Group Cohomology *

Zhiyuan Bai

Compiled on March 14, 2023

This document serves as a set of revision materials for the Cambridge Mathematical Tripos Part III course *Group Cohomology* in Lent 2023. However, despite its primary focus, readers should note that it is NOT a verbatim recall of the lectures, since the author might have made further amendments in the content. Therefore, there should always be provisions for errors and typos while this material is being used.

Contents

1 Cohomology of Groups

1.1 The Basics

Let G be a group.

*Based on the lectures under the same name taught by Dr. C. J. B. Brookes in Lent 2023.

Definition 1.1. The integral group ring is the free abelian group on the letters of G equipped with the obvious multiplication

$$\left(\sum_h n_h h\right)\left(\sum_k n_k k\right) = \sum_g \left(\sum_{hk=g} n_h n_k\right) g.$$

Definition 1.2. A (left) $\mathbb{Z}G$-module M is an abelian group equipped with an action $\mathbb{Z}G \times M \to M, (r,m) \mapsto rm$ such that $1m = m$, $r(m_1+m_2) = rm_1+rm_2$ and $r_1(r_2m) = (r_1r_2)m$.

A trivial $\mathbb{Z}G$-module is one where the action of G is trivial, i.e. $gm = m$ for all $g \in G, m \in M$. We call the trivial module structure on $M = \mathbb{Z}$ "the" trivial $\mathbb{Z}G$-module.

Definition 1.3. The free $\mathbb{Z}G$-module $\mathbb{Z}G\{X\}$ on X is the set of finite formal sums of letters in X with coefficients in $\mathbb{Z}G$, with the obvious addition and $\mathbb{Z}G$-action.

Submodules and quotients are defined in the standard way.

Definition 1.4. A $\mathbb{Z}G$-map (or a $\mathbb{Z}G$-morphism) $\alpha : M_1 \to M_2$ between $\mathbb{Z}G$-modules is a map of abelian groups such that $\alpha(rm) = r\alpha(m)$. We write $\mathrm{Hom}_G(M_1, M_2)$ to denote the abelian group (in fact $\mathbb{Z}G$-module) of $\mathbb{Z}G$-maps $M_1 \to M_2$.

Example 1.1. 1. We have the augmentation map $\epsilon : \mathbb{Z}G \to \mathbb{Z}$, where $\mathbb{Z}G$ is viewed as a $\mathbb{Z}G$-module via ring multiplication and $\mathbb{Z}$ is the trivial $\mathbb{Z}G$-module. It is defined by $\sum_g a_g g \mapsto \sum_g a_g$. It is both a $\mathbb{Z}G$-map and a ring map.
2. Regard $\mathbb{Z}G$ as a $\mathbb{Z}G$-module again. Then $\mathrm{Hom}_G(\mathbb{Z}G, M) \cong M$ via $\alpha \mapsto \alpha(1)$. In particular, if we take $M = \mathbb{Z}G$, then we see $\mathrm{Hom}_G(\mathbb{Z}G, \mathbb{Z}G) \cong \mathbb{Z}G$, and $\alpha \in \mathrm{Hom}_G(\mathbb{Z}G, \mathbb{Z}G)$ is multiplication on the right by $\alpha(1)$.

Definition 1.5. If $f : M_1 \to M_2$ is a $\mathbb{Z}G$-map and N is a $\mathbb{Z}G$-module, then the dual map of f (relative to N) is $f^* : \mathrm{Hom}_G(M_2, N) \to \mathrm{Hom}_G(M_1, N), \alpha \mapsto \alpha \circ f$. Similarly, for a $\mathbb{Z}G$-map $f : N_1 \to N_2$ and a $\mathbb{Z}G$-module M, the induced map of f relative to M is $f_* : \mathrm{Hom}_G(M, N_1) \to \mathrm{Hom}_G(M, N_2), \alpha \mapsto f \circ \alpha$.

Example 1.2. Consider the case of an infinite cyclic group $G = \langle t \rangle \cong \mathbb{Z}$ which acts on $\mathbb{R}$ by translation. Consider $\mathbb{R}$ as a graph with vertices V at the integers and edges E between adjascent integers. Write v_0 to denote the vertex at 0 and e the edge connecting 0 to 1. Then $\mathbb{Z}V \cong \mathbb{Z}G\{v\}, \mathbb{Z}E \cong \mathbb{Z}G\{e\}$ are both free $\mathbb{Z}G$-modules, and there is a $\mathbb{Z}G$-map $\mathbb{Z}V \to \mathbb{Z}$ corresponding to the augmentation map.

Definition 1.6. A chain complex $M_\bullet$ of $\mathbb{Z}G$-modules is a sequence

$$M_s \xrightarrow{d_s} M_{s-1} \xrightarrow{d_{s-1}} \cdots \xrightarrow{d_{t+1}} M_{t+1} \xrightarrow{d_t} M_t$$

such that $d_n d_{n+1} = 0$ for all $t < n < s$.
$M_\bullet$ is exact at M_n if $\mathrm{Im}\, d_{n+1} = \ker d_n$, and it is exact if it is exact at every M_n.

We allow exact sequences to go on forever on either side.

Definition 1.7. The homology of the chain complex $M_\bullet$ is given by $H_s(M_\bullet) = \ker d_s$, $H_t(M_\bullet) = M_t/\operatorname{Im} d_{t+1}$ and $H_n(M_\bullet) = \ker d_n/\operatorname{Im} d_{n+1}$.

Definition 1.8. A short exact sequence is an exact chain complex of the form

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

Example 1.3. Take $G = \langle t \rangle \cong \mathbb{Z}$ again. We have a short exact sequence

$$0 \longrightarrow \mathbb{Z}G \xrightarrow{t-1} \mathbb{Z}G \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

which can be interpreted as the sequence

$$0 \longrightarrow \mathbb{Z}E \xrightarrow{t-1} \mathbb{Z}V \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

as in Example 1.2.

1.2 Resolutions

Definition 1.9. A $\mathbb{Z}G$-module P is projective if, whenever there is a surjective $\mathbb{Z}G$-map $M_1 \to M_2$ and a $\mathbb{Z}G$-map $P \to M_2$, there exists a map $P \to M_1$ making the diagram

$$\begin{array}{ccccc} & & P & & \\ & \overset{\exists}{\swarrow} & \downarrow & & \\ M_1 & \longrightarrow & M_2 & \longrightarrow & 0 \end{array}$$

commute.

If we have a short exact sequence

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

Then can form a chain complex

$$0 \longrightarrow \operatorname{Hom}_G(P, M_1) \longrightarrow \operatorname{Hom}_G(P, M_2) \longrightarrow \operatorname{Hom}_G(P, M_3) \longrightarrow 0$$

which is always exact except at $\operatorname{Hom}_G(P, M_3)$. P is projective if and only if this sequence is always exact at $\operatorname{Hom}_G(P, M_3)$ too.

Lemma 1.1. *Free modules are projective.*

Proof. Suppose we have $\alpha : M_1 \to M_2$ surjective and $\beta : \mathbb{Z}G\{X\} \to M_2$. For each $x \in X$, there is some $m_x \in M_1$ such that $\alpha(m_x) = \beta(x)$ by surjectivity. Then define $\bar{\beta} : P \to M_1$ via $\bar{\beta}(\sum_x r_x x) = \sum_x r_x m_x$. □

Definition 1.10. A projective (resp. free) resolution of $\mathbb{Z}$ is an exact sequence

$$\cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

with all P_i projective (resp. free).

Example 1.4. 1. Take $G = \langle t \rangle \cong \mathbb{Z}$ again. Then

$$0 \longrightarrow \mathbb{Z}G \xrightarrow{t-1} \mathbb{Z}G \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

is a free resolution of $\mathbb{Z}$.
2. Suppose $G = \langle t \rangle \cong \mathbb{Z}/n\mathbb{Z}$. Then a free resolution of $\mathbb{Z}$ is given by

$$\cdots \longrightarrow \mathbb{Z}G \xrightarrow{\beta} \mathbb{Z}G \xrightarrow{\alpha} \mathbb{Z}G \xrightarrow{\beta} \mathbb{Z}G \xrightarrow{\alpha} \mathbb{Z}G \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

where $\alpha(x) = x(t-1)$ and $\beta(x) = x(1 + t + \cdots + t^{n-1})$.

Suppose X is a connected simplicial complex, G its fundamental group and $\tilde{X}$ its universal cover which is contractible. Then X contains information about G. We will try to replicate the study of (co)homology of X when studying G algebraically.
Suppose we have a partial free or projective resolution

$$P_s \xrightarrow{d_s} \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

of $\mathbb{Z}$. Write $X_{s+1} = \ker d_s$ and $P_{s+1} = \mathbb{Z}G\{X_{s+1}\}$. The natural map $d_{s+1} : P_{s+1} \to P_s$ gives rise to a slightly longer partial resolution

$$P_{s+1} \xrightarrow{d_{s+1}} P_s \xrightarrow{d_s} \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

This is not quite nice, since P_{s+1} could very often have infinite rank. But we can replace $\mathbb{Z}G\{X_{s+1}\}$ with $\mathbb{Z}G\{S\}$ with S generating X_{s+1}. This way, if X_{s+1} is finitely generated then P_{s+1} would have finite rank.

Definition 1.11. *G is of type FP_n if the trivial $\mathbb{Z}G$-module $\mathbb{Z}$ has a projective resolution*

$$\cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

such that $P_n, \ldots, P_0$ are finitely-generated $\mathbb{Z}G$-modules.
G is of type FP_∞ if $\mathbb{Z}$ has a projective resolution with all terms finitely generated.
G is of type FP if $\mathbb{Z}$ has a projective resolution of finite length (i.e. all but finitely many terms are zero) with all terms finitely generated.

Example 1.5. 1. $G = \langle t \rangle \cong \mathbb{Z}$ is of type FP.
2. $G = \langle t \rangle \cong \mathbb{Z}/n\mathbb{Z}$ is of type FP_∞. It turns out that it is not of type FP, as we'll see after we developed the theory of cohomology.

These are finiteness conditions. For example, FP_n is analogous to G being the fundamental group of a simplicial complex X with X contractible with finite n-skeleton.

Definition 1.12. *The standard (or bar) resolution of $\mathbb{Z}$ is defined as follows: Let $G^{(n)}$ be the set of symbols $[g_1|\cdots|g_n]$ with $g_1, \ldots, g_n \in G$ and $G^{(0)} = \{[]\}$. Set $F_n = \mathbb{Z}G\{G^{(n)}\}$ and $d_n : F_n \to F_{n-1}$ defined on the level of symbols by*

$$\begin{aligned} d_n([g_1|\cdots|g_n]) = g_1[g_2|\cdots|g_n] - [g_1g_2|g_3|\cdots|g_n] + [g_1|g_2g_3|\cdots|g_n] \\ - \cdots + (-1)^{n-1}[g_1|\cdots|g_{n-2}|g_{n-1}g_n] + (-1)^n[g_1|\cdots|g_{n-1}] \end{aligned}$$

One checks that $d_{n-1}d_n = 0$ and so

$$\cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

is a chain complex.

Lemma 1.2. *This chain complex is exact.*

So the standard resolution is indeed a resolution.

Proof. We check exactness at the level of abelain groups.
F_n is a free abelian group on $G \times G^{(n)} = \{g_0[g_1|\cdots|g_n] : g_i \in G\}$. We'll define maps of abelian groups $s_n : F_n \to F_{n+1}$ such that $\mathrm{id}_{F_n} = d_{n+1}s_n + s_{n-1}d_n$. This is given by $s_n(g_0[g_1|\cdots|g_n]) = [g_0|\cdots|g_n]$. Now $x = \mathrm{id}_{F_n}(x) = d_{n+1}s_n(x) + s_{n-1}d_n(x)$, so any $x \in \ker d_n$ lives in $\operatorname{Im} d_{n+1}$. □

Corollary 1.3. *A finite group is of type* FP_∞.

1.3 Cohomology

Definition 1.13. Take a projective resolution

$$\cdots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

Let M be a $\mathbb{Z}G$-module. Applying $\mathrm{Hom}_G(-, M)$ to get

$$\cdots \xleftarrow{d^2} \mathrm{Hom}_G(P_1, M) \xleftarrow{d^1} \mathrm{Hom}_G(P_0, M)$$

where $d^n = d_n^*$.
The n-th cohomology group $H^n(G, M)$ with coefficients in M is the abelian group $H^n(G, M) = \ker d^{n+1} / \operatorname{Im} d^n$ for $n \geq 1$ and $H^0(G, M) = \ker d^1$.

Remark. These are independent of the choice of projective resolution. In particular, they are the homology groups of the chain complex $C_n = \mathrm{Hom}_G(F_{-n}, M)$ defined for $-\infty < n \leq 0$, and are

Example 1.6. Back to Example 1.2. We have the free, hence projective, resolution

$$0 \longrightarrow \mathbb{Z}G \xrightarrow{t-1} \mathbb{Z}G \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

For $\phi \in \mathrm{Hom}_G(\mathbb{Z}G, M)$ and $x \in \mathbb{Z}G$, we have $d^1(\phi)(x) = \phi(d_1(x)) = \phi(x(t-1))$. We have an identification of $\mathrm{Hom}_G(\mathbb{Z}G, M)$ with M sending θ to $\theta(1)$. So $d^1(\phi)$ corresponds to $\phi(t-1) = (t-1)\phi(1)$. This means that $H^0(G, M) = \ker(t-1) = \{m \in M : tm = m\} = M^G$ and $H^1(G, M) = M/\{(t-1)M : m \in M\} = M_G$ (and $H^n(G, M) = 0$ for $n \neq 0, 1$). M^G is the largest submodule fixed by G, and M_G is the largest quotient fixed by G.

Remark. 1. $H^0(G, M) = M^G = \{m \in M : tm - m\}$ is true in general, but the descrption of $H^1(G, M)$ as M_G is special to $G \cong \mathbb{Z}$.
2. If G is of type FP, then $H^n(G, M)$ eventually vanishes.

Definition 1.14. G is of cohomological dimension m (over $\mathbb{Z}$) if there exists some (left) $\mathbb{Z}G$-module M such that $H^m(G, M) \neq 0$, and $H^n(G, N) = 0$ for all $n > m$ and (left) $\mathbb{Z}G$-module N.

Example 1.7. $G = \langle t \rangle$ is of cohomological dimension 1. In fact, if G is of cohomological dimension 1 whenever it is free (and nontrivial). The converse is also true (proved by Stallings in 1968 when G is finitely-generated, and Swan in 1969 in general).

As is nobody has ever done before (totally), let's actually show that the cohomology groups are independent of resolution.

Definition 1.15. Let $(A_\bullet, \alpha_\bullet)$ and $(B_\bullet, \beta_\bullet)$ be chain complexes of $\mathbb{Z}G$-modules. Then a chain map $f_\bullet : A_\bullet \to B_\bullet$ is a collection of $\mathbb{Z}G$-maps $f_n : A_n \to B_n$ such that

$$\begin{array}{ccc} A_n & \xrightarrow{\alpha_n} & A_{n-1} \\ {\scriptstyle f_n}\downarrow & & \downarrow{\scriptstyle f_{n-1}} \\ B_n & \xrightarrow[\beta_n]{} & B_{n-1} \end{array}$$

commutes for each n.

Lemma 1.4. *Given a chain map (f_n) as above. For every n, it induces a well-defined map on homology $f_* : H_n(A_\bullet) \to H_n(B_\bullet)$.*

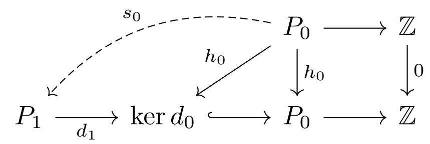
Proof. For $x \in \ker \alpha_n$, define $f_*([x]) = [f_n(x)]$ where $[x]$ denotes the class of x in $H_n(A_\bullet)$. Observe that $f_n(x) \in \ker \beta_n$ since $\beta_n f_n(x) = f_{n-1}\alpha_n(x) = f_{n-1}(0) = 0$, so indeed $f_n(x) \in \ker \beta_n$. Now if $x' = x + \alpha_{n+1}(y)$ for some y, then $f_n(x') = f_n(x) + f_n\alpha_{n+1}(y) = f_n(x) + \beta_{n+1}f_{n+1}(y) \in [f_n(x)]$, so this map is well-defined. $\square$

Theorem 1.5. *The definition of $H^n(G, M)$ is independent of the choice of projective resolution.*

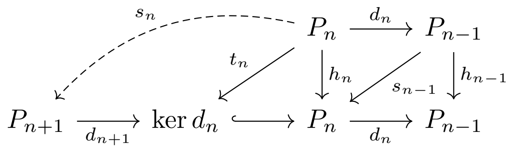
Proof. Take projective resolutions of $\mathbb{Z}$ by $\mathbb{Z}G$-modules $(P_\bullet, d_\bullet), (P'_\bullet, d'_\bullet)$. We produce $\mathbb{Z}G$-maps $f_n : P_n \to P'_n$ with $f_{n-1}d_n = d'_n f_n$, $g_n : P'_n \to P_n$ with $g_{n-1}d'_n = d_n g_n$, $s_n : P_n \to P_{n+1}$ with $d_{n+1}s_n + s_{n-1}d_n = g_n f_n - \mathrm{id}$ and $s'_n : P'_n \to P'_{n+1}$ with $d'_{n+1}s'_n + s'_{n-1}d'_n = f_n g_n - \mathrm{id}$.
Suppose we have constructed these, then $f^*_\bullet$ gives a chain map $\mathrm{Hom}_G(P'_\bullet, M) \to \mathrm{Hom}_G(P_\bullet, M)$, and $g^*_\bullet$ gives a chain map $\mathrm{Hom}_G(P_\bullet, M) \to \mathrm{Hom}_G(P'_\bullet, M)$. They induce maps on the respective homologies by the preceding lemma. For $\phi \in \ker d^{n+1} \in \mathrm{Hom}_G(P_n, M)$, we have $f^*_n g^*_n(\phi)(x) = \phi(g_n f_n(x)) = \phi(x) + \phi(d_{n+1}s_n(x)) + \phi(s_{n-1}d_n(x)) = \phi(x) + s^*_n d^{n+1}\phi(x) + d^n s^*_{n-1}\phi(x) = \phi(x) + 0 + d^n(s^*_{n-1}\phi)(x)$. Therefore $f^*_\bullet g^*_\bullet$ induces the identity map on homology. Similarly $g^*_\bullet f^*_\bullet$ induces the identity map on homology, so we are done.
g, f, s, s' are constructed as follows:
At the end of the resolutions, we take $f_{-1} : \mathbb{Z} \to \mathbb{Z}$ as the identity and $f_{-2} : 0 \to 0$ as the zero map. Now suppose we've constructed f_{n-1} and f_n. Then $f_n d_{n+1} : P_{n+1} \to P'_n$ and $d'_n(f_n d_{n+1}) = f_{n-1}d_n d_{n+1} = 0$. So the image of $f_n d_{n+1}$ lies in $\ker d'_n$. f_{n+1} is defined using the projectivity of P_{n+1} by the diagram

$$\begin{array}{ccccccc} & & P_{n+1} & \xrightarrow{d_{n+1}} & P_n & \xrightarrow{d_n} & P_{n-1} \\ & {\scriptstyle f_{n+1}}\swarrow & \downarrow{\scriptstyle f_n d_{n+1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} \\ P'_{n+1} & \xrightarrow[d'_{n+1}]{} & \ker d'_n & \hookrightarrow & P'_n & \xrightarrow[d'_n]{} & P'_{n-1} \end{array}$$

We similarly define g. To define s, first set $h_n = g_n f_n - \mathrm{id} : P_n \to P_n$, which is a chain map with $h_{-1} = 0$. Set $s_{-1} : \mathbb{Z} \to P_0$ to be the zero map. Note that $d_0 h_0 = h_{-1} d_0 = 0$, so $\operatorname{Im} h_0 \leq \ker d_0$. We obtain s_0 by the projectivity of P_0:



Now suppose s_{n-1} and s_{n-2} are defined, then consider $t_n = h_n - s_{n-1} d_n : P_n \to P_n$. We have $d_n t_n = d_n h_n - d_n s_{n-1} d_n = h_{n-1} d_n - (h_{n-1} - s_{n-2} d_{n-1}) d_n = s_{n-2} d_{n-1} d_n = 0$. So $\operatorname{Im} t_n \leq \ker d_n$. Pulling the same trick, noting that P_n is projective, gives



And the procedure for s' is completely analogous. $\square$

Remark. If we use projective resolutions of any $\mathbb{Z}G$-module N, then our definition gives us what's known as $\operatorname{Ext}^n_{\mathbb{Z}G}(N, M)$. Thus $\operatorname{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, M) = H^n(G, M)$.

1.4 Computation of Cohomology

Now consider the definition of $H^n(G, M)$ applied to the standard resolution

$$\cdots \longrightarrow \mathbb{Z}G\{G^{(1)}\} \longrightarrow \mathbb{Z}G\{G^{(0)}\} \longrightarrow \mathbb{Z}$$

Note that $\operatorname{Hom}_G(\mathbb{Z}G\{G^{(n)}\}, M) \cong \{$(set-theoretic) functions $f : G^n \to M\}$. We set this to be $C^n(G, M)$. In particular $C^0(G, M) \cong M$.

Definition 1.16. The group of n cochains of G with coefficients in M is $C^n(G, M)$ under addition. The n-th coboundary map is $d^n : C^{n-1}(G, M) \to C^n(G, M)$ dual to d_n of the standard resolution.

Explicitly,

$$\begin{aligned}(d^n \phi)(g_1, \ldots, g_n) = g_1 \phi(g_2, \ldots, g_n) &- \phi(g_1 g_2, g_3, \ldots, g_n) + \cdots \\ &+ (-1)^{n-1} \phi(g_1, \ldots, g_{n-2}, g_{n-1} g_n) \\ &+ (-1)^n \phi(g_1, \ldots, g_{n-2}, g_{n-1})\end{aligned}$$

Definition 1.17. $Z^n(G, M) = \ker d^{n+1} \leq C^n(G, M)$ is known as the group of n-cocycles. $B^n(G, M) = \operatorname{Im} d^n \leq C^n(G, M)$ is known as the group of n-coboundaries.

So $H^n(G, M) \cong Z^n(G, M)/B^n(G, M)$.

Maybe it's time to draw a connection between our standard resolution and the usual one in algebraic topology. Consider the free abelian group $\mathbb{Z}G^{n+1}$. G acts on G^{n+1} via $g(g_0, g_1, \ldots, g_n) = (gg_0, \ldots, gg_n)$. $\mathbb{Z}G^{n+1}$ is a free $\mathbb{Z}G$-module with basis given by $(n+1)$-tuples with $g_0 = 1$. The symbol $(g_1 \mid \cdot \mid g_n)$ corresponds to $(n+1)$-tuple $(1, g_1, g_1g_2, g_1g_2g_3, \dots, g_1 \cdots g_n)$. Note that in the usual resolution in algebraic topology we have boundary maps given by an alternating sum of n-tuples with one of the entries missing. If we do this with the $(n+1)$-tuple here, we get the terms in our version of the boundary map.

2 Low Degree Cohomology and Extensions

2.1 The First Cohomology

$H^0(G, M)$ is always the group M^G of G-invariants in M (by the standard resolution or otherwise). What does $H^1(G, M)$ entail?

Definition 2.1. A derivation (or crossed homomorphism) of G with coefficients in M is a function $\phi : G \to M$ such that $\phi(gh) = g\phi(h) + \phi(g)$.

Note that $Z^1(G, M)$ is exactly the abelian group $\mathrm{Der}(G, M)$ of derivations (under $+$).

Definition 2.2. An inner derivation is a derivation of the form $\phi(g) = gm - m$ for some fixed $m \in M$.

Aaaaaaaaand of course the subgroup of inner derivations is just $B^1(G, M)$. This gives an interpretation of $H^1(G, M)$. In particular, if M is a trivial $\mathbb{Z}G$-module, then $H^1(G, M) = \mathrm{Hom}(G, M)$ (the set of group homomorphisms $G \to M$).

Definition 2.3. Let G be a group and M a (left) G-module. We can construct their semidirect product $M \rtimes G = (M \times G, *)$ via $(m_1, g_1) * (m_2, g_2) = (m_1 + g_1m_2, g_1g_2)$.

The abelian normal subgroup $\{(m, 1) : m \in M\} \leq M \rtimes G$ is isomorphic to M. The subgroup $\{(0, g) : g \in G\}$ is isomorphic to G, and the conjugation action of whose element in $M \lhd M \rtimes G$ corresponds to the $\mathbb{Z}G$-module action. This is an example of an extension of G by M, since we have an isomorphism $M \rtimes G/M \cong G$. Note that there is a homomorphism (the "splitting") $s : G \to M \rtimes G, g \mapsto (0, g)$ such that $G \to M \rtimes G \to M \rtimes G/M \cong G$ is the identity map. So the semidirect is an example of a split extension of G by M. Write $E = M \rtimes G$. Now consider another splitting $s_1 : G \to E$ (i.e. a homomorphism such that $G \to E \to E/M \cong G$ is the identity). Define $\psi_{s_1} : G \to M$ by $s_1(g) = (\psi_{s_1}(g), g) \in E$. Then in fact $\psi_{s_1} \in Z^1(G, M)$ (example sheet). Furthermore, suppose we have two splitting $s_1, s_2 : G \to E$, then $\psi_{s_1} - \psi_{s_2} \in B^1(G, M)$ iff there is some m such that $(m, 1)s_1(g)(m, 1)^{-1} = s_2(g)$ for all $g \in G$ (also example sheet). So ψ_{s_1}, ψ_{s_2} define different elements in $H^1(G, M)$ iff they are conjugates under M, and therefore $H^1(G, M)$ can be interpreted as M-conjugation classes of splittings.

2.2 The Second Cohomology

Suppose we have an extension of G by an abelian group M, i.e. a short exact sequence

$$1 \longrightarrow M \longrightarrow E \longrightarrow G \longrightarrow 1$$

where maps are group homomorphisms. We are gonna write the (abelian) operation in M multiplicatively as well 'coz otherwise it's annoying to keep track. M embeds in E as a normal subgroup and E acts on (the embedded copy of) M by conjugation, with M acting trivially on itself. So we may regard M as a $\mathbb{Z}G$-module.

Definition 2.4. Two extensions E, E' are equivalent iff there is a commuting diagram of group homomorphisms

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

It follows from easy computation (or five lemma) that this middle arrow has to be an isomorphism, so the equivalence of extensions is a bona fide equivalence relation. The converse is of course not necessarily true.

Definition 2.5. E is a central extension if M is a trivial $\mathbb{Z}G$-module.

Proposition 2.1. *Let E be an extension of G by M. If there is a splitting $s_1 : G \to E$, then E is equivalent to the semidirect product of G by M (with the $\mathbb{Z}G$-module structure on M given by the earlier discussion).*

Proof. Exercise. □

Write $\pi : E \to G$ to denote the quotient map. For general extensions, there is a set-theoretic section $s : G \to E$ such that $\pi \circ s = \mathrm{id}_G$. But it may fail to be a group homomorphism.
Suppose WLOG $s(1) = 1$. Define $\phi(g_1, g_2) = s(g_1)s(g_2)s(g_1^{-1}g_2^{-1})$, which intends to measure how s fails to be a group homomorphism. So $\pi(\phi(g_1, g_2)) = 1$ and so $\phi(g_1, g_2) \in M$ and $\phi : G^2 \to M$ is a 2-cochain.
In fact, it is a 2-cocycle. Consider $s(g_1)s(g_2)s(g_3)$ in two different ways. On one hand, it equals

$$\phi(g_1, g_2)s(g_1g_2)s(g_3) = \phi(g_1, g_2)\phi(g_1g_2, g_3)s(g_1g_2g_3)$$

On the other hand, it equals

$$s(g_1)\phi(g_2, g_3)s(g_2g_3) = s(g_1)\phi(g_2, g_3)s(g_1)^{-1}\phi(g_1, g_2g_3)s(g_1g_2g_3)$$

Equating the two, we get $\phi(g_1, g_2)\phi(g_1g_2, g_3) = s(g_1)\phi(g_2, g_3)s(g_1)^{-1}\phi(g_1, g_2g_3)$.
Converting to additive notation, this becomes

$$\phi(g_1, g_2) + \phi(g_1g_2, g_3) = g_1\phi(g_2, g_3) + \phi(g_1, g_2g_3)$$

But this means that $(d^3\phi)(g_1, g_2, g_3) = 0$, i.e. ϕ is a 2-cocycle. ϕ is also normalised in the sense that $\phi(1, g) = \phi(g, 1) = 0$.
Now take a different choice $s' : G \to E$ of section with $s(1) = 1$ as before. Then $\pi(s(g)s'(g)^{-1}) = 1$ for all $g \in G$. So $\psi(g) = s'(g)s(g)^{-1}$ lives in M.
Now,

$$\begin{aligned} s'(g_1)s'(g_2) &= \psi(g_1)s(g_1)\psi(g_2)s(g_2) = \psi(g_1)s(g_1)\psi(g_2)s(g_1)^{-1}s(g_1)s(g_2) \\ &= \psi(g_1)s(g_1)\psi(g_2)s(g_1)^{-1}\phi(g_1, g_2)s(g_1g_2) \\ &= \psi(g_1)s(g_1)\psi(g_2)s(g_1)^{-1}\phi(g_1, g_2)\psi(g_1g_2)^{-1}s'(g_1g_2) \end{aligned}$$

Switch to additive notation,

$$\phi'(g_1, g_2) = \psi(g_1) + g_1\psi(g_2) + \phi(g_1, g_2) - \psi(g_1 g_2) = \phi(g_1, g_2) + (d^2\psi)(g_1, g_2)$$

That is, ϕ, ϕ' differ by a coboundary. So we get an element of $H^2(G, M)$ out of any extension E¿

Theorem 2.2. *Let G be a group and M a $\mathbb{Z}G$-module. Then there's a bijection between equivalence classes of extensions of G by M and $H^2(G, M)$.*

It's fairly clear that equivalent extensions give rise to the same cohomology class, so our construction gives the map from one side. We need some work in order to introduce the map to the other direction.

Lemma 2.3. *Let $\phi \in Z^2(G, M)$, then there's a cochain $\psi \in C^1(G, M)$ such that $\phi + d^2\psi$ is normalised.*

Proof. Let $\psi(g) = -\phi(1, g)$. Then $(\phi + d^2\psi)(1, g) = \phi(1, g) - (\phi(1, g) - \phi(1, g) + \phi(1, 1)) = \phi(1, g) - \phi(1, 1)$ and similarly $(\phi + d^2\psi)(g, 1) = \phi(g, 1) - g\phi(1, 1)$. But $d^3\phi = 0$, in particular $d^3\phi(g, 1, 1) = 0 = d^3\phi(1, 1, g)$. Expanding everything gives the result. ☐

Now take a normalised cocycle $\phi \in Z^2(G, M)$ representing a given cohomology class. Consider the group E_ϕ on the set $M \times G$ with group operation $*_\phi$ given by

$$(m_1, g_1) *_\phi (m_2, g_2) = (m_1 + g_1 m_2 + \phi(g_1, g_2), g_1 g_2)$$

which as one can check is an actual group operation (note that this uses the fact that ϕ is normalised). E_ϕ is an extension of G by M since $M \cong \{(m, 1) \in E_\phi\}$ and $E_\phi/M \cong G$. The equivalence class of E_ϕ is independent of the choice of representative of $[\phi] \in H^2(G, M)$. Indeed, if ϕ' is a different normalised cocycle representing this class, then $\phi - \phi' = d^2\psi$ for some ψ. Then we have a homomorphism $E_\phi \to E'_\phi, (m, g) \mapsto (m + \psi(g), g)$.

Example 2.1. Consider the central extensions of $T = \mathbb{Z}^2$ by $\mathbb{Z}$. There are two such extensions, namely

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}^3 \longrightarrow \mathbb{Z}^2 \longrightarrow 0$$

and

$$0 \longrightarrow \mathbb{Z} \longrightarrow H \longrightarrow \mathbb{Z}^2 \longrightarrow 0$$

where H is the Heisenburg group

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

which receives a map from $\mathbb{Z}$ at b and maps into $\mathbb{Z}^2$ at (a, c).
To analyse the equivalence classes of extensions, let's work out $H^2(T, \mathbb{Z})$. We have a free resolution

$$0 \longrightarrow \mathbb{Z}T \xrightarrow{\beta} \mathbb{Z}T^2 \xrightarrow{\alpha} \mathbb{Z}T \xrightarrow{\epsilon} \mathbb{Z}$$

of the free $\mathbb{Z}T$-module $\mathbb{Z}$, where $\beta(z) = (z(1-b), z(a-1)), \alpha(x,y) = x(a-1) + y(b-1)$ where a, b are the generators of T. Applying $\mathrm{Hom}_T(-,\mathbb{Z})$ gives a chain complex

$$0 \longleftarrow \mathrm{Hom}_T(\mathbb{Z}T,\mathbb{Z}) \xleftarrow{\beta^*} \mathrm{Hom}_T(\mathbb{Z}T^2,\mathbb{Z}) \xleftarrow{\alpha^*} \mathrm{Hom}_T(\mathbb{Z}T,\mathbb{Z})$$

But $\beta^* = 0$ (in fact also $\alpha^* = 0$). Indeed, for a $\mathbb{Z}T$-map $f : \mathbb{Z}T^2 \to \mathbb{Z}$ and $z \in \mathbb{Z}T$, we have

$$\begin{aligned}(\beta^* f)(z) &= f(\beta(z)) = f(z(1-b), z(a-1)) = f((z-bz,0)+(0,za-z)) \\ &= (1-b)f(z,0) + (a-1)f(0,z) = 0\end{aligned}$$

since T acts trivially on $\mathbb{Z}$.
So $H^2(T,\mathbb{Z}) \cong \mathrm{Hom}_T(\mathbb{Z}T,\mathbb{Z}) \cong \mathbb{Z}$. It has a generator represented by the augmentation map.
Let's understand $H^2(T,\mathbb{Z})$ in terms of cocycles. We'll construct a chain map between our resolution above and the standard resolution.

$$\begin{array}{ccccccccc} \mathbb{Z}T\{T^{(2)}\} & \xrightarrow{d_2} & \mathbb{Z}T\{T^{(1)}\} & \xrightarrow{d_1} & \mathbb{Z}T\{T^{(0)}\} & \xrightarrow{\epsilon} & \mathbb{Z} & \longrightarrow & 0 \\ \downarrow f_2 & & \downarrow f_1 & & \downarrow \mathrm{id} & & \| & & \\ \mathbb{Z}T & \xrightarrow[\beta]{} & \mathbb{Z}T^2 & \xrightarrow[\alpha]{} & \mathbb{Z}T & \xrightarrow[\epsilon]{} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

To construct f_1 such that $\alpha f_1 = d_1$, we just need to give the image of symbols $[a^r b^s], r, s \in \mathbb{Z}$. If it is mapped to $(x_{r,s}, y_{r,s}) \in \mathbb{Z}T^2$, then we need $\alpha(x_{r,s}, y_{r,s}) = a^r b^s - 1 = (a^r - 1)b^s + (b^s - 1)$.
Let

$$S(a,r) = \begin{cases} 1 + a + a^2 + \cdots + a^{r-1} & \text{if } r > 0 \\ -a^{-1} - \cdots - a^r & \text{if } r \leq 0 \end{cases}$$

So we always have $S(a,r)(a-1) = a^r - 1$. Then $\alpha(S(a,r)b^s, S(b,s)) = d_1([a^r b^s])$, so we may define $f_1([a^r b_s]) = (S(a,r)b^s, S(b,s))$.
Now let's define f_2. We need to define it for each symbol $[a^r b^s \mid a^t b^u]$. So we need to find $z_{r,s,t,u} \in \mathbb{Z}T$ such that $f_1 d_2([a^r b^s \mid a^t b^u]) = \beta(z_{r,s,t,u})$. With a bit of calculations we see that $z_{r,s,t,u} = S(a,r)b^s S(b,u)$ works. Define $f_2([a^r b^s \mid a^t b^u]) = z_{r,s,t,u}$.
For a cochain $\phi : T^2 \to \mathbb{Z}$ which represents a cohomology class $p \in \mathbb{Z} = \mathrm{Hom}_T(\mathbb{Z}T,\mathbb{Z}) = H^2(T,\mathbb{Z})$. Then we have a factorisation $\phi = (p\epsilon) \circ f_2$. Since $\epsilon(S(a,r)) = r$, we find $\phi(a^r b^s, a^t b^u) = p\epsilon(z_{r,s,t,u}) = pru$. The group structure on $Z \times T$ corresponding to ϕ is then $(m, a^r b^s) * (n, a^t b^u) = (m+n+pru, a^{r+t} b^{s+u})$. This corresponds to groups

$$\left\{ \begin{pmatrix} 1 & pr & m \\ & 1 & s \\ & & 1 \end{pmatrix} : r, s, m \in \mathbb{Z} \right\}$$

2.3 Group Extensions by Group Presentations

Express G in terms of generators and relations and let F be the free group on the set X of generators. We thus get a surjection $F \to G$ and let $R \lhd F$ be its

kernel. Usually we just specify R by a set of elements generating it as a normal subgroup of F.
Let $R_{\text{ab}} = R/[R,R]$ be the abelianisation of R. The conjugation action of F on R gives an action of F on R_{ab}. But $R \leq F$ acts trivially on R_{ab}, so R_{ab} may be regarded as a $\mathbb{Z}(F/R)$-module, i.e. a $\mathbb{Z}G$-module. It is called the relation module. And

$$1 \longrightarrow R_{\text{ab}} \longrightarrow F/[R,R] \longrightarrow G \longrightarrow 1$$

is an extension of G by R_{ab}.
For a central extension, rather than using $R/R' = R/[R,R]$, one can use $R/[R,F]$. Whence

$$1 \longrightarrow R/[R,F] \longrightarrow F/[R,F] \longrightarrow G \longrightarrow 1$$

We introduce these to answer the following question: Is there, in some sense, a largest (or universal) central extension?
We can obviously make larger and larger extensions by taking direct products of abelian groups. However, we do have a universal one.

Theorem 2.4 (MacLane)**.** *Given a presentation $G = \langle X \mid R\rangle$ and let F be the free group on X. Let M be a $\mathbb{Z}G$-module, then there's an exact sequence*

$$H^1(F,M) \longrightarrow \text{Hom}_G(R_{\text{ab}},M) \longrightarrow H^2(G,M) \longrightarrow 0$$

where we regard M as a $\mathbb{Z}F$-module via the map $F \to G$.
Thus any (equivalence class of) extension of G by M corresponding to a cohomology class arises from taking a $\mathbb{Z}G$-map $R_{\text{ab}} \to M$.

Corollary 2.5. *If M is a trivial module, then we get the exact sequence*

$$\text{Hom}_G(F,M) \longrightarrow \text{Hom}_G(R/[R,F],M) \longrightarrow H^2(G,M) \longrightarrow 0$$

Proof. For trivial module M, $H^1(F,M) = \text{Hom}(F,M) = \text{Hom}(F_{\text{ab}},M)$ and $\text{Hom}(R_{\text{ab}},M) = \text{Hom}(R/[R,F],M)$. □

There is also a connection with group homology. Given a projective resolution of $\mathbb{Z}$, we can apply the functor $\mathbb{Z} \otimes_{\mathbb{Z}G} -$ to it. This gives a chain complex, whose homology groups we shall denote as $H_n(G,\mathbb{Z})$.

Definition 2.6. The Schur multiplier (or multiplicator) is $\text{M}(G) = H_2(G,\mathbb{Z})$.

It has importance in the study of central extensions.

Theorem 2.6 (Universal Coefficient Theorem)**.** *Let G be a group and M a trivial $\mathbb{Z}G$-module. Then there is a short exact sequence*

$$0 \longrightarrow \text{Ext}^1(G_{\text{ab}},M) \longrightarrow H^2(G,M) \longrightarrow \text{Hom}(\text{M}(G),M) \longrightarrow 0$$

Corollary 2.7. *Suppose $G_{\text{ab}} = 1$, then $H^2(G,M) \cong \text{Hom}(\text{M}(G),M)$.*

Remark. 1. When $G_{\text{ab}} = 1$, we say that G is perfect.
2. To confuse you, some authors refer to $H^2(G,\mathbb{C}^\times)$ as the Schur multiplier.

Theorem 2.8 (Hopf)**.** *Given* $G = \langle X \mid R\rangle$*,* $\mathrm{M}(G) = ([F,F] \cap R)/[R,F]$*.*

Remark. This shows that $([F,F] \cap R)/[R,F]$ is independent of the choice of presentation.

How do we prove these theorems? Recall from geometric group theory that all subgroups of free groups are free. R is therefore a free group. Let Y be a basis of it. Then R_{ab} is a free abelian group on Y.

Proposition 2.9. *Given a presentation* $G = \langle F \mid R\rangle$*, there is an exact sequence*

$$\bar{I}_R/\bar{I}_R^2 \xrightarrow{d_2} I_F/(\bar{I}_R I_F) \xrightarrow{d_1} \mathbb{Z}G \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

where $I_F = \ker(\epsilon : \mathbb{Z}F \to \mathbb{Z})$ *and* $\bar{I}_R = \ker(\mathbb{Z}F \to \mathbb{Z}G)$*. Furthermore,* $I_F/(\bar{I}_R I_F)$ *is a free* $\mathbb{Z}G$*-module with basis* $\{x-1 : x \in X\}$*, and* $\bar{I}_R/\bar{I}_R^2$ *is a free* $\mathbb{Z}G$*-module with basis* $\{y-1 : y \in Y\}$*. We also have a* $\mathbb{Z}G$*-isomorphism* $\operatorname{Im} d_2 \cong R_{\mathrm{ab}}$*.*

Lemma 2.10. *Let* G *be a group and let* M *be a* $\mathbb{Z}G$*-module.*
(a) $I_G = \ker(\epsilon : \mathbb{Z}G \to \mathbb{Z})$ *is a free abelian group (under addition) on the basis* $\{g-1 : g \in G \setminus \{1\}\}$*.*
(b) $I_G/I_G^2 \cong G_{\mathrm{ab}}$*.*
(c) $\mathrm{Der}(G,M) \cong \mathrm{Hom}_G(I_G, M)$*.*

Proof. (a) $I_G = \ker\epsilon = \{\sum_g n_g g : \sum_g n_g = 0\}$. So if $\sum_g n_g g \in I_G$, then $\sum_g n_g g = \sum_g n_g(g-1)$. Also everything of the form $\sum_g n_g(g-1)$ clearly lies in I_G. So I_G is spanned by $\{g-1 : g \in G\}$. Now if $\sum_g n_g(g-1) = 0$, then $\sum_g n_g g - \sum_g n_g 1 = 0$ and so $n_g = 0$ for all $g \neq 1$.
(b) Since I_G is free abelian on $\{g-1 : g \in G \setminus \{1\}\}$, we can define a group homomorphism $\theta : I_G \to G_{\mathrm{ab}}$ by asking it to send $g-1$ to $g[G,G]$. But $(g_1-1)(g_2-1) = (g_1g_2-1) - (g_1-1) - (g_2-1)$ and so $I_G^2 \subset \ker\theta$, so θ induces a homomorphism $\bar{\theta} : I_G/I_G^2 \to G_{\mathrm{ab}}$.
Conversely, the map $\phi : G \to I_G/I_G^2, g \mapsto (g-1) + I_G^2$ induces a map $\bar{\phi} : G_{\mathrm{ab}} \to I_G/I_G^2$ since I_G/I_G^2 is abelian. It's clear that $\bar{\phi}, \bar{\theta}$ are inverses.
(c) $\phi \in \mathrm{Der}(G,M)$ corresponds to $\theta : g-1 \mapsto \phi(g)$, and θ recovers $\phi : g \mapsto \theta(g-1)$. □

Lemma 2.11. *(a) Let* F *be a free group on* X*. Then* I_F *is a free* $\mathbb{Z}F$*-module on* $\tilde{X} = \{x-1 : x \in X\}$*.*
(b) Let $R \lhd F$ *be a normal subgroup. Suppose* R *is free on* Y*. Then* $\bar{I}_R = \ker(\mathbb{Z}F \to \mathbb{Z}G)$ *is a free* $\mathbb{Z}F$*-module on the basis* $\tilde{Y} = \{y-1 : y \in Y\}$*.*

Proof. (a) Let $\alpha : \tilde{X} \to M$ be a map to some $\mathbb{Z}F$-module M. To establish freeness, it suffices to show that α uniquely extends to a $\mathbb{Z}F$-map $I_F \to M$. First consider the map $\alpha' : F \to M \rtimes F$ extending from $x \mapsto (\alpha(x-1), x)$. Write $\alpha'(f) = (\bar{\alpha}(f), f)$. Now $\alpha'(f_1f_2) = \alpha'(f_1) * \alpha'(f_2) = (\bar{\alpha}(f_1), f_1) * (\bar{\alpha}(f_2), f_2) = (\bar{\alpha}(f) + f_1\bar{\alpha}(f_2), f_1f_2)$. So $\bar{\alpha}$ is a derivation $F \to M$.
Take the corresponding $\mathbb{Z}F$-map $I_F \to M$ as in the preceding lemma. Uniqueness is clear.
(b) Suppose $\sum_{y\in Y} r_y(y-1) = 0$ where $r_y \in \mathbb{Z}F$. Choose a transversal T to the cosets of R in F. We can write $r_y = \sum_{t\in T} t s_{t,y}$ where $s_{t,y} \in \mathbb{Z}R$. So $\sum_{y\in Y, t\in T} t s_{t,y}(y-1) = 0$ and therefore $\sum_{y\in Y} s_{t,y}(y-1) = 0$ for each $t \in T$ by the preceding lemma.
I_R is a free $\mathbb{Z}R$-module on $\{y-1 : y \in Y\}$ by (a), so $s_{t,y} = 0$ for all y, t. □

Proof of Proposition 2.9. By part (a) of the preceding lemma, I_F is a free $\mathbb{Z}F$-module on $\{x-1 : x \in X\}$, so $I_F/(\bar{I}_R I_F)$ is a free $\mathbb{Z}(F/R) = \mathbb{Z}G$-module on $\{x-1 : x \in X\}$. On the other hand $\bar{I}_R$ is a free $\mathbb{Z}F$-module on $\{y-1 : y \in Y\}$ by part (b) of the preceding lemma. So $\bar{I}_R/\bar{I}_R^2$ is a free $\mathbb{Z}G$-module on $\{y-1 : y \in Y\}$.
The image of d_2 is $\bar{I}_R/(\bar{I}_R I_F)$. We consider $\bar{I}_R$ as a right $\mathbb{Z}F$-module, permissible as it is a two-sided ideal (as the kernel of a ring map). Our lemmas have obvious analogies for right modules, so $\bar{I}_R$ is a free right $\mathbb{Z}F$-module on $\{y-1 : y \in Y\}$. So $\bar{I}_R/(\bar{I}_R I_F)$ is a free abelian group on $\{y-1 : y \in Y\}$, which is isomorphic to R_{ab}.
Now for the left $\mathbb{Z}G$-module action, we have $g(y-1) = (gyg^{-1}-1)g \equiv (gyg^{-1}-1) \pmod{\bar{I}_R I_F}$. So this left $\mathbb{Z}G$-action corresponds to the G-action on R_{ab} inherited from conjugation. □

The proposition gives a partial free resolution, which can be extedned to a full resolution known as the Gruenberg resolution.

Theorem 2.12. *Let $G = \langle X \mid R \rangle$ be a presentation of G. Then the following is a free $\mathbb{Z}G$-resolution of $\mathbb{Z}$:*

$$\cdots \longrightarrow \bar{I}_R^n/\bar{I}_R^{n+1} \longrightarrow (\bar{I}_R^{n-1} I_F)/(\bar{I}_R^n I_F) \longrightarrow \bar{I}_R^{n-1}/\bar{I}_R^n \longrightarrow \cdots$$

$$\longrightarrow \bar{I}_R/\bar{I}_R^2 \longrightarrow I_F/(\bar{I}_R I_F) \longrightarrow \mathbb{Z}G \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

Proof. Exercise. □

Lemma 2.13. *Given a projective resolution $P_1 \to P_0 \to \mathbb{Z} \to 0$*

$$\cdots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

Denote $J_n = \operatorname{Im} d_n \subset P_{n-1}$ and let $\psi : P_n \to J_n$ be the induced map. Then for a $\mathbb{Z}G$-module M, there are exact sequences

$$\operatorname{Hom}_G(P_{n-1}, M) \longrightarrow \operatorname{Hom}_G(J_n, M) \longrightarrow H^n(G, M) \longrightarrow 0$$

and

$$0 \longrightarrow H_n(G, \mathbb{Z}) \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}G} J_n \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}G} P_{n-1}$$

Proof. We'll show the first sequence is exact. A similar argument works for the second.
We have

$$\begin{array}{ccccccc} P_{n+1} & \xrightarrow{d_{n+1}} & P_n & \xrightarrow{\psi} & J_n & \longrightarrow & 0 \\ & & & \searrow^{d_n} & \downarrow i & & \\ & & & & P_{n-1} & & \end{array}$$

with the row exact. Applying $\operatorname{Hom}_G(-, M)$ gives the diagram

$$\begin{array}{ccccccc} \operatorname{Hom}_G(P_{n+1}, M) & \xleftarrow{d^{n+1}} & \operatorname{Hom}_G(P_n, M) & \xleftarrow{\psi} & \operatorname{Hom}_G(J_n, M) & \longleftarrow & 0 \\ & & & \nwarrow^{d^n} & \uparrow i^* & & \\ & & & & \operatorname{Hom}_G(P_{n-1}, M) & & \end{array}$$

where i^* is essentially the natural restriction map. The exactness of the row implies that ψ^* is injective and $\operatorname{Im}\psi^* = \ker d^{n+1}$. Therefore $\ker d^{n+1} = \operatorname{Im}\psi^* \cong \operatorname{Hom}_G(J_n, M)$ and $\operatorname{Im} d^n = \operatorname{Im}(\psi^* \circ i^*) \cong \operatorname{Im} i^*$. So we get $H^n(G,M) \cong \operatorname{Hom}_G(J_n, M)/\operatorname{Im} i^*$ as required. □

Proof of Theorem 2.4. Since R_{ab} is the image of the boundary map, the preceding lemma gives the exact sequence

$$\operatorname{Hom}_G(I_F/(\bar{I}_R I_F), M) \longrightarrow \operatorname{Hom}_G(R_{\text{ab}}, M) \longrightarrow H^2(G,M) \longrightarrow 0$$

On the other hand, noting

$$\operatorname{Hom}_G(I_F/(\bar{I}_R I_F), M) = \operatorname{Hom}_F(I_F/(\bar{I}_R I_F), M) = \operatorname{Hom}_F(I_F, M) = H^1(F,M)$$

Noting that M is trivial as an $\mathbb{Z}R$-module. □

Proof of Theorem 2.8. Use the lemma again, we get

$$0 \longrightarrow H_2(G,\mathbb{Z}) \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}G} R_{\text{ab}} \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}G} I_F/(\bar{I}_R I_F)$$

But tensoring with $\mathbb{Z}$ is the same as taking the coinvariants: $\mathbb{Z} \otimes_{\mathbb{Z}G} R_{\text{ab}} = R/[R,F]$, $\mathbb{Z} \otimes_{\mathbb{Z}G} I_F/(\bar{I}_R I_F) = I_F/I_F^2 = F/[F,F]$. On the other hand, the kernel of $R/[R,F] \to F/[F,F]$ is exactly $([F,F] \cap R)/[R,F]$. □

Remark. 1. Theorem 2.6 and its corollary are proved in example sheet.
2. We'll learn more about the exact sequence appearing in Theorem 2.4 after we've met the five-term exact sequence, coming soon.

3 Some General Theory

3.1 The Long Exact Sequence of Cohomology

In any cohomology theory, we expect a long exact sequence.
Give a short exact sequence

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

of $\mathbb{Z}G$-modules, we would like some relationship between the cohomology of M_1, M_2, M_3 (duh). Recall that applying $\operatorname{Hom}(P, -)$ to the short exact sequence gives another short exact sequence if P is projective. In general, the new sequence is only exact on one side.

Proposition 3.1 (Long Exact Sequence of Cohomology). *We have an exact sequence*

$$\cdots \to H^n(G,M_2) \to H^n(G,M_3) \xrightarrow{\delta} H^{n+1}(G,M_1) \to H^{n+1}(G,M_2) \to \cdots$$

Lemma 3.2 (Snake Lemma). *Suppose*

$$0 \longrightarrow A_\bullet \xrightarrow{f_\bullet} B_\bullet \xrightarrow{g_\bullet} C_\bullet \longrightarrow 0$$

is a short exact sequence of chain complexes (i.e. $f_\bullet, g_\bullet$ are chain maps which is exact at each entry). Then there exists maps $\delta_n : H_{n+1}(C_\bullet) \to H_n(A_\bullet)$ such that the sequence

$$\cdots \longrightarrow H_{n+1}(B_\bullet) \xrightarrow{g_*} H_{n+1}(C_\bullet) \xrightarrow{\delta_n} H_n(A_\bullet) \xrightarrow{f_*} H_n(B_\bullet) \longrightarrow \cdots$$

is exact.

Proof. Omitted. □

Proof of Proposition 3.1. Consider a projective resolution $P_\bullet$ of $\mathbb{Z}$. Since the modules in the resolution are projective, we have a short exact sequence of chain complexes

$$0 \longrightarrow \mathrm{Hom}_G(P_\bullet, M_1) \longrightarrow \mathrm{Hom}_G(P_\bullet, M_2) \longrightarrow \mathrm{Hom}_G(P_\bullet, M_3) \longrightarrow 0$$

We concludes by applying the preceding lemma. □

3.2 The Five-Term Exact Sequence

We want to know the relationship between the cohomology of a group and that of its subgroups and quotients.

Theorem 3.3. *Let H be a normal subgroup of a group G with quotient Q. Let M be a $\mathbb{Z}G$-module. Then there is an exact sequence*

$$0 \to H^1(Q, M^H) \to H^1(G, M) \to H^1(H, M)^Q \to H^2(Q, M^H) \to H^2(G, M)$$

Remark. We'll see how to extend this sequence using the technique of spectral sequences.

We'll see shortly how exactly does Q act on $H^1(H, M)$. But first, examples.

Corollary 3.4. *If $G = \langle X \mid R \rangle$ is a presentation, then there is an exact sequence*

$$0 \longrightarrow H^1(G, M) \longrightarrow H^1(F, M) \longrightarrow \mathrm{Hom}_G(R_{\mathrm{ab}}, M) \longrightarrow H^2(G, M) \longrightarrow 0$$

Remark. Compare this with Theorem 2.4.

Proof. We can regard M as a $\mathbb{Z}F$-module which becomes a trivial $\mathbb{Z}R$-module. Now $H^2(F, M) = 0$ and $M^R = M$. So we need $\mathrm{Hom}_G(R_{\mathrm{ab}}, M) = H^1(R, M)^G$. But $H^1(R, M) = \mathrm{Hom}(R_{\mathrm{ab}}, M)$. We haven't really defined the G-action on $\mathrm{Hom}(R_{\mathrm{ab}}, M)$, but in this instant it will turn out to be $(g\phi)(x) = g\phi(g^{-1}x)$, so the corollary follows. □

Corollary 3.5. *If $G = [G, G]$ (so $G_{\mathrm{ab}} = 1$) and M is a trivial $\mathbb{Z}G$-module, then we have a short exact sequence*

$$0 \longrightarrow \mathrm{Hom}(F_{\mathrm{ab}}, M) \longrightarrow \mathrm{Hom}_G(R_{\mathrm{ab}}, M) \longrightarrow H^2(G, M) \longrightarrow 0$$

And so $H^2(G, M) = \mathrm{Hom}_G(R_{\mathrm{ab}}, M)/\mathrm{Hom}(F_{\mathrm{ab}}, M)$.

Proof. $H^1(G, M) = \mathrm{Hom}(G_{\mathrm{ab}}, M) = 0$ and $H^1(F, M) = \mathrm{Hom}(F_{\mathrm{ab}}, M)$. □

Back to the theorem. Let's finally define the Q-action on $H^1(H, M)$.

Lemma 3.6. *Let $H \lhd G$ be a normal subgroup and let M be a $\mathbb{Z}G$-module. G acts on $C^n(H, M)$ by $(g\phi)(h_1, \dots, h_n) = g\phi(g^{-1}h_1g, \dots, g^{-1}h_ng)$. This action descends to an action of G on $H^n(H, M)$. Moreover, the action restricts to a trivial action by H. In particular, we get an action of $Q = G/H$ on $H^n(H, M)$.*

Proof. We need to check that the G-action on $C^n(H, M)$ are given by chain maps, i.e. that $g(d^n\phi) = d^n(g\phi)$ for any $\phi \in C^{n-1}(H, M)$. The lecturer was in a good enough mood to check this but I wasn't.
To show that H acts trivially, we need to check that applying $h \in H$ to a cocycle only adds a coboundary. Ditto but let's check this for 1-cocyles. Let $\phi \in Z^1(H, M)$ and $h, h_1 \in H$, then

$$\begin{aligned}(h\phi)(h_1) - \phi(h_1) &= h\phi(h^{-1}h_1h) - \phi(h_1) = h(h^{-1}\phi(h_1h) + \phi(h^{-1})) - \phi(h_1) \\ &= h_1\phi(h) + \phi(h_1) + h\phi(h^{-1}) - \phi(h_1) = h_1\phi(h) - \phi(h) \\ &= (h_1 - 1)\phi(h) = \psi(h_1)\end{aligned}$$

for a coboundary ψ. □

For $n = 1$, for $[\phi] \in H^1(H, M)$ represented by a derivation $\phi : H \to M$, the G-action becomes $(g\phi)(h) = g\phi(g^{-1}hg)$. In particular, $\phi \in H^1(H, M)^G$ iff $[\phi(g^{-1}hg)] = [g\phi(h)]$.
We have a map $H^n(G, M) \to H^n(H, M)^Q$ induced by the map on cochains taking $f : G^n \to M$ to $\operatorname{res} f : H^n \hookrightarrow G^n \to M$. After some checking, this is indeed well-defined, and is known as the restriction map.
We also have a map $H^n(Q, M^H) \to H^n(G, M)$, called the inflation map, which is defined again on the level of cochains by sending $f : Q^n \to M^H$ to $\inf f : G^n \to Q^n \to M^H \hookrightarrow M$.
Finally, we have the transgression map $\mathrm{Tg} : H^1(H, M)^Q \to H^2(Q, M^H)$. Let $s : Q \to G$ be a set-theoretic section with $s(1) = 1$. We then define $\rho : G \to H$ by $\rho(g) = gs(gH)^{-1}$.
For a 1-cohomology class invariant under Q, let $f : H \to M$ be a cocycle representing it, then define $\mathrm{Tg}(f) : G^2 \to M$ by $(g_1, g_2) \mapsto f(\rho(g_1)\rho(g_2)) - f(\rho(g_1, g_2))$. Changing g_1, g_2 by multiplying with elements of H doesn't change this cochain, so this defines a cochain $Q^2 \to M$.
To establish Theorem 3.3, we need to check that all these maps are well-defined and that the sequence is exact, which are left as exercise.

3.3 The Transfer Map; Cup Product

Let $K \leq G$ be a subgroup. Recall from example sheet that we have a coinduced module $\operatorname{coind}_G^K(M) = \operatorname{Hom}_K(\mathbb{Z}G, M)$ with G-action $(gf)(x) = f(xg)$ for $f \in \operatorname{Hom}_K(\mathbb{Z}G, M)$ and $x \in \mathbb{Z}G$, and it has the property that:

Lemma 3.7 (Shapiro's Lemma)**.** $H^n(K, M) \cong H^n(G, \operatorname{coind}_G^K(M))$.

Definition 3.1. Given any $\mathbb{Z}K$-module V, its induced module is the $\mathbb{Z}G$-module $\operatorname{ind}_K^G(V) = \mathbb{Z}G \otimes_{\mathbb{Z}K} V = \bigoplus_{t \in T} t \otimes V$ where T is a transversal of K in G. The G-action is given by $g(t \otimes v) = t' \otimes kv$ wherre $gt = t'k$ for some $t' \in T, k \in K$.

Observe that if one has a $\mathbb{Z}G$-module M generated by a $\mathbb{Z}K$-module V (i.e. $M = \mathbb{Z}GV$), then there is a canonical map $\operatorname{ind}_K^G(V) \to M, t \otimes v \mapsto tv$.

Lemma 3.8. *Suppose $[G:K]<\infty$ and M is a $\mathbb{Z}G$-module, then* $\operatorname{coind}_G^K(M)\cong \operatorname{Ind}_K^G(M)$.

Proof. There is a $\mathbb{Z}K$-map $\phi_0 : M \to \operatorname{Hom}_K(\mathbb{Z}G, M)$ where $m\in M$ sends g to gm if $g\in K$ and 0 otherwise. This extends to a $\mathbb{Z}G$-map $\mathbb{Z}G\otimes_{\mathbb{Z}K} M \to \operatorname{Hom}_K(\mathbb{Z}G, M)$.
We have a map to the other direction $\psi : \operatorname{Hom}_K(\mathbb{Z}G, M)\to \mathbb{Z}G\otimes_{\mathbb{Z}K} M$ via $f\mapsto \sum_{t\in T} t\otimes f(t^{-1})$, which provides an inverse. □

So in the case where $K\le G$ has finite index (and M a $\mathbb{Z}G$-module), there is a map $H^n(K,M)\to H^n(G,M)$ defined as follows:

Definition 3.2. The transfer (or corestriction) map $\operatorname{cores}_K^G : H^n(K,M)\to H^n(G,M)$ given by $H^n(K,M)\cong H^n(G,\operatorname{coind}_G^K(M))\cong H^n(G,\operatorname{ind}_K^G(M))\to H^n(G,M)$ where $\alpha^* : H^n(G,\operatorname{ind}_K^G(M))\to H^n(G,M)$ is induced by the canonical map $\alpha : \operatorname{ind}_K^G(M)\to M$.

Lemma 3.9. *For $z\in H^n(G,M)$, we have* $\operatorname{cores}_K^G \operatorname{res}_K^G(z) = [G:K]z$.

Proof. Example sheet. □

Ok. Now products.

Definition 3.3. Given $[u]\in H^p(G,M)$ and $[v]\in H^q(G,N)$, their cup product is $[u]\smile[v]=[u\smile v]\in H^{p+q}(G,M\otimes_{\mathbb{Z}}N)$, defined on cochains in a second. Here, $M\otimes_{\mathbb{Z}}N$ is a $\mathbb{Z}G$-module via the diagonal action $g(m\otimes n)=(gm)\otimes(gn)$.

For $u\in C^p(G,M)$ and $v\in C^q(G,N)$, we set $u\smile v\in C^{p+q}(G,M\otimes N)$ via

$$(u\smile v)(g_1,\dots,g_{p+q}) = (-1)^{pq}u(g_1,\dots,g_p)\otimes(g_1\cdots g_p v(g_{p+1},\dots,g_{p+q}))$$

In degree 0, the cup product is $H^0(G,M)\times H^0(G,N)\to H^0(G,M\otimes N)$ which is the map $M^G\otimes N^G\to(M\otimes N)^G$ induced by inclusions.
Needless to say, this construction is natural: Given $\mathbb{Z}G$-maps $f: M\to M'$ and $g: N\to N'$ both $\mathbb{Z}G$-maps, we have $(f\otimes g)_*(u\smile v)=(f_*u)\smile(g_*v)$.
The element $1\in H^0(G,\mathbb{Z})=\mathbb{Z}$ satisfies $1\smile u = u = u\smile 1$ for all $u\in H^*(G,M)$ via $\mathbb{Z}\otimes M = M = M\otimes\mathbb{Z}$.
The cup product is also associative in the obvious way. On the other hand, it is graded-commutative, in the sense that if $u\in H^p(G,M), v\in H^q(G,N)$, then $u\smile v = (-1)^{pq}\alpha_*(v\smile u)$ where $\alpha : N\otimes M\to M\otimes n$ is given by $n\otimes m\mapsto m\otimes n$.
So $H^*(G,\mathbb{Z})$ is a graded-commutative associative unital ring under $\smile$. The subring given by the sum of the even degree terms is then a commutative ring. And the whole cohomology ring is a module for this ring.
Given $\alpha : H\to G$ a group homomorphism, we have $\alpha^*(u\smile v)=\alpha^*(u)\smile\alpha^*(v)$, so we get a ring homomorphism $\alpha^* : H^*(G,\mathbb{Z})\to H^*(H,\mathbb{Z})$. When $H\le G$ has finite index, then for $u\in H^p(G,M)$ and $v\in H^q(H,N)$ we have

$$\operatorname{cores}_H^G(\operatorname{res}_H^G(u)\smile v) = u\smile \operatorname{cores}_H^G(v)$$

Thus the transfer map $H^*(H,\mathbb{Z})\to H^*(G,\mathbb{Z})$ is a homomorphism of $H^*(G,\mathbb{Z})$-modules.
Randomly we decided to observe that $\operatorname{Ext}^*_{\mathbb{Z}G}(M,M)$ is a module for the cohomology ring $H^*(G,\mathbb{Z})$. We can study M via this module.

4 Brauer Groups

4.1 Central Simple Algebras and Artin-Wedderburn

Fix a field k.

Definition 4.1. A simple algebra over k (or a simple k-algebra) is an algebra A whose only two-sided ideals are 0 and A. A central simple algebra over k (or a central simple k-algebra) is a simple algebra over k whose center is k.

We will only concern ourselves with finite-dimensional algebras.

Example 4.1. 1. $\mathrm{Mat}_n(k)$ is a central simple k-algebra.
2. Take $k = \mathbb{R}$. The quarternions $\mathbb{H}$ is spanned by the $\mathbb{R}$-basis $1, i, j, k$ subject to the relations $ij = k = -ji, i^2 = j^2 = k^2 = -1$. This is a 4-dimensional $\mathbb{R}$-algebra. This is in fact a division algebra (in the sense that every nonzero element has a multiplicative inverse), hence it is simple. We also have $Z(\mathbb{H}) = \mathbb{R}$.

We want to classify central simple algebras over a field k.

Theorem 4.1 (Artin-Wedderburn)**.** *Any finite-dimensional simple k-algebra A is isomorphic to a matrix ring over a division algebra D over k.*

Proof. Consider a minimal nonzero right A-submodule M of A_A (i.e. A regarded as a right A-module). So $0, M$ are the only right A-submodules of M (i.e. M is a simple right A-module).
Then $\sum_{a \in A} aM$ is a two-sided ideal of A, and it's nonzero since M is. Simplicity of A implies that $A = \sum_{a \in A} aM$.
Consider $\theta_a : M \to aM, m \mapsto am$ which is a right A-module map. Since M doesn't have trivial submodules, θ_a is either zero or injective (hence an isomorphism). Consequently, $\sum_{a \in A} aM$ is a sum of copies of M. An easy induction argument shows that finite sums of simple modules are in fact direct sums. Since A is finite-dimensional, this shows that $A_A = \bigoplus_i M_i$ is a finite direct sum of copies of M.
Now consider $D = \mathrm{End}_A(M)$ which is a division algebra since any right A-module map $M \to M$ is either zero or an isomorphism. And from our direct sum decomposition we see that $\mathrm{End}_A(A_A)$ is a matrix algebra over D.
Finally, $A \cong \mathrm{End}_A(A_A)$ as k-algebras. Indeed, an isomorphism is given by mapping $a \in A$ to left-multiplication by a. □

Corollary 4.2. *Using the notation as in the proof, every finitely generated right A-module V is isomorphic to a direct sum of finitely many copies of M. In particular, any two submodules of the same dimension are isomorphic, and $\mathrm{End}_A V \cong \mathrm{Mat}_r(D)$ where r is the number of copies of M in the direct sum and $D = \mathrm{End}_A(M)$.*

Proof. Since V is finitely generated, it is a quotient of a direct sum of finitely many copies of A_A, hence finitely many copies of M. Induction shows that such a quotient is a direct sum of copies of M. □

Note that $Z(\mathrm{Mat}_n(D)) = \{\lambda I : \lambda \in Z(D)\}$. So to classify central simple algebras, it suffices to classify central simple division algebras.

Definition 4.2. Two central simple algebras A, B are equivalent, written $A \sim B$, if $A \otimes_k \mathrm{Mat}_n(k) \cong B \otimes_k \mathrm{Mat}_m(k)$ for some m, n. We write $[A]$ for the equivalence class of A.

The preceding theorem shows that every equivalence class contains a central simple division algebra.

4.2 Brauer Groups

Definition 4.3. The Brauer group $\mathrm{Br}(k)$ is the set of equivalence classes of central simple k-algebras, with group operation $[A][B] = [A \otimes_k B]$.

Let us be reminded that $(a_1 \otimes b_1)(a_2 \otimes b_2) = (a_1 a_2) \otimes (b_1 b_2)$ in $A \otimes_k B$. To see this is well-defined, we need the following result:

Lemma 4.3. *If A, B are central simple k-algebras, so is $A \otimes_k B$.*

Definition 4.4. Let V be a finite-dimensional k-vector space with a chosen basis $\{e_i\}_{i \in I}$. For $v \in V$, its support is $J(\sum_i a_i e_i) = \{i \in I : a_i \neq 0\}$. For a subspace $W \leq V$, $w \in W \setminus \{0\}$ is primordial (with respect to the same basis) if $J(w)$ is minimal among any $J(w')$ for $w' \in W$ nonzero, and $a_i = 1$ for some i (where $w = \sum_i a_i e_i$).

Lemma 4.4. *(i) Suppose $w \in W$ nonzero has $J(w)$ minimal. Then $J(w') \subset J(w)$ if and only if $w' = cw$ for some $c \in k$, in which case we in fact have $J(w') = J(w)$.*
(ii) W is spanned by primordial elements.

Proof. Trivial. □

Remark. The same is true for D-vector spaces, with D a division ring.

Lemma 4.5. *Let A be a k-algebra and D a central division k-algebra. Then every 2-sided ideal I in $A \otimes_k D$ is generated, as a left D-vector space, by $J = I \cap (A \otimes 1)$ (which by the way is an ideal of $A \otimes 1 \cong A$).*

Proof. The D-vector space structure on $A \otimes_k D$ is explicitly given by $\delta(a \otimes \delta') = a \otimes (\delta\delta')$. I is a left D-submodule of $A \otimes_k D$.
Let $\{e_i\}_i$ be a basis for A as a k-vector space. Then $\{e_i \otimes 1\}_i$ is a basis for $A \otimes_k D$ as a left D-vector space.
Suppose r is primordial with respect to this basis. Write $r = \sum_{i \in J(r)} \delta_i (e_i \otimes 1) = \sum_{i \in J(r)} e_i \otimes \delta_i$.
Now for any $\delta \in D$ nonzero, $r\delta \in I$ and $r\delta = \sum \delta_i \delta (e_i \otimes 1)$. In particular, $J(r\delta) = J(r)$. So $r\delta = \delta' r$ for some $\delta' \in D$. As $\delta_j = 1$ for some j (since r is primordial), we have $\delta = \delta'$. So $\delta_i \in Z(D) = k$, i.e. $r \in A \otimes 1$ and we are done. □

By Theorem 4.1, we have

Corollary 4.6. *The tensor product of two finite-dimensional simple k-algebras, at least one of which is central, is again simple.*

And so Lemma 4.3 follows (noting $Z(A \otimes_k B) = Z(A) \otimes_k Z(B)$) and therefore the product on $\mathrm{Br}(k)$ is defined. This group is of course abelian. Its identity is $[k]$. And for a central simple k-algebra A, its inverse is $[A]^{-1} = [A^{\mathrm{op}}]$ where

Definition 4.5. For a ring A, its opposite ring A^{op} has the same underlying set and addition, but whose multiplication is given by $a \cdot_{A^{\mathrm{op}}} b = b \cdot_A a$.

Remark. A right A-module M may be regarded as a left A^{op}-module in the obvious way.

Lemma 4.7. *$A \otimes_k A^{\mathrm{op}} \cong \mathrm{Mat}_n(k)$ where $n = \dim_k A$.*

Proof. Let V be the underlying k-vector space of A (and A^{op}). Consider the k-homomorphism $A \otimes A^{\mathrm{op}} \to \mathrm{End}_k(V), a \otimes a' \mapsto (v \mapsto ava')$. This is injective since $A \otimes_k A^{\mathrm{op}}$ is simple and $1 \otimes 1$ is not mapped to 0, and hence an isomorphism by dimension-counting. □

Example 4.2. 1. If k is algebraically closed, then $\mathrm{Br}(k)$ is trivial. Indeed, any finite-dimensional division algebra has all its elements algebraic over k, and therefore in k.
2. If $k = \mathbb{R}$, then $\mathrm{Br}(k) = \{[\mathbb{R}], [\mathbb{H}]\}$. We'll prove it after drawing connections to cohomology.

4.3 Brauer Groups and Cohomology

Definition 4.6. Let L/k be a field extension. The subgroup $\mathrm{Br}(L/k)$ is the group of classes represented by central simple k-algebras A such that $A \otimes_k L = \mathrm{Mat}_n(L)$ for some n. If this happens, we say A is split by L.

Proposition 4.8. $\mathrm{Br}(k) = \bigcup_{L/k \text{ finite Galois}} \mathrm{Br}(L/k)$.

Theorem 4.9. *Suppose L is finite Galois over k, then we have an isomorphism* $\mathrm{Br}(L/k) \cong H^2(\mathrm{Gal}(L/k), L^\times)$.

Example 4.3. Take $A = \mathbb{H}, k = \mathbb{R}, L = \mathbb{C}, G = \mathrm{Gal}(L/k) = \langle \sigma \rangle \cong \mathbb{Z}/2\mathbb{Z}$. We have $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i \subset \mathbb{H}$ and $\mathbb{H} = \mathbb{C} \oplus \mathbb{C}j$. $\mathbb{C}$ is a maximal subfield of $\mathbb{H}$ and there is a basis $e_1 = 1, e_\sigma = j$ of $\mathbb{H}$ over $\mathbb{C}$ indexed by elements of G. So $e_\sigma x e_\sigma^{-1} = \sigma(x)$ for all $x \in \mathbb{C}$ (for example $ji(-j) = ijk = -i$).
In this case and in general, we define $\phi : G \times G \to L^\times$ via $e_\sigma e_\tau = \phi(\sigma, \tau) e_{\sigma\tau}$. We want to think of an extension of G by $L^\times$ given by a subgroup of the group of units in our algebra. This algebra is associative if and only if ϕ is a 2-cocycle. Note that if we take $e_1 = 1$ then the 2-cocycle is normalised.

Definition 4.7. For a finite Galois extension L/k with Galois group $G = \mathrm{Gal}(L/k)$ and a given normalised 2-cocycle $\phi : G \times G \to L^\times$, the cross product $A = A(L, G, \phi)$ of them is defined as follows:
First, A is an L-vector space with basis $\{e_\sigma : \sigma \in G\}$ given by elements of G. The multiplication law is $e_\sigma e_\tau = \phi(\sigma, \tau) e_{\sigma\tau}$. Since ϕ is a 2-cocycle, this extends to give an associative multiplication with e_1 the multiplicative identity.

The centre of $A(L, G, \phi)$ is $k = ke_1$: Suppose $x = \sum_{\sigma \in G} \lambda_\sigma e_\sigma \in Z(A)$. Then for any $\beta \in L$, we have

$$\sum_{\sigma \in G} \lambda_\sigma \beta e_\sigma = \beta \left(\sum_{\sigma \in G} \lambda_\sigma e_\sigma \right) = \beta x = x \beta = \left(\sum_{\sigma \in G} \lambda_\sigma e_\sigma \right) \beta = \sum_{\sigma \in G} \lambda_\sigma \sigma(\beta) e_\sigma$$

So $\sigma(\beta) = \beta$ whenever $\lambda_\sigma \neq 0$. But this means that $\lambda_\sigma = 0$ for all $\sigma \neq 1$.
So $x = \lambda_1 e_1$ for some $\lambda_1 \in L$. But for all $\tau \in G$ we have $xe_\tau = e_\tau x$ and so

$\tau(\lambda_1) = \lambda_1$. This means that $\lambda_1 \in k$.
A is also simple: Let $I \neq 0$ be a two-sided ideal of A. Take $x = \lambda_{\sigma_1} e_{\sigma_1} + \cdots + \lambda_{\sigma_m} e_{\sigma_m} \in I$ be such that m is minimal. If $m > 1$, we can find $\beta \in L^\times$ such that $\sigma_m(\beta) \neq \sigma_{m-1}(\beta)$. Then $y = x - \sigma_m(\beta) x \beta^{-1} \in I$ is nonzero and has fewer nonzero terms than x, violating minimality of m. Thus $x = \lambda e_\sigma$ for some $\lambda \in L^\times$ and is a unit since it has inverse $x^{-1} = \sigma^{-1}(\lambda^{-1}) e_{\sigma^{-1}}$. Hence $I = A$.
We also have $\dim_k A(L, G, \phi) = (\dim_k L)^2$.
Now suppose ϕ, ϕ' are two cocycles giving the same cohomology class. They they differ by a coboundary. Say $\phi'(\sigma, \tau) = \phi(\sigma, \tau)\sigma(u_\tau) u_{\sigma\tau}^{-1} u_\sigma$ for some $u : G \to L^\times$. Consider the L-linear map $F : A(L, G, \phi') \to A(L, G, \phi), e'_\sigma \mapsto u_\sigma e_\sigma$. One can check that $F(e'_\sigma)F(e'_\tau) = F(e'_\sigma e'_\tau)$ and so F in fact gives a homomorphism $A(L, G, \phi') \to A(L, G, \phi)$. But simplicity and the respective dimension formulae shows that F has to be an isomorphism.
Therefore we get a map $H^2(G, L^\times) \to \mathrm{Br}(k), [\phi] \mapsto [A(L, G, \phi)]$.

Lemma 4.10 (Double Centraliser Theorem)**.** *Let A be a central simple k-algebra with a simple subalgebra B. Then:*
(i) The centraliser $C_A(B)$ is simple.
(ii) $(\dim B)(\dim C_A(B)) = \dim A$.
(iii) $C_A(C_A(B)) = B$.
(iv) If B is central, then $C_A(B)$ is also central and $A = B \otimes_k C_A(B)$.

Proof. Exercise. □

Proposition 4.11. *The map $H^2(G, L^\times) \to \mathrm{Br}(k)$ is a homomorphism.*

Proof. We need to show that if ϕ, ϕ' are 2-cocycles, then $A(L, G, \phi + \phi') \sim A(L, G, \phi) \otimes A(L, G, \phi + \phi')$.
Write $A = A(L, G, \phi), B = A(L, G, \phi'), C = A(L, G, \phi + \phi')$ with L-bases $(e_\sigma), (e'_\sigma), (e''_\sigma)$ respectively. Regard A, B as (left) L-vector spaces, so we can form $V = A \otimes_L B \cong A \otimes_k B / \langle (la) \otimes b - a \otimes (lb) \rangle$. V has a unique right $A \otimes_k B$-structure given by $(a' \otimes_L b')(a \otimes_k b) = (a'a) \otimes_L (b'b)$. It also has a unique left C-structure via $(le''_\sigma)(a \otimes_L b) = (le_\sigma a) \otimes (e'_\sigma b)$.
The two actions commute. So the right action of $A \otimes_k B$ defines a homomorphism $(A \otimes_k B)^{\mathrm{op}} \to \mathrm{End}_C(V)$, which is injective since $A \otimes_k B$ is simple, and surjective by dimension-counting: Certainly the left hand side has dimension n^4 where $n = [L : k]$. We can get $\dim \mathrm{End}_C V = n^4$ by the preceding lemma. Although in this special case, we can prove it directly:
Since C is simple, so is C^{op}. As V is a left C-module, it is a right C^{op}-module. Write $V = \bigoplus^r M$ for a simple C^{op}-module M, and so $\mathrm{End}_C(V) \cong M_r(D^{\mathrm{op}})$ where $D^{\mathrm{op}} = \mathrm{End}_{C^{\mathrm{op}}}(M)$. Also $C^{\mathrm{op}} = \bigoplus^m M$ for some m and $C^{\mathrm{op}} \cong M_m(D^{\mathrm{op}})$ by Theorem 4.1.
Looking at dimensions, we get $\dim V = r \dim M$, $\dim C = m \dim M$, and $\dim \mathrm{End}_C(V) = r^2 \dim D$. Therefore $\dim \mathrm{End}_C(V) \dim C = (\dim V)^2$, and hence our claim.
Consequently, $(A \otimes_k B)^{\mathrm{op}} \to \mathrm{End}_C(V)$ is an isomorphism. But $\mathrm{End}_C(V) \cong \mathrm{Mat}_r(D)^{\mathrm{op}}$ for some division algebra D which is the endomorphism algebra of a simple C-module and $[C] = [D]$. So we are done. □

Remark. 1. By counting dimensions, $[A(L, G, \phi)] = [A(L, G, \phi')]$ iff $A(L, G, \phi) \cong A(L, G, \phi')$, so the map in the proposition is injective.
2. The image of the map is in fact $\mathrm{Br}(L/k)$, hence Theorem 4.9.

3. Conversely, given a class of central simple algebras, we can produce a 2-cocycle: In a central simple division algebra A, we can look at a maximal subfield $L \subset A$ (equivalently maximal commutative subalgebras). From Lemma 4.10, we get $\dim_k A = (\dim_k L)^2$.
Take an L-basis for A, which has size $\dim_k L = [L : k]$. The multiplication of two basis elements give a 2-cocycle for $G = \mathrm{Gal}(L/k)$. Also, within A, L is invariant under conjugation and the action is the Galois action.
4a. A theorem of Wedderburn says that if $\mathrm{Br}(k) = 0$ if k is finite.
4b. For a non-Archimedean local field k, $\mathrm{Br}(k) \cong \mathbb{Q}/\mathbb{Z}$.
4c. For a number field k, we have an exact sequence

$$0 \longrightarrow \mathrm{Br}(k) \longrightarrow \bigoplus_v \mathrm{Br}(k_v) \xrightarrow{\text{sum}} \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

where v runs over all places of k.

5 Lyndon-Hochschild-Serre Spectral Sequence

Let's related the cohomology of a group G with that of a normal subgroup $H \lhd G$ and that of its quotient $Q = G/H$. We already saw an instance of this in Theorem 3.3.
To do this, we might just want to construct a double cochain complex, i.e. data of the form $A = \{A^{\bullet,\bullet}, d', d''\}$, where d' is a map of bidegree $(1,0)$ (i.e. $d' : A^{p,q} \to A^{p+1,q}$), d'' of bidegree $(0,1)$, and we have

$$\begin{cases} (d')^2 = (d'')^2 = 0 \\ d'd'' + d''d' = 0 \end{cases}$$

We may also write $A^n = \bigoplus_{p+q=n} A^{p,q}$ and $d = d' + d''$. Then the identites give $d^2 = 0$. $(A^\bullet, d)$ is known as the total complex. The total cohomology $H^*(A)$ is the cohomology of the total complex.
In our context, we will always have $A^{p,q} = 0$ if one of p, q is negative.
Take projective resolutions $X^\bullet \to \mathbb{Z} \to 0, Y^\bullet \to \mathbb{Z} \to 0$ of the trivial $\mathbb{Z}G$-module and the trivial $\mathbb{Z}Q$-module respectively. $X^\bullet$ is therefore also a projective resolution of the trivial $\mathbb{Z}H$-module.
Let M be a $\mathbb{Z}G$-module, then $\mathrm{Hom}_H(X^\bullet, M)$ is also a $\mathbb{Z}G$-module by $(gf)(x) = g(f(g^{-1}x))$. Since this action restricts to the trivial action of H, we may view $\mathrm{Hom}_H(X^\bullet, M)$ as a $\mathbb{Z}Q$-module.
Set $A^{\bullet,\bullet} = \mathrm{Hom}_Q(Y^\bullet, \mathrm{Hom}_H(X^\bullet, M))$ with $d' = \mathrm{Hom}_Q(d_Y, \mathrm{id})$ and $d'' = (-1)^\bullet \mathrm{Hom}_Q(\mathrm{id}, d_X^*)$.

Remark. There are different conventions for the alternating sign $(-1)^\bullet$. Cartan-Eilenberg puts $(-1)^p$ where p is the degree with respect to the grading of X and we will too.

The total cohomology of A can be approximated in different ways. We will do this by filtering the double complex, in order to filter the cohomology. Spectral sequences give information about the associated graded version of H^*A with respect to this filtration.
First we calculate the cohomology $H''(A)$ with respect to d''. Since $d'd'' = -d''d'$, d' induces a differential on $H''(A)$. We may then calculate $H'(H''(A))$

(alternatively, one could also have calculated $H''(H'(A))$), which is a "first order approximation" to the total complex, known as the E_2-page of the spectral sequence.
Let's consider how $H'(H''(A))$ is computed. Let $a^{p,q}$ be a vertical cocycle (i.e. $d''a^{p,q} = 0$). It defines a class in $H''(A)$ modulo the image under d'' of elements in the $(p, q-1)$-th position.
For $a^{p,q}$ to represent a horizontal cocyle in $H''(A)$ (i.e. under d'), it must be true that $d'a^{p,q}$ (which is at position $(p+1, q)$) is the image under d'' of an element $a^{p+1,q-1}$ in the $(p+1, q-1)$-th position. Thus $d(a^{p,q} - a^{p+1,q-1}) = -d'a^{p+1,q-1} \in A^{p+2,q-1}$. So $a^{p,q} - a^{p+1,q-1}$ is a cocycle modulo everythig two steps to the right of (p, q).
Similarly, $a^{p,q}$ represents a coboundary in $H'(A)$ under d' if there are $b^{p-1,q}$ and $b^{p,q-1}$ such that $d''b^{p-1,q} = 0$, $d'b^{p-1,q} = d''b^{p,q-1} + a^{p,q}$. Thus $d(b^{p-1,q} - b^{p,q-1}) \equiv a^{p,q}$ modulo everything two steps to the right of $(p-1, q)$ (or one step to the right of (p, q)).
These calculations motivate the idea that filtrations of the complex might be helpful.
Let F^pA be the double subcomplex where components to the left of the p-th column is zero. So $(F^pA)^n = \bigoplus_{p'+q=n, p'\geq p} A^{p',q}$. Note that $(F^0A)^n = A^n$ and $(F^pA)^n = 0$ for $p > n$.
Let $C_r^{p,q}$ be the set of elements in $(F^pA)^{p+q}$ whose image under d lies in $(F^{p+r}A)^{p+q+1}$. Each such element is a sum of components along the line $\{(p', q') : p' + q' = n\}$, starting at the (p, q)-th position, such that the vertical and horizontal maps cancel within the band $p \leq p' \leq p + r$. Note that the image under d of such an element lies in $(F^{p+r}A)^{n+1}$ (i.e. it starts at coordinates $(p + r, q - r + 1)$).

Definition 5.1.

$$E_r^{p,q} = \frac{C_r^{p,q} + (F^{p+1}A)^{p+q}}{\mathrm{d}(C_{r-1}^{p-r+1,q+r-2}) + (F^{p+1}A)^{p+q}}$$

Then d induces maps $d_r^{p,q} = E_r^{p,q} \to E_r^{p+r,q-r+1}$ with $d_r^2 = 0$. If we compute the cohomology of the resulting complex (exercise *demonic laughter*), we get $H(E_r, d_r) = E_{r+1}$.
In other words, $E_{r+1}^{p,q} = \ker d_r^{p,q} / \operatorname{Im} d_r^{p-r,q+r-1}$. A representative of an element a in $E_r^{p,q}$ defines an element of a subquotient of $A^{p,q}$ at its upper left (p, q). But its extended structure to the right is crucial in calculating d_r. In particular, $da \in F^{p+1}A$ represents d_r of the element represented by a.
For each fixed (p, q), the differential $d_r^{p,q}$ which starts there and the differental $d_r^{p-r,q+r-1}$ which ends there must vanish for sufficiently large r, since all our terms are in the top left quadrant. It follows that, for each fixed (p, q), $E_r^{p,q}$ eventually stabilises at a common value, denoted by $E_\infty^{p,q}$.
Suppose that $a \in A^n$ is a cocyle starting at $A^{p,q}$ where $p+q = n$ (i.e. $a \in (F^pA)^n$ but $a \notin (F^{p+1}A)^n$). Since $da = 0$, a determines an element of $E_\infty^{p,q}$ since it determines an element of $E_r^{p,q}$ on which $d_r = 0$ for all r. In other words, we have a surjective map from $F^pH^{p+q}(A) = \operatorname{Im}(H^{p+q}(F^pA) \to H^{p+q}(A))$ to $E_\infty^{p,q}$ whose kernel is $F^{p+1}H^{p+q}(A)$.
Thus the filtration of the double complex A induces a (descending) filtration of

the total cohomology $H^n(A)$ for each $n = p + q$, and its factors are

$$\frac{F^pH^{p+q}(A)}{F^{p+1}H^{p+q}(A)} \cong E_\infty^{p,q}$$

Note that the spectral sequence $E_r^{\bullet,\bullet}$ determines these factors, and hence determines the associated graded version $\operatorname{gr} H^*A$ of the totoal cohomology. So we have reduced the calculation of $H^*(A)$ to an extension problem involving $E_\infty^{\bullet,\bullet}$.
Back to group cohomology with $A^{\bullet,\bullet} = \operatorname{Hom}_Q(Y^\bullet, \operatorname{Hom}_H(X^\bullet, M))$. We can take two spectral sequences arising from either $H'(H''(A))$ or $H''(H'(A))$ as the E_2 page. One can prove that the second one shows, relatively easily, that the total cohomology $H^*(A)$ is just $H^*(G, M)$. Then we can use the first sequence to calculate what this cohomology is, using knowledge about the cohomology of H and Q.
We have

$$H''(\operatorname{Hom}_Q(Y^\bullet, \operatorname{Hom}_H(X^\bullet, M))) = \operatorname{Hom}_Q(Y^\bullet, H^*(\operatorname{Hom}_H(X^\bullet, M)))$$

since terms of Y are $\mathbb{Z}Q$-projective and so $\operatorname{Hom}_Q(Y, -)$ is exact. Thus $E_2 = H^*(Q, H^*(H, M))$.
On the other hand, if we look at the second spectral sequence, then we get

$$H'(\operatorname{Hom}_Q(Y^\bullet, \operatorname{Hom}_H(X^\bullet, M))) = H^*(Q, \operatorname{Hom}_H(X^\bullet, M))$$

Lemma 5.1. *$H^p(Q, \operatorname{Hom}_H(X^\bullet, M)) = 0$ for $p > 0$.*

Proof. Since each X^q is $\mathbb{Z}G$-projective, it is a direct summand of a free $\mathbb{Z}G$-module. So it suffices to show the case where $X = \mathbb{Z}G$.
Let $\tilde{M}$ be a trivial $\mathbb{Z}G$-module with the same underlying additive group as M. We claim that there is a $\mathbb{Z}G$-isomorphism $\operatorname{Hom}_H(\mathbb{Z}G, M) \cong \operatorname{Hom}_H(\mathbb{Z}G, \tilde{M})$, where G acts on the left hand side via $(gf)(x) = gf(g^{-1}x)$, and G acts on the right hand side via $(gf')(x) = f'(xg)$ (i.e. as if it were the coinduced module). For $f \in \operatorname{Hom}_H(\mathbb{Z}G, M)$, the isomorphism is meant to take it to $f' \in \operatorname{Hom}_H(\mathbb{Z}G, \tilde{M})$ with $f'(x) = xf(x^{-1})$. And given f', we recover f by $f(x) = xf'(x^{-1})$.
The lemma then follows from Lemma 3.7, noting that we have an isomorphism $\operatorname{Hom}_H(\mathbb{Z}G, \tilde{M}) \cong \operatorname{Hom}(\mathbb{Z}Q, \tilde{M})$. □

Thus $H'(A)$ is concentrated on the line $p = 0$ (i.e. all other terms are zero). Now, $H^0(G/H, \operatorname{Hom}_H(X^\bullet, M)) = \operatorname{Hom}_H(X^\bullet, M)^G = \operatorname{Hom}_G(X^\bullet, M)$. Hence (!!!) $H''(H'(A)) = H^*(\operatorname{Hom}_G(X^\bullet, M)) = H^*(G, M)$. So the E_2-page gives $H^*(G, M)$. Moreover, since this E_2-page is concentrated at $p = 0$, it follows that $E_r = E_\infty$ for $r \geq 2$ and thus E_∞ is concentrated on $p = 0$. The filtration of $H^n(A)$ then has only one nontrivial factor $E_\infty^{0,n} = H^n(G, M)$, i.e. $H^n(A) = H^n(G, M)$.

Example 5.1. Take $G = S_3$ viewed as the extension

$$1 \longrightarrow C_3 \longrightarrow G \longrightarrow C_2 \longrightarrow 1$$

We know that we can calculate $H^*(G, \mathbb{Z})$ from the first spectral sequence, i.e. one with E_2-page $E_2^{p,q} = H^p(C_2, H^q(C_3, \mathbb{Z}))$. The action of C_2 on $H^q(C_3, \mathbb{Z})$ is

induced by conjugation $(12)(123)(12)^{-1} = (132)$.
Since the inversion map on C_3 is a group homomorphism, the induced map is a ring homomorphism on the cohomology ring $H^*(C_3, \mathbb{Z})$. We know that $H^0(C_3, \mathbb{Z}) \cong \mathbb{Z}, H^{2k}(C_3, \mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z}, H^{2k-1}(C_3, \mathbb{Z}) = 0$ for $k > 0$. In fact, $H^*(C_3, \mathbb{Z}) \cong \mathbb{Z}[c]/(3c)$ with c having degree 2.
The action of C_2 on $H^2(C_3, \mathbb{Z})$ is just multiplication by -1. Thus it acts trivially on $H^{4k}(C_3, \mathbb{Z})$ and acts by -1 on $H^{4k+2}(C_3, \mathbb{Z})$. So $H^0(C_2, H^{4k+2}(C_3, \mathbb{Z})) = 0$ and $H^0(C_2, H^{4k}(C_3, \mathbb{Z})) \cong \mathbb{Z}/3\mathbb{Z}$. We also know from example sheet that $H^p(C_2, \mathbb{Z}/3\mathbb{Z}) = 0$ for any $p \geq 1$. So the E_2-page we are calculating is just

$$\begin{array}{ccccccc}
\vdots \\
0 \\
\mathbb{Z}/3\mathbb{Z} \\
0 \\
0 \\
0 & \overset{d_2}{\searrow} \\
\mathbb{Z} & 0 & \mathbb{Z}/2\mathbb{Z} & 0 & \mathbb{Z}/2\mathbb{Z} & 0 & \cdots
\end{array}$$

All differentials either start or finish at 0, so $E_2 = E_\infty$. There is also no nontrivial extension problems. For example, we have

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow H^4(A) \longrightarrow \mathbb{Z}/3\mathbb{Z} \longrightarrow 0$$

which forces $H^4(A)$ to be $\mathbb{Z}/6\mathbb{Z}$. In conclusion,

$$H^n(S_3, \mathbb{Z}) = \begin{cases} \mathbb{Z} & \text{if } n = 0 \\ 0 & \text{if } n \text{ is odd} \\ \mathbb{Z}/2\mathbb{Z} & \text{if } n \equiv 2 \pmod 4 \\ \mathbb{Z}/6\mathbb{Z} & \text{if } n \neq 0, n \equiv 0 \pmod 4 \end{cases}$$

Remark. 1. Usually, calculations of spectral sequences can be quite hard, especially when the differentials are nontrivial.
2. Some information about the product structure on the cohomology are embedded in the spectral sequence.