MAT 250C: Abstract Algebra

Greg DePaul

June 3, 2021

1 Representation Theory of Groups

1.1 Basic Definitions

Let G be a group (usually finite), and F be a field.
Representation theory of G is the study of group actions of G on F-vector spaces V that "respect the vector space structure" in the following sense:

$$g \cdot (v + w) = g \cdot v + g \cdot w \quad \forall g \in G, v, w \in V$$

and

$$g \cdot (\lambda v) = \lambda (g \cdot v) \quad \forall g \in G, \lambda \in F, v \in V$$

We can think of this in terms of representing G via matrices.
A linear G-action as above is the same as given a group homomorphism

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

where $GL(V)$ is the group of invertable F-linear endomorphisms of V. We can justify this since for any given F-linear action, we can let

$$\rho(g) : V \to V$$

be given by $v \to g \cdot v$. Then $\rho(g) \in End_F(V)$ and it is invertible. Also,

$$(\rho(g) \circ \rho(g^{-1}))(v) = g \cdot (g^{-1} v) = (g g^{-1}) \cdot v = v$$

Thats is, $\rho(g) \in GL(V)$. Also,

$$\rho(gh)(v) = (gh) \cdot v = g \cdot (h \cdot v) = (\rho(g) \cdot \rho(h))(v)$$

and similarly $\rho(g^{-1}) = (\rho(g))^{-1}$, which allows us to conclude ρ is a group homomorphism.
On the other hand, given a homomorphism

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

then we can simply define a linear action on V via

$$g \cdot v := f(g)(v)$$

There is a third viewpoint to define these group representations: Consider V is a module and not just over F but over (in general) a non-commutative group ring. Specifically, the set

$$FG := \left\{ \sum_{g_i \in G} a_i g_i : a_i \in F \right\}$$

equipped with the obvious F-vector space structure. Moreover,

$$dim_F(FG) = |G|$$

Such a structure has a multiplication operator which is induced by multiplication in G.

Example 1.1. *Let $F = \mathbb{R}$ and $g_1, \ldots, g_4 \in G$. Then*

$$(7g_1 - \pi g_2) \cdot (g_3 + g_4) = 7g_1g_3 - \pi g_2 g_3 + 7g_1 g_4 - \pi g_2 g4$$

Obviously if G is non-abelian, then so is FG.

Proposition 1.2. *Any given F-linear G-action on V is the same as an FG-module structure on V.*

Proof. ($\Rightarrow$) Given an F-linear G-action on V, we define an FG-module structure on V by linearity, specifically

$$\left(\sum_{g_i \in G} a_i g_i\right) \cdot v := \sum_{g_i \in G} a_i \underbrace{(g_i \cdot v)}_{linear\ G-action}$$

From the property of group actions $g \cdot (h \cdot v) = (gh) \cdot v$, one sees that the above gives an FG-module structure.
($\Leftarrow$) Define a linear G-action simply by restriction. Here, one then obtains:

$$g \cdot (\lambda v) := g \cdot (\lambda e \cdot v) = (g \cdot \lambda e) \cdot v = \lambda (g \cdot e) \cdot v = \lambda g \cdot v$$

where e is the identify of the group. ■

From this section, we have seen 3 slightly different formalisms to talk about group representations.

Example 1.3. *Let $G = D_6 := \langle x, y : x^3 = y^2 = e, yxy^{-1} = x^{-1} \rangle = \{e, x, x^2, y, xy, x^2y\}$. If we have two matrices A and B with*

$$A^3 = B^2 = id$$
$$BAB^{-1} = A^{-1}$$

then we can define a group representation

$$\rho : G \to GL(V)$$
$$x \to A$$
$$y \to B$$

Specifically, such matrices in $GL_2(\mathbb{Z})$ can be:

$$A = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

But we can ask if there exists a 1-dimensional representation?

$$A^3 = B^2 = 1$$

$$A = BAB^{-1} = A^{-1}$$

since 1-dimensional representations over $\mathbb{Z}$ are $\mathbb{Z}$ and therefore commutative. So we see that

$$A^2 = 1 = A^3 \implies A = 1$$

and so $B = \pm 1$. If $\mathbf{1}$ denotes the representation of D_6 with $A = B = 1$ and χ denotes the representation with $A = 1, B = -1,$, then we will show later in the course that every complex finite dimensional representation is isomorphic as G-modules to

$$D_6 \cong \rho^a \oplus \mathbf{1}^b \oplus \chi^c$$

with $a, b, c \geq 0$.

1.2 Direct Sum Decomposition for FG-modules

Assumption: We will assume that G is a finite group and all the FG-modules considered are finitely generated. That is, all group representations are of finite F-dimensions.

First, consider F-modules instead of FG-modules. Recall from linear algebra, if U is a F-vector space and $V \leq U$, then there exists $W \leq U$ with

$$U \cong V \oplus W$$

Maschke showed in 1898 that this result can be generalized for FG-modules.

Theorem 1.4 (Maschke)**.** *Suppose U is a FG-module and V is an FG-submodule. Then if $char(F)$ does not divide $|G|$, there is an FG-submodule W of U with*

$$U \cong V \oplus W$$

as FG-modules.

Proof. Idea: We can use the linear algebraic analogous result together with a clever "averaging map"

$$\phi : U \to U$$

Namely, fix a vector space decomposition $U \cong V \oplus W$, which exists for any FG-module from our study of finite modules over PIDs. Now, we define

$$\phi(u) := \frac{1}{|G|} \sum_{g \in G} g \cdot \pi(g^{-1} \cdot u)$$

where $\pi : U \to V$ is the canonical projection map. Notice, dividing by $|G|$ only makes sense provided $char(F)$ does not divide $|G|$. Now we can make note of a couple of *crucial* observations of ϕ :

- Let $h \in G$. Then

$$\begin{aligned}
\phi(h \cdot u) &= \frac{1}{|G|} \sum_{g \in G} g \cdot \pi(g^{-1} \cdot (h \cdot u)) \\
&= \frac{1}{|G|} \sum_{g \in G} g \cdot \pi(g^{-1} h \cdot u) \\
&= \frac{1}{|G|} \sum_{g \in G} g \cdot \pi((h^{-1} g)^{-1} \cdot u) \\
&= \frac{1}{|G|} \sum_{g \in G} (hh^{-1}) g \cdot \pi((h^{-1} g)^{-1} \cdot u) \\
&= h \cdot \left(\frac{1}{|G|} \sum_{g \in G} h^{-1} g \cdot \pi((h^{-1} g)^{-1} \cdot u) \right) \\
&= h \cdot \left(\frac{1}{|G|} \sum_{g \in G} g \cdot \pi(g^{-1} \cdot u) \right) \\
&= h \cdot \phi(u)
\end{aligned}$$

  So ϕ is not just F-linear, but also respects the FG-module structure. That is, it's an FG-module homomorphism!

- Further, one sees from the definition of ϕ that not only is $Im(\phi) \subset U$, but in fact, $Im(\phi) \subset V$.

- Also, for any $v \in V$, we see that

$$\phi(v) = \frac{1}{|G|} \sum_{g \in G} g \cdot \pi(g^{-1} \cdot v) = \frac{1}{|G|} \sum_{g \in G} g \cdot g^{-1} \cdot v = \frac{1}{|G|} \sum_{g \in G} e \cdot v = v$$

  Hence, $\phi|_V = id$.

So as F-vector space, one has $U \cong V \oplus W$ where $W = Ker(\phi)$ as a result of the First Isomorphism Theorem. But W is in fact an FG-submodule of U since for any $w \in W$

$$\phi(g \cdot w) = g \cdot \phi(w) = 0 \implies g \cdot w \in W$$

Therefore,

$$U \cong V \oplus W$$

now as FG-modules. ■

Definition 1.5. *A semi-simple module is a module that is isomorphic to a direct sum of simple modules.*

Corollary 1.5.1 (Variant of Maschke)**.** *Suppose $char(F)$ does not divide $|G|$. Then every finitely generated FG-module is semi-simple.*

Proof. Let M be a such a finitely generated FG-module. Clearly, if M is simple, then the conclusion is immediate. So suppose M is not simple. That is, M has a nontrivial FG-submodule N. Then by Maschke's Theorem, there exists an FG-submodule P of M with

$$M \cong N \oplus P$$

isomorphic as FG-modules. Turning to the dimensions as F-vector spaces, we notice that $0 < dim_F(N) < dim_F(M) \implies 0 < dim_F(P) < dim_F(M)$. Making a nod to induction, we assume that modules of F-dimension smaller than that of M already satisfy the variant. ■

For the remainder of the course, our hope is to apply Maschke's Theorem in order to give a more general structure result for F-algebras having the above type of property. We can then specialize these result to FG-modules.

1.3 Semi-Simple Algebras

Definition 1.6. *Given F is a field, an F-algebra A is a ring with F-vector space structure such that*

$$a \cdot (\lambda b) = \lambda \cdot (ab) = (\lambda a) \cdot b$$

for all $a, b \in A$ and $\lambda \in F$.

Remark 1.7. *We assume our F-algebras are finite dimensional F-vector spaces and all modules are finitely generated.*

Definition 1.8. *An algebra is semi-simple if all non-zero A-modules are semi-simple.*

Example 1.9. *If $char(F)$ does not divide $|G|$, then FG is a semi-simple algebra.*

Theorem 1.10. *The algebra A is semi-simple if and only if the A-module A is semi-simple.*

To prove this theorem, we will need a small lemma.

Lemma 1.11. *The following statements are equivalent.*

1. *If $N \leq M$, then $N \oplus \tilde{N} \cong M$ for some $\tilde{N}$.*
2. *M is a semi-simple module.*
3. *M is a sum of simple modules.*

Proof.
- (1) $\implies$ (2) By induction on F-dimension.

- (2) $\implies$ (3)
- (3) $\implies$ (1): Let $N \leq M$ and let $\tilde{N} \leq M$ be maximal among submodules of M that satisfy $N \cap \tilde{N} = \{0\}$. We will show that $M = N \oplus \tilde{N}$. If suffices to show that $N + \tilde{N} = M$. Suppose for contradiction that $N + \tilde{N} \neq M$. By assumption (3), there is a simple submodule S of M with the property that $S \not\subset N + \tilde{N}$. Then $S \cap (N + \tilde{N})$ is a submodule of S, which is simple, so it follows that $S \cap (N + \tilde{N}) = \{0\}$. In particular, $\tilde{N} \subset \tilde{N} + S$. But this contradicts the maximality of $\tilde{N}$. Therefore, $N + \tilde{N} = M$.

■

Proof. (Of definition simplification) The forward direction is obvious. To see the other direction, assume A is a semi-simple A-module. Let M be an arbitrary, nonzero, finitely generated A-module. There is a surjection for a suitable r

$$A^r \to M$$
$$(a_i)_i \to \sum_{i=1}^{r} a_i \cdot m_i$$

where $\{m_1, \ldots, m_r\}$ is a generating set of M. But by our assumption, A and hence also A^r is a semi-simple A-module. To complete the proof, it suffices to show that quotients of semi-simple modules are again semi-simple, which we do in the next proposition. ■

Proposition 1.12. *Submodules and quotients of semi-simple modules are semi-simple.*

Proof. We already know that submodules N of a module M aid in the decomposition of M:

$$M \cong N \oplus \tilde{N}$$

Therefore, $N \cong M/\tilde{N}$, and so we simply need to show that quotients of semi-simple modules are semi-simple. Since M is a semi-simple module, we can write

$$M \cong \oplus_{i=1}^{k} S_i$$

with each S_i simple. So we can consider the restriction $\phi|_{S_i}$. Then its kernel either $\{0\}$ or S_i.

- *Case:* If $Ker(\phi) = \{0\}$, then $Im(\phi|_{S_i}) \cong S_i$.
- *Case:* If $Ker(\phi) = S_i$, then $Im(\phi|_{S_i}) \cong \{0\}$.

Since ϕ is surjective, then

$$N = \phi(S_1) + \ldots + \phi(S_k)$$

in which each summand is either $\{0\}$ or isomorphic to S_i for some i. So if $N \neq \{0\}$, then N is the sum of simple modules. But by the previous lemma, we know this implies that N is the direct sum of simple modules, and therefore N is semi-simple. ■

Lemma 1.13 (Schur)**.** *A non-zero A-module homomorphism between simple A-modules is an isomorphism.*

Proof. Suppose $\phi : V \to W$ a homomorphism between simple modules V and W. Then $Ker(\phi) \leq V \implies Ker(\phi) = \{0\}$ or $Ker(\phi) = V$. Since we assume $\phi \neq 0$,t hen $Ker(\phi) = \{0\} \implies$ injective.
Also, $Im(\phi) \leq W \implies Im(\phi) = \{0\}$ or $Im(\phi) = W$. Since $\phi \neq 0$, then $Im(\phi) = 0 \implies$ surjective. ■

Theorem 1.14. *Suppose A is a semi-simple algebra and decompose A as*

$$A \cong S_1 \oplus \ldots \oplus S_k$$

as the direct sum of simple A-modules. Then any A-module is isomorphic to

$$S_1^{a_1} \oplus \ldots \oplus S_k^{a_k}$$

for integers $a_i \geq 0$.

Proof. It suffices to show that each simple A-module V is isomorphic to some S_i. Let $v \in V, v \neq 0$. Consider

$$\begin{aligned} \phi : A &\to V \\ a &\to a \cdot v \end{aligned}$$

Clearly this is an A-module homomorphism. Now $A \cong \bigoplus_i S_i$.. Then ϕ is a non-zero homomorphism. So there is an i such that

$$\phi|_{S_i} \neq 0$$

By Schur's Lemma, we know $\phi|_{S_i}$ is an isomorphism, so $V \cong S_i$. ■

1.4 Classifying Semi-Simple F-Algebras

Motivation: We can apply this to FG and hence to representation theory of G.

Definition 1.15. *Recall, a division algebra is an algebra such that every non-zero element has an inverse.*

Theorem 1.16 (Wedderburn)**.** *An algebra A is semi-simple if and only if it is isomorphic to a direct sum of matrix algebras over division algebras.*

Question 1.17. *Where do the division algebras come into play?*

Proposition 1.18. *Suppose M is a simple A-module. Then $End_A(M)$ is a division algebra.*

Proof. Suppose M is a simple A-module. Consider $End_A(M)$. If $\phi \in End_A(M)$ is nonzero, then by Schur's lemma, ϕ is an isomorphism and therefore there must exist an inverse. Then we see that $End_A(M)$ is a division algebra. ■

Remark 1.19. *These division algebras $End_A(M)$ will, in practice, simply be isomorphic to F.*

Proposition 1.20. *Suppose F is algebraically closed. Let $\phi \in End_A(M)$. Then we claim ϕ is just scalar multiplication by some scalar in F.*

Proof. View M as a finitely dimensional F-vector space. Then, since ϕ is algebraically closed, ϕ as an eigenvalue λ in F! Hence,

$$\phi - \lambda \cdot id : M \to M$$

has a non-trivial kernel. But, since M is simple, then $Ker(\phi - \lambda \cdot id) = M$. Hence, ϕ is given by scalar multiplication by λ. ■

Corollary 1.20.1.

$$\begin{aligned} End_A(M) &\cong F \\ \phi &\to \lambda \end{aligned}$$

Proposition 1.21. *If D is a division algebra, then $M_n(D)$ is a semi-simple algebra. Moreover, $M_n(D) \cong (D^n)^n$ where D^n is the unique simple $M_n(D)$ module.*

Proof. By the previous results, in order to show that $M_n(D)$ is a semi-simple algebra, it suffices to show that $M_n(D)$ is a semi-simple $M_n(D)$-module. First, we notice that D^n, viewed as the column vectors of entries in D, is simple since letting $V \leq D^n$ be non-zero, then we want to show that $V = D^n$. Since the submodule is non-zero, there is a non-zero $v \in V$, written

$$v = \begin{pmatrix} \vdots \\ * \\ \vdots \end{pmatrix}$$

where $*$ is a non-zero k-th entry. We can act on this element by elements in this matrix algebra. Specifically,

$$A = \begin{pmatrix} 0 & & & & & \\ & \ddots & & & & \\ & & *^{-1} & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

where $*^{-1}$ is located at the $[k,k]$ entry. Then we see that by direct calculation:

$$A \cdot v = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = e_k \in V$$

Surely, we can multiply by permutation matrices in order to get all of the other canonical basis elements $\{e_1, \ldots, e_n\}$ all of which are in V. Moreover, it follows that

$$D^n = span\{e_1, \ldots, e_n\} \subset V \subset D^n$$

So we get $V = D^n$. Hence, D^n is a simple $M_n(D)$-module.

Let us use this to show that $M_n(D)$ is a semi-simple $M_n(D)$-module. Consider

$$c_i := \left\{ \begin{pmatrix} \vdots & \ldots & \vdots & *_1 & \vdots & \ldots & \vdots \\ 0 & \ldots & 0 & \vdots & 0 & \ldots & 0 \\ \vdots & \ldots & \vdots & *_n & \vdots & \ldots & \vdots \end{pmatrix} : *_i \in D \right\}$$

Then we see that

$$M_N(D) \cong C_1 \oplus \ldots \oplus C_n \cong (D^n)^n$$

as $M_n(D)$-modules. Since $(D^n)^n$ is a simple $M_n(D)$-module, then $M_n(D)$ is a semi-simple $M_n(D)$-module, so by our classification theorem, $M_n(D)$ is a semi-simple algebra and we also see that the unique simple $M_n(D)$-module is isomorphic to D^n.

■

Corollary 1.21.1. *If $A \cong \oplus_i M_{n_i}(D_i)$ with D_i all division algebras, then A is semi-simple.*

Proof. We have shown that each $M_{n_i}(D_i)$ is a semi-simple $M_{n_i}(D_i)$-module by the previous result. Therefore, $M_{n_i}(D_i)$ is a semi-simple A-module. Looking at all of A, we see that A is a semi-simple A-module and hence a semi-simple algebra. ■

Proof. (Wedderburn's Theorem)
($\Rightarrow$) We want to show that if $A \cong S_1^{n_1} \oplus \ldots \oplus S_r^{n_r}$ as A-modules, where each S_i is simple and $S_i \neq S_j$ if $i \neq j$, then

$$A \cong M_{n_1}(End_A(S_1)^{op}) \oplus \ldots \oplus M_{n_r}(End_A(S_r)^{op})$$

which gives one direction of the theorem. This is demonstrated by the previous proposition and corollary.

Note 1.22. *If B is an algebra, then the "opposite algebra" B^{op} is obtained from B by defining the product via*

$$a * b := b \cdot a$$

($\Leftarrow$) To prove this, we make use of the following lemmas:

Lemma 1.23. $B^{op} \cong End_B(B)$

Proof. An obvious set-theoretic map

$$\begin{aligned} \nu : End_B(B) &\to B^{op} \\ \phi &\to \phi(1) \end{aligned}$$

Further, we see that

$$\phi(b) = \phi(b \cdot 1) = b \cdot \phi(1)$$

and hence ν is injective. Clearly, ν is surjective. Further,

$$\nu(\phi \circ \psi) = \phi(\psi(1)) = \phi \circ (\psi(1) \cdot 1) = \psi(1) \cdot \phi(1) = \nu(\psi) \cdot v(\phi) = \nu(\phi) * \nu(\psi)$$

So we conclude that ν is an algebra isomorphism. ■

Lemma 1.24. *Suppose $S_1, S_2, \ldots, S_r$ are distinct simple A-modules. Let*

$$U_1 \cong S_1^{n_1}, \ldots, U_r \cong S_r^{n_r}$$

Then

$$End_A(U_1 \oplus U_2 \oplus \ldots \oplus U_r) \cong End_A(U_1) \oplus End_A(U_2) \oplus \ldots \oplus End_A(U_r)$$

Proof. We want to construct an F-algebra homomorphism

$$End_A(\bigoplus_{i=1}^{r} U_i) \to \bigoplus_{i=1}^{r} End_A(U_i)$$

To do so, we need to make use of the Jordan-Holder Theorem over A-modules, in that there exists a composition series and they are all equivalent. So we consider

$$\phi(U_i) = \phi(S_i^{n_i}) \cong S_i$$

is well-defined. Suppose for contradiction that $\phi(U_i) \not\subset U_i$. Then the image of $\phi(U_i)$ in $\bigoplus_{j=1}^{r} U_j/U_i \cong \bigoplus_{j \neq i} U_j$ is non-zero $\implies$ contradiction. Hence $\phi(U_i) \subset U_i$ for all $1 \leq i \leq r$. This tells us that

$$\phi|_{U_i} \in End_A(U_i)$$

and therefore, we may define a map

$$\begin{aligned} \nu : End_A(\bigoplus_{i=1}^{r} U_i) &\to \bigoplus_{i=1}^{r} End_A(U_i) \\ \phi &\to (\phi|_{U_i})_i \end{aligned}$$

Clearly, $\nu(\phi \circ \psi) = \nu(\phi) \circ \nu(\psi)$ since $(\phi \circ \psi)|_{U_i} = \phi|_{U_i} \circ \psi|_{U_i} \implies \nu$ is an F-algebra homomorphism. If $\nu(\phi) = 0 \implies \phi|_{U_i} = 0$ for all i, so $\phi = 0 \implies$ injective. Given $(\phi_i)_i \in \bigoplus_{i=1}^{r} End_A(U_i)$, we can simply define $\phi \in End_A(\bigoplus_{i=1}^{r} U_i)$ via

$$\phi\left(\sum_{i=1}^{r} v_i\right) = \sum_{i=1}^{r} \phi_i(v_i)$$

Then $\nu(\phi) = (\phi_i)_i \implies$ surjective. ■

So we see that to understand algebras like $End_A(\bigoplus_{i=1}^{r} U_i)$, it suffices to understand algebras like

$$End_A(S^n)$$

where S is a simple A-module. To do so, we turn to one final lemma:

Lemma 1.25. *$End_A(S^n) \cong M_n(End_A(S))$ if S is a simple A-module.*

Proof. Suppose we start with a matrix in $M_n(End_A(S))$. Then we can try to identify a bijection into $End_A(S^n)$. Let

$$B = (b_{i,j})_{n\times n} \in M_n(End_A(S))$$

Now we can define an element $\alpha(B)$ in $End_A(S^n)$ simply by matrix-vector multiplication:

$$B \cdot \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} \vdots \\ \sum_{j=1}^{n} b_{i,j}(s_j) \\ \vdots \end{pmatrix}$$

Then, clearly, we see that

$$\alpha(B)(\bar{s} + \bar{t}) = \alpha(B)(\bar{s}) + \alpha(B)(\bar{t})$$

since $b_{i,j}(s_j + t_j) = b_{i,j}(s_j) + b_{i,j}(t_j)$. Similarly, for some $a \in A$

$$\alpha(B)(a \cdot \bar{s}) = a \cdot \alpha(B)(\bar{s})$$

Therefore, we see that $\alpha(B) \in End_A(S^n)$. Moreover, we have a map

$$\alpha : M_n(End_A(S)) \to End_A(S^n)$$

which is an F-algebra homomorphism, with the properties:

$$\alpha(B + C)(\bar{s}) = \alpha(B)(\bar{s}) + \alpha(C)(\bar{s})$$

$$\alpha(B \cdot C)(\bar{s}) = (\alpha(B) \cdot \alpha(C))(\bar{s})$$

Notice, α is injective since if $\alpha(B) = 0$, then

$$\alpha(B) \begin{pmatrix} 0 \\ \vdots \\ s_j \\ 0 \\ \vdots \end{pmatrix} = 0 = \begin{pmatrix} b_{0,j}s_j \\ \vdots \\ b_{n,j}s_j \end{pmatrix}$$

So each $b_{i,j}$ $(1 \leq i, j \leq n)$ has non-zero kernel! So

$$b_{i,j} : S \to S$$

where S is a simple A-module, and so by Schur's lemma, we can conclude $b_{i,j} = 0$ for all i, j. Therefore, $B = 0$.

Also, α is surjective, which we can showing by starting with $\phi \in End_A(S^n)$. Then we notice that

$$\phi \begin{pmatrix} 0 \\ \vdots \\ s_j \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} \phi_{i,j}(s_j) \\ \vdots \\ \phi_{i,j}(s_j) \end{pmatrix}$$

Then $\phi_{i,j} \in End_A(S)$. Then $\alpha((\phi_{i,j})_{n\times n}) = \phi \implies$ surjective! ∎

Finally, we can finish the proof Wedderburn's Theorem! Suppose A is a semi-simple A-module. Then A is a semi-simple A-module, and hence we can write

$$A \cong \bigoplus_{i=1}^{r} S_i^{n_i}$$

where each S_i is a simple A-module and $S_i \ncong S_j$ if $i \neq j$. Now comes the key trick in the proof: Then

$$A^{op} \cong End_A(A) \cong End_A(\bigoplus_{i=1}^{r} S_i^{n_i}) \cong \bigoplus_{i=1}^{r} End_A(S_i^{n_i}) \cong \bigoplus_{i=1}^{r} M_{n_i}(End_A(S_i))$$

So clearly,

$$A \cong (A^{op})^{op} \cong \left(\bigoplus_{i=1}^{r} M_{n_i}(End_A(S_i))\right)^{op} \cong \bigoplus_{i=1}^{r} M_{n_i}(End_A(S_i))^{op} \cong \bigoplus_{i=1}^{r} M_{n_i}(End_A(S_i)^{op})$$

Recall $End_A(S_i)$ is a division algebra $\implies$ $End_A(S_i)^{op}$ is a division algebra as well, completing the proof. ■

1.5 Consequences of Wedderburn's Theorem on FG

Let's go back from general semi-simple algebras and instead focus on the group ring FG. **Assume** $char(F)$ does not divide $|G|$.
Recall that if we write

$$FG \cong \bigoplus_{i=1}^{r} S_i^{n_i}$$

where each S_i is a simple FG-module, and $S_i \ncong S_j$ for $i \neq j$, then $S_1, \ldots, S_r$ are exactly all the simple FG-modules and every FG-module M is isomorphic to

$$M \cong \bigoplus_{i=1}^{n} S_i^{a_i}$$

for unique a_i's.
We would like to answer two questions:

1. Given a group, what is this r? Does this value have a group theoretic meaning?
2. Can we get a handle on $dim_F(S_i)$. We saw earlier that we can identify representations in arbitrary dimensions.

We can motivate the second of these questions by the following calculation.

Example 1.26. *Suppose it happens that F is algebraically closed and $FG \cong S^n$ for some n and some simple FG-module S. Then*

$$dim_F(FG) = n \cdot dim_F(S)$$

Moreover, using Wedderburn, we see that

$$FG \cong M_n(F) \implies dim_F(FG) = n^2$$

Therefore, we can conclude that

$$dim_F(S) = n$$

which is equal to the multiplicity of S in the decomposition of FG in terms of simple modules.

This phenomenon can be extended generally:

Example 1.27. *Suppose*

$$FG \cong \bigoplus_{i=1}^{r} S_i^{n_i} \cong \bigoplus_{i=1}^{r} \underbrace{M_{n_i}(F)}_{(\mathbb{C}^{n_i})^{n_i}}$$

So we see that

$$dim_F(S_i) = multiplicity\ within\ decomposition = n_i$$

Definition 1.28. *The set* $\{n_i := dim_F(S_i) : 1 \leq i \leq r\}$ *is called the* degrees of G.

Proposition 1.29. $\sum_{i=1}^{r} dim_F(S_i)^2 = |G|$

Proof. Clearly,

$$|G| = dim_F(FG) = dim_F(\bigoplus_{i=1}^{r} M_{n_i}(F)) = \sum_{i=1}^{r} n_i^2 = \sum_{i=1}^{r} dim_F(S_i)^2$$

■

Now we turn to the first question.

Proposition 1.30. *The number* r *of simple* $\mathbb{C}F$*-modules equals the number of conjugacy classes in* G.

Proof. The key idea of this proof relies on calculating the $\mathbb{C}$-dimension of $Z(\mathbb{C}G)$ in two different ways. Recall

$$Z(\mathbb{C}G) = \{z \in \mathbb{C}G : zy = yz \ \ \forall\ y \in \mathbb{C}G\}$$

Initially using Wedderburn's Theorem, we see

$$Z(\mathbb{C}G) \cong Z(\bigoplus_{i=1}^{r} M_{n_i}(\mathbb{C})) \cong \bigoplus_{i=1}^{r} Z(M_{n_i}\mathbb{C})$$

The only matrices within $Z(M_{n_i}\mathbb{C})$ are the matrices of the form

$$\begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda \end{pmatrix} = \lambda I_{n\times n}$$

for some $\lambda \in \mathbb{C}$. So $dim_{\mathbb{C}}(Z(\mathbb{C}G)) = r$. On the other hand,

$$\sum_{g\in G} a_g g \in Z(\mathbb{C}G)$$

if and only if

$$\sum_{g\in G} a_g g\tilde{g} = \sum_{g\in G} a_g \tilde{g} g$$

for any $\tilde{g} \in G$. So

$$\implies \sum_{g\in G} a_g g = \sum_{g\in G} a_g \tilde{g} g \tilde{g}^{-1}$$

But then a_g is constant within the conjugacy class of g. Therefore, by this calculation, we see

$$r = dim_{\mathbb{C}} Z(\mathbb{C}G) = \text{number of conjugacy classes}$$

■

1.6 The Character Function

Let V be a $\mathbb{C}G$-module and

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

be the corresponding group representation. We assume G is a finite group. Since G is finite, we can stipulate for each $g \in G$, let $i := ord(g)$, so

$$p(g)^i - id = \rho(g^i) - id = 0$$

So we see that the minimal polynomial $x^i - 1$ has distinct roots and hence $\rho(g)$ is a diagonalizable matrix. Note, the group matrix representations aren't necessarily simultaneously diagonalizable. Furthermore, since $\rho(g)^i = id$, then all eigenvalues of $\rho(g)$ are ith roots of unity. So we can write

$$A\rho(g)A^{-1} = \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix}$$

So we can define

$$\chi(g) := trace(\rho(g)) = \lambda_1 + \ldots + \lambda_n$$

to get a function

$$\chi : G \to \mathbb{C}$$

This is called the character of ρ. We would like to identify some basic properties of the character function.

Proposition 1.31. $\chi(e) :=$ *dimension of* ρ *and*

$$|\chi(g)| = |\lambda_1 + \ldots + \lambda_n| \leq \chi(e) = \textit{dimension of } \rho$$

Proposition 1.32. $\chi(g^{-1}) = trace(\rho(g^{-1})) = \lambda_1^{-1} + \ldots + \lambda_n^{-1} = \bar{\lambda}_1 + \ldots + \bar{\lambda}_n = \overline{\sum_{i=1}^n \lambda_i} = \overline{\chi(g)}$

Question 1.33. *Does the process*

$$\mathbb{C}G\textit{-module} \to \chi$$

loose information?

Theorem 1.34. *Two* $\mathbb{C}G$*-modules are isomorphic if and only if they have the same character.*

Proof. Let $S_1, S_2, \ldots, S_r$ be the simple $\mathbb{C}G$-modules and let $\chi_1, \ldots, \chi_r$ be the corresponding characters. We can extend these characters linearly to functions

$$\chi_i : \mathbb{C}G \to \mathbb{C}$$

Recall from Wedderburns theorem,

$$\mathbb{C}G \cong \bigoplus_{i=1}^{r} M_{n_i}(\mathbb{C})$$

Let e_i in $\mathbb{C}G$ that maps to id_{n_i} in $M_{n_i}(\mathbb{C})$ while acting as the zero function on all other simple modules. Then

$$\chi_i(e_i) = n_i \quad \chi_j(e_i) = 0$$

for all $i \neq j$. Suppose now there are complex scalars $c_1, \ldots, c_r$ that satisfy

$$\sum_{i=1}^{r} c_i \chi_i \equiv 0$$

Evaluating on e_i, $\implies c_i n_i = c_i \chi_i(e_i) = 0 \implies c_i = 0$. Then we see that the irreducible characters are linearly independent over $\mathbb{C}$. So suppose now V_1, V_2 are $\mathbb{C}G$-modules with

$$\chi_{V_1} = \chi_{V_2}$$

we know

$$V_1 = \bigoplus_{i=1}^{r} S_i^{a_i}$$

for some unique a_i's. Also,

$$V_2 \cong \bigoplus_{i=1}^{r} S_i^{b_i}$$

for some unique b_i's. Then it follows,

$$\sum_{i=1}^{r} a_i \chi_i = \chi_{V_1} = \chi_{V_2} = \sum_{i=1}^{r} b_i \chi_i$$

But by the linear independence of characters, we see that $a_i = b_i$ for all i. Therefore, $V_1 \cong V_2$. ■

1.7 Extension of Tensor Products

Definition 1.35. *Let R and S be rings and let V be an (R, S)-bimodule with the properties*

$$(r \cdot m) \cdot s = r \cdot (m \cdot s)$$

for all $r \in R, s \in S, v \in V$. Let W be a left S-module. Let U be another R-module. A set theoretic map

$$\phi : V \times W \to U$$

is called <u>balanced</u> provided

$$\phi(v_1 + v_2, w) = \phi(v_1, w) + \phi(v_2, w)$$
$$\phi(v, w_1 + w_2) = \phi(v, w_1) + \phi(v, w_2)$$
$$\phi(v \cdot s, w) = \phi(v, s \cdot w)$$
$$\phi(r \cdot v, w) = r \cdot \phi(v, w)$$

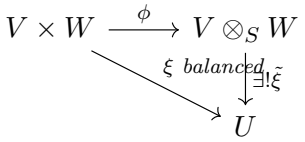
Definition 1.36. *Let R and S be rings and let V be an (R, S)-bimodule with the properties*

$$(r \cdot m) \cdot s = r \cdot (m \cdot s)$$

for all $r \in R, s \in S, v \in V$. Let W be a left S-module. Then we define the <u>tensor product</u> $V \otimes_S W$ with the balanced map

$$\phi : V \times W \to V \otimes_S W$$

such that ϕ satisfies the universal property that the diagram



commutes. Moreover,

$$\xi = \tilde{\xi} \circ \phi$$

Note 1.37. *We can often use $v \otimes w = \phi(v, w)$.*

Proposition 1.38. *$V \otimes_S W$ exists and is unique up to isomorphism.*

Proof. The R-module generated by symbols $v \otimes w$ and the following relations works:

$$(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$$
$$v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2$$
$$v \cdot s \otimes w = v \otimes s \cdot w$$
$$(r \cdot v) \otimes w = r \cdot (v \otimes w)$$

■

Remark 1.39. *If $R = S$ and is a field, then we recall that*

$$\textit{left } R\textit{-modules} \leftrightarrow \textit{right } R^{op}\textit{-modules}$$

But since fields are commutative, then F-vector space is (F, F)-bimodule and we can apply the previous tensor product construction obtain

$$V \otimes_F W$$

for F-vector spaces V, W. Further, one sees that if $\{v_i\}_i, \{w_j\}_j$ are bases of V, W, then $\{v_i \otimes w_j\}$ is a F-vector space basis of $V \otimes_F W$.

Question 1.40. *Can we extend this into FG-modules?*

Let V, W be FG-modules. Then we want our definition to follow a diagonal action for the elements of $V \otimes_F W$:

$$v \otimes w \to gv \otimes gw$$

To make this rigorous, we consider the mapping

$$\begin{aligned} \nu : V \times W &\to V \otimes_F W \\ (v, w) &\to gv \otimes gw \end{aligned}$$

Clearly ν is a balanced mapping. Further, we see that

$$\nu(\lambda v, w) = g \cdot (\lambda v) \otimes g \cdot w = \lambda \cdot (gv) \otimes (gw) = (g \cdot v) \cdot \lambda \otimes g \cdot w = g \cdot v \otimes \lambda \cdot (g \cdot w) = gv \otimes g(\lambda w) = \nu(v, \lambda w)$$

Then, by the universal property of the balanced map, there exists $\tilde{n}u$ with

$$\begin{array}{ccc} V \times W & \xrightarrow{\phi} & V \otimes_F W \\ & \overset{\nu}{\searrow} & \downarrow \exists ! \tilde{\nu} \\ & & V \otimes_F W \end{array}$$

explicitly,

$$\tilde{\nu} : v \otimes w \to gv \otimes gw$$

Remark 1.41. *We can now compare this structure to another FG-module.*

Let U, V be FG-modules. Consider the F-vector space $Hom_F(U, V)$. Then, putting the FG-module structure on this, we see for $\phi \in Hom_F(U, V)$ and $g \in G$, $g\phi \in Hom_F(U, V)$ is given by

$$(g\phi)(u) = g \cdot \phi(g^{-1} \cdot v)$$

Further, we can see this action respects addition by

$$\begin{aligned} (g \cdot (\phi_1 + \phi_2))(v) &= g \cdot (\phi_1 + \phi_2)(g^{-1}u) \\ &= g(\phi_1(g^{-1}u) + \phi_2(g^{-1}u)) \\ &= g\phi_1(g^{-1}u) + g\phi_2(g^{-1}u) \\ &= (g \cdot \phi_1)(u) + (g \cdot \phi_2)(u) \end{aligned}$$

and also

$$\begin{aligned} (g(h\phi))(u) &= g \cdot (h\phi)(g^{-1}v) \\ &= g(h\phi(h^{-1}g^{-1}u)) \\ &= (gh)\phi((gh)^{-1}u) \\ &= ((gh) \cdot \phi)(u) \end{aligned}$$

Definition 1.42. *Let $V = F$ with the trivial G-action. Then*

$$U^* := Hom_F(U, F)$$

is the dual representation of U.

Proposition 1.43. *For FG-modules U, V, then*

$$U^* \otimes_F V \cong Hom_F(U, V)$$

as FG-modules.

Proof. First, we define the isomorphism of F-vector space

$$\xi : U^* \otimes_F V \to Hom_F(U, V)$$
$$\xi(\phi \otimes v)(u) = \phi(u) \cdot v$$

Namely, let $u_1, \ldots, u_n$ be a basis of U, let $\phi_1, \ldots, \phi_n \in U^*$ be the dual basis. Then

$$\phi_i(u_j) = \delta_{i,j}$$

Let $\sum_{i,j} a_{i,j}\phi_i \otimes v_j \in U^* \otimes_F V$. Then we see

$$\sum_{i,j} a_{i,j}\phi_i \otimes v_j = \sum_{i,j} \phi_i \otimes a_{i,j}v_j$$

Then every element of $U^* \otimes_F V$ can be written as

$$\sum_{i=1}^{n} \phi_i \otimes w_i$$

for some $w_i \in V$. Suppose now

$$\xi\left(\sum_{i=1}^{n} \phi_i \otimes w_i\right) = 0 \in Hom_F(U, V)$$

In particular, evaluating on u_j, we get

$$0 = \sum_{i=1}^{n} \phi_i(u_j) \otimes w_i = w_j$$

for all $j \implies Ker(\xi) = 0$. So

$$\xi : U^* \otimes_F V \to Hom_F(U, V)$$

is an injective mapping. Since these two share the same dimension, then we see immediately that ξ is surjective. Lastly, to see that ξ is an FG-module isomorphism,

$$\begin{aligned}
\xi\left(g \cdot \sum_{i=1}^{n} \phi_i \otimes w\right)(u) &= \xi\left(\sum_{i=1}^{n} g\phi_i \otimes gw\right)(u) \\
&= \sum_{i=1}^{n} (g\phi_i)(u) g w_i \\
&= \sum_{i=1}^{n} \phi_i(g^{-1}u) g w_i
\end{aligned}$$

compared with

$$\begin{aligned}(g \cdot \xi(\sum_{i=1}^{n} \phi_i \otimes w_i))(u) &= g(\xi(\sum_{i=1}^{n} \phi_i \otimes w_i))(g^{-1}u) \\ &= g \sum_{i=1}^{n} \phi_i(g^{-1}u) w_i \\ &= \sum_{i=1}^{n} \phi_i(g^{-1}u) g w_i\end{aligned}$$

■

1.8 Calculating Characters for these Tensor Extensions!

Proposition 1.44. $\chi_{U \otimes_F V} = \chi_U \cdot \chi_V$

Proof. Let $g \in G$, let $\{v_i\}_i$ and $\{v_j\}_j$ be eigenbases for g with eigenvalues $\{\lambda_i\}_i$ and $\{\mu_j\}_j$, respectively

$$g \cdot (v_i \otimes v_j) = g u_i \otimes g v_j = \lambda_i v_i \otimes \mu_j v_j = \lambda_i \mu_j \cdot (u_i \otimes v_j)$$

$$\implies \chi_{U \otimes_F V}(g) = \sum_{i,j} \lambda_i \mu_j = \sum_i \lambda_i \cdot \sum_j \mu_j = \chi_U(g) \cdot \chi_V(g)$$

■

Proposition 1.45. $\chi_{U^*} = \overline{\chi_U}$

Proof. Let $g \in G$, let $\{u_i\}_i$ be an eigenbasis of U with eigenvalues $\{\lambda_i\}$. Then

$$g u_i = \lambda_i u_i \implies g^{-1} u_i = \lambda_i^{-1} u_i$$

This makes sense because eigenvalues are roots of unity. Now let $\{\phi_i\}_i$ be the dual basis. Then

$$\phi_i(u_j) = \delta_{i,j}$$

Then

$$(g \cdot \phi_i)(u_j) = g \cdot \phi_i(g^{-1} u_j) = g \lambda_j^{-1} \phi_i(u_j) = \lambda_j^{-1} \phi_i(u_j) = \lambda_j^{-1} \delta_{i,j}$$

Hence, $g \cdot \phi_i = \lambda_i^{-1} \phi_i = \overline{\lambda_i} \cdot \phi_i \implies \chi_{U^*}(g) = \sum_i \overline{\lambda_i} = \overline{\sum_i \lambda_i} = \overline{\chi_U(g)}$. ■

Proposition 1.46. $\chi_{Hom_F(U,V)} = \overline{\chi_U} \cdot \chi_V$

Proof.

$$\chi_{Hom_F(U,V)} = \chi_{U^* \otimes_F V} = \chi_{U^*} \cdot \chi_V = \overline{\chi_U} \cdot \chi_V$$

■

1.9 Inner Product of Characters

Definition 1.47. *Let χ_1, χ_2 be characters of $\mathbb{C}G$-modules. Then define*

$$\langle \chi_1, \chi_2 \rangle := \frac{1}{|G|} \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)}$$

Question 1.48. *What is the representation theoretic meaning of this inner product?*

To foreshadow the answer, this is related to how $\mathbb{C}G$-modules associated to χ_1 and χ_2 are related to one another.

Lemma 1.49. *For a $\mathbb{C}G$-module W, let*

$$W^G := \{w \in W : gw = w \ \forall \ g \in G\}$$

Then

$$dim_{\mathbb{C}} W^G = \frac{1}{|G|} \sum_{g \in G} \chi_W(g)$$

where χ_W is the character of W.

Proof. Let $A = \sum_{g \in G} g$ and $a = A/|G|$. We can view a as a map

$$a : W \to W$$

One sees that $Im(a) = W^G$. Also, notice

$$a^2 = \frac{\sum_{h \in G} h \sum_{g \in G} g}{|G|^2} = \frac{\sum_{h \in G} a}{|G|} = a$$

So the minimal polynomial of a must divide $x^2 - x = x(x-1)$. So the eigenvalues of a are either 0 or 1. Hence,

$$dim_{\mathbb{C}} W^G = dim_{\mathbb{C}} Im(a) = Trace(a) = Trace\left(\frac{1}{|G|} \sum_{g \in G} g\right) = \frac{1}{|G|} \sum_{g \in G} \chi_W(g)$$

■

Now we have to tools necessary to get a handle on the meaning of $\langle \chi_Y, \chi_V \langle$.

Theorem 1.50. *Suppose U, V are $\mathbb{C}G$-modules. Then*

$$\langle \chi_U, \chi_V \rangle = dim_{\mathbb{C}} Hom_{\mathbb{C}G}(U, V)$$

Proof. We can relate $Hom_{\mathbb{C}G}(U, V)$ to the space of G-invariants. Recall, that $Hom_{\mathbb{C}}(U, V)$ has a $\mathbb{C}G$-module structure given by

$$(g \cdot \phi)(u) = g \cdot \phi(g^{-1}u)$$

Now, $\phi \in Hom_{\mathbb{C}}(U, V)^G$ if and only if

$$g \cdot \phi(g^{-1}u) = \phi(u)$$

for all u, g. Then

$$\phi(g^{-1}u) = g^{-1}\phi(u)$$

So ϕ commutes with the action of g. This means precisely

$$\phi \in Hom_{\mathbb{C}G}(U, V)$$

So

$$\begin{aligned} dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(U, V)) &= dim_{\mathbb{C}}(Hom_{\mathbb{C}}(U, V)^G) \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_{Hom_{\mathbb{C}}(U,V)}(g) \\ &= \frac{1}{|G|} \sum_{g \in G} \overline{\chi_U(g)} \chi_V(g) \\ &= \langle \chi_V, \chi_U \rangle = \overline{\langle \chi_U, \chi_V \rangle} = \langle \chi_U, \chi_V \rangle \end{aligned}$$

since $dim_{\mathbb{C}} Hom_{\mathbb{C}G}(U, V) = \langle \chi_V, \chi_U \rangle \in \mathbb{R}$. ■

1.10 Character Tables

We can use this table to indicate a lot of useful properties of a group.
Let G be a finite group with $r :=$ the number of distinct conjugacy classes. We saw as a consequence of Wedderburn's theorem as a calculation on the center of a group ring:

$$r = \text{the number of non-isomorphic simple } \mathbb{C}G\text{-modules.}$$

This allows us to enumerate the characters $\chi_1, \ldots, \chi_r$ that correspond to these simple modules. Often we call these the "irreducible characters."
Let $g_1, \ldots, g_r$ be conjugacy class representatives.

Definition 1.51. *The <u>character table</u> is the $r \times r$ matrix T such that*

$$T_{i,j} := \chi_i(g_j)$$

Question 1.52. *How can we efficiently calculate this character table for a given group?*

The key tool in this case is to investigate the row and column relations of this table.

Lemma 1.53. *For any $1 \leq i, j \leq r, \langle \chi_i, \chi_j \rangle = \delta_{i,j}$.*

Proof. Let S_i, S_j be the simple $\mathbb{C}G$-modules corresponding to χ_i, χ_j. By Schur's Lemma, we recall if $i \neq j$

$$\langle \chi_i, \chi_j \rangle = dim_{\mathbb{C}} Hom_{\mathbb{C}G}(S_i, S_j) = 0$$

On the other hand, we know if $i = j$, then as a consequence of Wedderburn's Theorem:

$$\langle \chi_i, \chi_i \rangle = dim_{\mathbb{C}} Hom_{\mathbb{C}G}(S_i, S_i) = 1$$

■

Proposition 1.54. *The rows of the character table are orthogonal to one another.*

Proof.

$$\begin{aligned}
\delta_{i,j} &= \langle \chi_i, \chi_j \rangle \\
&= \frac{1}{|G|} \sum_{g \in G} \chi_i(g) \overline{\chi_j(g)} \\
&= \frac{1}{|G|} \sum_{s=1}^{r} |class(g_s)| \chi_i(g_s) \overline{\chi_j(g_s)}
\end{aligned}$$

■

Next, we can deduce a "column orthogonality". Before we do so, we need a useful lemma:

Lemma 1.55. *Suppose A, B are two square matrices such that*

$$A \cdot B = \lambda \cdot id$$

Then

$$A \cdot (\lambda^{-1} B) = id$$
$$(\lambda^{-1} \cdot B) \cdot A = id$$
$$B \cdot A = \lambda id$$

We can use this lemma to show the following proposition on column orthogonality:

Proposition 1.56.

$$\sum_{s=1}^{r} \chi_s(g_i) \cdot \overline{\chi_s(g_j)} = \frac{|G|}{|class(g_i)|}\delta_{i,j}$$

Proof. To adjust for discrepancy between summing over g in G versus $g_1, \ldots, g_r$, we can introduce an $r \times r$ diagonal matrix. Then

$$K = \begin{pmatrix} |class(g_1)| & & & & \\ & |class(g_2)| & & & \\ & & |class(g_3)| & & \\ & & & \ddots & \\ & & & & |class(g_r)| \end{pmatrix}$$

Let X be the character table matrix. Then

$$\begin{aligned}(XK\bar{X}^T)_{i,j} &= \sum_{a=1}^{r} \chi_i(g_a)|class(g_a)|\overline{\chi_j(g_a)} \\ &= \sum_{g\in G} \chi_i(g)\overline{\chi_j(g)} \\ &= |G|\langle \chi_i, \chi_j\rangle = |G| \cdot \delta_{i,j}\end{aligned}$$

Hence,

$$X \cdot K \cdot \bar{X}^T = |G| \cdot id$$

And by our lemma:

$$\begin{aligned}&\implies K \cdot \bar{X}^T \cdot X = |G|id \\ &\implies (K\bar{X}^T X)_{i,j} = \sum_{a=1}^{r} |class(g_a)|\overline{\chi_a(g_i)}\chi_a(g_j) \\ &\implies \sum_{a=1}^{r} \overline{\chi_a(g_i)}\chi_a(g_j) = \frac{|G|}{|class(g_i)|}\delta_{i,j} \\ &\implies \sum_{a=1}^{r} \chi_a(g_i)\overline{\chi_a(g_j)} = \frac{|G|}{|class(g_i)|}\delta_{i,j}\end{aligned}$$

■

Example 1.57. *Consider $G \cong S_3$. Then the conjugacy class is equivalent to the angle type. Specifically, we have 3 conjugacy classes:*

$$\{id\}, \{(12), (23), (13)\}, \{(123), (132)\}$$

Notice, $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$, which is abelian and therefore has a character table of exactly 2 characters. We can further use this to lift to irreducible characters of S_3 via the action $S_3 \to S_3/A_3$.
We can get the table for S_3/A_3 by:

	id	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1

The next question we need to ask is how much is missing from our table? To check, we recall the formula:

$$\underbrace{1^2 + 1^2 + ?^2}_{3 \text{ conjugacy classes}} = 6 \implies ? = 2$$

So it appears we're missing a 2-dimensional representation. So we will find χ_3 without having to know the concrete realization of the corresponding representation! Since we know the dimension of the character is it's evaluation on the identity, we can immediately fill in the first element of the third row. Namely:

	id	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	c_1	c_2

Further, leveraging column orthogonality, we see that checking the orthogonality between column 1 with columns 2 and 3:

$$1 \cdot \bar{1} + 1 \cdot \overline{-1} + 2 \cdot \bar{c}_1 = 0 \implies c_1 = 0$$

$$1 \cdot \bar{1} + 1 \cdot \bar{1} + 2 \cdot \bar{c}_2 = 0 \implies c_3 = -1$$

So we can finally fill in our character table!

	id	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

To understand where χ_3 came from, let us relate χ_3 to the character χ_p of the 3D permutation representation of S_3. χ_p can be calculated easily:

$$\chi_p(g) := \#\text{ of fixed points of } g$$

and hence $\chi_p(id) = 3, \chi_p((12)) = 1, \chi_p((123)) = 0$. Now consider an example of a virtual character $\chi_p - \chi_1$.

	id	(12)	(123)
$\chi_p - \chi_1$	2	0	-1

But notice $\chi_p - \chi_1 = \chi_3$! How can obtain this result from relying on more basic numerical calculations?

Remark 1.58. *We can define an "inner product" for all <u>class functions</u>*

$$\left\langle \sum_{i=1}^{r} a_i \chi_i, \sum_{j=1}^{r} b_j \chi_b \right\rangle = \sum_{i,j} a_i b_j \langle \chi_i, \chi_j \rangle = \sum_{i=1}^{r} a_i b_i$$

Now, suppose χ is a character with

$$\langle \chi, \chi \rangle = 1$$

Then we see that

$$\chi = \sum_{i=1}^{r} a_i \chi_i \implies \sum_{i=1}^{r} a_i^2 = 1$$

But since each $a_i \in \mathbb{Z}_{\geq 1}$, then $a_i = 0$ for all i except 1. Therefore, we can define that χ is <u>irreducible</u> provided all $a_i = 0$ for all i except 1.
Further, we see by the calculation

$$\langle \chi_p - \chi_1, \chi_p - \chi_1 \rangle = \frac{1}{6}(1 \cdot 2 \cdot 2 + 3 \cdot 0 \cdot 0 + 2 \cdot (-1) \cdot (-1)) = 1$$

So by the last lecture,

$$\chi_p - \chi_1 = \sum_{i=1}^{r} a_i \chi_i$$

with $\sum_{i=1}^{r} a_i^2 = 1$. Hence, $\chi_p - \chi_1 = \pm \chi_i$ for some i. But $(\chi_p - \chi_1)(id) = 2 > 0$. So we know $\chi_p - \chi_1$ is the missing character χ_3!

Example 1.59. *Let $G = S_4$. Then there are 5 conjugacy classes:*

$$\{id\}, \underbrace{\{2-cycles\}}_{6\ elements}, \underbrace{\{3-cycles\}}_{8\ elements}, \underbrace{\{2-cycles\ times\ 2-cycles\}}_{3\ elements}, \underbrace{\{4-cycles\}}_{6\ elements}$$

which accounts for all 24 elements of S_4. Now we would like to use a non-trivial normal subgroup of S_4, specifically $A_4 \trianglelefteq S_4$. Notice,

$$S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}$$

so we can fill in the first two characters:

	id	(12)	(123)	(1234)	$(12)(34)$
χ_1	1	1	1	1	1
χ_2	-1	1	1	-1	1

But we also have another interesting normal subgroup that we may consider! Specifically the Klein 4-Group

$$V = \{id, (12)(34), (13)(24), (14)(23)\}$$

which gives us $S_4/V \cong S_3$. Further S_3 can be realized as a subgroup of S_4! Since $V \cap S_3 = \{id\}$ then we see that

$$S_4 \cong V \rtimes S_3$$

So we can pull back the S_3 characters to S_4! We can make use of the fact in S_3 that the order of $g \in S_3$ determines the conjugacy class. Hence, under the mapping

$$\begin{aligned} S_4 \to S_3 \cong S_4/V \\ id \to id \\ (12) \to (12) \\ (123) \to (123) \\ (12)(34) \to id \\ (1234) \to (12) \end{aligned}$$

We can use this action to pullback characters from S_3 to S_4 :

	id	(12)	(123)	(1234)	$(12)(34)$
$\chi_1^{S_3}$	1	1	1	1	1
$\chi_2^{S_3}$	1	-1	1	-1	1
$\chi_3^{S_3}$	2	0	-1	0	2

Now we notice that

$$\langle \chi_3, \chi_3 \rangle = \frac{1}{24}(4 + 8 + 3 \cdot 4) = 1 \implies \chi_3 \text{ is an irreducible character}$$

Looking at the 4D permutation representation of S_4,

	id	(12)	(123)	(1234)	$(12)(34)$
χ_p	4	2	1	0	0

Checking the inner product on this permutation character,

$$\langle \chi_p, \chi_p \rangle = \frac{1}{24}(16 + 6 \cdot 4 + 8 \cdot 1) = 2$$

So χ_p must be the sum of two irreducible characters. Further,

$$\langle \chi_p - \chi_1, \chi_p - \chi_1 \rangle = 1$$

Therefore, $\chi_4 = \chi_p - \chi_1$ is an irreducible character of a 3D representation. For the fifth character, we can check the products of the previous characters:

$$\chi_3 \cdot \chi_2 = \chi_3$$

$$\chi_4 \cdot \chi_2 = \textit{ something new!}$$

	id	(12)	(123)	(1234)	(12)(34)
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	1	0	-1	-1
$\chi_4 \cdot \chi_2$	3	-1	0	1	-1

We can check the irreducibility of $\chi_4 \cdot \chi_2$, and we see that

$$\langle \chi_4 \cdot \chi_2, \chi_4 \cdot \chi_2 \rangle = 1 \implies \textit{ irreducible}$$

Therefore, we have all 5 irreducible characters on S_4, completing our table!

2 Homological Algebra

2.1 Homological Algebra in Action!

We'll start our exploration of homological algebra via group theory since that is the area we've already been working within for the last several weeks.

Theorem 2.1 (Abelian Schur-Zassenhaus)**.** *Given a finite group G and an abelian, normal subgroup $A \trianglelefteq G$ such that $|A|$ and $|G/A|$ are co-prime. Then A has a complement in G, meaning*

$$G = A \rtimes H$$

for some $H \leqslant G$.

Proof. From standard results about semi-direct products, it suffices to show that there is a subgroup $H \leqslant G$ with the following two properties:

1. $H \cap A = \{e\}$
2. $|H| = |G/A|$

Our strategy to find H is to construct a special injective homomorphism

$$B = G/A \to G$$

But to do so, we need a very crucial ingredient, specifically defining the action B on A via conjugating in the following sense:
Pick $\tilde{b} \in G$ mapping to b in $B = G/A$ under the projection $G \to G/A$. Let $a \in A$. Then we define the action via

$$a \to \tilde{b}a\tilde{b}^{-1}$$

If instead we consider the action of $\tilde{b}$ on $\tilde{a}$, we can see this action is well-defined by:

$$a \to \tilde{b}\tilde{a}a\tilde{a}^{-1}\tilde{b}^{-1} = \tilde{b}\tilde{a}\tilde{a}^{-1}a\tilde{b}^{-1} = \tilde{b}a\tilde{b}^{-1}$$

by the Abelian nature of A. So we have a well-defined action of B on A, and we write it as $a \to b_a$. Let us use this action to clarify the following:
For each $b \in G$, choose a coset representative t_b in G. Can we compare $t_{b_1b_2}$ and $t_{b_1} \cdot t_{b_2}$?
Claim: The "difference lies in A", namely

$$t_{b_1b_2}^{-1}A = (t_{b_1b_2}A)^{-1} = (b_1b_2)^{-1} = b_2^{-1}b_1^{-1} = t_{b_2}^{-1}t_{b_1}^{-1}A$$

Therefore,

$$t_{b_1}t_{b_2}t_{b_1b_2}^{-1} \in A$$

This allows us to define the mapping

$$\begin{aligned} f : B \times B &\to A \\ (b_1, b_2) &\to t_{b_1}t_{b_2}t_{b_1b_2}^{-1} \end{aligned}$$

We can then relate this function f to a function $B \to A$ and use this to obtain an injective homomorphism $B \to G$. To do so, we make a couple of observations:

- f satisfies an interesting identity (We finally get to see some Homological Algebra!) The 2-cocycle: Namely, from

  $$(t_{b_1} \cdot t_{b_2})t_{b_3} = t_{b_1} \cdot (t_{b_2} \cdot t_{b_3})$$

  We get, by using the B action on A, and interesting constraint on f:

  $$(t_{b_1} \cdot t_{b_2})t_{b_3} = f(b_1, b_2)t_{b_1b_2}t_{b_3} = f(b_1, b_2)f(b_1b_2, b_3)t_{b_1b_2b_3}$$

So

$$\begin{aligned} t_{b_1}(t_{b_2}t_{b_3}) &= t_{b_1}f(b_2,b_3)t_{b_2b_3} \\ &= t_{b_1}f(b_2,b_3)t_{b_1}^{-1}t_{b_1}t_{b_2b_3} \\ &= b_{1_{f(b_1,b_2)}} \cdot t_{b_1}t_{b_2b_3} \\ &= b_{1_{f(b_1,b_2)}}f(b_1,b_2b_3)t_{b_1b_2b_3} \end{aligned}$$

Since A is Abelian, let's write this relation multiplicatively to get for all $b_1, b_2, b_3 \in B$:

$$b_{1_{f(b_2,b_3)}} + f(b_1,b_2b_3) = f(b_1,b_2) + f(b_1b_2,b_3)$$

This final statement is referred to as the *2-cocycle identity.*

- Such a function f is FORCED to be of a very special form:

  This can summarized as proving "every 2-cocycle is a 2-coboundary." From the perspective of group theory, we define

$$\begin{aligned} e : B &\to A \\ b &\to \sum_{c\in B} f(b,c) \end{aligned}$$

  Let $n = |B|$. Then we see that one has

$$\begin{aligned} nf(b_1,b_2) + e(b_1,b_2) &= \sum_{b_3\in B} \underbrace{f(b_1,b_2) + f(b_1b_2,b_3)}_{\text{RHS of 2-cocycle identify}} \\ &= \sum_{b_3\in B} b_{1_{f(b_2,b_3)}} + f(b_1,b_2b_3) \\ &= b_{1_{\sum_{b_3\in B} f(b_2,b_3)}} + \sum_{b_3\in B} f(b_1,b_2b_3) \\ &= b_{1_{\sum_{b_3\in B} f(b_2,b_3)}} + \sum_{b_3\in B} f(b_1,b_3) \\ &= b_{1_{e(b_2)}} + e(b_1) \end{aligned}$$

  Therefore,

$$nf(b_1,b_2) = -e(b_1b_2) + b_{1_{e(b_2)}} + e(b_1)$$

  Now we want to define a function

$$\begin{aligned} c : B &\to A \\ b &\to \frac{-1}{n}e(b) \end{aligned}$$

  We should justify that such a function is well-defined. Since A is abelian, then multiplication is a homomorphism. Moreover, since $gcd(n,|A|) = 1$, then it must also be an automorphism. Therefore, such a function c can be defined.

  As a result, we can rewrite the function f as:

$$f(b_1,b_2) = c(b_1b_2) - c(b_1) - b_{1_{c(b_2)}}$$

As a consequence,

$$\begin{aligned} c(b_1b_2)t_{b_1b_2} &= c(b_1) \cdot b_{1_{c(b_2)}}f(b_1b_2) \\ &= c(b_1) \cdot b_{1_{c(b_2)}}t_{b_1} \cdot t_{b_2} \\ &= c(b_1)t_{b_1}c(b_2)t_{b_2} \end{aligned}$$

Hence,

$$\begin{aligned} \nu : B &\to G \\ b &\to c(b)t_b \end{aligned}$$

is a group homomorphism. We notice that

- *Claim:* ν is injective:
  If $c(b) \cdot t_b = id \in G$, then $t_b \in A$ and hence $b = id \in G/A$.
- *Claim:* $Im(\nu)$ is a subgroup of order $n = |B|$.
- *Claim:* $Im(\nu) \cap A = \{id\}$, proven above.

■

In order to understand subtle aspects of the proof, such as the 2-cocycle identity, we need to develop the general machinery of homological algebra.

2.2 Basic Category Theory

Example 2.2. *Consider R a ring, and the category of R-modules as well as R-module homomorphisms.*

Definition 2.3. *A category C is a class of objects, denoted by $Ob(C)$, such that for each $A, B \in Ob(C)$, we have a set $Hom_C(A, B)$ of morphisms that satisfy the following set of properties:*

1. *There exists a notion of "composition"*
$$Hom_C(A, B) \times Hom_C(B, D) \to Hom_C(A, D)$$
2. *Associativity of morphism elements:*
$$(f \circ g) \circ h = f \circ (g \circ h)$$
3. *For each $A \in Ob(C)$, there exists $id_A \in Hom(A, A)$ (similarly for $B \in Ob(C)$) such that for any $f \in Hom_C(A, B)$,*
$$id_B \circ f = f \circ id_A = f$$

Example 2.4. *R-modules and R-module homomorphisms. We denote this category by $R - Mod$.*

Example 2.5. *Let C be the category of sets. Then the elements in $ob(C)$ are simply sets and the morphisms are set theoretic maps.*

Definition 2.6. *A function $F : C_1 \to C_2$ is a functor between categories C_1 and C_2 if for each $A \in Ob(C)$ one associates $F(A) \in Ob(C_2)$, and for each $f \in Hom_{C_1}(A, B)$ one has $F(f)$ in $Hom_{C_2}(F(A), F(B))$ such that*

1. *$F(id_A) = id_{F(A)}$ for all A*
2. *$F(f \circ g) = F(f) \circ F(g)$ for all f, g*

Example 2.7. *Let $C_1 := R - Mod$ and $C_2 := \mathbb{Z} - Mod$ (The Abelian Groups). Then*

$$\begin{aligned} F : R - Mod &\to \mathbb{Z} - Mod \\ A &\to F(A) \\ f &\to F(f) \end{aligned}$$

This example is referred to as the forgetful functor.

Example 2.8. *Let $C_1 := R - Mod$ and $C_2 := \mathbb{Z} - Mod$ (The Abelian Groups). Fix R-module M, and define the functor*

$$\begin{aligned} F : R - Mod &\to \mathbb{Z} - Mod \\ N &\to Hom_R(M, N) \end{aligned}$$

Further, we obtain via composition:

$$F(N_1 \xrightarrow{f} N_2) = \begin{cases} Hom_R(M, N_1) \to Hom_R(M, N_2) \\ M \xrightarrow{\xi} N_1 \xrightarrow{f} N_2 \end{cases}$$

This functor is often written as $Hom_R(M, -)$.

Example 2.9. *Let $C_1 := R - Mod$ and $C_2 := \mathbb{Z} - Mod$ (The Abelian Groups). Define the functor*

$$\begin{aligned} F : \mathbb{Z}G - Mod &\to \mathbb{Z} - Mod \\ M &\to M^G := \{m \in M : gm = m \ \forall g \in G\} \\ (M_1 \xrightarrow{f} M_2) &\to M_1^G \xrightarrow{Res(f)} M_2^G \end{aligned}$$

As a result,

$$g \cdot f(m) = f(g \cdot m) = f(m) \implies f(m) \in M_2^G$$

2.3 Chain Complexes

The function $M \to M^G$ from above leads via its derived functions to group cohomology, which will give us the concept backing of the Schur-Zassenhaus theorem. Before we can define these however, we need to define several necessary ingredients. The first step will be chain complexes and their homology.

Definition 2.10. *A chain complex C_0 is*

$$\ldots \to C_n \xrightarrow{d_n} C_{n-1} \xrightarrow{d_{n-1}} C_{n-2} \to \ldots$$

where each C_i is an R-module and $d_i \in Hom_R(C_i, C_{i-1})$ such that

$$d_i \circ d_{i+1} = 0 \quad \forall i$$

As a consequence, we see that

$$Im(d_{i+1}) \subset Ker(d_i)$$

Moreover, we will refer to these sets by the names

$$o\text{"-boundaries"} = B_i = Im(d_{i+1}) \subset Ker(d_i) = Z_i = i\text{"-cycle"}$$

A natural question is what is the discrepancy between these two sets, which mathematical is answered via taking the quotient of these two objects.

Definition 2.11. *The i'th homology of C_0 is*

$$H_i(C_0) = Z_i / B_i = Ker(d_i)/Im(d_{i+1})$$

Definition 2.12. *A morphism between chain complexes is a collection of morphisms "respecting" the differential d:*

$$\begin{array}{ccccccccc} \ldots & \longrightarrow & C_{n+1} & \xrightarrow{d_{n+1}} & C_n & \xrightarrow{d_n} & C_{n-1} & \longrightarrow & \ldots \\ & & \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \\ \ldots & \longrightarrow & D_{n+1} & \xrightarrow{d_{n+1}} & D_n & \xrightarrow{d_n} & D_{n-1} & \longrightarrow & \ldots \end{array}$$

That is, a morphism $C_0 \to D_0$ is a collection $\{f_n\}_n$ with $f_n \in Hom_R(C_n, D_n)$ such that the above diagram commutes

$$d_n \circ f_n = f_{n-1} \circ d_n \quad \forall n$$

To see why this is a good notion of morphism, we make an easy yet important observation.

Proposition 2.13. *A Morphism of chain complexes $C_0 \to D_0$ induces maps on homology*

$$H_n(C_0) \to H_n(D_0)$$

Proof. To see this, consider $[z] \in H_n(C_0)$ for some $z \in Z_n$. Then

$$\begin{aligned}(f_{n-1} \circ d_n)(z) = f_{n-1}(0) = 0 \\ \implies (d_n \circ f_n)(z) = 0 \\ \implies [f_n(z)] \in H_n(D_0)\end{aligned}$$

Notice, $[z] \to [f_n(z)]$ is well-defined. If we change z to $z + b$ with b within boundary B_n, then

$$b = d_{n+1}(\xi)$$

for some ξ. Then by commutativity one has

$$f_n(b) = d_{n+1}$$

Hence,

$$\begin{aligned}f_n(z+b) &= f_n(z) + f_n(b) \\ &= f_n(z) + d_{n+1}(f_{n+1}(\xi)) \\ \implies [f_n(z)] &= [f_n(z+b)]\end{aligned}$$

which is what we desired. Thus we have constructed $H_n(C_0) \to H_n(D_0)$. ∎

We then move our attention to the development of an extremely important fact.

Definition 2.14. *A sequence*

$$0 \to A_0 \to B_0 \to C_0 \to 0$$

of chain complexes is called <u>exact</u> if and only if

$$0 \to A_n \to B_n \to C_n \to 0$$

is <u>exact</u> for all n.

Remark 2.15. *Short exact seuqneces of chain complexes give rise to long exact sequences of homology.*

We can make this more precise in the following theorem.

Theorem 2.16 (Fundamental Theorem)**.** *Given a short exact sequence*

$$0 \to A_0 \xrightarrow{f} B_0 \xrightarrow{g} C_0 \to 0$$

there is a long exact sequence

$$\ldots \to H_{n+1}(C_0) \xrightarrow{\delta} H_n(A_0) \xrightarrow{f} H_n(B_0) \xrightarrow{g} H_n(C_0) \xrightarrow{\delta} H_{n-1}(A) \to \ldots$$

where the connecting homomorphisms δ are "natural" in the following sense: If whenever there is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_0 & \longrightarrow & B_0 & \longrightarrow & C_0 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E_0 & \longrightarrow & F_0 & \longrightarrow & G_0 & \longrightarrow & 0 \end{array}$$

There there is a commutative diagram:

$$\begin{array}{ccccccc} \ldots & \longrightarrow & H_{n+1}(C_0) & \xrightarrow{\delta} & H_n(A_0) & \longrightarrow & \ldots \\ & & \downarrow & & \downarrow & & \\ \ldots & \longrightarrow & H_{n+1}(G_0) & \xrightarrow{\delta} & H_n(E_0) & \longrightarrow & \ldots \end{array}$$

A key tool in the proof is the following result:

Lemma 2.17 (Snake)**.** *Given a commutative diagram of R-modules*

$$\begin{array}{ccccccccc} & & A & \longrightarrow & B & \xrightarrow{p} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & E & \xrightarrow{i} & F & \longrightarrow & G & & \end{array}$$

with exact rows, then there is an exact sequence

$$ker(f) \to ker(g) \to ker(h) \xrightarrow{\delta} coker(f) \to coker(g) \to coker(h)$$

where

$$\delta(c) = [i^{-1}gp^{-1}(c)]$$

Proof. Clearly, there are maps

$$ker(f) \to ker(g) \to ker(h)$$
$$coker(f) \to coker(g) \to coker(h)$$

and they are exact. To see the exactness at $Ker(g)$, suppose $b \in Ker(g)$, which maps to 0 in h. Then by row exactness, $b \in Im(f)$. So let $a \in A$ such that $f(a) = b$. But we see that

$$i(f(a)) = 0$$

Since i is injective, then $f(a) = 0 \implies a \in Ker(f)$. The converse is also clear in this case.
Now we focus on the form of δ.

- We claim that $\delta(c)$ is well-defined since as a result of the commutativity of the diagram:

  $$h(c) = 0 \implies gp^{-1}(c) \in ker(F \to G)$$

  By the exactness of the bottom row,

  $$ker(F \to G) = Im(E \to F)$$

  and $E \xrightarrow{i} F$ is injective. Hence, there is a unique element in E mapping to $gp^{-1}(c)$. So the formula with well-defined.

  We also have to check that $[i^{-1}gp^{-1}(c)]$ is a well-defined element of $coker(f)$, specifically that it is independent of any choice of $p^{-1}(c)$. Suppose we change $p^{-1}(c)$ to

  $$p^{-1}(c) + \underbrace{\cdots}_{\in Ker(B \to C)}$$

  Since $Ker(B \to C) = Im(A \to B)$, then we can simply write,

  $$p^{-1}(c) + b$$

  where some element $a \in A$ maps to $b \in B$. Then

  $$\begin{aligned} g(p^{-1}(c) + b) &= gp^{-1}(c) + g(b) \\ &= gp^{-1}(c) + if(a) \end{aligned}$$

  $$\begin{aligned} \implies i^{-1}g(p^{-1}(c) + b) &= i^{-1}gp^{-1}(c) + i^{-1}g(b) \\ &= i^{-1}gp^{-1}(c) + f(a) \end{aligned}$$

  We allow elements within the same class to be related by some image element of a since there are in the same class in coker(f). Therefore, δ is well-defined.

- To check exactness:

  1. *Claim:* $ker(g) \to ker(h) \xrightarrow{\delta} coker(f)$ is exact.
     Since i is injective, $ker(\delta)$ are those $c \in ker(h)$ with $gp^{-1}(c) = 0$. So $ker(\delta) = Im(ker(g))$.
  2. *Claim:* $ker(h) \xrightarrow{\delta} coker(f) \to coker(g)$ is exact.
     So suppose $[e]$ is in $ker(coker(f) \to coker(g)) \iff i(e) \in Im(g)$. But since $\delta(c) = [i^{-1}gp^{-1}(c)]$, then this is precisely $Im(\delta)$.

■

Returning to the proof of the "fundamental theorem":

Proof. (Of Fundamental Theorem)
Consider the sequence

$$0 \to A_0 \to B_0 \to C_0 \to 0$$

We claim that the following diagram is commutative with exact rows:

$$\begin{array}{ccccccccc} & & A_n/dA_{n+1} & \longrightarrow & B_n/dB_{n+1} & \longrightarrow & C_n/dC_{n+1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} & & \\ 0 & \longrightarrow & Z_{n-1}(A_0) & \longrightarrow & Z_{n-1}(B_0) & \longrightarrow & Z_{n-1}(C_0) & & \end{array}$$

Checking the exactness:

- $0 \to Z_{n-1}(A_0) \to Z_{n-1}(B_0)$ is exact since $0 \to A_{n-1} \to B_{n-1}$ is exact.
- We know $B_n \to C_n \to 0$ is exact because $B_n/dB_{n+1} \to C_n/dC_{n+1} \to 0$ is exact.

Now we can apply the snake lemma, taking note that $H_n(A_0) = Z_n(A_0)/dA_{n+1}$ sits inside A_n/dA_{n+1}. Observe,

$$ker\left(A_n/dA_{n+1} \xrightarrow{d} Z_{n-1}(A_0)\right) = ker(A_n/dA_{n+1} \to A_{n-1}) = H_n(A_0)$$

Similarly,

$$coker(A_n/dA_{n+1} \xrightarrow{d} Z_{n-1}(A_0)) = H_{n-1}(A_0)$$

The same can be done for B_0 and C_0. So such a lemma gives us an exact sequence on homology:

$$H_n(A_0) \to H_n(B_0) \to H_n(C_0) \xrightarrow{\delta} H_{n-1}(A_0) \to H_{n-1}(B_0) \to H_{n-1}(C_0)$$

This is our long exact sequence on homology. But we're not done! We still want "naturalness" of δ, meaning if we are given a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_0 & \longrightarrow & B_0 & \longrightarrow & C_0 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E_0 & \longrightarrow & F_0 & \longrightarrow & G_0 & \longrightarrow & 0 \end{array}$$

Then for all n,

$$\begin{array}{ccccccc} \dots & \longrightarrow & H_n(C_0) & \xrightarrow{\delta} & H_{n-1}(A_0) & \longrightarrow & \dots \\ & & \downarrow & & \downarrow & & \\ \dots & \longrightarrow & H_n(G_0) & \xrightarrow{\delta} & H_n(E_0) & \longrightarrow & \dots \end{array}$$

This diagram is commutative. To prove this, consider $[c_n] \in H_n(C_0)$. Then $\delta([c_n])$ is as follows:
Let $b_n \to c_n$ and $a_{n-1} \to db_n$. Then

$$\delta([c_n]) = [a_{n-1}]$$

Finish Lecture 16 ■

2.4 Chain Homotopies

We need to develop an important calculational tool for studying homology of chain complexes. Suppose, given a morphism of chain complexes

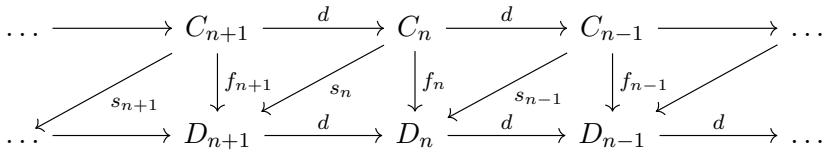
$$f : C_0 \to D_0$$

Recall, f gives rise to a map

$$f_* : H_n(C_0) \to H_n(D_0)$$

for all n.
A special type of f yields zero maps on homology:

Definition 2.18. *Suppose $f : C_0 \to D_0$ a morphism of chain complexes. Suppose there are maps $\{s_n\}_n$ (the "chain contractions")*



with the property

$$f_n = d \circ s_n + s_{n-1} \circ d$$

Then f is called null homotopic.

Proposition 2.19. *If $f : C_0 \to D_0$ is null homotopic, then*

$$f_* : H_n(C_0) \to H_n(D_n)$$

is the zero map for all n.

Proof. Let $[c_n] \in H_n(C_0)$. Then

$$\begin{aligned} f_*[c_n] &= [f_n(c_n)] \\ &= [(d \circ s_n)(c_n + (s_{n-1} \circ d)(c_n)] \\ &= [d(s_n(c_n)) + s_{n-1}(\underbrace{d(c_n)}_{=0})] \\ &= [d(s_n(c_n))] \\ &= [0] \end{aligned}$$

■

Definition 2.20. *Two chain complex maps*

$$f_1 : C_0 \to D_0$$
$$f_2 : C_0 \to D_0$$

are called (chain) homotopic if $f_1 - f_2$ is null homotopic.

Corollary 2.20.1. *Homotopic chain maps yield the same morphisms on homology.*

Proof.

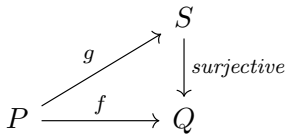
$$0 = (f_1 - f_2)_* = f_{1*} - f_{2*}$$

■

2.5 Projective Resolutions of R-Modules

Derived functors correspond to homology of certain chain complexes. A natural question for us it then where do these chain complexes come from. The answer is that these projective resolutions are used to cook up these chain complexes.

Definition 2.21. *An R-module P is projective if there $\exists g$ such that the following diagram commutes.*



Remark 2.22. *This is referred to as a "lifting property".*

Note 2.23. *If elements in ϕ "satisfy relation" there could be an issue. This is because projective is related to being free, but these two are not identical concepts.*

Proposition 2.24. *P is projective if and only if P is the a direct summand of a free R-module. That is,*

$$P \oplus \text{ something } \cong \text{ free } R-\text{module}$$

In particular, every free module is projective.

Remark 2.25. *There are projective, non-free R-modules.*

Example 2.26. *$R = M_n\mathbb{F}$, where $\mathbb{F}$ is a field. As a consequence of Wedderburn, we see that as R-modules*

$$R \cong C_1 \oplus \dots C_n$$

and

$$R \cong \mathbb{F}^n \oplus \dots \oplus \mathbb{F}^n$$

So $\mathbb{F}^n$ is a projective R-module but it is not free!

One can see that the category $R-Mod$ of R-modules "has enough projections" in the following sense:

Proposition 2.27. *For every object of $R-Mod$, there is a projective R-module P and a surjection $P \to M$.*

Proof. Consider the surjective mapping $R^{|M|} \to M$. Clearly $R^{|M|}$ is free, and hence projective. ■

Remark 2.28. *This property of having enough projectives can be generalized to yield the resolutions involved in the definition of derived functors.*

Definition 2.29. *A (left) resolution of M is*

- *a chain complex P_0 such that $P_i = 0$ for $i < 0$, and*
- *an $\epsilon : P_0 \to M$ such that*

$$\xrightarrow{d} P_2 \xrightarrow{d} P_1 \xrightarrow{d} P_0 \xrightarrow{\epsilon} M \to 0$$

is exact.

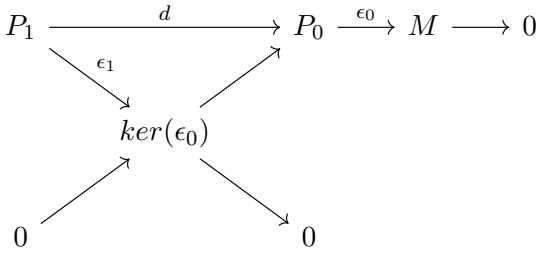
Definition 2.30. *A resolution is called a projective resolution if each P_i is projective.*

Lemma 2.31. *Every R-module M has a projective resolution.*

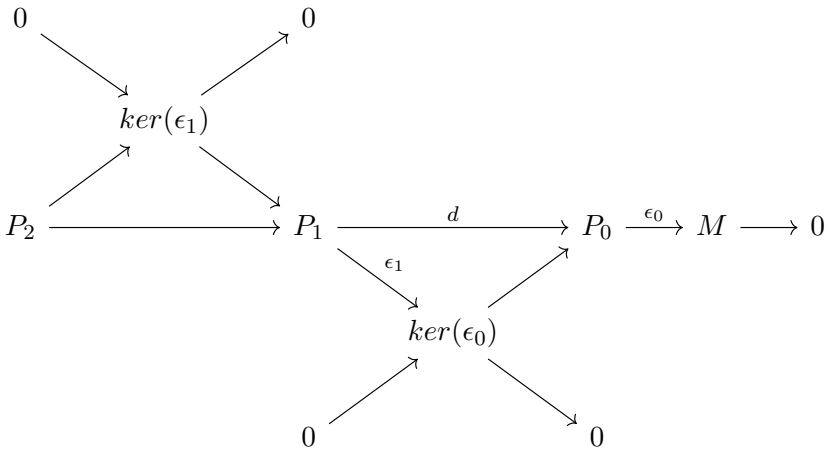
Proof. We can do this by inductively drawing our commutative diagram. We know there is an exact sequence

$$P_0 \xrightarrow{\epsilon} M \to 0$$

with P_0, which yields our first commutative diagram.



Further, we claim $Imd = ker(\epsilon_0)$.
Since P_1 is projective, we can continue our diagram as follows:



We can continue this process of identifying kernels of ϵ_i. ■

Remark 2.32. *In applications to derived functors, it will be crucial to control the issue of existence of* many *projective resolutions. We will make use of the next theorem to do this:*

Theorem 2.33 (Comparison)**.** *Suppose $P_0 \xrightarrow{\epsilon} M$ is a projective resolution and $g : M \to N$ a morphism and $Q_0 \xrightarrow{\eta} N$ is a resolution. Then there is a chain map $f : P_0 \to Q_0$ "lifting" g in the sense that the following diagram commutes:*

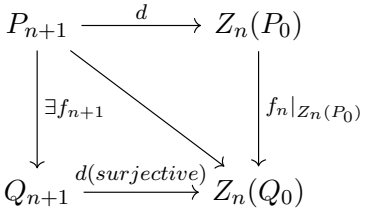
$$\begin{array}{ccccccccc} \dots & \longrightarrow & P_1 & \longrightarrow & P_0 & \xrightarrow{\epsilon} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle g} & & \\ \dots & \longrightarrow & Q_1 & \longrightarrow & Q_0 & \xrightarrow{\eta} & N & \longrightarrow & 0 \end{array}$$

Furthermore, f is unique up to chain homotopy equivalence.

Proof.
- (Existence) Let us show existence of f_n by induction on n. Let $f_{-1} = g$. Now, assume f_i for $i \leq n$ has been constructed. Notice,

$$f_n|_{Z_n(P_0)} : Z_n(P_0) \to Z_n(Q_0)$$

Hence,

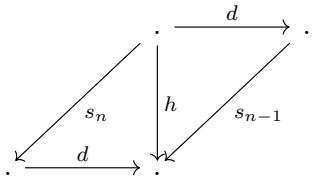


f exists since P_{n+1} is projective.

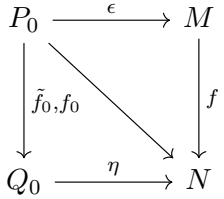
- (Uniqueness) To see the uniqueness of f up to chain homotopy, suppose $f, \tilde{f}$ are two lifts of g. Let $h = f - \tilde{f}$. We need to construct and chain contraction for h. Specifically,

$$\{s_n : P_n \to Q\}$$

for h. Recall,



By induction on n, we first consider the base case when $n = 0$. One has:



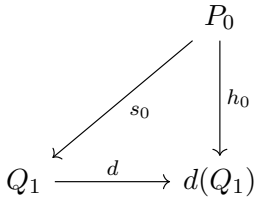
which obeys the relation

$$\eta_0 \circ h_0 = \eta \circ (f_0 - \tilde{f}_0) = g \circ \epsilon - g \circ \epsilon = 0$$

Hence

$$h_0(P_0) \subset ker(\eta) = d(Q_1)$$

which gives us the diagram thanks to the projectiveness of P_0:



with the relations

$$h_0 = d \circ s_0 = d_0 s_0 + s_{-1} \circ d$$

if we see $s_{-1} = 0$. This serves as a basis for induction!

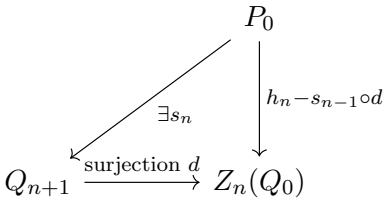
Now, taking the inductive step, consider the mapping:

$$h_n - s_{n-1} \circ d : P_n \to Q_n$$

Then we see that by applying the inductive hypothesis

$$\begin{aligned} d \circ (h_n - s_{n-1} \circ d) &= d \circ h_n - (d \circ s_{n-1}) \circ d \\ &= d \circ h_n - (h_{n-1} - s_{n-2} \circ d) \circ d \\ &= d \circ h_n - h_{n-1} \circ d && d^2 = 0 \\ &= 0 && \text{by commutativity} \end{aligned}$$

Hence ,



So $h_n - s_{n-1} \circ d = d \circ s_n \implies h_n = d \circ s_n + s_{n-1} \circ d$ as desired.

■

2.6 Derived Functors

Consider a functor

$$F : R_1 - Mod \to R_2 - Mod$$

between two categories of modules over two different rings.

Definition 2.34. *Such a function F is <u>additive</u> provided for R_1-modules M and N,*

$$F : Hom_{R_1}(M, N) \to Hom_{R_2}(F(M), F(N))$$

is a homomorphism of abelian groups under addition.

Definition 2.35. *A function F is <u>right exact</u> provided that when given a sequence*

$$Q \to R \to S \to 0$$

is exact in $R_1 - Mod$, then

$$F(Q) \to F(R) \to F(S) \to 0$$

in R_2-Mod.

Now let A be an R_1-module and choose a projective resolution

$$P_0 \to A$$

Then apply an additive, right exact functor F to P_0. As a result, one sees that $F(P_0)$ is a chain complex:

$$F(d) \circ F(d) = F(d^2) = F(0) = 0$$

We can now finally define left derived functors!

Definition 2.36. *Given an additive, right exact functor F, and R_1-module and a chosen projective resolution P_0, then the <u>(left) derived functors</u> $\{L_iF\}_{i\geq 0}$ are the homologies:*

$$L_iF(A) = H_i(F(P_0))$$

Observation 2.37. *When $i = 0$, we see that the left derived functor recovers F. Namely, given the sequence*

$$\ldots \to P_1 \to P_0 \to A \to 0$$

We know that F is right exact, so

$$F(P_1) \xrightarrow{\alpha} F(P_0) \to F(A) \to 0$$

is exact. Further,

$$F(P_0)/\alpha(F(P_1)) = F(A)$$

But we also know that $F(P_0)$ looks like

$$\ldots \to F(P_1) \xrightarrow{\alpha} F(P_0) \to F(P_{-1}) = F(0) = 0$$

So we see that

$$H_0(F(P_0)) = F(P_0)/\alpha F(P_1) = F(A)$$

as desired.

Example 2.38. *We can consider the special case when A is projective, where we can choose the projective resolution*

$$\ldots \to A \to A \to 0$$

Applying F to this resolution, we see

$$0 \to F(A) \to F(A) \to 0$$

but this immediately tells us that the derived left functors are:

$$L_0F(A) = F(A)$$

$$L_iF(A) = 0 \quad \forall i > 0$$

Question 2.39. *What if we choose a different projective resolution? More generally, how do derived functors depend on the (non-canonical) choice of projective resolution?*

Proposition 2.40. *The isomorphism class of $L_iF(A)$ is independent of the choice of projective resolution?*

Proof. Suppose $P_0 \to A$ and $Q_0 \to A$ are two projective resolutions. Apply the comparison theorem!

$$\begin{array}{ccccccc} \dots & \longrightarrow & P_0 & \longrightarrow & A & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle id} & & \\ \dots & \longrightarrow & Q_0 & \longrightarrow & A & \longrightarrow & 0 \end{array}$$

As a result, we get $f : P_0 \to Q_0$ by lifting id.

$$\begin{array}{ccccccc} \dots & \longrightarrow & P_0 & \longrightarrow & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \exists f} & & \downarrow{\scriptstyle id} & & \\ \dots & \longrightarrow & Q_0 & \longrightarrow & A & \longrightarrow & 0 \end{array}$$

Now, consider the other direction:

$$\begin{array}{ccccccc} \dots & \longrightarrow & P_0 & \longrightarrow & A & \longrightarrow & 0 \\ & & & & \uparrow{\scriptstyle id} & & \\ \dots & \longrightarrow & Q_0 & \longrightarrow & A & \longrightarrow & 0 \end{array}$$

We are able to get $g : Q_0 \to P$ by lifting id:

$$\begin{array}{ccccccc} \dots & \longrightarrow & P_0 & \longrightarrow & A & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle g} & & \uparrow{\scriptstyle id} & & \\ \dots & \longrightarrow & Q_0 & \longrightarrow & A & \longrightarrow & 0 \end{array}$$

Then we see that $g \circ f$ is a chain complex map $P_0 \to P_0$ lifting the identity map $id : A \to A$. But, also, the identity maps on $P_0, P_1, \dots$ lift $id : A \to A$. Therefore, we get the same map on homology:

$$\underbrace{id_*}_{id \text{ on homology}} = (g \circ f)_* = g_* \circ f_*$$

Analogously, we obtain $f_* \circ g_* = id_*$. So

$$H_iF(P_0) \cong H_iF(Q_0)$$

for all i. ∎

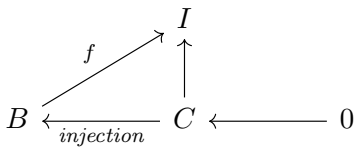
We can also take a look at Right Derived Functors, which we have neglected to define thus far. Our left functors thus far relied on exact functors applied to projective resolutions. Instead, we dualize this concept of projection to learn about injective resolutions!

Definition 2.41. *Recall, an R-module P is projective if there $\exists g$ such that the following diagram commutes.*

$$\begin{array}{ccccc} & & P & & \\ & \swarrow^{g} & \downarrow{\scriptstyle surjection} & & \\ B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

Reversing the arrows allows us to define the injective R-module:

Definition 2.42. *An R-module I is injective if there $\exists f$ such that the following diagram commutes.*



Remark 2.43. *The category of R-modules has enough injectives provided for every R-module M, there is an injection $M \to I$ with I injective.*

Definition 2.44. *A (right) injective resolution is*

- *a cochain-complex*
$$\ldots \to C^{n-1} \xrightarrow{d} C^n \xrightarrow{d} C^{n+1} \to \ldots$$
with $I^i = 0$ for $i < 0$, as well as
- *a mapping $M \to I^0$ such that*
$$0 \to M \to I^0 \xrightarrow{d} I^1 \to \ldots$$
is exact with each I^i injective modules.

Definition 2.45. *A function $F : R_1 - Mod \to R_2 - Mod$ is right-exact provided whenever*

$$0 \to A \to B \to C$$

is an exact sequence, then

$$0 \to F(A) \to F(B) \to F(C)$$

is an exact sequence.

Definition 2.46. *Given an additive, left exact functor F, and R_1-module and a chosen injective resolution $A \to I^0$, then the right derived functors $\{R^iF\}_{i\geq 0}$ are the homologies:*

$$R^iF(A) = H^i(F(I^0))$$

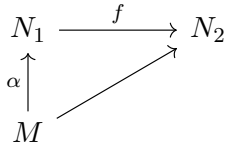
Note 2.47. *This is a cohomology of a cochain complex C^0 and is given by*

$$H^i(C^0) = ker(C^i \xrightarrow{d} C^{i+1})/Im(C^{i-1} \xrightarrow{d} C^i)$$

Example 2.48. *Fix and R-module M and let $F(N) = Hom_R(M, N)$ and if $N_1 \xrightarrow{f} N_2$, then we can define a map*

$$Hom_R(M, N_1) \to Hom_R(M, N_2)$$

via the diagram



We claim that $F = Hom_R(M, \cdot)$ is left exact.
Suppose we have an exact sequence

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

Then we claim

$$0 \to Hom_R(M, A) \xrightarrow{f_*} Hom_R(M, B) \xrightarrow{g_*} Hom_R(M, C) \to 0$$

is exact. To see this, suppose $f_*\alpha = 0$. Then we obtain the sequence

$$M \xrightarrow{\alpha} A \xrightarrow{f} B$$

Since f is injective, then $\alpha = 0$. Suppose now $g_*(\beta) = 0$. Then we obtain the sequence

$$M \xrightarrow{\beta} B \xrightarrow{g} C$$

So $g(\beta(m)) = 0$ for all $m \in M$. But then

$$\beta(m) \in ker(g)$$

By the exactness, we know $ker(g) = Im(f)$. So there exists a unique $a \in A$ such that

$$\beta(m) = f(a)$$

We then can define a mapping

$$\begin{aligned} M &\to A \\ m &\to f^{-1}(\beta(m)) \end{aligned}$$

This is an R-module homomorphism α with the property that

$$f_*\alpha = \beta$$

So $ker(g_*) = Im(f_*)$. Moreover, the converse is also pretty obvious with $g_*(f_*(\alpha)) = 0$.

Now we continue our discussion of right derived functors.

Question 2.49. *What is R^0F given a left exact functor?*

We can consider the cochain complex

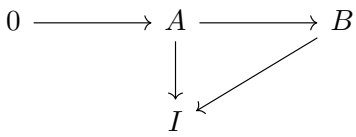
$$0 \to F(A) \to F(I^0) \to F(I^1)$$

is exact. Then

$$F(A) \cong ker(F(I^0) \to F(I^1)) = H^0(F(I^\cdot) = R^0F(A)$$

Remark 2.50. *One can show that $R - Mod$ has enough injectives.*

Example 2.51. *Showing this for $R = \mathbb{Z}$, it will be convenient to use Baer's injectivity criterion: Instead of considering all diagrams*



We can assume that A is an ideal in R and $B = R$.
Claim: *A $\mathbb{Z}$-module M is injective if and only if for all $n \in \mathbb{Z} \setminus \{0\}$ and for all $m \in M$, then*

$$m = n \cdot \tilde{m}$$

for some $\tilde{m} \in M$.

Proof. Let $A = [n]$ and suppose a mapping

$$\begin{aligned} A &\to M \\ n &\to m \end{aligned}$$

Then we can extend $\mathbb{Z} \to M$ provided $m = n \cdot \tilde{m}$. ■

In particular, $(\mathbb{Q}/\mathbb{Z}, +)$ *is injective since*

$$[a/b] = n \cdot [a/(nb)]$$

Now, for a $\mathbb{Z}$*-module* M*, let*

$$I = (\mathbb{Q}/\mathbb{Z})^{Hom_{\mathbb{Z}-Mod}(M,\mathbb{Q}/\mathbb{Z})}$$

Then I *is injective by the same argument of considering the mapping*

$$\begin{aligned} M &\to I \\ m &\to (f(m))_{f \in Hom_{\mathbb{Z}-Mod}(M,\mathbb{Q}/\mathbb{Z})} \end{aligned}$$

Now suppose $m \to 0$ *and hence* $f(m) = [0]$ *for all* f*. Assume* $m \neq 0$*. Define*

$$\begin{aligned} \tilde{f} : \langle m \rangle &\to \mathbb{Q}/\mathbb{Z} \\ m &\to [\frac{1}{Ord(m)}] \end{aligned}$$

provided $Ord(m)$ *is finite, otherwise* $m \to \xi$ *for some* $\xi \neq 0$*. Since* $\mathbb{Q}/\mathbb{Z}$ *is injective, we can extend* $\tilde{f}$ *to* $f : M \to \mathbb{Q}/\mathbb{Z}$ *and* $f(m) \neq [0]$*. But this is a contradiction! Therefore,*

$$0 \to M \to I$$

is exact, as desired.

Proposition 2.52. *Now, suppose there is an exact sequence of* R*-modules:*

$$0 \to A \to B \to C \to 0$$

as well as an additive, right exact functor F*. Then there exists a long exact sequence*

$$\ldots \xrightarrow{\delta} L_2F(A) \to L_1F(A) \to L_1F(B) \to L_1F(C) \xrightarrow{\delta} F(A) \to F(B) \to F(C) \to 0$$

which is "natural" in the following sense: if

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \xrightarrow{\epsilon} & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E & \longrightarrow & F & \longrightarrow & G & \longrightarrow & 0 \end{array}$$

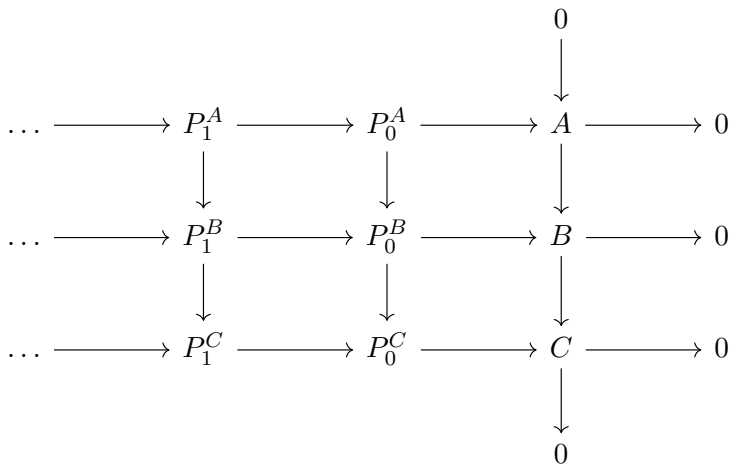
is a commutative diagram with exact rows, then

$$\begin{array}{ccc} L_iF(C) & \xrightarrow{\delta} & L_{i-1}F(A) \\ \downarrow & & \downarrow \\ L_iF(G) & \xrightarrow{\delta} & L_{i-1}F(E) \end{array}$$

is also commutative.

Proof. One way to show this is to use δ from our results on chain complexes. The situation to be explored can be

described by the diagram:



We want the columns of this diagram to interact nicely. To create this, we take the following approach:

1. Choose the 3 projective resolutions to get short exact sequence of chain complexes.

■

2.7 Ext (Extension) Functors

We saw earlier that

$$F = Hom_R(A, \cdot)$$

is a left exact, additive functor.

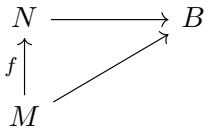
Definition 2.53.

$$Ext_R^i(A, B) := R^i Hom_R(A, \dots)(B)$$

There is a natural, yet different, candidate for this. If we fix B, we can then consider the "functor"

$$G = Hom_R(\dots, B)$$

If $M \xrightarrow{f} N$, then we have $G(M) \to G(N)$ via



Such a "functor" is called a contravariant functor, as opposed to the usual covariant functors.

Note 2.54. *A contravariant functor $G : C \to D$ can be viewed as a convariant functor*

$$C^{op} \to D$$

where C^{op} is composed of the same objects as C, but the morphisms are reversed.

Then we see that $G = Hom_R(\dots, B)$ is a contravariant, left exact functor. Concretely, if the sequence

$$0 \to X \to Y \to Z \to 0$$

is exact, then

$$0 \to G(X) \to G(Y) \to G(Z) \to 0$$

is exact. Therefore, we can define the right derived functor $R^i Hom_R(\dots, B)$.

Theorem 2.55. $R^iHom_R(A,\cdot)(B) = Ext^i_R(A,B) = R^iHom_R(\cdot,B)(A)$

To prove this, we need to develop some general tools.

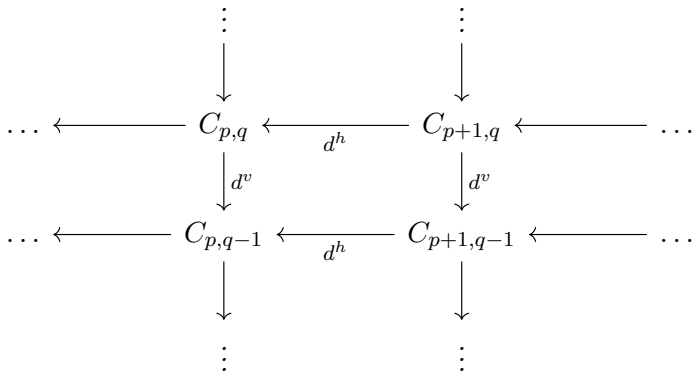
Definition 2.56. *A <u>double complex</u> in $R-Mod$ is a family $\{C_{p,q}\}_{p,q\in\mathbb{Z}}$ of R-modules equipped with morphisms:*

$$d^h : C_{p,q} \to C_{p-1,q}$$
$$d^v : C_{p,q} \to C_{p,q-1}$$

with

$$d^h \circ d^h = 0$$
$$d^v \circ d^v = 0$$
$$d^v \circ d^h + d^h \circ d^v = 0$$

Schematically:



Remark 2.57. *Each row and each column is a chain complex. However, since $d^v \circ d^h + d^h \circ d^v = 0$ rather than $d^v \circ d^h - d^h \circ d^v = 0$, we see that d^v does not usually yield a map of chain complexes between rows.*

Question 2.58. *Why do we assume $d^v \circ d^h + d^h \circ d^v = 0$?*

Definition 2.59. *Given a double complex C, define the <u>total complex</u> $Tot(C)$ via*

$$Tot(C)_n = \prod_{p+q=n} C_{p,q}$$

equipped with the morphisms:

$$d : Tot(C)_n \to Tot(C)_{n-1}$$
$$x \to d^h(x) + d^v(x)$$

where $h+v = n-1$.

Proposition 2.60. *$Tot(C)$ is a chain complex with $d^2 = 0$.*

Proof. Consider $x \in C_{p,q}$ with $p+q = n+1$. Then

$$d(x) = d^h(x) + d^v(x)$$

So

$$\begin{aligned}[d]^2(x) &= [d^h + d^v]^2(x) \\ &= \underbrace{d^h d^h(x)}_{=0} + \underbrace{d^v d^v(x)}_{=0} + \underbrace{d^h d^v(x) + d^v d^h(x)}_{=0} \\ &= 0\end{aligned}$$

■

Lemma 2.61. *Suppose C is a double complex such that C is an upper half-plane complex ($C_{p,q} = 0$ if $q < 0$) with exact columns. Then $Tot(C)$ is acyclic, with trivial homology.*

Proof. It suffices to show that

$$H_0(Tot(C)) = 0$$

So suppose $c = (C_{-p,p})_p \in Z_0$. If we can find elements

$$b_{-p,p+1} \in C_{-p,p+1},$$

$$b_{-p+1,p} \in C_{-p+1,p},$$

with

$$d^v(b_{-p,p+1}) + d^h(b_{-p+1,p}) = c_{-p,p}$$

then

$$d((b_{-p,p+1})_p) = c$$

We can do so via induction on p:

- *Base Case:* For $C_{0,0}$, use $b_{0,1}$ and $b_{1,0}$ by column exactness!
- *Inductive Step:* Assume we have identified $b_{-p_2,p-1}$ for $c_{-p+1,p-1}$. Then observe,

$$\begin{aligned} d^v(c_{-p,p} - d^h(b_{-p+1,p})) &= d^v(c_{-p,p}) + d^h d^v(b_{-p+1,p}) \\ &= d^v(c_{-p,p}) + d^h(c_{-p+1,p-1} + d^h(b_{-p+2,p-1})) \\ &= d^v(c_{-p,p}) + d^h(c_{-p+1,p-1}) && \text{since } d^h \circ d^v = 0 \\ &= d(c_{-p,p-1}) \\ &= 0 && \text{since } c \in Z_0 \end{aligned}$$

  So $d^v(c_{-p,p} - d^h(b_{-p+1,p})) = 0$, and hence by column exactness, there is a $b_{-p,p+1}$ such that

$$d^v(b_{-p,p+1}) = c_{-p,p} - d^h(b_{-p+1,p})$$

  Further,

$$c_{-p,p} = d^v(b_{-p,p+1}) + d^h(b_{-p+1,p})$$

  as desired.

■

Definition 2.62. *Given a map of chain complexes $f : B_\cdot \to C_\cdot$, the mapping cone, denoted $cone(f)$, is a new chain complex*

$$cone(f)_n = B_{n-1} \oplus C_n$$

equipped with the morphisms

$$d(b, c) = (-d(b), d(c) - f(b))$$

Proposition 2.63. *There is a short exact sequence of chain complexes*

$$0 \to C_\cdot \xrightarrow{\alpha} cone(f) \xrightarrow{\beta} B_\cdot[-1] \to 0$$

where $B_\cdot[-1]_n = B_{n-1}$ and the differential defined

$$\alpha(c) = (0, c)$$

$$\beta(b, c) = -b$$

To justify its existence, clearly, at each n, it is a map of chain complexes:

$$\begin{array}{ccc} c & \xrightarrow{\alpha} & (0,c) \\ \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} \\ d(c) & \xrightarrow{\alpha} & (0, d(c) - f(0)) \end{array}$$

$$\begin{array}{ccc} (b,c) & \xrightarrow{\beta} & -b \\ \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} \\ (-d(b), d(c) - f(b)) & \xrightarrow{\alpha} & (-d)(-b) = d(b) \end{array}$$

Corollary 2.63.1. *Since $H_{n+1}(B.[-1]) = H_n(B.)$, the previous proposition gives rise to the existence of a long exact sequence of homology:*

$$\ldots \to H_{n+1}(cone(f)) \to H_n(B.) \xrightarrow{\delta} H_n(C.) \to H_n(cone(f)) \to \ldots$$

Proof. We can prove this by showing the existence of some δ. Recall that the purpose of δ was to take any element $b \in Z_n(B.)$, lift it to $cone(f)$, apply d, then pull-back to $C.$. We want to show that δ will turn out to be f_*. Performing the procedure described, observe:

- Lift an element into $cone(f)$: $(-b, 0) \to b$
- Apply d: $d(-b, 0) = (-d(-b), 0 - f(b)) = (0, f(b))$
- Pull-back to $C.$: $(0, f(b)) \to f(b)$

Hence, $\delta : [b] \to [f(b)]$. ∎

Definition 2.64. *A map of chain complexes $f : B. \to C.$ is called a quasi-isomorphism if f_* is an isomorphism.*

Proposition 2.65. *$f : B. \to C.$ is a quasi-isomorphism if and only if $cone(f)$ is an exact complex (with trivial homology).*

Proof. ($\Rightarrow$) Suppose f is a quasi-isomorphism. By the previous result, we know the existence of the long exact sequence of homology:

$$\ldots \to H_{n+1}(cone(f)) \to H_n(B.) \xrightarrow{f_*} H_n(C.) \to H_n(cone(f)) \to \ldots$$

Notice, $Im(H_{n+1}(cone(f))) = Ker(\delta) = 0$ Further, we can iterate n to get the next chain:

$$\ldots \to H_{n+1}(B.) \xrightarrow{f_*} H_{n+1}(C.) \to H_{n+1}(cone(f)) \to H_n(B.) \to \ldots$$

From here, we see that $0 = Im(H_{n+1}(C_0)) = Ker(H_{n+1}(cone(f)) \to H_n(B.))$. These two results prove that

$$H_n(cone(f)) = 0$$

for all n. So $cone(f)$ is exact.
($\Leftarrow$) Conversely, assume $cone(f)$ is exact. Then we immediately have the long exact sequence

$$\ldots \to 0 \to H_n(B.) \xrightarrow{f_*} H_n(C.) \to 0 \to \ldots$$

So f_* is an isomorphism. ∎

Now we have the tools to prove:

Theorem 2.66. $R^i Hom_R(A, \cdot)(B) = Ext^i_R(A, B) = R^i Hom_R(\cdot, B)(A)$

Proof. Choose a projective resolution of A:

$$\to P_1 \to P_0 \to A \to 0$$

as well as an injective resolution of B:

$$0 \to B \to I^0 \to I^1 \to 0$$

The object resulting from $R^i Hom_R(A, \cdot)(B)$ as well as $R^i Hom_R(\cdot, B)(A)$ will be the total complex of the double cochain complex

$$Hom(P_\cdot, I^\cdot)$$

In comparison to a double chain complex, we reverse the direction of arrows. Looking at the details for $p, q \geq 0$, then

$$Hom(P_\cdot, I^\cdot)_{p,q} = Hom(P_p, I^q)$$

Describing the differentials schematically,

$$\begin{array}{ccccccc}
 & & \vdots & & \vdots & & \\
 & & \uparrow & & \uparrow & & \\
\dots & \longrightarrow & Hom(P_p, I^{q+1}) & \xrightarrow{d^h} & Hom(P_{p+1}, I^{q+1}) & \longrightarrow & \dots \\
 & & \uparrow{\scriptstyle d^v} & & \uparrow{\scriptstyle d^v} & & \\
\dots & \longrightarrow & Hom(P_p, I^q) & \xrightarrow{d^h} & Hom(P_{p+1}, I^q) & \longrightarrow & \dots \\
 & & \uparrow & & \uparrow & & \\
 & & \vdots & & \vdots & &
\end{array}$$

where $f : P_p \to I^q$ implies

$$\begin{aligned} d^v f : P_p &\to I^{q+1} \\ x &\to (-1)^{p+q+1} \cdot (d \circ f)(x) \end{aligned}$$

$$\begin{aligned} d^h f : P_{p+1} &\to I^q \\ x &\to (f \circ d)(x) \end{aligned}$$

which will result in

$$d^v d^h + d^h d^v = 0$$

since $P_p \xrightarrow{f} I^q$ maps to $(-1)^{p+q+1} P_p \xrightarrow{f} I^q \xrightarrow{d} I^{q+1}$

$$(-1)^{p+q+1} P_{p+1} \xrightarrow{d} P_p \xrightarrow{f} I^q \xrightarrow{d} I^{q+1}$$

whereas, we can look at the reverse direction $P_p \to I^q$ maps to $P_{p+1} \xrightarrow{d} P_p \xrightarrow{f} I^q$ maps to

$$(-1)^{p+q+1} P_{p+1} \xrightarrow{d} P_p \xrightarrow{f} I^q \xrightarrow{d} I^{q+1}$$

Now, consider the morphism of cochain complexes:

$$\nu : Hom(A, I^\cdot) \to TotHom(P_\cdot, I^\cdot)$$

coming from

$$\begin{array}{ccccccc}
\vdots & & \vdots & & & & \\
\uparrow & & \uparrow & & & & \\
Hom(A, I^2) & \longrightarrow & Hom(P_0, I^2) & \longrightarrow & \dots & & \\
\uparrow & & \uparrow & & \uparrow & & \\
Hom(A, I^1) & \longrightarrow & Hom(P_0, I^1) & \longrightarrow & Hom(P_1, I^1) & \longrightarrow & \dots \\
\uparrow & & \uparrow & & \uparrow & & \\
Hom(A, I^0) & \longrightarrow & Hom(P_0, I^0) & \longrightarrow & Hom(P_1, I^0) & \longrightarrow & \dots
\end{array}$$

We want to consider the mapping cone of ν. Recall that the mapping of a morphism cone

$$f : B^{\cdot} \to C^{\cdot}$$

of cochain complexes has

$$cone(f)^n = B^{n+1} \oplus C^n$$

In particular,

$$cone(\nu) = Hom(A, I^{n+1}) \oplus Tot^n(Hom(P_{\cdot}, I^{\cdot}))$$

This cone is essentially the total complex obtained from the double complex where we add the "column" $Hom(A, I^{\cdot})$ to the left of $Hom(P_{\cdot}, I^{\cdot})$. Each row of this new double complex is obtained by applying the functor $Hom(\cdot, I^q)$ where I^q is an injective module.
Every such functor is exact, mapping short exact sequences to short exact sequences.
Suppose we have a sequence

$$0 \to A \to B \to C \to 0$$

is exact. Then we have:

$$0 \to Hom(C, I^q) \to Hom(B, I^q) \to Hom(A, I^q) \to 0$$

Such a functor is surjective since I^q is an injective module.
Hence, all the rows of our new enlarged analogue of $Hom(P_{\cdot}, I^{\cdot})$ are exact. By a corollary of the acyclic assembly lemma for double cochain complexes, we know that this enlarged complex has an exact cochain complex. Therefore, the mapping cone

$$\nu : Hom(A, I^{\cdot}) \to TotHom(P_{\cdot}, I^{\cdot})$$

is exact! By the previous proposition, we then know that ν_* is an isomorphism for cohomology. Similarly, there is a morphism

$$\kappa : Hom(P_{\cdot}, A) \to TotHom(P_{\cdot}, I^{\cdot})$$

such that κ_* is an isomorphism. Therefore, we have justified the steps to show that

$$\begin{aligned}
R^i Hom(A, \cdot)(B) &= H^i Hom(A, I^{\cdot}) \\
&= H^i TotHom(P_{\cdot}, I^{\cdot}) \\
&= H^i Hom(P_{\cdot}, B) \\
&= R^i Hom(\cdot, B)(A)
\end{aligned}$$

■

2.8 Group Cohomology

Let G be a group and consider the functor

$$\mathbb{Z}G - Mod \to \mathbb{Z} - Mod$$
$$A \to A^G := \{a \in A : ga = a \ \ \forall g \in G\}$$

as well as the morphism $f : A \to B$ and its restriction $f|_{A^G} : A^G \to B$. We can see that this is a left exact functor. Let $H^i(G, \cdot)$ denote its ith right derived functor. We refer to $H^i(G, \cdot)$ as the group cohomology groups associated to G.

Proposition 2.67. *If $\mathbb{Z}$ is viewed as a $\mathbb{Z}G$-module via the trivial G-action, then $A^G \cong Hom_{\mathbb{Z}G}(\mathbb{Z}, A)$.*

Corollary 2.67.1. $H^i(G, A) \cong Ext^i_{\mathbb{Z}G}(\mathbb{Z}, A)$.

Proof. Taking $a \in A$, with the homomorphism ϕ, we perform evaluation $\phi(1) = a$ to get the desired result. ■

We want to develop some results in order to get a concrete resolution of $\mathbb{Z}$ within $\mathbb{Z}G - Mod$. This should give us concrete descriptions of the group cohomology $H^i(G, \cdot)$ that will allow us to relate cohomology to the proof of the Schur-Zassenhaus Theorem.

Definition 2.68. *The resolution*

$$B_\cdot \to \mathbb{Z}$$

of $\mathbb{Z}$ by free $\mathbb{Z}G$-modules is called the <u>bar resolution.</u>

By simply calculation, we see:

$$\begin{aligned} H^i(G, A) &= Ext^i_{\mathbb{Z}G}(\mathbb{Z}, A) && \text{previous result} \\ &= R^i Hom_{\mathbb{Z}G}(\cdot, A)(\mathbb{Z}) && \text{balancing theorem} \\ &= H^i(Hom_{\mathbb{Z}G}(B_\cdot, A)) \end{aligned}$$

But we should attempt to construct such a bar resolution.
Let us define the resolution

$$\ldots \xrightarrow{d} B_1 \xrightarrow{d} B_0 \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

Let $B_0 = \mathbb{Z}G$ and define ϵ via

$$\epsilon(e) = 1$$

For $n \geq 1$, let B_n be the free $\mathbb{Z}G$-module on the symbols $[g_1|\ldots|g_n]$ with $g_i \in G \setminus \{e\}$. Define

$$d : B_n \to B_{n-1}$$

via

$$d = d_0 - d_1 + d_2 + \ldots + (-1)^n d_n$$

where

$$d_0[g_1|\ldots|g_n] = g_1[g_2|\ldots|g_n]$$
$$d_n[g_1|\ldots|g_n] = [g_1|\ldots|g_{n-1}]$$

and for $1 \leq i \leq n-1$,

$$d_i[g_1|\ldots|g_n] = [g_1|\ldots|g_i g_{i+1}|\ldots|g_n]$$

By convention, the above symbol is zero when $g_i g_{i+1} = e$. To complete the definition of the d_i's, we can leverage $\mathbb{Z}G$-linearity to extend the definition.

- *Claim:* $(B_\cdot, d)$ is a chain complex with $d^2 = 0$.

Proof. We will show that relation that if $i \leq j-1$, then

$$d_i d_j = d_{j-1} d_i$$

then

$$\begin{aligned} d^2 &= \sum_{i=1}^{n-1} (-1)^i d_i \sum_{j=0}^{n-1} (-i)^j d_j \\ &= \sum_{i,j=1}^{n-1} (-1)^{i+j} d_i d_j \\ &= 0 \end{aligned}$$

since this results in a telescoping sum. But to see the above relation, observe if $i < j-1$

$$\begin{aligned} d_i d_j [g_1|\dots|g_n] &= d_i [g_1|\dots|g_j g_{j+1}|\dots|g_n] \\ &= d_i [g_1|\dots|g_i g_{i+1}|\dots|g_j g_{j+1}|\dots|g_n] \end{aligned}$$

$$\begin{aligned} d_{j-1} d_i [g_1|\dots|g_n] &= d_{j-1} [g_1|\dots|g_i g_{i+1}|\dots|g_n] \\ &= d_i [g_1|\dots|g_i g_{i+1}|\dots|g_j g_{j+1}|\dots|g_n] \end{aligned}$$

and if $i = j-1$, then

$$\begin{aligned} d_i d_j [g_1|\dots|g_n] &= d_i [g_1|\dots|g_j g_{j+1}|\dots|g_n] \\ &= d_i [g_1|\dots|g_i g_j g_{j+1}|\dots|g_n] \end{aligned}$$

$$\begin{aligned} d_{j-1} d_i [g_1|\dots|g_n] &= d_{j-1} [g_1|\dots|g_i g_{i+1}|\dots|g_n] \\ &= d_i [g_1|\dots|g_i g_j g_{j+1}|\dots|g_n] \end{aligned}$$

These together prove the relation as desired. ■

- *Claim:* $B.$ is a free resolution of $\mathbb{Z}$ in $\mathbb{Z}G - Mod$.

Proof. We have already shown that $(B., d)$ is a complex of free $\mathbb{Z}G$-modules. It remains to show that

$$\xrightarrow{d} B_1 \xrightarrow{d} B_0 \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

is exact with trivial homology. We will show this by constructing a chain contraction of the identity map. This can by done by working with the underlying $\mathbb{Z}$-module structure. Consider

$$\begin{aligned} s_{-1} : \mathbb{Z} &\to B_0 \\ k &\to ke \end{aligned}$$

Then for $n \geq 1$, we define the mappings:

$$\begin{aligned} s_n : B_n &\to B_{n+1} \\ g_0[g_1|\dots|g_n] &\to [g_0|g_1|\dots|g_n] \end{aligned}$$

Then we see that $\epsilon s_{-1} = id$ and also

$$\begin{aligned} d s_n (g_0[g_1|\dots|g_n]) &= d[g_0|g_1|\dots|g_n] \\ &= g_0[g_1|\dots|g_n] - [g_0 g_1|\dots|g_n] - \dots + (-1)^{n+1}[g_0|g_1|\dots|g_{n-1}] \end{aligned}$$

which we can compare to

$$\begin{aligned} s_{n-1}d(g_0[g_1|\dots|g_n]) &= s_{n-1}(g_0(g_1[g_2|\dots|g_n] - [g_1g_2|\dots|g_n] - \dots + (-1)^{n+1}[g_1|\dots|g_{n-1}])) \\ &= [g_0g_1|\dots|g_n] - [g_0|g_1g_2|\dots|g_n] - \dots + (-1)^{n+1}[g_0|g_1|\dots|g_{n-1}] \end{aligned}$$

and hence we can establish the relation

$$ds_n + s_{n-1}d = id$$

■

Now that we know that each B_n is a free $\mathbb{Z}G$-module on the symbol $[g_1|\dots|g_n]$, then we have a way to compute for each element in $Hom_{\mathbb{Z}G}(B_n, A)$ means exactly to give a set-theoretic map

$$\phi : G^n \to A$$

with $\phi(g_1, \dots, g_n) = 0$ if $g_i = e$ for some i. The differential

$$d = d_0 - d_1 + \dots$$

on $B_\cdot$ yields

$$(d\phi)(g_0, \dots, g_n) = g_0\phi(g_1, \dots, g_n) - \phi(g_0g_1, g_2, \dots, g_n) + \dots + (-1)^{n+1}\phi(g_0, \dots, g_{n-1})$$

Let $Z^i(G, A)$ be the i-cocycles in $Hom_{\mathbb{Z}G}(B_i, A)$. Recall this will be the kernel of d. On the other hand, let $B^i(G, A)$ be the i-coboundaries in $Hom_{\mathbb{Z}G}(B_i, A)$. Recall this will be the kernel of $Im(d)$ where

$$d : Hom_{\mathbb{Z}G}(B_{i-1}, A) \to Hom_{\mathbb{Z}G}(B_i, A)$$

Hence, we get an explicit description of the group cohomology

$$H^i(G, A) \cong Z^i(G, A)/B^i(G, A)$$

Example 2.69. *Let us describe $H^1(G, A)$. Every 1-cycle in $Z^1(G, A)$ corresponds to some $\phi : G \to A$ with $d\phi = 0$. Then*

$$\begin{aligned} 0 = (d\phi)(g, h) &= g\phi(h) - \phi(gh) + \phi(g) \\ \implies \phi(gh) &= g \cdot \phi(h) + \phi(g) \end{aligned}$$

This form of function ϕ is typically referred to as a twisted homomorphism. In particular, if G acts trivially, the $Z^i(G, A)$ are simply the homomorphisms.
But what about $B^1(G, A)$? Observe,

$$B_1 \to B_0 = \mathbb{Z}G$$

with $d_0[g] = g$ and $d_1[g] = e$. Then we see that

$$(d\phi)(g) = \phi(g) - \phi(e) = g\phi(e) - \phi(e)$$

In other words, $B^1(G, A)$ consists exactly of functions $\psi : G \to A$ of the form

$$\psi(g) = g \cdot a - a$$

for some $a \in A$.
Notice, these functions are cocycles:

$$\begin{aligned} \psi(g) + g \cdot \psi(h) &= g \cdot a - a + g \cdot (h \cdot a - a) \\ &= (gh) \cdot a - a \\ &= \psi(gh) \end{aligned}$$

So, in conclusion, $H^1(G, A)$ is given as the quotient of the space of twisted homomorphisms by those of the form $g \to g \cdot a - a$.

2.9 $H^2(G, A)$ and Extensions

For applications to the Schur-Zassenhaus theorem, we need to develop our understanding of $H^2(G, A)$. Let G be a group and let A be an abelian group.

Definition 2.70. *An extension of G by A is a short exact sequence of groups*

$$0 \to A \to E \xrightarrow{\pi} G \to 1$$

Definition 2.71. *An extension is called split if there is a group homomorphism $\sigma : G \to E$ such that*

$$\pi \circ \sigma = id_G$$

Exercise 2.72. *One can show that an extension is split if and only if $E \cong A \rtimes G$.*

Proposition 2.73. *If we fix an extension of G by A, then we can define a group action of G on A in the following manner:*
For $g \in G$ and $a \in A$, we can let $g \cdot a$ be given by $\tilde{g}a\tilde{g}^{-1}$ where $\tilde{g} \in E$ with $\pi(\tilde{g}) = g$.

Note 2.74. *This is independent of the choice of $\tilde{g}$ since A is abelian.*

Corollary 2.74.1. *For every extension*

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

we have the $\mathbb{Z}G$-module on A.

Question 2.75. *Can we classify the result of extensions in terms of cohomology? (This can be done by fixing a corresponding G-action on A.)*

Definition 2.76. *Suppose we fix the G-action on A. Two extensions are equivalent with this action if there is a commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E_1 & \longrightarrow & G & \longrightarrow & 0 \\ & & \downarrow{=} & & \downarrow{\cong} & & \downarrow{=} & & \\ 0 & \longrightarrow & A & \longrightarrow & E_2 & \longrightarrow & G & \longrightarrow & 0 \end{array}$$

Theorem 2.77. *There is a bijection between such equivalence classes of extensions and $H^2(G, A)$.*

In order to prove this, we need to develop a procedure that associates to an extension a "special function" $G^2 \to A$.

1. Fix an extension:
$$0 \to A \to E \to G \to 1$$

2. Choose a "set theoretic section" of $\pi : E \to G$ such that the map $\sigma : G \to E$ where $\sigma(id_G) = id_E$ plays nicely with π :
$$\pi \circ \sigma = id$$
Note,
$$\pi(\sigma(gh)) = gh$$
$$\pi(\sigma(g)\sigma(h)) = \pi(\sigma(g)) \cdot \pi(\sigma(h)) = gh$$
So it must follow that
$$[g, h] = \sigma(g)\sigma(h)\sigma(gh)^{-1} \in Im(A \to E)$$
Remark 2.78. *From now on, we wish to identify A with its image in E.*

3. We now define the function
$$G^2 \to A$$
$$(g, h) \to [g, h]$$
and call this the factor set associated to the extension (and our choice of σ)

We can use this special function to classify extensions.

Lemma 2.79. *If two extensions yield the same factor set, then the extensions are equivalent.*

Proof. For $i = 1, 2$, we see

$$0 \longrightarrow A \xrightarrow{\pi_i} E_1 \longrightarrow G \longrightarrow 0 \qquad (\sigma_i : G \to E_1)$$

So there is a bijection of sets

$$E_1 \leftrightarrow A \times G \leftrightarrow E_2$$

defined as follows: Fix $g \in G$, let

$$\sigma_i(g) \to (0, g)$$

Notice every element $x \in E_i$ with $\pi(x) = g$ is of the form $a \cdot \sigma_i(g)$ for a unique $a \in A$. Let

$$x \to (a, g)$$

We claim that the resulting bijection between E_1 and E_2 is a group homomorphism and hence yields $E_1 \cong E_2$. To see this, let us write the group structure of E_1 in terms of $A \times G$:

$$(x, 1) \cdot (y, 1) = (x + y, 1)$$

$$(x, 1) \cdot (0, g) = (x, g)$$

$$(0, g) \cdot (x, 1) = (g_x, g)$$

where $x \to g \cdot x := g_x$ is the G-action on A. This makes sense because

$$\sigma_i(g) \cdot x = x'$$

$$\implies g_x = x' = \sigma_i(g) x \sigma_i(g)^{-1}$$

It remains to describe $(0, g) \cdot (0, h)$ to get the full group structure on $A \times G$. At this point, we have

$$\sigma_i(g)\sigma_i(h) = [g, h]\sigma_i(gh)$$

$$(0, g) \cdot (0, h) = ([g, h], gh)$$

Since we assume the two extensions have the same factors set, then the group structure obtained on $A \times G$ via the described bijection with E_i is independent of i. So we obtain $E_1 \xrightarrow{\sim} E_2$ which is just id on A and gives the commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E_1 & \longrightarrow & G & \longrightarrow & 0 \\ & & \downarrow{=} & & \downarrow{\cong} & & \downarrow{=} & & \\ 0 & \longrightarrow & A & \longrightarrow & E_2 & \longrightarrow & G & \longrightarrow & 0 \end{array}$$

■

Observation 2.80. *Fix A, G and the G-action on A, as above. We can define $A \rtimes G$ and this is an extension of G by A.*

Proof. The group structure is

$$\sigma : G \to A \rtimes G$$
$$g \to (0, g)$$

Then we see that $gh \to (0, gh)$ and $(0, g) \cdot (0, h) = (0, gh)$. Hence σ is a homomorphism. Therefore, the factor set associated to σ is the zero function. ■

Remark 2.81. *So the previous lemma implies that if the factor set of an extension is 0, then the extension is split.*

Now let us try to bring cohomology into this picture, with analyzing $H^2(G, A)$.

Question 2.82. *What does role $Z^2(G, A)$ play?*

Recall, from the bar resolution $B_\cdot \to \mathbb{Z}$, we saw that the 2-cycles are functions

$$\begin{aligned} [,] : G^2 &\to A \\ [g, 1] &\to 0 \\ [1, g] &\to 0 \end{aligned}$$

and

$$f \cdot [g, h] - [fg, h] + [f, gh] - [f, g] = 0$$

for all $f, g, h \in G$.

Proposition 2.83. *A function $[,]^2 : G^2 \to A$ is a factor set if and only if it is an element of $Z^2(G, A)$.*

Proof.

- ($\Rightarrow$) Suppose $[,]$ is a factor set associated to some $\sigma : G \to E$. Then

$$0 = \sigma(g)\sigma(g)^{-1} = \sigma(g)\sigma(1)\sigma(g \cdot 1)^{-1} = [g, 1]$$

Similarly,

$$0 = \sigma(1)\sigma(g)\sigma(g \cdot 1)^{-1} = [1, g]$$

Furthermore, let $f, g, h \in G$. Checking all of our properties, we see:

$$(\sigma(f)\sigma(g))\sigma(h) = \sigma(f)(\sigma(g)\sigma(h))$$

Evaluating the left hand side, we get:

$$\begin{aligned} (\sigma(f)\sigma(g))\sigma(h) &= [f, g]\sigma(fg)\sigma(h) \\ &= [f, g][fg, h]\sigma(fgh) \end{aligned}$$

and evaluating the right-hand side:

$$\begin{aligned} \sigma(f)(\sigma(g)\sigma(h)) &= \sigma(f)[g, h]\sigma(gh) \\ &= \sigma(f)[g, h]\sigma(f)^{-1}\sigma(f)\sigma(gh) \\ &= f \cdot [g, h]\sigma(f)\sigma(gh) \\ &= f \cdot [g, h][f, gh]\sigma(fgh) \end{aligned}$$

By writing the operation additively, we obtain

$$\begin{aligned} [f, g] + [fg, h] &= f \cdot [g, h] + [f, gh] \\ \implies f \cdot [g, h] - [fg, h] + [f, gh] - [f, g] &= 0 \end{aligned}$$

Therefore, we have a factor set induced on $Z^2(G, A)$.

- ($\Leftarrow$) Now, suppose $[,] : G^2 \to A$ is a 2-cocycle. Let $E = A \times G$ with multiplication

$$(a, g) \cdot (b, h) = (a + g \cdot b + [g, h], gh)$$

We claim this yields a group structure!

– Identity:

$$(a,g)\cdot(0,1) = (a+0+[g,1],g) = (a,g)$$
$$(0,1)\cdot(a,g) = (0+a+[1,g],g) = (a,g)$$

– Associativity: Observe,

$$\begin{aligned}((a,g)\cdot(b,h))\cdot(c,i) &= (a+g\cdot b+[g,h],gh)\cdot(c,i)\\ &= (a+g\cdot b+[g,h]\cdot c+[gh,i],ghi)\end{aligned}$$

We compare this to

$$(a,g)\cdot((b,h)\cdot(c,i)) = (a+g\cdot b+g\cdot(h\cdot c)+g[h,i]+[g,hi],ghi)$$

For these to be equal, we need to have

$$[g,h]+[gh,i] = g[h,i]+[g,hi]$$

This holds since $[,]$ is in $Z^2(G,A)$!

– Inverses:

$$(a,g)\cdot(-g^{-1}\cdot a - g^{-1}[g,g^{-1}],g^{-1}) = (0,1)$$

since $(0,1)$ is a 2-sided identity, we in fact can deduce from the above equation that E is a group.

Therefore, $E = A\times G$ is a group and there is an exact sequence

$$0\to A\to E\xrightarrow{\pi} G\to 1$$

where $a\to(a,1)$ for $a\in A$ and $\pi:(a,g)\to g$. Notice, the G action on A via conjugation is the G-action that we started with:

$$\begin{aligned}(0,g)\cdot(a,1)\cdot(0,g)^{-1} &= (0,g)\cdot(a,1)\cdot(-g^{-1}[g,g^{-1}],g^{-1})\\ &= (0+g\cdot a+[g,1],g)\cdot(-g^{-1}[g,g^{-1}],g^{-1})\\ &= (g\cdot a-[g,g^{-1}]+[g,g^{-1}],1)\\ &= (g\cdot a,1)\end{aligned}$$

Next, we calculate the factor set

$$(,):G^2\to A$$

associated to $\sigma:G\to E$ with $\sigma(g)=(0,g)$. Observe,

$$\begin{aligned}(g,h) &= \sigma(g)\sigma(h)\sigma(gh)^{-1}\\ &= (0,g)\cdot(0,h)\cdot(0,gh)^{-1}\\ &= (0+0+[g,h],gh)\cdot(-(gh)^{-1}[gh,(gh)^{-1}],(gh)^{-1})\\ &= ([g,h]-[gh,(gh)^{-1}]+[gh,(gh)^{-1},1)\\ &= ([g,h],1)\end{aligned}$$

which is the image of $[g,h]$ under $A\to E$. Therefore, it follows that $[,]\in Z^2(G,A)$, and is indeed a factor set!

■