class of their Baer sum. Under this operation $H^2(G, A)$ becomes an abelian group in which the zero element is the semidirect product. At this point these facts and the background justification that the Baer sum is well defined on equivalence classes, could be taken as an exercise. We will establish the group structure on $H^2(G, A)$ in a later section. We will also show as an example 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 $E \cong Q_8$.

1. 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).

(1.1) LEMMA. *Given a short exact sequence of R-modules*

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

the following are equivalent:

(i) there exists $\phi : B \to A$ such that $\phi\alpha = 1_A$,

(ii) there exists $\theta : C \to B$ such that $\beta\theta = 1_C$,

(iii) there is a commutative diagram

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

where i_1 is inclusion and π_2 is projection.

DEFINITION. If any of (i), (ii) or (iii) is satisfied we say the sequence $0 \to A \to B \to C \to 0$ is *split*. Also we say α is *split mono* and β is *split epi*.

(1.2) LEMMA. *Let A, B, C and M be left R-modules, N a right R-module.*

(i) If $A \to B \to C \to 0$ is exact then
$0 \to \mathrm{Hom}_R(C, M) \to \mathrm{Hom}_R(B, M) \to \mathrm{Hom}_R(A, M)$ *is exact and*
$N \otimes_R A \to N \otimes_R B \to N \otimes_R C \to 0$ *is exact.*

(ii) If $0 \to A \to B \to C$ is exact then
$0 \to \mathrm{Hom}_R(M, A) \to \mathrm{Hom}_R(M, B) \to \mathrm{Hom}_R(M, C)$ *is exact.*

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

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

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

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

(1.3) LEMMA. *The following are equivalent for an R-module P:*

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

There is a similar (dual) definition of an *injective* module, and:
I is injective if and only if $\mathrm{Hom}_R(\quad, I)$ is an exact functor.
Finally,
N is *flat* if and only if $N \otimes \_\_$ is an exact functor.
One easily sees that free modules R^n are flat, and hence projective modules are flat since they are summands of free modules.

DEFINITION. A *chain complex* is a sequence of modules

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

such that $d_i d_{i+1} = 0$ always. We may form the nth *homology group* of $\mathcal{M}$, which is $H_n(\mathcal{M}) = \mathrm{Ker}(d_n)/\mathrm{Im}(d_{n+1})$. A morphism of complexes $\phi : \mathcal{M} \to \mathcal{N}$ is a sequence of morphisms $\phi_i : M_i \to N_i$ such that

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

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

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

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

(1.4) PROPOSITION.

(i) *If ϕ and θ are homotopic then $H_n(\phi) = H_n(\theta) : H_n(\mathcal{M}) \to H_n(\mathcal{N})$.*
(ii) *If there are chain maps $\phi : \mathcal{M} \to \mathcal{N}$ and $\psi : \mathcal{N} \to \mathcal{M}$ with $\phi\psi \simeq 1_{\mathcal{N}}$ and $\psi\phi \simeq 1_{\mathcal{M}}$ then $H_n(\phi)$ and $H_n(\psi)$ are inverse isomorphisms on homology.*

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

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

Then there is an exact sequence

$$\begin{array}{ccccc} \operatorname{Ker}\alpha & \to & \operatorname{Ker}\beta & \to & \operatorname{Ker}\gamma \\ & & \omega & & \\ \operatorname{Coker}\alpha & \to & \operatorname{Coker}\beta & \to & \operatorname{Coker}\gamma \end{array}$$

Furthermore, if ϕ is mono so is $\operatorname{Ker}\alpha \to \operatorname{Ker}\beta$, *if θ' is epi so is* $\operatorname{Coker}\beta \to \operatorname{Coker}\gamma$.

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

DEFINITION. 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.

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

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

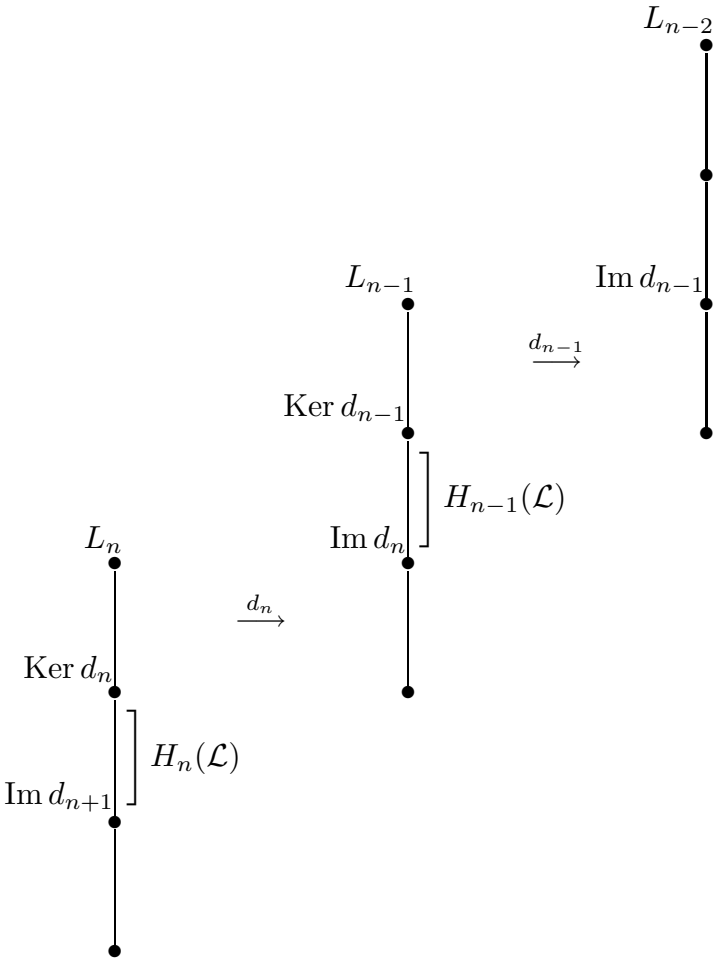
The 'connecting homomorphism' ω is natural, in the sense that a commutative diagram of chain complexes

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

with exact rows yields a commutative square

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

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



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

and columns of which are exact:

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

The naturality is an exercise. □

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

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

2. Ext and Tor

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

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

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

We may always construct resolutions of a module M as follows. Given M, choose a free module P_0 with $P_0 \to M$ and form the kernel K_0. Repeat this now with K_0 instead of M.

Given a second module N we may form the cochain complex

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

by applying $\mathrm{Hom}_R(\_\_, N)$ to $\mathcal{P}$. We now define

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

the nth homology group of this complex.

The above definition depends on the choice of resolution $\mathcal{P}$. It is the case that if we use another resolution we obtain Ext groups naturally isomorphic to the above. More of this later.

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

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

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

is exact by 1.2(i), and the result follows.

(2.2) THEOREM. *Let $0 \to A \to B \to C \to 0$ be exact and let M be another R-module. There are exact sequences*

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

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

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

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

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

At each level in the grading this sequence is

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

obtained by applying $\mathrm{Hom}_R(P_n, \_\_)$. We check that this gives a map of complexes. Since P_n is projective, $\mathrm{Hom}_R(P_n, \_\_)$ 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:

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

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

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

Proof. (1) If P is projective then $\cdots \to 0 \to P \to P \to 0$ is a projective resolution of P, so that the complex $\mathrm{Hom}_R(\mathcal{P}, M)$ is zero above degree 0 and hence so is its cohomology.

Conversely, if $\operatorname{Ext}^n_R(P,M)=0$ for all $n\geq 1$ then whenever we have a short exact sequence $0\to A\to B\to C\to 0$ the long exact sequence becomes

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

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

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

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

(2.4) COROLLARY. *Let $0\to A\to B\to C\to 0$ be a short exact sequence of R-modules.*
(1) If B is projective then $\operatorname{Ext}^n_R(C,M)\cong \operatorname{Ext}^{n-1}_R(A,M)$ for all modules M, provided $n\geq 2$.
(2) If B is injective then $\operatorname{Ext}^{n-1}_R(C,M)\cong \operatorname{Ext}^n_R(A,M)$ for all modules M, provided $n\geq 2$.

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

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

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

The process of changing the degree of an Ext group at the expense of changing the module as indicated in the above corollary is known as *dimension shifting*. The next result is an important tool in computing Ext groups.

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

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

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

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

By dimension shifting we have

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

□

As an example, we calculate that if M is an abelian group and d an integer then $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/d\mathbb{Z}, M) \cong M/dM$.

(2.6) THEOREM. *Let $\mathcal{P} \to M$ and $\mathcal{Q} \to N$ be projective resolutions of R-modules M and N. Every homomorphism $\phi : M \to N$ 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 liftings are chain homotopic.

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

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

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

We remark also that $Ext^n_R(M, N)$ can also be defined by taking an injective resolution $N \to \mathcal{I}$ of N and forming $H_n(\mathrm{Hom}_R(M, \mathcal{I}))$. It is a theorem that we get a group which 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. Let M be a left R-module, N a right R-module, and $\mathcal{P} \to N$ a resolution of N by projective right modules. We put

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

which is the nth homology of the complex

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

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

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

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

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

and

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

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

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

Remarks. (i) In particular $\mathrm{Tor}_n^R(N, M) = 0$ if M or N is projective, because projective implies flat.

(ii) This allows 'dimension shifting' analogous to that for Ext.

Let

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

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

(2.11) PROPOSITION. *There is an exact sequence*

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

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

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

3. Group Cohomology

Let G be a group and let $\mathbb{Z}G$ be its *integral group ring*. This means that as an additive group $\mathbb{Z}G$ is the free abelian group with the elements of G as a basis, and multiplication within the ring is determined by multiplication of the basis elements, which is multiplication in G. A typical element of $\mathbb{Z}G$ is a formal sum $\sum_{x\in G}\lambda_x x$ with $\lambda_x \in \mathbb{Z}$, where all but finitely many λ_x are zero. The formula for multiplication of two general elements is

$$(\sum_{x\in G}\lambda_x x)(\sum_{y\in G}\mu_y y) = \sum_{x,y\in G}(\lambda_x\lambda_y)xy.$$

Specifying a $\mathbb{Z}G$-*module* M is the same thing as specifying an abelian group M on which G acts, i.e. there is a homomorphism $G \to \mathrm{Aut}(M)$. We denote by $\mathbb{Z}$ the $\mathbb{Z}G$-module which is $\mathbb{Z}$ as an additive group, and where the action of G is trivial, i.e. $gn = n$ for all $n \in \mathbb{Z}$ and $g \in G$. This defines the (left) *trivial module*, the right trivial module being defined similarly.

We define $H^n(G, M) := \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, M)$ to be the *nth cohomology group* of G with coefficients in the left $\mathbb{Z}G$-module M, and $H_n(G, M) := \mathrm{Tor}_n^{\mathbb{Z}G}(M, \mathbb{Z})$ to be the *nth homology group* of G with coefficients in the right $\mathbb{Z}G$-module M.

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

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

We now start to explore these cohomology groups by identifying them in low degrees and by construction of some particular resolutions of $\mathbb{Z}$. We define a mapping $\epsilon : \mathbb{Z}G \to \mathbb{Z}$

by the assignment $g \mapsto 1$ for every $g \in G$, extended by linearity to the whole of $\mathbb{Z}G$. Thus the effect of ϵ on a general element of $\mathbb{Z}G$ is

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

This is the *augmentation map* and it is a ring homomorphism, and also a homomorphism of $\mathbb{Z}G$-modules. We write $IG := \operatorname{Ker}\epsilon$ 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 $gm - m$, $m \in M$, $g \in G$.

(3.1) PROPOSITION. *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) $H^0(G, M) = \operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M) \cong M^G$. The fixed point set M^G coincides with the set of elements of M annihilated by IG.
(3) $H_0(G, M) = \mathbb{Z} \otimes_{\mathbb{Z}G} M \cong M/(IG \cdot M) = M_G$ is the largest quotient of M on which G acts trivially.
(4) $(\mathbb{Z}G)_G = \mathbb{Z}G/IG \cong \mathbb{Z}$. If G is finite then $(\mathbb{Z}G)^G = \mathbb{Z} \cdot N \cong \mathbb{Z}$, while if G is infinite then $(\mathbb{Z}G)^G = 0$.
(5) If $G = \langle g_1, \ldots, g_n\rangle$ then $g_1 - 1, \ldots, g_n - 1$ generate IG as a $\mathbb{Z}G$-module.

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

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

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

(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 $u_1u_2\cdots u_t$ where each u_i is either one of the given generators or its inverse. Now

$$u_1u_2\cdots u_t - 1 = u_1u_2\cdots u_{t-1}(u_t - 1) + u_1u_2\cdots u_{t-2}(u_{t-1} - 1) + \cdots + (u_1 - 1)$$

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. □

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

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

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

getting an exact sequence

$$0 = H^1(G, \mathbb{Z}G) \to H^1(G, \mathbb{Z}) \to \mathbb{Z} \otimes_{\mathbb{Z}G} IG \to \mathbb{Z} \otimes_{\mathbb{Z}G} \mathbb{Z}G \to \mathbb{Z} \otimes_{\mathbb{Z}G} \mathbb{Z} \to 0.$$

The left term is zero since $\mathbb{Z}G$ is projective and hence flat. The two right terms identify as $\mathbb{Z} \to \mathbb{Z}$ via the identity map, so we deduce that $H^1(G, \mathbb{Z}) \cong \mathbb{Z} \otimes_{\mathbb{Z}G} IG \cong IG/(IG)^2$.

We now construct an isomorphism $G/G' \to IG/(IG)^2$. We will write elements of G/G' multiplicatively as cosets gG' and elements of $IG/(IG)^2$ additively as cosets $x + IG^2$. Consider the mapping $G \to IG/(IG)^2$ specified by $g \mapsto (g - 1) + IG^2$. It sends a product gh to $gh - 1 + IG^2 = (g - 1)(h - 1) + (g - 1) + (h - 1) + IG^2 = (g - 1) + (h - 1) + IG^2$, 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 $G/G' \to IG/(IG^2)$. An inverse homomorphism is constructed as follows. First consider the homomorphism of abelian groups $IG \to G/G'$ specified on the basis elements of IG by $(g-1) \mapsto gG'$. It sends a product $(g-1)(h-1) = (gh-1) - (g-1) - (h-1)$ to $(gh)(g^{-1})(h^{-1})G' = G'$ and hence induces a homomorphism $IG/(IG^2) \to G/G'$. Evidently these two mappings are mutually inverse. □

(3.3) EXAMPLE. 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

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

so that this is a projective resolution of $\mathbb{Z}$. We see various things from this:

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

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

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

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

In the above example we see the connection between the topological approach to group (co)homology as the (co)homology of an aspherical space with fundamental group G, and the algebraic approach which 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 which 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.

(3.5) THEOREM. *Let $G = \langle g \rangle$ be a finite cyclic group. There is a periodic resolution*

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

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 $\operatorname{Ker} d_1 = \mathbb{Z} \cdot N \cong \mathbb{Z}$. We now iterate this start of the resolution. □

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

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

and

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

For example, If G is cyclic of order n and $M = \mathbb{Z}$ then $H^1(G, \mathbb{Z}) = 0$ and $H^2(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$, while if $M = \mathbb{Z}/n\mathbb{Z}$ then $H^1(G, \mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$ and $H^2(G, \mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$.

Proof. We apply $\operatorname{Hom}_{\mathbb{Z}G}(-M)$ to the resolution in 3.5 to get a complex

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

where N and $g - 1$ denote the maps which 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). □

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

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.

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

Proof. 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 $g, h \in G$. □

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

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

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

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

(3.9) COROLLARY. *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 $f : X \to M$ extends uniquely to a derivation $d : F \to M$. This is because the mapping $X \to M \rtimes F$ given by $x \mapsto (f(x), x)$ extends uniquely to a group homomorphism $F \to M \rtimes F$ of the form $g \mapsto (d(g), g)$ for some uniquely specified derivation d. We deduce that the mapping $(x-1) \mapsto f(x)$ where $x \in X$ extends uniquely to a $\mathbb{Z}F$-module homomorphism $IF \to M$, by 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. □

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

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

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

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

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

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

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

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.

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

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

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

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

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

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 $1 \to G \to G \to 1 \to 1$.

Proof. We note that $IK \cdot IE = IK \cdot \mathbb{Z}E \cdot IE = \overline{IK} \cdot IE$ and 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

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

where the lower sequence is exact by the snake lemma. Since $IK \cdot IE \subseteq \overline{IK}$, 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

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

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

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

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

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

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

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

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

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

The $\mathbb{Z}G$-module R/R' arising from the presentation of G is called the *relation module* associated to the presentation. If the presentation is determined by generators $G = \langle g_1, \ldots, g_n \rangle$ then the mapping $\mathbb{Z}G^{d(F)} \to IG$ sends the ith 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 $\mathbb{Z}F^{d(F)} \to IF$ is an isomorphism, thereby confirming Corollary 3.9.

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

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

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 $1 + x + \cdots + x^{n-1}$. 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 3.5.

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.

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

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

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

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

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

It remains to observe that $\mathrm{Hom}_{\mathbb{Z}G}(IF/(IR \cdot IF), M) = \mathrm{Hom}_{\mathbb{Z}G}(IF, M) = \mathrm{Der}(F, M)$ 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. □

(3.17) THEOREM. *Let M be a $\mathbb{Z}G$-module. There is a bijection*

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

Proof. We use the short exact sequence

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

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

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

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

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

using the fact that IR acts as 0 on M, and by Lemma 3.7. Hence two homomorphisms $\theta, \theta' : R/R' \to M$ represent the same element of $H^2(G, M)$ if and only if they differ by the restriction of a derivation from F to M.

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

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

where $E = M \rtimes F/R'/\{(-\theta(rR'), rR') \mid r \in R\}$. The map η is determined by $x \mapsto (0, x)$ and the map $M \to E$ is determined by $m \mapsto (m, 1)$. We check that the left hand square

commutes. We now exploit the fact that in any two such commutative diagrams with the same map θ and the same top row, the bottom row is determined up to equivalence.

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

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

commutes.

We next define a mapping

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

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

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

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

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

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

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

Evidently ϕ and ψ are mutually inverse. $\square$

REMARKS: (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 $H^2(G, M) \cong \mathrm{Ext}^1_{\mathbb{Z}G}(IG, M)$, so that group extensions of G correspond to module extensions of IG. This correspondence is the one we have already seen in Proposition 3.13.

(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 which is relevant in this situation and we may call it the *explicit pushout*.

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

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

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

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

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

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

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

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

since we are now dealing with modules with trivial action.

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 $0 \to R/R' \to \mathbb{Z}G^2 \to IG \to 0$, 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 $0 \to \mathbb{F}_2\otimes R/R' \to \mathbb{F}_2G^2 \to \mathbb{F}_2\otimes IG \to 0$ 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 $\phi : R/R' \to \mathbb{F}_2$, and there are 8 possibilities given by the values of ϕ on the generators. Given such a ϕ the corresponding extension is $1 \to \mathbb{F}_2 \to F/R' \,/\, \operatorname{Ker}\phi \to G \to 1$. This is because this extension appears in a commutative diagram

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

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

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

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

In general a presentation for an extension $1 \to M \to E \to G \to 1$ is obtained by taking a presentation of M as a group, adjoining generators for G and imposing relations which define the module action of G on M, and finally adjoining relators which 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 which arise in this general procedure.

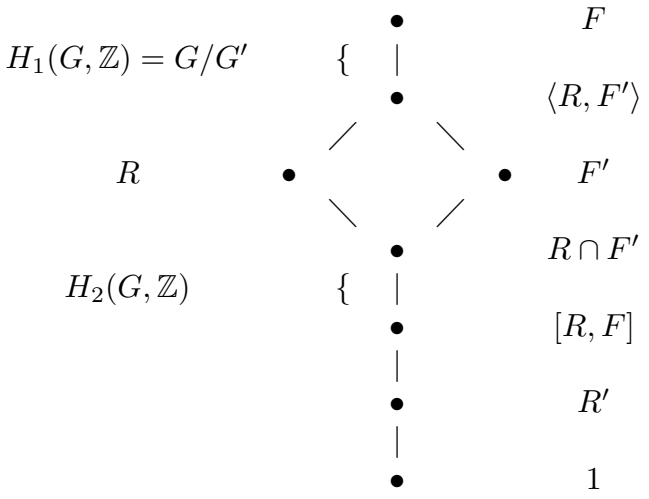
We turn attention to the *Schur multiplier* of G, which we may define to be $H_2(G, \mathbb{Z})$. When G is finite there are isomorphisms

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

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 $k \in K$.

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

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 $0 \to \overline{IR}/(IR \cdot IF) \to IF/(IR \cdot IF) \to IG \to 0$ to compute $H_2(G, \mathbb{Z})$. After applying $\mathbb{Z} \otimes_{\mathbb{Z}G} -$ to it we obtain

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

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

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

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

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

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

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

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

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

(3.21) PROPOSITION. *Let $1 \to M \to E \to G \to 1$ be a central group extension. Then*

(1) in any commutative diagram of groups

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

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

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

We say that a central extension $1 \to M \to E \to G \to 1$ is a *stem extension* if $M \subseteq E'$ (or equivalently if $E/E' \to G/G'$ 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.

(3.22) PROPOSITION. *Let G be a perfect group. A central extension $1 \to M \to E \to G \to 1$ is stem if and only if E is perfect.*

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

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

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

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

Proof. Let $1 \to R \to F \to G \to 1$ be a presentation of G. The extension with the special property we seek is in fact $1 \to R \cap F'/[R,F] \to F'/[R,F] \to G' = G \to 1$ 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

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

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

The group $\hat{G}$ is 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 $H^2(G, \mathbb{Z})$.

(3.24) PROPOSITION. *Let G be a perfect group and $1 \to M \to E \to G \to 1$ 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 $\hat{E} \to E \to G$. An argument similar to the snake lemma applied to the diagram

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

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

We show that $K \leq \zeta(\hat{E})$. 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 $1 \to K \to \hat{E} \to G \to 1$ is a covering of G.

Now by universality of E we have a commutative diagram

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

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

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.

(3.25) PROPOSITION. *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 $d(H_2(G, \mathbb{Z})) \leq r - d$.*

(3.26) EXAMPLE. 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 mulitpliers are 0. Furthermore $SL(2, 5)$ is perfect (the abelianization may be computed from the presentation), and since there is a short exact sequence $1 \to C_2 \to SL(2, 5) \to A_5 \to 1$ 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.

4. Finite Groups

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

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

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

Proof. Let

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

be a projective resolution of A, so that

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

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

The argument for Tor is similar. □

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

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

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

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

Proof. Since multiplication $|G| : M \to M$ is an isomorphism, so is $|G| : H^n(G, M) \to H^n(G, M)$ by functoriality of cohomology. This map is zero if $n \geq 1$, by Proposition 4.2, so it follows that $H^n(G, M) = 0$ if $n \geq 1$. The argument with $H_n(G, M)$ is similar. □

(4.5) COROLLARY. *(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 $\mathbb{R}^\times_{>0} \times S^1$ via the correspondence $z \leftrightarrow (|z|, \arg(z))$. We thus have a short exact sequence $1 \to \mathbb{Z} \to \mathbb{R}^\times_{>0} \times \mathbb{R}^+ \to \mathbb{C}^\times \to 1$. Because $\mathbb{R}^\times_{>0} \cong \mathbb{R}^+$ via the natural logarithm, the term in the middle of this sequence is uniquely divisible and now the long exact sequence associated to the exact sequence gives the result. □

We present an application of this and a result known as the integral duality theorem which 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.

(4.6) COROLLARY (Schur-Zassenhaus). *Let $1 \to M \to E \to G \to 1$ be a short exact sequence of finite groups where g.c.d.$(|M|, |G|) = 1$. Then the extension is split, $E \cong M \rtimes G$, 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. □

Let C be an abelian group. We will call any module of the form $\mathbb{Z}G \otimes_{\mathbb{Z}} C$ an *induced module*, and any module of the form $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, C)$ a coinduced module. The latter is made into a $\mathbb{Z}G$-module using the right action on $\mathbb{Z}G$.

(4.7) LEMMA. *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 $M = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, C)$ for some abelian group C we compute cohomology with coefficients in M by applying the functor $\mathrm{Hom}_{\mathbb{Z}G}(-, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, C))$ to a projective resolution and taking homology. Now for any module P we have a natural isomorphism $\mathrm{Hom}_{\mathbb{Z}G}(P, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, C)) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G \otimes_{\mathbb{Z}G} P, C) \cong \mathrm{Hom}_{\mathbb{Z}}(P, C)$ and when we apply the functor $\mathrm{Hom}_{\mathbb{Z}}(-, C)$ 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. □

(4.8) PROPOSITION. *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 $\mathbb{Z}G \otimes_{\mathbb{Z}} C \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, C)$ by $g \otimes c \mapsto \phi_{(g,c)}$ where $\phi_{(g,c)} : \mathbb{Z}G \to C$ is the homomorphism determined by

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

We check that this is a homomorphism of $\mathbb{Z}G$-modules which 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. □

(4.9) COROLLARY. *Let C be an abelian group. Any group extension*

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

with G finite must split, 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. □

5. Crystallography

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 $\mathbb{E}^n \to \mathbb{E}^n$, 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:

(a) 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 $\mathbb{E}^n$.

(b) 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 $\mathbb{E}^n \lhd R(n)$ 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

(i) Among the rigid motions of $\mathbb{E}^n$ which send $\mathcal{C} \to \mathcal{C}$, there exist n linearly independent translations.

(ii) 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 $\mathbb{E}^n \to \mathbb{E}^n$ which 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 $1 \to T \to S(\mathcal{C}) \to P \to 1$ 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 $\mathbb{E}^n$.

(5.1) LEMMA. *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 $\mathbb{E}^n$ which 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 $v \in X$ which 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 $v_1 + \langle v \rangle, \ldots, v_{n-1} + \langle v \rangle$. Now $v_1, \ldots, v_{n-1}, v$ 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 which acted trivially would also act trivially on $\mathbb{E}^n$.

Let $T = \langle t_1, \ldots, t_n \rangle$. We write the set of all images of these generators under the action of P as $P\{t_1, \ldots, t_n\}$, 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 $|P| < \infty$. □

(5.2) PROPOSITION. *G is a space group in dimension n if and only if G is a discrete subgroup of $R(n)$ which 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 which 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 $s = g \in G$. □

(5.3) THEOREM. *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

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

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 $\mathbb{R}^n$ which is preserved by P. This is done by taking any inner product $\langle \quad , \quad \rangle_1$ and defining

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

Now P acts orthogonally, so there exists an isomorphism $\sigma : \mathbb{R}^n \to \mathbb{E}^n$ and a map $\tau : P \to$

$O(n)$ such that $\sigma(g \cdot v) = \tau(g) \cdot \sigma(v)$. The diagram

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

may thus be completed to a commutative diagram by a map $\mathbb{R}^n \rtimes P \to R(n)$, 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 $G \cap \mathbb{E}^n \cong \mathbb{Z}^n$. □

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

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

is exact and XT/T is a subgroup of P which 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 $\mathbb{Z}^n$. □

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.

(5.5) PROPOSITION. *Let* $1 \to T_1 \to G_1 \to P_1 \to 1$ *and* $1 \to T_2 \to G_2 \to P_2 \to 1$ *be space groups acting on* $\mathbb{E}^n$. *The following are equivalent.*

(i) The space groups are equivalent.

(ii) There exists a commutative diagram

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

(iii) $G_1 \cong G_2$ *as abstract groups.*

Proof. (i) $\Rightarrow$ (iii) is clear.

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

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

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

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

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

In this manner we may assume that $T_i \leq \mathbb{R}^n$ and $P_i \leq O(n)$ for $i = 1, 2$. Since both T_1 and T_2 contain a basis of $\mathbb{R}^n$ they are conjugate within $GL(n, \mathbb{R})$, and so after applying such a conjugation we may assume $T_1 = T_2 = T$, say. Now $\gamma : P_1 \to P_2$ 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 $O(n)$ acts faithfully on $\mathbb{R}^n$. We write P for the group $P_1 = P_2$. Let E denote the preimage of P in $\mathbb{R}^n \rtimes O(n)$, so that β extends to an automorphism $\tilde{\beta} : E \to E$ as follows:

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

We show that $\tilde{\beta}$ is conjugation by some translation in $\mathbb{R}^n$. Firstly, both extensions here split, because $H^2(P, \mathbb{R}^n) = 0$; and now $\tilde{\beta}$ is conjugation by an element of $\mathbb{R}^n$ since $H^1(P, \mathbb{R}^n) = 0$. Since β is the restriction of $\tilde{\beta}$ it is also given by conjugation by an element of $\mathbb{R}^n$. (It is possible to give a geometric argument for this conjugation, assuming splitting of the extensions. If C is a complement to $\mathbb{R}^n$ in E then $\tilde{\beta}(C)$ is another complement, and both may be regarded as groups of orthogonal transformations with different vectors $u, v \in \mathbb{E}^n$ taken to be the origin. Now conjugation by the translation from u to v induces $\tilde{\beta}$, and hence β.) □

As a summary of the results so far, we have now shown that to classify space groups of dimension n up to affine equivalence it is equivalent to classify extensions $1 \to T \to G \to P \to 1$ where $T \cong \mathbb{Z}^n$ and P is a finite group acting faithfully on T, up to equivalence by diagrams as in 6.5(ii).

THEOREM. *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.

Classification of 2-dimensional spacegroups.

We must determine:
(i) the finite groups P with a faithful action on $\mathbb{Z}^2$, i.e. the finite subgroups of $GL(2, \mathbb{Z})$,
(ii) 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 wither T or T',
(iii) the possible extensions for each P and T. Thus we calculate $H^2(P, T)$.

As in 6.3 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.

(5.6) LEMMA. *If g is an automorphism of T of finite order then g has order 1, 2, 3, 4 or 6.*

Proof. We may suppose that g acts as an orthogonal transformation of T, and 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.

□

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

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

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

(5.8) PROPOSITION. *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 which 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. □

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.

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

The attribution of this corollary is given by Hermann Weyl in his book 'Symmetry'.

(5.10) THEOREM. *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. □

At this point we mention a further piece of terminology, which 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 which 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 which arises by grouping together all those space groups with the same point group P and such that the $\mathbb{Q}P$-modules $\mathbb{Q} \otimes_{\mathbb{Z}} T$ are isomorphic. We obtain in this way a *geometric crystal class* of space groups. For example in dimension 2, pm and pg constitute an arithmetic crystal class, and cm is also in the same geometric crystal class.

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 which is due to Zassenhaus.

(5.11) THEOREM. *Let P be a finite group given by a presentation*

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

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

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

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

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

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

In connection with this result we recall the following theorem of H.J.S. Smith from 1861, which is equivalent to the structure theorem for finitely generated abelian groups.

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

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

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

Proof of 5.11. We embed T in the n-dimensional real vector space $\mathbb{R}T = \mathbb{R} \otimes_{\mathbb{Z}} T$, which becomes a $\mathbb{Z}P$-module through the action on T. Since $\mathbb{R}$ is uniquely divisible, we have $H^2(P, \mathbb{R}T) = 0$. From the resolution

$$\begin{array}{ccccccccccc} \mathbb{Z}P^t & & \to & & \mathbb{Z}P^d & & \to & & \mathbb{Z}P & \to & \mathbb{Z} & \to & 0 \\ & \searrow & & \nearrow & & \searrow & & \nearrow & & & & & \\ & & R/R' & & & & IP & & & & & & \end{array}$$

we obtain the following commutative diagram in which the rows are the sequences used to calculate $H^2(P,T)$ and $H^2(P,\mathbb{R}T) = 0$:

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

All the rows and columns here are exact and β is injective. We see that α is surjective. Let

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

Then

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

is exact, and so the composite surjection $X \to \mathrm{Hom}(R/R', T) \to H^2(P, T)$ has kernel $\beta(\mathrm{Hom}(IP, \mathbb{R}T)) + \mathrm{Hom}(\mathbb{Z}P^d, T)$.

Now $\mathbb{Z}P^d$ is a free module, so homomorphisms $\phi : \mathbb{Z}P^d \to \mathbb{R}T$ biject with d-tuples $(v_1, \ldots, v_d)$ of elements of $\mathbb{R}T$, where v_i is the image of the ith basis vector of $\mathbb{Z}P^d$. The generators of R/R' have coordinates which the 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

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

In a similar way

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

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

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

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

$$\{\underline{x} \in \mathbb{Z}^q \;\big|\; b_i x_i \in \mathbb{Z} \text{ for all } i\}/\mathbb{Z}^q = (\oplus \frac{1}{b_i}\mathbb{Z})/\mathbb{Z}^q = \oplus \mathbb{Z}/b_i\mathbb{Z}$$

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

Example. Let $P = \langle x, y \;\big|\; x^2 = y^2 = (xy)^2 = 1\rangle$ 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

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

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

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

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

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 which are equivalent as space groups? It happens if and only if there is a commutative diagram

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

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 extension, 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.

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

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

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

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

(5.14) PROPOSITION. *If $\mathcal{E}$ is an extension represented by f then the extension $\alpha\mathcal{E}$ is represented by ${}^{\alpha}f$.*

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

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

BIBLIOGRAPHY

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.

H. Brown, R. Bülow, J. Neubüser, H. Wondratschek & H. Zassenhaus, *Crystallographic groups of four-dimensional space,* Wiley 1978.

J. Burkhardt, *Die Bewegungsgruppen der Kristallographie,* 2nd ed. Birkhäuser, Basel 1966.

D.R. Farkas, *Crystallographic groups and their mathematics,* Rocky Mountain J. Math. 11 (1981), 511-551.

R. Lyndon, *Groups and geometry*, LMS lecture notes in math. 101, Cambridge University Press 1985.

C.H. MacGillavry, *Symmetry aspects of M.C. Escher's periodic drawings*, Bohn, Scheltema & Holkema, Utrecht 1976.

D. Schattschneider, *The plane symmetry groups: their recognition and notation*, Amer. Math. Monthly 85 (1978), 439-450.

R.L.E. Schwartzenberger, *N-dimensional crystallography*, Pitman 1980.

J.A. Wolf, *Spaces of constant curvature*, 4th ed. Publish or Perish 1977.