Algebra

Prof. Hiro Lee Tanaka

Preface

This script is mainly based on Prof. Hiro Lee Tanaka's course on Algebra 1: Theory of Groups and Vector Spaces for Harvard college in fall 2014-2015.

This script was written with the goal of providing a clear and structured introduction to algebraic concepts, aimed at undergraduate students. Algebra, with its focus on abstract structures such as groups, rings, and fields, serves as a foundation for many branches of mathematics, including geometry, number theory, and topology, as well as numerous applications in computer science, cryptography, and physics.

In this text, we have endeavored to balance rigor with intuition. Each concept is introduced with motivating examples, followed by formal definitions, propositions, and proofs. We believe that understanding comes not only from studying abstract definitions but also from seeing how these ideas operate in concrete settings. As such, the book contains a variety of examples and applications, ranging from classical results to more modern insights.

The material presented here spans the essential topics in algebra, starting with group theory, progressing through rings and fields, and concluding with more advanced topics like modules and vector spaces. Special attention has been given to the theorems and ideas that form the core of algebraic thought, such as the Sylow theorems, the isomorphism theorems, and Lagrange's theorem, along with more recent developments in algebraic structures.

This book is intended as both a learning resource and a reference. Each chapter builds on the last, but the material is modular enough to allow readers to dive into specific sections as needed. We hope this flexibility makes the book accessible to a wide range of students with varying levels of mathematical maturity.

I am deeply grateful to Lehel Csillag who has excellent discussions with me and contributions for this project. I also wish to express my gratitude to the many mathematicians whose work has shaped the field of algebra, as this book stands on the shoulders of their groundbreaking contributions.

I hope that this book serves as both an educational resource and an inspiration for further exploration into the beautiful world of algebra. If, in the process of reading, you gain a deeper appreciation for the elegance and power of algebra, then this book will have fulfilled its purpose.

Xumin Liang
October 22, 2024

Contents

Chapter 0

Introduction

(Name for) concept	Whole #'s	Derivatives	Groups	Rings
This concept expresses...? (Math is a language for conveying ideas; So what idea do these words embody?)	Counting, Quantity	Rate of change, Linearization	Symmetries	Functions on spaces
Some mathematical consequences			"Algebraization" of geometry (Descartes \to Present Day), "Geometrization" of algebra	
Some Applications (Outside of pure math)			Noether's Theorem (Physics) RSA algorithm (Crytography) Logic circuits as "cosheaves" Homology lshape of data sets, etc	

Chapter 1

Basic Concepts of Groups

1.1 Group

Fix some object X.
Question: What do we mean by a **symmetry** of X?
We usually have some structure of X in mind (Shapes, distance, linearity, etc)
A symmetry of X should be a map

$$\phi : X \to X$$

which

(1) preserves the structure ($\text{dist}(x, y) = \text{dist}(\phi(x), \phi(y))$, $\phi(x + y) = \phi(x) + \phi(y)$), and

(2) can be undone.

Let's take a stab at expressing this (at first glance arbitrary) heuristic:
Let $G = \{\phi\}$ be the set of symmetries of X.

(1) If ϕ_1, ϕ_2 preserve structure, so should $\phi_2 \circ \phi_1$ and $\phi_1 \circ \phi_2$. $\Rightarrow$ Can compose elements of G. $\Rightarrow$ $G \times G \xrightarrow{m} G$, associative.

(2) "Doing nothing" should be a symmetry of X. $\Rightarrow \text{id}_X \in G$, $\text{id}_X \circ \phi = \phi \circ \text{id}_X = \phi$.

(3) Since every ϕ can be undone, we should have $\phi^{-1} \in G$, so $\phi \circ \phi^{-1} = \text{id}_X$, $\phi^{-1} \circ \phi = \text{id}_X$.

1.1.1 Definition of Groups

Now we define this without any reference to X.

Definition 1.1. A **group** is a pair (G, m), where G is a set, and m is a map called the **group multiplication**

$$G \times G \to G$$
$$(g_1, g_2) \mapsto m(g_1, g_2) =: g_1 \cdot g_2 =: g_1 g_2$$

such that

(1) m is associative, i.e.,

$$m(m(g_1, g_2), g_3) = m(g_1, m(g_2, g_3))$$

i.e.

$$(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3) \quad \text{or} \quad (g_1 g_2) g_3 = g_1 (g_2 g_3)$$

(2) $\exists$ an element $1_G \in G$, called **identity** s.t.

$$m(1_G, g) = g = m(g, 1_G)$$

i.e.

$$1_G \cdot g = g = g \cdot 1_G \quad \text{or} \quad 1_G g = g = g 1_G$$

(3) $\forall g \in G$, $\exists$ elements $h \in G$, s.t.

$$m(g,h) = 1_G = m(h,g)$$

i.e.

$$g \cdot h = 1_G = h \cdot g \quad \text{or} \quad gh = 1_G = hg$$

We often write $g^{-1} := h$, "the **inverse** of g".

1.1.2 Examples of Groups

Example 1.1. Let

$$G = \{\ldots, -1, 0, 1, \ldots\} =: \mathbb{Z}$$

be the set of integers.
Define

$$G \times G \xrightarrow{m} G$$

by

$$m(g,h) = g + h \qquad \text{(i.e. addition)}$$

For example, we have

$$m(-2,3) = 1$$

Then (G, m) is a group.

Proof. $(\mathbb{Z}, +)$ is a group, since

(1) m is associative, since

$$(g+h)+k = g+(h+k)$$

(2) $0 = 1_G$ is the identity, since

$$m(0,g) = 0 + g = g$$
$$m(g,0) = g + 0 = g$$

(3) Every element has an inverse:

$$m(g,-g) = g + (-g) = 0$$

□

Example 1.2. Let

$$G = \{\ldots, -1, 0, 1, \ldots\} =: \mathbb{Z}$$

and let

$$m : G \times G \to G$$
$$(a,b) \mapsto a \times b$$

For example

$$(2,3) \to 6$$

We conclude that (G, m) is *not* a group.

Proof. $(\mathbb{Z}, \times)$ is not a group, since not every element $z \in \mathbb{Z}$ has an inverse. Take for example $z = 2$. Its inverse should be $\frac{1}{2}$, but this does not lie in $\mathbb{Z}$. □

The above two examples

$$(\mathbb{Z}, +) \text{ is a group.}$$
$$(\mathbb{Z}, \times) \text{ is not a group.}$$

show it's important to know m. Regardless, we will often abbreviate, and say things like "Let G be a group" omitting mention of m.

Example 1.3. Let $G = \mathbb{R} \setminus \{0\}$ (the set of real numbers with 0 removed). Let

$$m : G \times G \to G$$
$$(a,b) \mapsto a \times b$$

Then G is a group. We denote it as $\mathbb{R}^\times$ from now on.

Proof. $\mathbb{R}^\times$ is a group, since

(1) multiplication of real numbers is associative.

(2) number 1 is the identity.

(3) $\forall g \in \mathbb{R} \setminus \{0\}$, there exists a $\frac{1}{g}$, s.t. $g\frac{1}{g} = \frac{1}{g}g = 1$.

□

1.1.3 Properties of Groups

Proposition 1.1 (Cancellation Law)**.** Let G be a group and $g, h, k \in G$. Suppose

$$gh = gk.$$

Then

$$h = k.$$

Likewise, we have

$$hg = kg \quad \Rightarrow \quad h = k$$

Proof. $\exists g^{-1}$, s.t. $g^{-1}g = 1_G$. (3)

$$\begin{aligned} gh = gk \quad &\Rightarrow \quad g^{-1}(gh) = g^{-1}(gk) \\ &\Rightarrow \quad (g^{-1}g)h = (g^{-1}g)k \qquad (1) \\ &\Rightarrow \quad 1_G h = 1_G k \qquad (3) \\ &\Rightarrow \quad h = k \qquad (2) \end{aligned}$$

We have used every property of being a group! □

Remark. Cancellation law is not true for matrix multiplication unless g, h, k are all invertible. e.g. if $g = 0$?

Proposition 1.2 (Uniqueness of Identity)**.** The identity element of a group G is unique. (That is, if two elements 1_G and $1'_G$ satisfy the defining property of the identity element, then $1_G = 1'_G$.)

Proof. If 1_G is the identity, then it must satisfy the equation

$$1_G g = g 1_G = g$$

for all g. In particular, if $1'_G = g$, we must have

$$1_G 1'_G = 1'_G.$$

On the other hand, if $1'_G$ is also the identity element, we must have

$$1_G 1'_G = 1_G.$$

By transitivity, we conclude

$$1_G = 1'_G.$$

□

Proposition 1.3 (Uniqueness of Inverse Element)**.** For any element $g \in G$, its inverse g^{-1} is unique. (That is, given elements h, h' satisfying the defining property of g^{-1}, then $h = h'$.)

Proof. Suppose h and h' are both inverses to g. Then

$$gh' = 1_G.$$

By multiplying both sides of the equation by h on the left, we obtain

$$h(gh') = h.$$

But by associativity, the left hand side becomes

$$(hg)h' = 1_G h' = h'.$$

By transitivity of equality, we have that

$$h' = h.$$

□

1.2 Abelian Groups

Example 1.4. Fix $n \geqslant 1$ and $n \in \mathbb{Z}$. Then

$$G = GL_n(\mathbb{R}) := \{n \times n \text{ real matrices } M \mid \det M \neq 0\}$$

is a group, where

$$m : G \times G \to G$$

is given by multiplication of matrices.

Proof. $GL_n(\mathbb{R})$ is a group, since

(1) matrix multiplication is associative.

(2) the identity matrix does the job as identity.

(3) $\det(g) \neq 0 \Rightarrow g$ invertible.

□

Since the multiplication of matrices might not satisfy commutativity. This shows $gh \neq hg$ in general! What if the group operation is commutative? We have the following definition:

Definition 1.2. A group G is called **abelian** if for all $g_1, g_2 \in G$, we have $g_1 g_2 = g_2 g_1$.

Definition 1.3. Groups where the commutative property does not hold for all elements are called **non-abelian groups**.

1.3 Cyclic Groups

While abelian groups offer useful structure through commutativity, some abelian groups are even simpler. What if we could generate the entire group from a single element? This brings us to the notion of a cyclic group, which serves as one of the most basic examples of an abelian group.

A cyclic group is special because it reduces the structure of the entire group to powers or multiples of one element, called the generator. This simplicity makes cyclic groups both a crucial building block in group theory and a key tool in solving more complex problems.

Definition 1.4. A group G is called **cyclic** if there exists an element $g \in G$, called **generator**, such that every element in G can be written as a power of g.

$$G = \langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$$

Example 1.5 (Integers under Addition)**.** The group $(\mathbb{Z}, +)$ is cyclic with generator 1:

$$\langle 1 \rangle = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

Example 1.6 (Modular Arithmetic Groups)**.** The group $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n\}$ under addition modulo n (i.e., with group operation $m(a, b) := (a + b) \bmod n$) is cyclic. The element 1 generates the entire group:

$$\langle 1 \rangle = \{1, 2, \ldots, n-1, 0\}$$

Proposition 1.4. Cyclic groups are abelian.

Proof. Call the cyclic group G, which is generated by the element g. Then $\forall x, y \in G$, $\exists m, n$ such that $g^m = x$ and $g^n = y$. Therefore,

$$xy = g^m g^n = g^{m+n} = g^n g^m = yx$$

Therefore, G is abelian. □

1.4 Order of Group

Definition 1.5. Let G be a group. We let

$$|G| \in \mathbb{Z}_{\geqslant 1} \cup \{\infty\}$$

be the number of elements in G. We call $|G|$ the **order** of G.

Definition 1.6. Fix $g \in G$. Consider the set

$$\langle g \rangle := \{\ldots, \underbrace{g^{-1} \cdot g^{-1}}_{=:g^{-2}}, g^{-1}, 1_G, g, \underbrace{g \cdot g}_{=:g^2}, \underbrace{g \cdot g \cdot g}_{=:g^3}, \ldots\}$$

We define the **order of** g to be

$$|\langle g \rangle|$$

Example 1.7.

- $1_G \in G$ has order 1.
- $n \in \mathbb{Z}$, $n \neq 0$ has infinite order.
- $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{R})$ has order 2, since

$$g^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_{GL_2(\mathbb{R})}$$

  So $\{\ldots, g^{-1}, 1, g, \ldots\} = \{1, g\}$.

Theorem 1.5 (Euler's Totient Function)**.** The number of generators of a cyclic group of order n is given by the Euler's totient function $\varphi(n)$.

1.5 Center of a Group

To study the structure of non-abelian groups, we often look for subsets where some form of commutativity still holds. One key concept in this regard is the center of a group.

Definition 1.7. The **center** of a group G, denoted $Z(G)$, is defined as:

$$Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}.$$

Proposition 1.6. The center of an abelian group is the whole group.

Proof. The center of a group G is:

$$Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}.$$

In an abelian group, every pair of elements commutes:

$$g_1 \cdot g_2 = g_2 \cdot g_1 \quad \text{for all } g_1, g_2 \in G.$$

So, every element of G is in the center, meaning:

$$Z(G) = G.$$

□

The center of a group G is the set of elements that commute with every element in G. This set is not just a collection of special elements, it actually forms a structure of G. We will introduce this structure in next chapter.

Chapter 2

Subgroups

2.1 Definition of Subgroups

Definition 2.1. Let G be a group, and $H \subset G$. H is called a **subgroup** of G if

(1) $\forall\ h_1, h_2 \in H$, $h_1 h_2 \in H$. (Closed under multiplication)

(2) $1_G \in H$.

(3) If $h \in H$, then $h^{-1} \in H$.

2.2 Examples of Subgroups

Example 2.1. $\mathbb{R}_{>0} \subset \mathbb{R}^\times$ is a subgroup.

Proof. $\mathbb{R}_{>0}$ is a subgroup of $\mathbb{R}^\times$, since

(1) $\forall\ h_1, h_2 \in \mathbb{R}_{>0}$, $h_1 h_2 \in \mathbb{R}_{>0}$.

(2) $1 \in \mathbb{R}_{>0}$.

(3) If $h \in \mathbb{R}_{>0}$, then $h^{-1} = \frac{1}{h} \in \mathbb{R}_{>0}$.

□

Example 2.2. $\mathbb{Z}_{\geqslant 0} \subset (\mathbb{Z}, +)$ is not a subgroup.

Proof. $\mathbb{Z}_{\geqslant 0}$ is not a subgroup of $\mathbb{Z}$, since not every element $z \in \mathbb{Z}$ has an inverse. Take for example $z = 1$. Its inverse should be -1, but this does not lie in $\mathbb{Z}_{\geqslant 0}$. □

Example 2.3. $SL_n(\mathbb{R}) := \{M \in GL_n(\mathbb{R}) \mid \det M = 1\} \subset GL_n(\mathbb{R})$ is a subgroup.

Proof. $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$, since

(1) $\forall M_1, M_2 \in SL_n(\mathbb{R})$, $M_1 M_2 \in SL_n(\mathbb{R})$, because

$$\det(M_1 M_2) = \det(M_1)\det(M_2) = 1 \times 1 = 1.$$

(2) identity matrix $I_{GL_n(\mathbb{R})} \in SL_n(\mathbb{R})$, because $\det(I_{GL_n(\mathbb{R})}) = 1$.

(3) $\forall M \in SL_n(\mathbb{R})$, then $M^{-1} \in SL_n(\mathbb{R})$, because $\det(M^{-1}) = \frac{1}{\det(M)} = 1$.

□

Example 2.4. Let $\mathbb{C}^\times := \mathbb{C} \setminus \{0\}$. Define m as multipilication of complex numbers: $\forall z_1, z_2 \in \mathbb{C}^\times$,

$$m(z_1, z_2) = z_1 \times z_2.$$

We have

(a) $\mathbb{C}^\times$ is a group.

(b) Let

$$S^1 = \{z \mid |z| = 1\}.$$

Then $S^1 \subset \mathbb{C}^\times$ is a subgroup.

Proof. (a) $\mathbb{C}^\times$ is a group, since

(1) complex multiplication is associative.

(2) $\forall z \in \mathbb{C}^\times$, $1 \times z = z \times 1 = z$.

(3) $\forall z \in \mathbb{C}^\times$, set $z^{-1} = \frac{\overline{z}}{||z||^2}$.

(b) S^1 is a subgroup of $\mathbb{C}^\times$, since

(1) $|z_1| = |z_2| = 1 \Rightarrow |z_1 \times z_2| = 1$, so S^1 is closed under $\times$.

(2) $|1| = 1$, so the unit is in S^1.

(3) If $|z| = 1$, then $|\overline{z}| = 1$, and $z^{-1} = \overline{z}$.

□

Chapter 3

Maps of Groups

Whenever you define an idea, it's good to know what kinds of functions are friends with that idea.
Question: What kinds of **functions** do we want to study?

Example 3.1.

$$\begin{aligned} \text{Sets } S,T &\leftrightarrow \text{any function } f: S \to T \\ \text{Spaces } X,Y &\leftrightarrow \text{continuous functions } f: X \to Y \\ \text{Smooth curves+surfaces } X,Y &\leftrightarrow \text{differentiable function } f: X \to Y \\ \text{Groups } G,H &\leftrightarrow \text{group homomorphism } \phi: G \to H \end{aligned}$$

3.1 Group Homomorphism

3.1.1 Definition of Group Homomorphism

Definition 3.1. Let G, H be groups. A **group homomorphism** from G to H is a function

$$\phi : G \to H$$

such that $\forall g_1, g_2 \in G$,

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2).$$

3.1.2 Examples of Group Homomorphism

Example 3.2. $\exp : (\mathbb{R}, +) \to \mathbb{R}^\times$ is a group homomorphism.
$t \mapsto \mathrm{e}^t$

Proof. $\forall t_1, t_2 \in (\mathbb{R}, +)$, $\mathrm{e}^{t_1+t_2} = \mathrm{e}^{t_1} \cdot \mathrm{e}^{t_2}$. □

Example 3.3. $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$ is a group homomorphism.
$M \mapsto \det(M)$

Proof. $\forall M_1, M_2 \in GL_n(\mathbb{R})$, $\det(M_1 M_2) = \det(M_1)\det(M_2)$. □

Example 3.4. $(\mathbb{R}, +) \to S^1$ is a group homomorphism.
$t \mapsto \mathrm{e}^{\mathrm{i}t}$

Proof. $\forall t_1, t_2 \in (\mathbb{R}, +)$, $\mathrm{e}^{\mathrm{i}(t_1+t_2)} = \mathrm{e}^{\mathrm{i}t_1} \cdot \mathrm{e}^{\mathrm{i}t_2}$. □

Example 3.5. If V, W are vector spaces, they are groups under $+$. Any linear map

$$\phi : V \to W$$

is a group homomorphism. Any linear subspace is a subgroup.

Proof. (a) V, W is vector spaces as groups, since it satisfies:

(1) Associativity: Addition in V is associative, i.e. $(v+u)+w = v+(u+w)$ for all $v, u, w \in V$.

(2) Identity element: There exists an element $0 \in V$ such that $v + 0 = v$ for all $v \in V$.

(3) Inverse element: For every $v \in V$, there exists $-v \in V$ such that $v + (-v) = 0$.

(b) Any linear map $\phi : V \to W$ is a group homomorphism, since it satisfies:

(1) Homomorphism property: For any $v, u \in V$,

$$\phi(v+u) = \phi(v) + \phi(u)$$

This follows directly from the definition of a linear map, where $\phi(v+u) = \phi(v) + \phi(u)$ for all $v, u \in V$.

(2) Preservation of identity: Since ϕ is linear,

$$\phi(0_V) = 0_W$$

where 0_V and 0_W are the identity elements in V and W, respectively.

(3) Preservation of inverse: For any $v \in V$,

$$\phi(-v) = -\phi(v).$$

This property holds because ϕ respects scalar multiplication and additive inverses due to its linearity.

Therefore ϕ preserves the group structure under addition:

$$\phi(v+u) = \phi(v) + \phi(u)$$

which means ϕ is a group homomorphism from $(V, +)$ to $(W, +)$.

(c) Any linear subspace is a subgroup, since

- A linear subspace $U \subset V$ is also a group under addition because it inherits the group structure from V.
- The identity element 0_V of V is also the identity element in U.
- Inverses in U are inherited from V.

□

3.1.3 Properties of Group Homomorphism

Proposition 3.1. Let $\phi : G \to H$ be a group homomorphism. We have

(a) $\phi(1_G) = 1_H$.

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

Proof. (a) For any $g \in G$,

$$\begin{aligned} \phi(g) &= \phi(1_G \cdot g) && (2) \\ &= \phi(1_G) \cdot \phi(g) && \text{(Definition of homomorphism)} \end{aligned}$$

Let h be the inverse of $\phi(g)$. Then

$$\begin{aligned} \phi(g) \cdot h = \phi(1_G) \cdot \phi(g) \cdot h \quad &\Rightarrow \quad 1_H = \phi(1_G) \cdot 1_H && (3) \\ &\Rightarrow \quad 1_H = \phi(1_G) && (2) \end{aligned}$$

(b) $1_H = \phi(1_G) = \phi(g \cdot g^{-1}) = \phi(g) \cdot \phi(g^{-1}) \quad \Rightarrow \phi(g^{-1}) = \phi(g)^{-1}$ □

Proposition 3.2. $\mathrm{id}_G : G \to G$ is a homomorphism.

Proof. Consider $\mathrm{id}_G : G \to G$, defined by $\mathrm{id}_G(g) = g$ for all $g \in G$.

To prove id_G is a homomorphism, we need to show:

$$\mathrm{id}_G(g_1 \cdot g_2) = \mathrm{id}_G(g_1) \cdot \mathrm{id}_G(g_2) \quad \text{for all } g_1, g_2 \in G.$$

Let $g_1, g_2 \in G$.

1.

$$\mathrm{id}_G(g_1 \cdot g_2) = g_1 \cdot g_2.$$

(By definition of id_G, $\mathrm{id}_G(g_1 \cdot g_2) = g_1 \cdot g_2$.)

2.

$$\mathrm{id}_G(g_1) \cdot \mathrm{id}_G(g_2) = g_1 \cdot g_2.$$

(Since $\mathrm{id}_G(g_1) = g_1$ and $\mathrm{id}_G(g_2) = g_2$.)

3. Since $\mathrm{id}_G(g_1 \cdot g_2) = g_1 \cdot g_2$ and $\mathrm{id}_G(g_1) \cdot \mathrm{id}_G(g_2) = g_1 \cdot g_2$, we have shown that $\mathrm{id}_G(g_1 \cdot g_2) = \mathrm{id}_G(g_1) \cdot \mathrm{id}_G(g_2)$ for all $g_1, g_2 \in G$.

Therefore, $\mathrm{id}_G : G \to G$ is a homomorphism. □

Proposition 3.3. If $G \xrightarrow{\phi} H$, $H \xrightarrow{\psi} K$ are homomorphisms, $\psi \circ \phi$ is a homomorphism.

Proof. To prove that if $\phi : G \to H$ and $\psi : H \to K$ are homomorphisms, then $\psi \circ \phi : G \to K$ is also a homomorphism, we need to verify that $\psi \circ \phi$ satisfies the homomorphism property: For all $g_1, g_2 \in G$,

$$(\psi \circ \phi)(g_1 \cdot g_2) = \psi(\phi(g_1 \cdot g_2)) = \psi(\phi(g_1) \cdot \phi(g_2)).$$

Here's the proof:

Compute $(\psi \circ \phi)(g_1 \cdot g_2)$:

$$(\psi \circ \phi)(g_1 \cdot g_2) = \psi(\phi(g_1 \cdot g_2)).$$

(This is by the definition of composition $\psi \circ \phi$.)

Apply the homomorphism property of ϕ: Since ϕ is a homomorphism, we have:

$$\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2).$$

Therefore,

$$(\psi \circ \phi)(g_1 \cdot g_2) = \psi(\phi(g_1) \cdot \phi(g_2)).$$

Apply the homomorphism property of ψ: ψ being a homomorphism implies:

$$\psi(\phi(g_1) \cdot \phi(g_2)) = \psi(\phi(g_1)) \cdot \psi(\phi(g_2)).$$

Thus, we have shown that

$$(\psi \circ \phi)(g_1 \cdot g_2) = \psi(\phi(g_1)) \cdot \psi(\phi(g_2)) = (\psi \circ \phi)(g_1) \cdot (\psi \circ \phi)(g_2).$$

Therefore, $\psi \circ \phi$ satisfies the homomorphism property, proving that $\psi \circ \phi : G \to K$ is indeed a homomorphism. □

Proposition 3.4. If $H \subset G$ is a subgroup, then the inclusion map $H \hookrightarrow G$ is a homomorphism.

Proof. To prove that the inclusion map $i : H \hookrightarrow G$ is a homomorphism, where $H \subset G$ is a subgroup, we need to verify the homomorphism property: For all $h_1, h_2 \in H$,

$$i(h_1 \cdot h_2) = i(h_1) \cdot i(h_2).$$

The inclusion map $i : H \hookrightarrow G$ is defined by $i(h) = h$ for all $h \in H$.

Since $h_1, h_2 \in H$,

$$i(h_1 \cdot h_2) = h_1 \cdot h_2.$$

(Here $\cdot$ denotes the group operation in H, and $h_1 \cdot h_2$ is the product in H.)

$$i(h_1) = h_1 \quad \text{and} \quad i(h_2) = h_2.$$

So,

$$i(h_1) \cdot i(h_2) = h_1 \cdot h_2.$$

Since $i(h_1 \cdot h_2) = h_1 \cdot h_2$ and $i(h_1) \cdot i(h_2) = h_1 \cdot h_2$, we have shown that $i(h_1 \cdot h_2) = i(h_1) \cdot i(h_2)$ for all $h_1, h_2 \in H$.

Therefore, the inclusion map $i : H \hookrightarrow G$ is a homomorphism. This completes the proof. □

3.1.4 Kernel and Image of Group Homomorphism

Definition 3.2. Given a group homomorphism

$$\phi : G \to H$$

the **kernel** of ϕ is the set

$$\ker(\phi) = \{g \in G \mid \phi(g) = 1_H\}.$$

The **image** of ϕ is the set

$$\mathrm{im}(\phi) = \{h \in H \mid h = \phi(g) \text{ for some } g \in G\}.$$

Proposition 3.5. $\ker(\phi) \subset G$, $\mathrm{im}(\phi) \subset H$ are subgroups.

Proof. $\ker(\phi)$ is subgroup of G, since:

(1) $\phi(g_1), \phi(g_2) = 1_H \Rightarrow \phi(g_1 g_2) = \phi(g_1) \cdot \phi(g_2) = 1_H \cdot 1_H = 1_H$

(2) $\phi(1_G) = 1_H$, so $1_G \in \ker(\phi)$.

(3) $\phi(g) = 1_H \Rightarrow \phi(g^{-1}) = 1_H^{-1} = 1_H \Rightarrow g^{-1} \in \ker(\phi)$

$\mathrm{im}(\phi)$ is subgroup of H, since

(1) $h_i = \phi(g_i) \Rightarrow h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2)$.

(2) $\phi(1_G) = 1_H$, so $1_H \in \mathrm{im}(\phi)$.

(3) $h = \phi(g) \Rightarrow h^{-1} = \phi(g^{-1})$.

□

3.2 Group Isomorphism

3.2.1 Definition of Group Isomorphism

Definition 3.3. If a group homomorphism ϕ is a bijection, ϕ is called a **group isomorphism**.

Isomorphism is not equality, just as bijection of sets is not.

Example 3.6. A set of five bananas is not equal to a set of five apples.

But we classify groups up to isomorphism. Just as we classify sets up to bijection.

3.2.2 Example of Group Isomorphism

Example 3.7. $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$ is a group isomorphism.

Proof. To prove that $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$ is a group isomorphism, we need to show two main things:
(1) Homomorphism: exp preserves the group operation, i.e., for all $x, y \in \mathbb{R}$,

$$\exp(x + y) = \exp(x) \cdot \exp(y).$$

(2) Bijectivity: exp is a bijection, meaning it is both injective and surjective.
For $x, y \in \mathbb{R}$,

$$\exp(x + y) = e^{x+y}.$$

Using the property of exponents,

$$e^{x+y} = e^x \cdot e^y = \exp(x) \cdot \exp(y).$$

Therefore, $\exp(x+y) = \exp(x) \cdot \exp(y)$, which shows that exp is a homomorphism.
To show exp is injective, suppose $\exp(x) = \exp(y)$ for some $x, y \in \mathbb{R}$.

$$\exp(x) = \exp(y) \Rightarrow e^x = e^y.$$

Taking the natural logarithm on both sides (which is valid since $e^x > 0$ for all x),

$$x = y.$$

Therefore, exp is injective.

To show exp is surjective, we need to show that for every $y \in \mathbb{R}_{>0}$, there exists $x \in \mathbb{R}$ such that $\exp(x) = y$. Since $y > 0$, there exists $x = \ln(y) \in \mathbb{R}$ (where ln denotes the natural logarithm) such that $\exp(x) = e^{\ln(y)} = y$. Therefore, exp is surjective.

Since exp is both a homomorphism and a bijection, it is a group isomorphism between $(\mathbb{R}, +)$ and $(\mathbb{R}_{>0}, \times)$.

Hence, $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$ is a group isomorphism. □

Theorem 3.6. Every finite cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Proof. Let $G = \langle g \rangle$ be a cyclic group of order n. Define a function $\phi : G \to \mathbb{Z}/n\mathbb{Z}$ by

$$\phi(g^k) = k \pmod{n}.$$

(1) Homomorphism:

$$\phi(g^a \cdot g^b) = \phi(g^{a+b}) = (a+b) \pmod{n}.$$

On the other hand,

$$\phi(g^a) + \phi(g^b) = a + b \pmod{n}.$$

Both sides are the same, so ϕ is a homomorphism.
(2) Injectivity: If $\phi(g^a) = \phi(g^b)$, then $a \equiv b \pmod{n}$, meaning $g^a = g^b$.
(3) Surjectivity: For any $k \in \mathbb{Z}/n\mathbb{Z}$, we have $\phi(g^k) = k \pmod{n}$. □

3.2.3 Property of Group Isomorphism

Proposition 3.7. If $\phi : G \to H$ is a group isomorphism, ϕ^{-1} is a group isomorphism.

Proof. It is obviously a bijection. Need to show ϕ^{-1} is a homomorphism: $\forall g_1, g_2 \in G$, $h_1 = \phi(g_1), h_2 = \phi(g_2)$, we have

$$\begin{aligned}
\phi^{-1}(h_1 \cdot h_2) &= \phi^{-1}(\phi(g_1) \cdot \phi(g_2)) && (\phi \text{ surjection}) \\
&= \phi^{-1}(\phi(g_1 \cdot g_2)) && (\phi \text{ homomorphism}) \\
&= (\phi^{-1} \circ \phi)(g_1 \cdot g_2) && (\text{notation}) \\
&= g_1 \cdot g_2 && (\text{definition of } \phi^{-1}) \\
&= \phi^{-1}(h_1) \cdot \phi^{-1}(h_2) && (\text{definition of } g_1,\ g_2)
\end{aligned}$$

□

3.3 Product Groups

A product group is a way to construct new groups from known ones by combining their elements and operations.

Definition 3.4. Given two groups G_1 and G_2, the **product group** $G_1 \times G_2$ is the set of ordered pairs:

$$G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$$

with the group operation defined as

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 \cdot h_1, g_2 \cdot h_2).$$

Proposition 3.8. Given two groups G_1 and G_2, $G_1 \times G_2$ is a group.

Proof. (1) Associativity: Follows from the associativity in G_1 and G_2.
(2) Identity Element: $(1_{G_1}, 1_{G_2})$ is the identity element.
(3) Inverse: $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$. □

Example 3.8 (Cartesian Product of Real Numbers)**.** The group $\mathbb{R} \times \mathbb{R}$ with standard addition is isomorphic to the Euclidean plane $\mathbb{R}^2$.

Example 3.9 (Klein Four Group)**.** $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is called **Klein four group**. It is the smallest non-cyclic group.

Example 3.10. If $\{z \in T \subset \mathbb{C} : |z| = 1\}$, then $\mathbb{C}^\times = \mathbb{R}^\times \times T$.

3.4 Automorphism

Understanding product groups naturally leads to the study of symmetries within groups. An automorphism is a bijective homomorphism from a group to itself, describing how a group's structure can be mapped onto itself in different ways. Automorphisms become especially interesting when applied to product groups, revealing how the internal structures of multiple groups interact under mappings.

Definition 3.5. Let X be a set. We write

$$\mathrm{Aut}(X) := \mathrm{Aut}_{\mathrm{set}}(X) := \{\text{bijections } X \to X\}$$

for the set of bijections from X to itself.

Proposition 3.9. $\mathrm{Aut}(X)$ is a group under composition.

Proof. $\mathrm{Aut}(X)$ is a group under composition, since

(1) composing functions is associative:

$$(f \circ g) \circ h = f \circ (g \circ h).$$

(2) $\mathrm{id}_X : X \to X$ is unit, because
$x \mapsto x$

$$f \circ \mathrm{id}_X = \mathrm{id}_X \circ f = f.$$

(3) f^{-1} is f's inverse:

$$f \circ f^{-1} = \mathrm{id}_X = f^{-1} \circ f.$$

□

3.5 Symmetric Group

Definition 3.6. Let

$$\underline{n} = \{1, \ldots, n\}.$$

Then

$$\mathrm{Aut}_{\mathrm{set}}(\underline{n}) =: S_n$$

is the **symmetric group** on a set of n elements.

Example 3.11. The following are the examples of symmetric groups:

- $n = 1$: $\mathrm{Aut}(\{1\})$ is the group with one element:

$$\begin{aligned} S_1 &= \{\text{bijections } \{1\} \to \{1\}\} \\ &= \{\mathrm{id}_{\underline{1}}\} \end{aligned}$$

- $n = 2$: $\mathrm{Aut}(\{1, 2\})$ is the group with two elements:

$$S_2 = \left\{ \left(\mathrm{id} : \begin{matrix} 1 \mapsto 1 \\ 2 \mapsto 2 \end{matrix} \right), \left(\sigma : \begin{matrix} 1 \mapsto 2 \\ 2 \mapsto 1 \end{matrix} \right) \right\}$$

  which satisfies

$$\sigma \circ \sigma = \sigma^2 = \mathrm{id}.$$

- S_3 has 3! elements. We will learn more about its structure soon.
- In general, S_n is group with $n!$ elements.

The definition of the symmetric group S_n on the finite set $\underline{n} = \{1, 2, \ldots, n\}$ can be extended to any set G, finite or infinite. We have the following definition:

Definition 3.7. Symmetric group on a set G is the group of all bijections from G to itself:

$$\mathrm{Sym}(G) = \mathrm{Aut}_{\mathrm{set}}(G).$$

This group consists of all permutations of the elements of G. When G is a finite set with n elements, $\mathrm{Sym}(G)$ is essentially the same as S_n, but this generalization allows us to consider permutations on any set G, regardless of its cardinality.

The symmetric groups are fundamental in the study of group theory because they capture the essence of symmetry by encompassing all possible permutations of a finite set. Interestingly, every group, finite or infinite, can be represented as a group of permutations. This profound connection is formalized in Cayley's theorem.

3.6 Cayley's Theorem

Theorem 3.10 (Cayley's Theorem)**.** Every group G is isomorphic to a subgroup of the symmetric group $\mathrm{Sym}(G)$ on the set G.

Proof. Let G be any group. We aim to construct an injective group homomorphism $\phi : G \to \mathrm{Sym}(G)$, demonstrating that G is isomorphic to a subgroup of $\mathrm{Sym}(G)$.

For each element $g \in G$, define a function $L_g : G \to G$ by left multiplication:

$$L_g(h) = gh \quad \text{for all } h \in G.$$

Since G is a group, each L_g is a bijection (with inverse $L_{g^{-1}}$), so $L_g \in \mathrm{Sym}(G)$.

Define the map $\phi : G \to \mathrm{Sym}(G)$ by

$$\phi(g) = L_g.$$

- Homomorphism Property: For all $g_1, g_2 \in G$ and $h \in G$,

$$\phi(g_1 g_2)(h) = L_{g_1 g_2}(h) = (g_1 g_2)h = g_1(g_2 h) = L_{g_1}(L_{g_2}(h)) = (\phi(g_1) \circ \phi(g_2))(h).$$

  Therefore, $\phi(g_1 g_2) = \phi(g_1) \circ \phi(g_2)$, so ϕ is a group homomorphism.

- Injectivity: Suppose $\phi(g) = \phi(h)$ for some $g, h \in G$. Then for all $k \in G$,

$$L_g(k) = L_h(k) \implies gk = hk.$$

  In particular, when k is the identity element e of G,

$$ge = he \implies g = h.$$

  Thus, ϕ is injective.

Since ϕ is an injective homomorphism, G is isomorphic to the subgroup $\phi(G)$ of $\mathrm{Sym}(G)$. □

Cayley's Theorem reveals that every group can be viewed as a group of permutations, emphasizing the central role of symmetric groups in understanding the structure of all groups.

Chapter 4

Group Actions

4.1 Motivation of Group Action

As one of the greatest mathematicians has said, let the math speak for itself – don't feel like you need to motivate everything. If it's beautiful, it'll motivate itself. So, that said, I don't want to have to motivate group actions for you, but the history is actually quite interesting, so it's worth discussing.

So, if you were a French or German mathematician in the mid-19th century, your definition of a group would not have been the one we gave you in the context. In fact, a group was simply defined to be the matrix group $GL_n(\mathbb{R})$, over maybe $\mathbb{C}$ if you wanted to work in a world that makes everything absolutely beautiful. Naturally, we had a bijection

$$GL_n(\mathbb{R}) \simeq \mathrm{Aut}(V), \tag{4.1}$$

for V a real vector space of finite dimension n. Thus, it was natural to study how the elements of $GL_n(\mathbb{R})$ behaved through the above bijection, instead of just row-reducing mindlessly – this"group action" in the automorphism (4.1) actually gives rise to the more abstract theory of linear algebra all of you learned before! This is actually something called a group representation, when you have a group homomorphism from G to the linear automorphism group of a vector space, which is something we'll also learn soon enough. The point is, group actions arose naturally from the study of the automorphism (4.1), so what we're studying isn't completely contrived. To see why/how we got from studying linear automorphisms of vector spaces to just automorphisms of sets, it turns out that this notion of group action is ubiquitous beyond the land of linear algebra, so why not "generalize" our theory of group actions from vector spaces to sets! It turns out that this type of procedure is very important in algebra. You want to see what you've got, try to take away any structure that you don't necessarily need to study the "abstract theory", and see if you have an interesting theory. It's this procedure that actually led Emmy Nöther to define our current notion of group in the early 20th century.

4.2 Definition of Group Action

Definition 4.1. Let X be a set and G be a group. A **group action** of G on X is a homomorphism

$$\phi : G \to \mathrm{Aut}(X).$$

Or alternatively, a map $\phi : G \to \mathrm{Aut}(X)$ such that:

- $\phi(1_G) = \mathrm{Id}_X$.
- $\phi(g_1 \cdot g_2) = \phi(g_1) \circ \phi(g_2)$.

The above definition really just says that we want a group to act on a set X in an invertible manner (since group elements are invertible!), and in a manner such that group multiplication corresponds to composition of automorphisms, so we can actually think of group elements as automorphisms on X themselves!

Definition 4.2. A **left group action** of G on X is a map

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto gx \end{aligned}$$

such that

- $1_G x = x$.
- $g(hx) = (gh)x$, for $g, h \in G$.

4.3 Examples of Group Action

Example 4.1. Let $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$. Define

$$\begin{aligned} \phi : S^1 &\to \mathrm{Aut}(\mathbb{C}) \\ z &\mapsto f_z \end{aligned}$$

where $f_z(\omega) := z \cdot \omega$ (rotation by z).

4.4 Proposition of Group Action

Proposition 4.1. A group action determines a map of sets

$$G \times X \to X$$

where we will write the value of (g, x) as gx.

The map satisfies

(a) $1_G x = x$

(b) $(gh)x = g(hx)$

Conversely, any map $G \times X \to X$ satisfying (a),(b) determines a group action.

Proof. Given

$$\phi : G \to \mathrm{Aut}_{\mathrm{set}}(X)$$

Let

$$\phi(g) = \phi_g$$

Then let

$$G \times X \to X$$

be

$$(g, x) \mapsto \phi_g(x)$$

(a) Then $\phi_{1_G} = \mathrm{id}_X$ (since ϕ is a homomorphism), so

$$\begin{aligned} (1, x) \mapsto \phi_1(x) &= \mathrm{id}_X(x) \\ &= x \end{aligned}$$

(b)$\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ since ϕ is group homomorphism.

Hence

$$\phi_{g_1 g_2}(x) = \phi_{g_1} \circ \phi_{g_2}(x) \qquad \forall x.$$

By notation,

$$\begin{aligned} (g_1 g_2)(x) &= \phi_{g_1}(g_2 x) \\ &= g_1(g_2 x). \end{aligned}$$

Conversely, if we're given a map $G \times X \to X$ satisfying (a),(b), restrict the map to the set $\{g\} \times X \subset G \times X$.

The map $\{g\} \times X \to X$ can be identified with a map

$$\begin{aligned} \psi_g : X \cong \{g\} \times X &\to X \\ x \mapsto (g, x) &\mapsto x \end{aligned}$$

ψ_g is a bijections because of (a) and (b). First, look at

$$\begin{aligned} \psi_{1_G} : X \cong \{1_G\} \times X &\to X \\ x \mapsto (1_G, x) &\mapsto 1_G \cdot x \end{aligned}$$

by (a), $1_G \cdot x = x \leqslant 0$

$$\psi_{1_G}(x) = x.$$

This means ψ_{1_G} is the identity bijections,

$$\psi_{1_G} = \mathrm{id}_X.$$

Equal as elements on the set of maps from X to X.

Next, note ψ_g is a bijections $\forall g$. This is because

Injection:

$$\begin{aligned}
& \psi_g(x) = \psi_g(y) && \text{Notation} \\
\Rightarrow \quad & gx = gy && \text{Since } G \times X \to X \text{ is given.} \\
\Rightarrow \quad & g^{-1}(gx) = g^{-1}(gy) && \text{(b) } (x' = x \Rightarrow hx' = hx,\ \forall h \in G) \\
\Rightarrow \quad & 1_G x = 1_G y && \\
\Rightarrow \quad & x = y && \text{(a)}
\end{aligned}$$

Surjection: If $x \in X$, let $y = g^{-1}x$, then

$$\begin{aligned}
\psi_g(y) &= g(g^{-1}x) \\
&= (gg^{-1})x \\
&= x.
\end{aligned}$$

So $\psi_g \in \mathrm{Aut}_{\mathrm{set}}(X)$, $\forall g \in G$. Finally, $g \mapsto \psi_g$ is a homomorphism since

$$g_1 g_2 \mapsto \psi_{g_1 g_2},$$

and

$$\begin{aligned}
\psi_{g_1 g_2}(x) &= (g_1 g_2)x \\
&= g_1(g_2)x \\
&= \psi_{g_1}(g_2)x \\
&= \psi_{g_1}(\psi_{g_2}(x)) \\
&= \psi_{g_1} \circ \psi_{g_2}(x) \qquad \forall x. \\
\Rightarrow \quad & \psi_{g_1 g_2} = \psi_{g_1} \circ \psi_{g_2}.
\end{aligned}$$

□

How do we show that two functions $f, g : A \to B$ are the same?
Show $f(a) = g(a)$ for all $a \in A$. That's the definition of $f = g$.
So you may find it harder to think of a group action as a map

$$G \times X \to X$$

satisfying (a),(b) rather than as a homomorphism

$$G \to \mathrm{Aut}_{\mathrm{set}}(X)$$

4.5 Orbits

Philosophy: Given a group action $G \to \mathrm{Aut}_{\mathrm{set}}(X)$, we can break X into **orbits**.

Definition 4.3. Let G act on a set X. Then $\forall x \in X$, the **orbits of** x is the set

$$\mathcal{O}_x = \{y \in X \mid y = gx \text{ for some } g\}$$

Example 4.2. Let $G \to \mathrm{Aut}_{\mathrm{set}}(X)$ be $g \mapsto \mathrm{id}_X$ (The trivial action.)

Then

$$\begin{aligned}
\mathcal{O}_x &= \{y \mid y = \mathrm{id}_X(X)\} \\
&= \{x\}.
\end{aligned}$$

Example 4.3. $G = S^1$, $X = \mathbb{C}$,

$$G \times X \to X$$
$$(e^{i\theta}, z) \mapsto z \times e^{i\theta}$$

Then $\mathcal{O}_z = \{\omega \mid \omega = z \times e^{i\theta} \text{ for some } \theta\}$ =circle of radius $|z|$, which means

$$\mathbb{C} = \bigsqcup_{z \in \mathbb{R}_{\geqslant 0}} \mathcal{O}_z$$

Also notice that $\mathcal{O}_0 = \{0\} \subset \mathbb{C}$.

Remark. Let $\mathcal{P}(X)$ be the power set of X. It's the set of all subsets of X. Then a group action determines a map

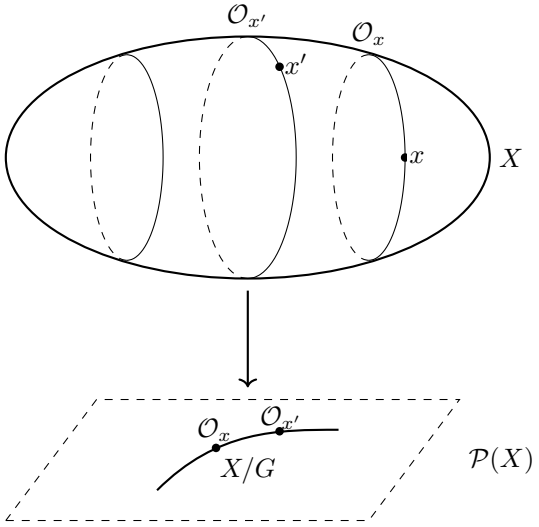
$$X \to \mathcal{P}(X)$$
$$x \mapsto \mathcal{O}_x$$

It certainly won't hit every element of $\mathcal{P}(X)$. For instance, empty subset. But we'll hit some of them.

Definition 4.4. The **orbit set**, or **orbit space**, of a group action is the image of $X \to \mathcal{P}(X)$. We denote it

$$X/G$$

Like dividing out X by G. If $y = gx$, then $\mathcal{O}_x = \mathcal{O}_y$, so y and x have the same image in $\mathcal{P}(X)$, i.e. are sent to the same element in X/G.



Proposition 4.2.

(i) $\forall x \in X$, $x \in \mathcal{O}_x$.

(ii) $\mathcal{O}_x = \mathcal{O}_y \Leftrightarrow y = gx$ for some $g \in G$.

Proof. (i) $x = 1_G x$, so $x \in \mathcal{O}_x$.
(ii) $\mathcal{O}_x = \mathcal{O}_y \Leftrightarrow y \in \mathcal{O}_y$ by (i) $\Leftrightarrow y = gx$ for some $g \in G$ (Definition of $\mathcal{O}_x$). □

We can then count elements of X (if X is finite) by counting orbits one by one.

Example 4.4. Let G be a group. $\forall g \in G$, we have a bijection

$$\phi_g : G \to G$$
$$x \mapsto gx$$

This is a bijection since:

- $y \in G \quad \Rightarrow \quad y = g(g^{-1}y) = \phi_g(g^{-1}y)$.
- $\phi_g(y) = \phi_g(y') \quad \Rightarrow \quad gy = gy' \quad \Rightarrow \quad y = y'$.

Moreover,

$$\begin{aligned}\phi_{g_1g_2}(x) &= (g_1g_2)(x)\\ &= g_1(g_2(x))\\ &= \phi_{g_1}\circ\phi_{g_2}(x)\end{aligned}$$

So the map

$$\begin{aligned}\phi : G &\to \mathrm{Aut}_{\mathrm{set}}(G)\\ g &\mapsto \phi_g\end{aligned}$$

is a homomorphism. i.e., every group acts on itself.

If $H \subset G$ is a subgroup, then

$$H \to G \to \mathrm{Aut}_{\mathrm{set}}(G)$$

is a group action. More concerely, we have

$$\begin{aligned}\phi_h : G &\to G\\ x &\mapsto h\cdot x\end{aligned}$$

$\forall h \in H$.

We introduced the group action of a group G on itself, given by left translation.

Proposition 4.3. Let H be a subgroup of G. The we saw last time H acts on G. Moreover, $\forall x, y \in G$, $|\mathcal{O}_x| = |\mathcal{O}_y|$.

Proof. Let $h = x^{-1}y \in G$. Then we have maps

$$\begin{aligned}\mathcal{O}_x &\to \mathcal{O}_y\\ gx &\mapsto gxh\\ \mathcal{O}_x &\leftarrow \mathcal{O}_y\\ gyh^{-1} &\leftarrow\!\shortmid gy\end{aligned}$$

in $\mathcal{O}_y$ since $gxh = gx(x^{-1}y) = gy \in \mathcal{O}_y$

These are inverse to each other, since

$$\begin{aligned}gx \mapsto gxh \mapsto gxhh^{-1} = gx\\ gy \mapsto gyh \mapsto gyh^{-1}h = gy\end{aligned}$$

□

4.6 Lagrangian Theorem

Proposition 4.4. $X = \bigcup_{\mathcal{O}\in X/G} \mathcal{O}$.
Moreover, $\mathcal{O} \neq \mathcal{O}' \Rightarrow \mathcal{O} \cap \mathcal{O}' = \varnothing$.

Proof. (1) Take any element $x \in X$.
By definition of the orbit, x belongs to the orbit $\mathcal{O}_x$ (the orbit containing x).
Therefore, $x \in \bigcup_{\mathcal{O}\in X/G} \mathcal{O}$.
Since this holds for every $x \in X$, we have $X = \bigcup_{\mathcal{O}\in X/G} \mathcal{O}$.

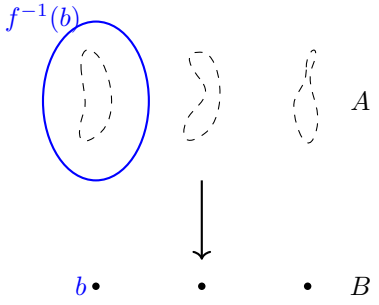
(2) For any map of sets,

$$f : A \to B,$$

we know

$$A = \bigcup_{b\in B} f^{-1}(b)$$

And $f^{-1}(b) \cap f^{-1}(b') = \varnothing$,
Here, $\mathcal{O} = f^{-1}(\mathcal{O})$, so $\mathcal{O} \neq \mathcal{O}' \Rightarrow \mathcal{O} \cap \mathcal{O}' = \varnothing$.

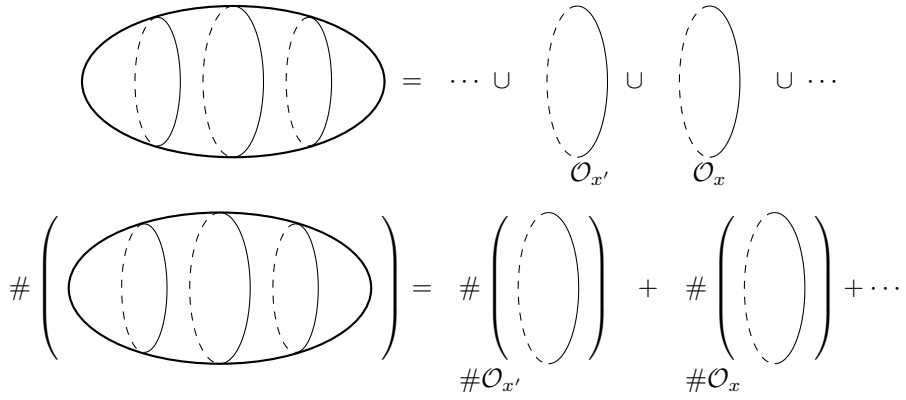


□

Corollary 4.5. $X = \bigsqcup_{\mathcal{O} \in X/G} \mathcal{O}$

Corollary 4.6. $|X| = \sum_{\mathcal{O} \in X/G} |\mathcal{O}|$

Proof.



□

Corollary 4.7. $|X| = |X/G| \cdot |\mathcal{O}_x|$ for any $x \in X$.

Proposition 4.8. $|\mathcal{O}_{\mathrm{id}_G}| = |H|$

Proof.

$$\begin{aligned} \mathcal{O}_{\mathrm{id}_G} &= \{y \mid y = h \cdot \mathrm{id}_G \text{ for some } h \in H\} \\ &= \{y \mid y = h \text{ for some } h \in H\} \\ &= H \end{aligned}$$

□

We've shown that if G is finite, then

$$|\mathcal{O}_x| = |H|$$

$\forall x \in G$.

Hence

$$G = \bigsqcup \mathcal{O}_x$$

$$|G| = \sum_{\substack{\text{summing over} \\ \text{set of orbits}}} |H|$$

This implies $|H|$ divides $|G|$.

This is **Lagrange's theorem** that we've proven.

Theorem 4.9 (Lagrange's Theorem)**.** Let G be finite. Then $|H|$ divides $|G|$.

4.7 Cosets and Normal Subgroups

Definition 4.5. Given $H \subset G$ a subgroup. Let $g \in G$. We define

$$Hg := \{hg \mid h \in H\}$$

be the **right coset** of H.

We saw

$$Hg = Hg' \quad \text{if and only if } hg = g'$$

for some $h \in H$.

Definition 4.6. We let

$$gH := \{gh \mid h \in H\}$$

be the **left coset** of H.

Example 4.5. Let $H = \langle(12)\rangle \subset S_3 = G$. Then for $g = (123)$.

$$\begin{aligned} gH &= \{(123), (123)(12)\} \\ &= \{(123), (13)\} \end{aligned}$$

while

$$\begin{aligned} Hg &= \{(123), (12)(123)\} \\ &= \{(123), (23)\} \end{aligned}$$

So $gH \neq Hg$ in general.

We will also write G/H for left coset, we will try, when possible, to never speak of right cosets again.

Definition 4.7. A subgroup $H \subset G$ is called **normal** if $\forall g \in G$,

$$\{ghg^{-1} \mid h \in H\} = H$$

The left hand side is also written as gHg^{-1}, i.e. H is normal if and only if

$$gHg^{-1} = H.$$

We denote as $H \triangleleft G$.

gH is the orbit for a group action from the right: $X \times H \to X$. So our definition of the group G/H is the same—same elements, same operation.

Proposition 4.10. (1) $gH = gH'$ if and only if $\exists h \in H$, s.t. $gh = g'$.
(2) $gH = Hg$, $\forall g \in G$ if and only if $H \triangleleft G$.

Proof. (1) $gH = g'H \Rightarrow \exists h_1, h_2 \in H$, s.t. $gh_1 = g'h_2$
$\Rightarrow gh_1h_2^{-1} = g'$.
Set $h_1h_2^{-1} = h$ and we get

$$gh = g'.$$

(2) $gH = Hg \Rightarrow \forall h \in H$, $\exists h' \in H$, s.t. $gh = h'g$
$\Rightarrow ghg^{-1} = h'$, i.e. $\forall h \in H$, $ghg^{-1} \in H$
$\Rightarrow gHg^{-1} \subset H$, $\forall g \in G$
$\Rightarrow H \triangleleft G$.
$H \triangleleft G \Rightarrow ghg^{-1} \in H$, $\forall g \in G$, $h \in H$
$\Rightarrow \forall g \in G$, $h \in H$, $\exists h' \in H$, s.t. $ghg^{-1} = h'$
$\Rightarrow \forall g \in G$, $h \in H$, $\exists h' \in H$, $gh = h'g$. □

4.8 Index

Definition 4.8. Let $H \subset G$ be a subgroup. The **index** of H in G is the number of elements in G/H. It is written as

$$[G : H] := |G/H| = \#\text{ of cosets } Hg = \#\text{ of orbits } \mathcal{O}_g$$

Proposition 4.11. Suppose $K \subset H \subset G$ are subgroups. (H is a subgroup of G, K is a subgroup of H. Note this also means K is a subgroup of G.) Then

$$[G : K] = [G : H][H : K].$$

Proof. In the proof of Lagrange theorem, we saw that

$$G = \bigsqcup_{\mathcal{O}_g \in G/H} \mathcal{O}_g$$

i.e. that G is a disjoint union of orbits of H's action on G. Moreover, all orbits have the same size $|\mathcal{O}_g| = |H|$, $\forall g \in G$.

Hence

$$|G| = n \cdot |H|$$

where n is the number of distinct orbits, i.e. $n = [G : H]$.

Hence

$$[G : K] = |G|/|K| = |G|/|H| \cdot |H|/|K| = [G : H][H : K].$$

□

This one brings many ideas together.

Proposition 4.12. Any subgroups of index 2 in a group is normal.

Proof. Since H has index 2 in G, there are exactly two distinct left cosets of H in G:

$$G = H \cup gH$$

where $g \in G \setminus H$. Similarly, there are exactly two right cosets:

$$G = H \cup Hg$$

for the same g.

We will consider two cases based on whether an element g belongs to H or $G \setminus H$.

- $g \in H$: If $g \in H$, then:
$$gH = H = Hg$$
because H is a subgroup and thus closed under group operations. Therefore, the left and right cosets coincide.
- $g \in G \setminus H$: If $g \notin H$, then gH and Hg are the other coset besides H. Since there are only two cosets, it follows that:
$$gH = G \setminus H = Hg$$
Thus, the left and right cosets are again the same.

In both cases, $gH = Hg$ for all $g \in G$. This equality of left and right cosets implies that H is a normal subgroup of G. □

4.9 Orbit-Stabilizer Theorem

Definition 4.9. Let $\phi : G \to \mathrm{Aut}_{\mathrm{set}}(X)$ be a group action. Given $x \in X$, the **stabilizer** of x is the subgroup

$$\begin{aligned} G_x &= \{g \mid gx = x\} = \{g \mid \phi_g(x) = x\} \\ &\subset G \end{aligned}$$

Proposition 4.13. G_x is a subgroup of G.

Proof. Since $\phi_g(x) = x$, $\phi_{g'}(x) = x$.
$\Rightarrow x = \phi_g(x) = \phi_g(\phi_{g'}(x)) = \phi_{gg'}(x)$ and $\phi_{1_G}(x) = \mathrm{id}_X x = x$ □

Now, given an action of G on X, we have two things we can associate to an element $x \in X$:

$$\begin{array}{cc} G_x \subset G, & \mathcal{O}_x \subset X \\ \text{Stabilizer} & \text{Orbit} \end{array}$$

Proposition 4.14. The function

$$\begin{aligned} G/G_x &\to \mathcal{O}_x \\ gG_x &\mapsto gx = \phi_g(x) \end{aligned}$$

is a bijection.

Proof. It is well-defined, since

$$\begin{aligned} gG_x = g'G_x &\Rightarrow g' = gh \text{ for some } h \in G_x \\ &\Rightarrow g'x = (gh)x \\ &\quad\;\; = g(hx) \\ &\quad\;\; = gx \end{aligned}$$

Injective:

$$\begin{aligned} g'x = gx &\Rightarrow g^{-1} \cdot g'x = x \\ &\Rightarrow g^{-1} \cdot g' \in G_x \\ &\Rightarrow g' = gh \text{ for some } h \in G_x \\ &\Rightarrow gG_x = g'G_x \end{aligned}$$

Surjective: $x' \in \mathcal{O}_x \Rightarrow x' = gx$ for some $g \in G$. □

Corollary 4.15 (Orbit-Stabilizer Theorem)**.** If $|G_x|$, $|\mathcal{O}_x|$ are finite, so is $|G|$. Moreover, $|G| = |G_x||\mathcal{O}_x|$.

Proof. From the proposition, there's a bijection between the set of left cosets G/G_x and the orbit $\mathcal{O}_x$, so:
Number of cosets: $|G/G_x| = |\mathcal{O}_x|$.
Each left coset gG_x has exactly $|G_x|$ elements because G_x is a subgroup of G.
Therefore, the total number of elements in G is the product of the number of cosets and the size of each coset:

$$|G| = |G/G_x||G_x| = |\mathcal{O}_x||G_x|.$$

Since both $|\mathcal{O}_x|$ and $|G_x|$ are finite, their product $|G|$ is also finite.
Therefore, If $|G_x|$ and $|\mathcal{O}_x|$ are finite, then G is finite with size $|G| = |G_x||\mathcal{O}_x|$. □

This is called the **Orbit-Stabilizer theorem**, and it's fantastic.

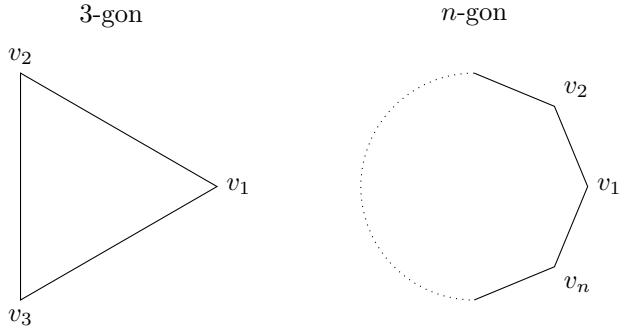
Example 4.6. Let $P_n \subset \mathbb{R}^2$ be a regular n-gon in $\mathbb{R}^2$ centered at the origin. Let $D_{2n} \subset GL_2(\mathbb{R})$ be the group of linear transformations, such that

$$\forall g \in D_{2n}, \quad g(P_n) = P_n$$

This means $g(P_n) \subset P_n$, $P_n \subset g(P_n)$. Does **NOT** mean $g(x) = x$, $\forall x \in P_n$.
i.e., D_{2n} is the set of linear symmetries of P_n.

Claim 4.16. $|D_{2n}| = 2n$

Definition 4.10. D_{2n} is called the n**th dihedral group**.



The set P_n won't help — it has infinitely many elements. But if D_{2n} acts on P_n, it must permute the vertices $v_1, v_2, \ldots, v_n$ of P_n. So D_{2n} acts on the set $V = \{v_1, v_2, \ldots, v_n\}$.

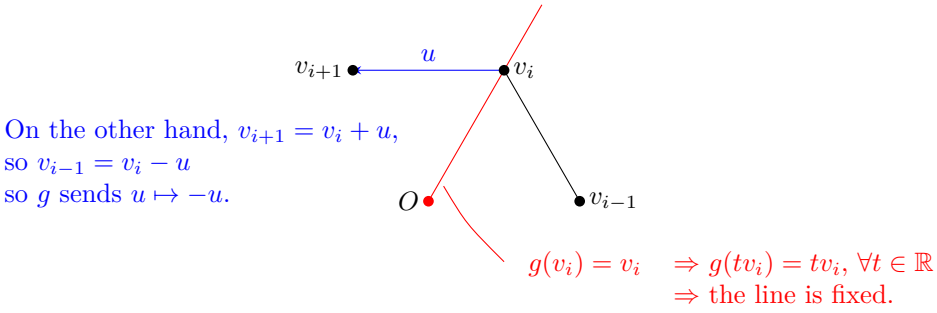
Given, say, v_i, we can see that

$$\mathcal{O}_{v_i} = V.$$

Why? The rotation by $\frac{2\pi}{n}$ is linear, and sends P_n to P_n (since we chose P_n to be centered at the origin). Hence rotations by $\frac{2\pi k}{n}$ are in D_{2n}, and rotating v_i by $\frac{2\pi k}{n}$ hits every v_j.
What's the stabilizer?

If v_i is fixed, what could $g \in D_{2n}$ do to v_{i-1} and v_{i+1}?

- If $g(v_{i-1}) = v_{i-1}$, we have two linear independent vectors——v_i, v_{i-1} fixed by g. Hence $g = \mathrm{id}_{\mathbb{R}^2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
- Otherwise, $g(v_{i-1}) = v_{i+1}$. Then g must be a reflection about the line through the origin $\vec{O}$ and v_i.



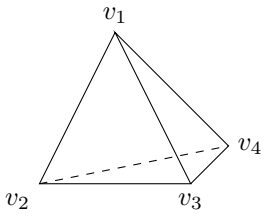
So $\exists$ exactly two elements of D_{2n} fixing v_i. i.e., the stabilizer of v_i has order two (hence is isomorphic to $\mathbb{Z}/2\mathbb{Z}$).

By the orbit-stabilizer theorem,

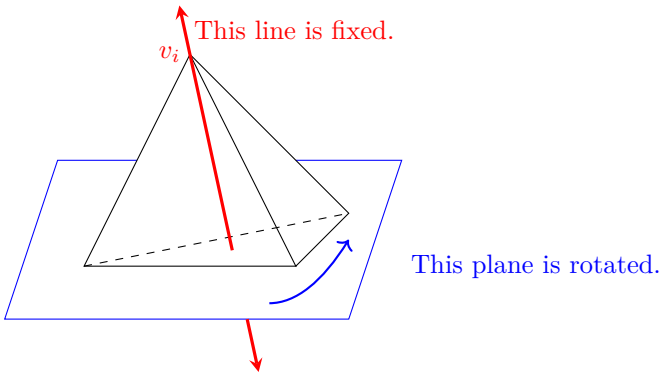
$$\begin{aligned} |D_{2n}| &= 2 \cdot |\mathcal{O}_{v_i}| \\ &= 2 \cdot |V| \\ &= 2 \cdot n \end{aligned}$$

Example 4.7 (Rotational symmetries)**.** Let T be a regular tetrahedron centered at the origin. Let $G \subset SO_3(\mathbb{R})$ be the group of rotations g, such that $g(T) = T$.

Well, G then acts on the set of vertices of T. T has four vertices: v_1, v_2, v_3, v_4.

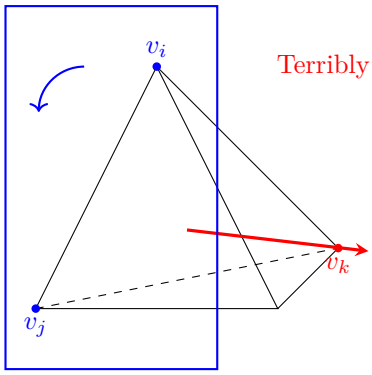


Let's first count the stabilizer of some v_i. Well, if g is a rotation fixing v_i, it must rotate the face opposite v_i, and fix the line through v_i.



Then there are three possible rotations of the plane——each by $\frac{2\pi}{3}$, $\frac{4\pi}{3}$, or 0 radians. So the stabilizer of v_i is a group of order 3 (hence isomorphic to $\mathbb{Z}/3\mathbb{Z}$).

What's the orbit? Every vertex! For if you want to find g, such that $g(v_i) = g(v_j)$, choose g to be a rotation fixing some v_k, $v_k \neq v_i, v_j$, and rotate!



Terribly not to scale.

By orbit-stabilizer theorem,

$$\begin{aligned} |G| &= 3 \cdot |\mathcal{O}_{v_i}| \\ &= 3 \cdot 4 \\ &= 12 \end{aligned}$$

We'll see eventually what group this is.

Chapter 5

Cycle Notation

Definition 5.1. Let

$$G \to \mathrm{Aut}_{\mathrm{set}}$$

be a group action of G on X. Fix $g \in G$. By **the action of g on X**, we mean the action

$$\langle g \rangle \to G \to \mathrm{Aut}_{\mathrm{set}}.$$

The $\langle g \rangle \to G$ is a group homomorphism since the inclusion of a subgroup is a group homomorphism. $\langle g \rangle \to \mathrm{Aut}_{\mathrm{set}}$ is a group homomorphism since the composition of two group homomorphism is a group homomorphism.

In essence, the action of g on X is represented in cycle notation by decomposing g into cycles, where each cycle corresponds to an orbit of g acting on X.

5.1 Cycle

Definition 5.2. An element $\sigma \in S_n$ is called a **cycle** if σ's action on $\underline{n}$ has at most one orbit of size $\geqslant 2$.

Example 5.1.

- $\sigma = 1_{S_n}$ has only orbits of size 1. So 1_{S_n} is a cycle.
- Let $\tau : \underline{4} \to \underline{4}$, which we will draw as $1 \rightleftarrows 2$.
  $1 \mapsto 2$
  $2 \mapsto 1$ $\qquad\qquad$ $4 \rightleftarrows 3$
  $3 \mapsto 4$
  $4 \mapsto 3$

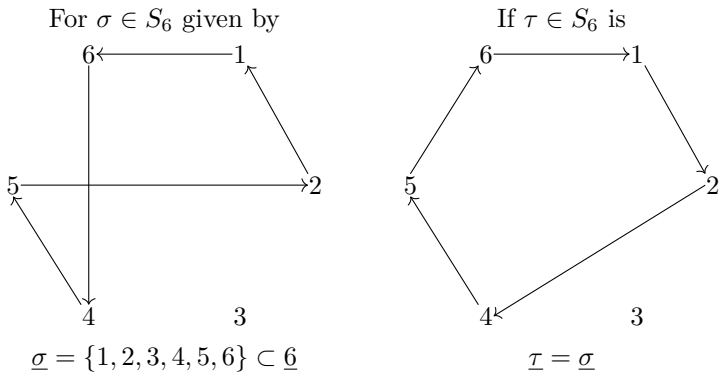
  This is NOT a cycle, as it has two orbits of size $\geqslant 2$: $\{1, 2\}$ and $\{3, 4\}$.
- $\tau : \underline{5} \to \underline{5}$, $\qquad$ 1 $\qquad$, is a cycle.
  $1 \mapsto 1$
  $2 \mapsto 2$ $\qquad$ 5 $\qquad\qquad$ 2
  $3 \mapsto 5$
  $4 \mapsto 3$ $\qquad\qquad$ 4 $\longrightarrow$ 3
  $5 \mapsto 4$

Definition 5.3. If $\sigma \in S_n$ is a cycle, we will let $\underline{\sigma} \subset \underline{n}$ denote the orbit of size $\geqslant 2$. For $\sigma = 1_G$, we let

$$\underline{1_G} := \varnothing.$$

5.2 Disjoint Cycles

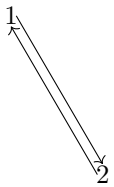
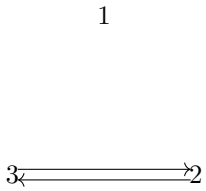
Example 5.2.



$\underline{\sigma}$ is a subset, so order of elements don't matter. e.g. It's not some set together with a choice of ordering.

Definition 5.4. Suppose $\sigma, \tau \in S_n$ are cycles. We say σ and τ are **disjoint cycles** if and only if $\underline{\sigma}$ and $\underline{\tau}$ don't intersect.

Example 5.3.

- 1_G is disjoint from any cycle.
- $\sigma =$  and $\tau =$  are NOT disjoint, since $\{1,2\}$ and $\{2,3\}$ intersect.
- $\sigma =$  and $\tau =$  are disjoint.

Proposition 5.1. Disjoint cycles in S_n commute.

Proof. Let σ, τ be disjoint cycles and let $k \in \underline{n} = \{1, \ldots, n\}$. Then

$$(\sigma \circ \tau)(k) = \begin{cases} \sigma(k) & \text{if } k \neq \underline{\tau} \\ \tau(k) & \text{if } k \in \underline{\tau} \end{cases}$$
$$= \begin{cases} \sigma(k) & \text{if } k \in \underline{\sigma} \\ k & \text{if } k \neq \underline{\sigma}, \underline{\tau} \\ \tau(k) & \text{if } k \in \underline{\tau} \end{cases}$$

since

$$\begin{aligned} k \neq \underline{\tau} &\Rightarrow \tau(k) = k \\ &\Rightarrow \sigma(\tau(k)) = \sigma(k) \\ k \in \underline{\tau} &\Rightarrow \tau(k) \in \underline{\tau} && \text{definition of orbit} \\ &\Rightarrow \tau(k) \neq \underline{\sigma} && \text{definition of disjoint} \\ &\Rightarrow \sigma(\tau(k)) = \tau(k) \end{aligned}$$

while

$$(\tau \circ \sigma)(k) = \begin{cases} \tau(k) & \text{if } k \neq \underline{\sigma} \\ \sigma(k) & \text{if } k \in \underline{\sigma} \end{cases}$$
$$= \begin{cases} \tau(k) & \text{if } k \in \underline{\tau} \\ k & \text{if } k \neq \underline{\sigma}, \underline{\tau} \\ \sigma(k) & \text{if } k \in \underline{\sigma} \end{cases}$$

So $\sigma \circ \tau = \tau \circ \sigma$. □

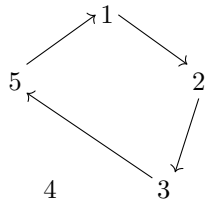
5.3 Cycle Notation

Definition 5.5. Let σ be a cycle. A **cycle notation** for σ is the expression

$$(a\ \sigma(a)\ \sigma^2(a)\ \cdots\ \sigma^{|\sigma|-1}(a))$$

for some $a \in \underline{\sigma}$.

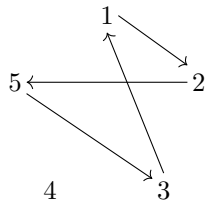
Example 5.4. If $\sigma \in S_5$ is pictured as



then the following are all cycle notations for σ:

$$\underset{a=1}{(1235)}, \quad \underset{a=2}{(2351)}, \quad \underset{a=5}{(5123)}, \quad \underset{a=3}{(3512)}.$$

Example 5.5. If $\tau \in S_5$ is pictured as



$\underline{\tau} = \underline{\sigma}$, but no cycle notation for τ is a cycle notation for σ.

$$(1253), (2531), (5312), (3125).$$

Implicitly, we are making identifications between the various cycle notation for σ.

Theorem 5.2. Every element

$$\sigma \in S_n$$

can be written as a product of disjoint cycles, and uniquely, up to reordering.

Proof. For $\sigma \in S_n$, let $\{\mathcal{O}_a\}$ be the set of orbits of σ's action on $\underline{n}$. $\forall \mathcal{O}_a \in \underline{n}/\langle\sigma\rangle$, choose $a \in \mathcal{O}_a$ and set

$$\sigma_a = (a\ \sigma(a)\ \cdots\ \sigma^{|\mathcal{O}_a|-1}(a))$$

by a cycle. Then by definition,

$$\sigma = \prod_{\mathcal{O}_a} \sigma_a$$

This is because

$$\prod_{\mathcal{O}_a} \sigma_a(k) = \sigma(k)$$

by definition. Also note I've written

$$\prod_{\mathcal{O}_a} \sigma_a = \sigma_a \cdot \sigma_b \cdot \cdots \cdot \sigma_z$$

without specifying an order. This is because each σ_a, σ_b is disjoint (by disjointedness of orbits) and hence commute. (i.e. order doesn't matter.)

As for uniqueness: If someone else were to write

$$\sigma = \prod \tau_i = \tau_1 \cdot \tau_2 \cdot \cdots \cdot \tau_k$$

for $\{\tau_i\}$ a collection of disjoint cycles, we note that

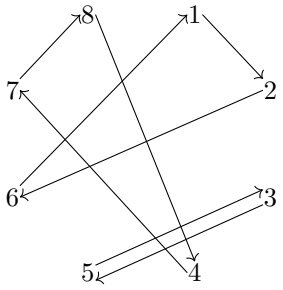
$$\{\tau_i\} = \underline{n}/\langle\sigma\rangle.$$

$\Rightarrow \forall i$, $\exists! \sigma_a$, s.t. $\underline{\sigma_a} = \underline{\tau_i}$. Writing $\tau_i = (b_0 b_1 \cdots b_{|\tau_i|-1})$, we see $\sigma(b_i) = b_{i+1}$ and we are done. □

Example 5.6. Let $\sigma \in S_8$ be given by

$$\begin{aligned} \sigma : \underline{8} &\to \underline{8} \\ 1 &\mapsto 2 \\ 2 &\mapsto 6 \\ 3 &\mapsto 5 \\ 4 &\mapsto 7 \\ 5 &\mapsto 3 \\ 6 &\mapsto 1 \\ 7 &\mapsto 8 \\ 8 &\mapsto 4 \end{aligned}$$

Takes up space

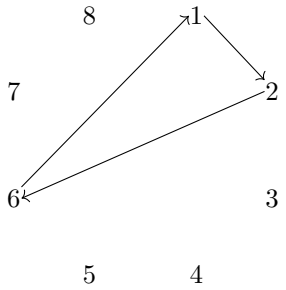


Hard to read

Then

$$\begin{aligned} \sigma &= (784) \circ (126) \circ (35) \\ &= (126)(784)(35) \\ &= (126)(35)(784) \quad \text{etc.} \end{aligned}$$

where we could identify (126) as a cycle in S_8 with its cycle notation. So (126) is the element of S_8 pictured as



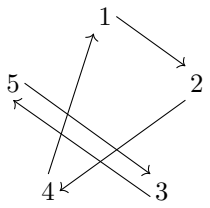
At the second equality, we drop the composition symbol "$\circ$" for brevity.

Definition 5.6. For $\sigma \in S_n$, a cycle notation for σ is an expression

$$\sigma = \sigma_1 \cdots \sigma_k$$

where each σ_i is a cycle and each pair σ_i, σ_j is disjoint when $i \neq j$.

Example 5.7. If $\sigma \in S_5$ is



then the following are cycle notations for σ:

$$\begin{array}{ll}(124)(35) & (35)(124)\\ (124)(53) & (53)(124)\\ (412)(35) & (35)(412)\\ (412)(53) & (53)(412)\\ (241)(35) & (35)(241)\\ (241)(53) & (53)(241)\end{array}$$

All these represent the same σ.

Example 5.8. Let

$$\sigma = (12)(34)$$
$$\tau = (123)$$

Then inverse of a cycle is just reading the cycle backward

$$\tau^{-1} = (321)$$
$$\sigma^{-1} = (21)(43) = \sigma$$

We could compute

$$\begin{aligned}\tau\sigma\tau^{-1} &= (123)\circ(12)(34)\circ(321)\\ &= (14)(23)\\ \sigma\tau\sigma^{-1} &= (12)(34)\circ(123)\circ(12)(34)\\ &= (3)(421)\\ &= (421)\end{aligned}$$

Note (blah)σ(blah)$^{-1}$ has the same cycle shape as σ. This will help us classify conjugacy classes of S_n.

5.4 Conjugacy Classes in S_n

Cycle notation gives us some nice consequences.

Proposition 5.3. (1) Let $\sigma \in S_n$ be a cycle, so

$$\sigma = (a_1 \cdots a_k)$$

where $a_{i+1} = \sigma(a_i)$. Then

$$\sigma^{-1} = (a_k \cdots a_1)$$

i.e., $\sigma^{-1} = (b_1 \cdots b_k)$ where $b_i = \sigma(b_{i+1})$ and $b_k = a_1$.

(2) More generally, if

$$\sigma = \sigma_1\sigma_2\cdots\sigma_k$$

where σ_i are disjoint cycles, then

$$\sigma^{-1} = \sigma_1^{-1}\cdots\sigma_k^{-1}$$

(3) Let $\sigma, \tau \in S_n$ and $a, b \in \underline{n}$. If $\sigma(a) = b$, then $\tau\sigma\tau^{-1}$ sends $\tau(a)$ to $\tau(b)$.

Proof. (1) Need to show that $\forall b \in \underline{n}$, we have

$$(a_k \cdots a_1)\circ(a_1 \cdots a_k) : b \mapsto b$$

and

$$(a_1 \cdots a_k)\circ(a_k \cdots a_1) : b \mapsto b$$

We will do the first composition, the second one is similar. Note

- $b \notin \{a_1, \ldots, a_k\} \Rightarrow b$ is fixed by σ
  $\Rightarrow b$ is fixed by $(a_k \cdots a_1)$
  $\Rightarrow (a_k \cdots a_1) \circ \sigma(b) = b$. ✓
- $b \in \{a_1, \ldots, a_k\} \Rightarrow b = a_i$ for some $i \in \{1, \ldots, k\}$
  $\Rightarrow \sigma(b) = a_{i+1}$ (definition of cycle notation)
  $\Rightarrow (a_k \cdots a_1)$ sends $\sigma(b)$ to b. ✓

(2) In general, if $g_1, \ldots, g_l \in G$,

$$(g_1 \cdots g_l)^{-1} = g_l^{-1} \cdots g_1^{-1}.$$

since

$$\begin{aligned}(g_1 \cdots g_l)(g_l^{-1} \cdots g_1^{-1}) &= g_1 \cdots g_{l-1} \underbrace{g_l g_l^{-1}}_{\text{cancel}} g_{l-1}^{-1} \cdots g_1^{-1} \\ &= g_1 \cdots \underbrace{g_{l-1} g_{l-1}^{-1}}_{\text{cancel}} \cdots g_1^{-1} \\ &\vdots \\ &= g_1 g_1^{-1} \\ &= 1_G.\end{aligned}$$

So

$$(\sigma_1 \cdots \sigma_l)^{-1} = \sigma_l^{-1} \cdots \sigma_1^{-1}$$

But disjoint cycles commute, so

$$\sigma_l^{-1} \cdots \sigma_1^{-1} = \sigma_1^{-1} \cdots \sigma_l^{-1}.$$

(3)

$$\begin{aligned}\tau\sigma\tau^{-1}(\tau(a)) &= \tau\sigma\tau^{-1} \circ \tau(a) \\ &= \tau\sigma(a) \\ &= \tau(b)\end{aligned}$$

□

Remark. Conjugation is like a change of basis. If $v_1, \ldots, v_k$ are a basis for $\mathbb{R}^k$, one has an invertible matrix T where i^{th} column is v_i. If a linear transformation A sends $\vec{a}$ to $\vec{b}$, then TAT^{-1} sends $T\vec{a}$ to $T\vec{b}$. So think of τ above as giving a "new basis" to $\underline{n}$.

Corollary 5.4. Let $\sigma, \sigma' \in S_n$. If $\sigma' = \tau\sigma\tau^{-1}$ for some $\tau \in S_n$, then we can write the cycle notation for σ' from the cycle notation for σ and from τ.

Proof. If σ is a cycle,

$$\sigma = (a_1 \cdots a_l)$$

then

$$\tau\sigma\tau^{-1} = (\tau(a_1) \cdots \tau(a_l)).$$

Proposition (3) tells us that $\tau(a_i)$ is sent to $\tau(a_{i+1})$ by $\tau\sigma\tau^{-1}$. It also tells us that $\sigma(a) = a \Rightarrow \tau\sigma\tau^{-1}$ fixes $\tau(a)$; So $\tau\sigma\tau^{-1}$ is another cycle whose non-trivial orbit is given by $\{\tau(a_i)\}$.

If σ is a product

$$\sigma = \sigma_1 \cdots \sigma_l$$

of disjoint cycles,

$$\tau\sigma\tau^{-1} = (\tau\sigma_1\tau^{-1})(\tau\sigma_2\tau^{-1}) \cdots (\tau\sigma_l\tau^{-1})$$

since conjugation by τ is a group homomorphism. So if

$$\sigma = (a_1 \cdots a_{k_1})(a_{k_1+1} \cdots a_{k_1+k_2}) \cdots (a_{k_1+\cdots+k_{l-1}+1} \cdots a_{k_1+\cdots+k_l})$$

is a cycle notation for σ, then

$$\tau\sigma\tau^{-1} = (\tau(a_1) \cdots \tau(a_{k_1}))(\tau(a_{k_1+1}) \cdots \tau(a_{k_1+k_2})) \cdots (\tau(a_{k_1+\cdots+k_{l-1}+1}) \cdots \tau(a_{k_1+\cdots+k_l}))$$

is a cycle notation for $\tau\sigma\tau^{-1}$. □

Let $\sigma \in S_n$.
Write σ as a product

$$\sigma = \sigma_1 \cdots \sigma_k$$

of disjoint cycles and consider

$$|\sigma_i|, \quad \forall i$$

(These are the sizes of the orbits associated to each σ_i.) In this way, we get some collection of numbers. It's most conveniently thought of as a n unordered collection, since we can reorder the σ_i.

Example 5.9. Let

$$\sigma = (123)(67)(459) \in S_9$$

Note we don't write (8), for sake of brevity. Then we have numbers

$$3, 2, 3$$

associated to σ.

Definition 5.7. We call the numbers $\{a_i\}$ the **cycle shape** of σ.

Example 5.10. Let

$$\sigma' = (345)(879)(26)$$

Then σ' has numbers $3, 3, 2$ associated to it.

Up to reordering, this is the same collection as for σ. We say σ and σ' have the **same cycle shape**.

Proposition 5.5. Two elements $\sigma, \sigma' \in S_n$ are conjugate (i.e. $\exists \tau$, s.t. $\sigma = \tau\sigma'\tau^{-1}$) if and only if they have the same cycle shape.

Proof. Let σ and σ' have the same cycle shape. We can then reorder any cycle notation for σ and σ', so

$$\begin{matrix} \sigma = \sigma_1 \circ \cdots \circ \sigma_k \\ \sigma' = \sigma'_1 \circ \cdots \circ \sigma'_k \end{matrix} \text{ which is product of disjoint cycles.}$$

where $|\sigma_i| = |\sigma'_i|$, $\forall i$.

Choose any i and number a that appears in the cycle notation for σ_i.

$$\sigma_i = (\cdots a \cdots).$$

In σ'_i, choose any number a',

$$\sigma'_i = (\cdots a' \cdots).$$

Define a bijection as follows:

$$\begin{aligned} \tau : a_i &\mapsto b_i \\ \sigma^j(a_i) &\mapsto (\sigma')^j(b_i) \end{aligned}$$

Then

$$\begin{aligned} \tau\sigma\tau^{-1}(b) &= \tau\sigma\tau^{-1}((\sigma')^j(b_i)) \\ &= \tau\sigma(\sigma^j(a_i)) \\ &= \tau(\sigma^{j+1}(a_i)) \\ &= (\sigma')^{j+1}(b_i) \\ &= \sigma'(b). \end{aligned}$$

i.e. $\tau\sigma\tau^{-1} = \sigma'$. The converse follows from the corollary. □

Example 5.11.

$$\begin{matrix} (123)(69) = \sigma \\ (45)(361) = \sigma' \end{matrix} \in S_9$$

have the same cycle shape. As do

$$\begin{matrix} \sigma = (12)(34)(567) \\ \sigma' = (78)(59)(142) \end{matrix} \in S_9$$

Remark. The cycle shape of σ just says: The action of σ breaks $\underline{n}$ into l many orbits; The "i^{th}" orbit has size k_i. If σ' also breaks $\underline{n}$ into l many orbits and we can match the sizes k_i' to those k_i of σ, then σ and σ' have the same cycle shape.

Example 5.12. How might you find τ?

$$\sigma = (123)(46)(785)$$
$$\sigma' = (157)(93)(684)$$

Well, if $\tau\sigma\tau^{-1} = \sigma'$, we know that a cycle

$$(b_1 \cdots b_k)$$

in the cycle notation for σ' equals

$$(\tau(a_1) \cdots \tau(a_k))$$

for some cycle $(a_1 \cdots a_k)$ of σ's cycle decomposition. This is NOT unique, but here's how you can find it: Pick a cycle and a number appearing in a cycle notation for it. For no reason, let's choose

$$4 \in (46)$$

Choose a cycle in σ''s cycle notation, with same length as (46). In this case, we're constrained to (93) (though in general, we may have many choices). Choose an element appearing in this cycle, say 9.

$$\begin{array}{c}(123)(46)(785)\\ \downarrow{\scriptstyle 3}\ \downarrow{\scriptstyle 1}\\ (157)(93)(684)\end{array}$$

So write

$$\tau = (\ 4\ 9 \quad \overset{1}{\nearrow}$$

then we see what cycle σ_i constrains 9. None in this case——9 is a fixed point of σ.

So choose any fixed point of σ'——here, our only choice is 2.

$$\tau = (\ 4\ 9\ 2 \quad \overset{1}{\nearrow}\ \overset{2}{\nearrow}$$

Now find a cycle σ_i that contains 2. In σ_i', find corresponding element. In this case, it's 5.

$$\tau = (\ 4\ 9\ 2\ 5 \quad \overset{3}{\nearrow}$$

So forth:

$$\begin{array}{c}(123)(46)(785)\\ \downarrow{\scriptstyle 7}\quad \downarrow{\scriptstyle 8}\ \downarrow{\scriptstyle 4}\\ (157)(93)(684)\end{array}$$

(5) After seeing (4925) is a cycle for τ, just choose any element not yet written. We choose 1 arbitrary.
(6) Likewise, we choose 3.

$$\tau = \begin{array}{c}\overset{4}{\downarrow}\overset{5}{\downarrow}\ \overset{6}{\downarrow}\\ (\ 4\ 9\ 2\ 5\ )(1)(\ 3\ 7\ 6\ )(8)\\ \quad\ \underset{7}{\searrow}\ \underset{8}{\nearrow}\end{array}$$

$$= (4925)(376)$$

Since we never write cycles of length 1.

5.5 Alternating Groups

Definition 5.8. The **alternating group** A_n is defined to be the kernel of the map

$$\begin{aligned} S_n \to GL_n(\mathbb{R}) &\xrightarrow{\det} \mathbb{R}^\times \\ \sigma &\mapsto B_\sigma \end{aligned}$$

s.t.

$$B_\sigma(e_i) = e_{\sigma(i)}$$

i.e. the collection of all σ such that B_σ has $\det 1$.

Proposition 5.6. A_n is the subgroup of S_n consisting of all even permutations, which are permutations that can be expressed as an even number of transpositions (swaps of two elements). Thus A_n has order $\frac{n!}{2}$.

Proposition 5.7. A_n is a normal subgroup of S_n.

There are three ways to prove it.
1. Kernel of the sign homomorphism

Proof. Define a map $\text{sgn} : S_n \to \{1, -1\}$, where

- $\text{sgn}(\sigma) = 1$ if σ is an even permutation.
- $\text{sgn}(\sigma) = -1$ if σ is an odd permutation.

This is a group homomorphism because

$$\text{sgn}(\sigma\tau) = \text{sgn}(\sigma) \cdot \text{sgn}(\tau).$$

We call it sign homomorphism.

The kernel of a homomorphism is the set of elements mapped to the identity element of the codomain. For sgn, the identity element is 1. Therefore, $\ker(\text{sgn}) = A_n$.

The kernel of a group homomorphism is always a normal subgroup of the domain group. Hence A_n is a normal subgroup of S_n. □

2. Conjugation preserves parity

Proof. For any $\sigma, \tau \in S_n$, conjugation preserves the cycle structure and the parity of permutations, if σ is even, the conjugation of σ by τ: $\tau\sigma\tau^{-1}$ is also even. A subgroup N of G is normal if it is invariant under conjugation by elements of G:

$$\tau N \tau^{-1} = N \quad \text{for all } \tau \in S_n$$

Since the conjugation of even permutations yields even permutations, A_n is normal in S_n. □

3. Index of A_n in S_n

Proof. Index of A_n in S_n:

$$[S_n : A_n] = \frac{|S_n|}{|A_n|} = \frac{n!}{n!/2} = 2.$$

Since any subgroup of index 2 in a group is normal, A_n is normal subgroup of S_n. □

Chapter 6

Free Groups

One way to define a group is to declare a collection of **generators** and a collection of **relations** that generators satisfy.
Question: What does a group with a set of generators, but with no relations look like? If the set of generators is S, this group is called the free group with generating set S.

Example 6.1. $\langle g \rangle = \text{image}(\mathbb{Z} \to G)$
$$n \mapsto g^n$$

We're about to generalize $\mathbb{Z}$, analogous statement for $\mathbb{Z}$:

$$\begin{array}{ccc} * & \xrightarrow{g} & G \\ & \Downarrow & \\ \mathbb{Z} & \longrightarrow & G \end{array}$$

For any map of sets
$$S \to G,$$
We'll produce a group homomorphism
$$F(S) \to G$$
where $F(S)$ is free group on the set S.

6.1 Words and Letters

Definition 6.1. Let X be a set. A **word in** X is a finite, ordered collection of elements in X. Given a word w, we call an element of w a **letter** of w.

Equivalently, a word is:

- an element of
$$X^n \qquad \text{for some } n \geqslant 0$$
- a sequence
$$X_1 X_2 \cdots X_{n-1} X_n$$
where each $X_i \in X$ and $n \geqslant 0$.

Remark. The empty word is a word with no letters.

We let $\text{Word}(X)$ denote the set of all words on X.

Example 6.2. If $X = \{a\}$
$$\text{Word}(X) = \{\varnothing, a, aa, aaa, \ldots\}$$
If $X = \{a, b\}$
$$\text{Word}(X) = \{\varnothing, a, b, ab, ba, aa, bb, \ldots\}$$
Gives two words in X, we can concatenate them to produce a new word:
$$\begin{aligned} \text{Word}(X) \times \text{Word}(X) &\to \text{Word}(X) \\ (w_1, w_2) &\mapsto w_1 w_2 \end{aligned}$$

Example 6.3.

$$(ba, ab) \mapsto baab$$
$$(ab, ba) \mapsto abba$$

This is clearly associative, and the empty word looks like an identity element. But no inverses! Let's fix that.

Given a set

$$S = \{a, b, c\}$$

let S' be the set of symbols

$$S' = \{a^{-1}, b^{-1}, c^{-1}, \ldots\}$$

(So S,S' are in bijection.)

We let

$$\begin{aligned}\overline{S} &= S \cup S' \\ &= \{a, a^{-1}, b, b^{-1}, \ldots\}\end{aligned}$$

Example 6.4. A word in $\overline{S}$ can look like

$$w = babb^{-1}a^{-1}c^{-1}ca.$$

6.2 Reduction of Words

Definition 6.2. A word in $\overline{S}$ is called **unreduced** if for some $a \in S$, the sequence

$$aa^{-1} \text{ or } a^{-1}a$$

appears in the word. A word is called **reduced** if it is not unreduced.

Example 6.5.

$$aaab^{-1}a^{-1}b \text{ is reduced}$$
$$\left.\begin{matrix} acbcb^{-1}bc^{-1} \\ acbcbb^{-1}c^{-1} \end{matrix}\right\} \text{both unreduced}$$

Definition 6.3. A word w' obtained from w by removing (also known as canceling) an appearance of aa^{-1} or $a^{-1}a$ is said to be obtained from w by cancellation. We'll write $w \rightsquigarrow w'$.

Example 6.6.

- The empty word is obtained from $b^{-1}b$ (and from bb^{-1}) by cancellation.
- ab is obtained from

$$\begin{matrix} abb^{-1}b \\ c^{-1}cab \\ acc^{-1}b \end{matrix} \qquad \text{can remove } a\underline{bb^{-1}}b \text{ or } ab\underline{b^{-1}b}$$

by cancellation.

Definition 6.4. A word w' is called a **reduction of** w if w' is obtained from w by cancellations,

$$w \rightsquigarrow \cdots \rightsquigarrow w'$$

and if w' is reduced.

Proposition 6.1. If w' and w'' are reductions of w, then

$$w' = w''.$$

Proof. Induction on length l of word w. (Note $w \rightsquigarrow u \Rightarrow \text{length}(u) < \text{lenght}(w)$).

$l = 0$: empty word is reduced.

$l = 1$: No a, a^{-1} can occur adjacently since there's one element in the word. So $l = 1$. $\Rightarrow$ Word is reduced.

Suppose we've shown every word of length $l - 1$ has unique reduction. Prove the same for l.

If w has length l and is reduced, done.

If not, $\exists aa^{-1}$ or $a^{-1}a$ somewhere. Potentially many of them!

As an example we could consider $a^{-1}aa^{-1}aa^{-1}a = w$, with length 6. Pick one of them.

$$\cdots \underline{a^{-1}a} \cdots$$

A reduction of w can be achieved by

(i) cancelling $\underline{a^{-1}a}$ at some stage.

(ii) never cancelling $\underline{a^{-1}a}$.

(ii) only happens if

$$\ldots \underline{a^{-1}a}a^{-1} \ldots \text{ appears at some stage, and we take} \tag{6.1}$$
$$\ldots \underbrace{\underline{a^{-1}a}a^{-1}}_{\text{cancel}} \ldots \rightsquigarrow \cdots \underline{a^{-1}} \cdots$$

$$\cdots \underline{aa^{-1}}a \cdots \text{ appears at some stage and we take} \tag{6.2}$$
$$\cdots \underbrace{a\underline{a^{-1}a}}_{\text{cancel}} \cdots \rightsquigarrow \cdots \underline{a} \cdots$$

In (6.1), cancelling $\underline{a^{-1}a}a^{-1}$ by $\underbrace{\underline{a^{-1}a}a^{-1}}$ or $\underline{a^{-1}}\underbrace{\underline{a}a^{-1}}$ produces the same word. Likewise for (6.2). So we can assume $\underline{a^{-1}a}$ is reduced at some point. (Any reduction achieved via (ii) can be achieved via (i).)

So we have a reduction

$$\begin{aligned} w &= \cdots \underline{aa^{-1}} \cdots \underbrace{b^{-1}b} \cdots c^{-1}c \\ &\wr \quad \text{Step one} \\ w_1 &= \cdots \underline{aa^{-1}} \cdots\cdots\cdots \underbrace{c^{-1}c} \\ &\wr \\ &\vdots \\ &\wr \quad \text{Step } n \\ w_n &\text{ reduced} \end{aligned}$$

Well, we get the same reduction if we cancel aa^{-1} in step 1, or in other step. □

6.3 Definition of Free Groups

Definition 6.5. Let S be a set. Then the **free group** $F(S)$ on S is

$$(F(S), m)$$

where

- $F(S)$ is the set of reduced words in $\overline{S} = S \cup S'$, where $S' := \{w^{-1} \mid w \in S\}$.
- $m : F(S) \times F(S) \to F(S)$ sends (w_1, w_2) to the reduction of $w_1 w_2$.

Example 6.7. Consider a set with one element $S = \{a\}$. A word in $\overline{S}$ looks like

$$aaaa^{-1}aa^{-1}aaa^{-1}a$$

If a word is reduced, it looks like

$$\underbrace{aaaaa\cdots a}_{n \text{ times}}$$

or

$$\underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{n \text{ times}}$$

So

$$\mathbb{Z} \to F(S)$$
$$n \mapsto \begin{cases} \underbrace{a\cdots a}_{n \text{ times}} & n > 0 \\ \underbrace{a^{-1}\cdots a^{-1}}_{n \text{ times}} & n < 0 \\ \varnothing & n = 0 \end{cases}$$

is a bijection. It is an isomorphism.

Example 6.8. Consider a set with two elements $S = \{a, b\}$. $F(S)$ is free group on two generators. The elements look like

$l = 0$ $\quad \varnothing =: 1$
$l = 1$ $\quad a, b, a^{-1}, b^{-1}$
$l = 2$ $\quad aa, bb, ba, ab, a^{-1}a^{-1}, b^{-1}b^{-1}, a^{-1}b^{-1}, b^{-1}a^{-1}$

Proposition 6.2. The inverse to $S_1 \cdots S_n$ is $S_n^{-1} \cdots S_1^{-1}$.

Proof. The inverse to $S_1 \cdots S_n$ is $S_n^{-1} \cdots S_1^{-1}$, since

$$\begin{array}{c} (S_1 \cdots S_n)(S_n^{-1} \cdots S_1^{-1}) \\ \wr \\ S_1 \cdots S_{n-1} S_{n-1}^{-1} \cdots S_1^{-1} \\ \wr \\ S_1 \cdots S_{n-2} S_{n-2}^{-1} \cdots S_1^{-1} \\ \wr \\ \vdots \\ \wr \\ S_1 S_1^{-1} \\ \wr \\ \varnothing \end{array}$$

□

6.4 Equivalence Relations

Definition 6.6. Let X be a set. An **equivalence relation** on X is a subset

$$R \subset X \times X$$

satisfying:

(1) $(x, x) \in R$, $\forall x \in X$.

(2) $(x, y) \in R \Rightarrow (y, x) \in R$.

(3) $(x, y) \in R$ and $(y, z) \in R \Rightarrow (x, z) \in R$.

We will say $x \sim y$ if $(x, y) \in R$.

Example 6.9. Let G act on a set X. Say $x \sim y \Leftrightarrow y = gx$ for some $g \in G$. This is an equivalence relation, since

(1) $x = 1_G x$, so $x \sim x$.

(2) $x \sim y \Rightarrow y = gx \Rightarrow x = g^{-1}y \Rightarrow y \sim x$ for some g.

(3) $y \sim z \Rightarrow z = g'z \Rightarrow z = g'gy \Rightarrow z \sim x$.

Then $\forall x$, $\mathcal{O}_x$ is just the equivalence class of x. (i.e. $\mathcal{O}_x = \{y \mid y \sim x\}$.) And X/G is the set of equivalence class.

Here is another example.

Example 6.10. Let S be a set and set

$$S' = \{x^{-1}\}_{x \in S}$$
$$\overline{S} = S \cup S'$$

6.5 Existence of Unique Reduction

Theorem 6.3. Every $w \in \text{Word}(\overline{S})$ has a unique reduction.

Proof. Induction on length l.

$l = 0$ obvious.

$l = 1$ obvious.

Assume that $\forall w'$ with length $\leqslant l - 1$, the set

$$\{\text{reduction of } w'\}$$

has only one element. We must prove this is true $\forall$ words w of length l.

- If w is already reduced, then no other word can be obtained from w by cancelling. Hence

$$\{\text{reduction of } w\} \text{ has only one element——}w \text{ itself.}$$

- Otherwise, $\exists$ an appearence of

$$aa^{-1} \quad \text{or} \quad a^{-1}a$$

somewhere in w.

Let's fix a single such appearence,

$$w = \cdots \underline{aa^{-1}} \cdots$$

which we've underlined.

Let's consider:

$$\left\{\begin{array}{l}\text{reductions of } w\\ \text{obtained by cancelling}\\ \underline{aa^{-1}} \text{ at the first step}\end{array}\right\} \overset{①}{=\!=} \left\{\begin{array}{l}\text{reductions of } w\\ \text{obtained by cancelling}\\ \underline{aa^{-1}} \text{ at the some step}\end{array}\right\}$$

$$② \;\vdots \quad \updownarrow \text{ Every reduction of } w \text{ is one of these sets!}$$

$$\left\{\begin{array}{l}\text{reductions of } w\\ \text{obtained by never}\\ \text{cancelling } \underline{aa^{-1}} \text{ itself}\end{array}\right\}$$

① is an equality, since if $\underline{aa^{-1}}$ is cancelled in step N, you'd get same reduction by first having cancelled $\underline{aa^{-1}}$, then performing step 1 through $N - 1$.

② is either an equality or the set is empty, since NOT cancelling $\underline{aa^{-1}}$ means you had to cancel like $\cancel{a^{-1}}\underline{aa^{-1}}$ or like $\underline{aa^{-1}}\cancel{a}$ at some stage.

$$\text{But} \quad \cdots \cancel{a^{-1}}\underline{aa^{-1}} \cdots = \cdots a^{-1}\cancel{aa^{-1}} \cdots$$
$$\text{And} \quad \cdots \cancel{aa^{-1}}a \cdots = \cdots \cancel{aa^{-1}}a \cdots$$

① and ② tell us that every reduction of w can be obtained by first cancelling $\underline{aa^{-1}}$. But

$$w' = \cdots \underline{aa^{-1}} \cdots$$

is a word of length $< l$!

Moreover, any reduction of w obtained by first cancelling $\underline{aa^{-1}}$ is a reduction of w'.

Hence

$$\left\{\begin{matrix}\text{reduction of } w \text{ obtained} \\ \text{by first cancelling } \underline{aa^{-1}}\end{matrix}\right\} = \{\text{reduction of } w'\} = \text{a set with one element.}$$

□

Example 6.11. If $S = \varnothing$, Word(S) is a set with one element——the empty word, i.e. the word of length zero.

Example 6.12. If $S = \varnothing$, Free$(S) = \{$reduced words in $\overline{S} = \varnothing\}$ =the set containing the empty word. So Free(S) is a group with one element when $S = \varnothing$!

6.6 Application of Free Groups

Proposition 6.4. Given a group G. Let $j : S \to G$ be a map of sets. It extends to a group homomorphism $F(S) \to G$.

Proof. Let $s \in S$ be an element of the set, and $j(s) \in G$ its image in G. Let us denote by $\bar{j} : \overline{S} \to G$ the function sending $s \mapsto j(s)$ and $s^{-1} \mapsto j(s)^{-1}$. We then define a function

$$\phi_j : \text{Word}(\overline{S}) \to G$$

by sending any word $W = s_1 \dots s_l$, with $s_i \in \overline{S}$, to the element

$$\phi_j(s_1) \cdot \phi_j(s_2) \cdot \dots \cdot \phi_j(s_l)$$

We must prove this is well-defined on $F(S)$, and a homomorphism. Well, if w is a reduction of W, it is obtained by canceling pairs of letters appearing next to their inverses. On the other hand, if any letter s appears next to its inverse s^{-1} inside W, the above string of multiplications in G will also see an appearance of $\phi_j(s)$ appearing next to $\phi_j\left(s^{-1}\right) = \phi_j(s)^{-1}$. Hence if we cancel two inverse letters in the word W to obtain a new word w', we see that $\phi_j(W) = \phi_j(w')$. More explicitly, given a product of many elements in G, omitting an appearance of $\phi_j(s)\phi_j(s)^{-1}$ (or of $\phi_j(s)^{-1}\phi_j(s)$) does not change the value of the multiplication:

$$\begin{aligned}\phi_j(s_1) \cdot \dots \cdot \phi_j(s)\phi_j(s)^{-1} \cdot \dots \cdot \phi_j(s_l) &= \phi_j(s_1) \cdot \dots \cdot 1_G \cdot \dots \cdot \phi_j(s_l) \\ &= \phi_j(s_1) \cdot \dots \cdot \phi_j(s_l)\end{aligned}$$

(and likewise for canceling the appearance of $\phi_j(s)^{-1}\phi_j(s)$). So if the words w'_i for $i = 1, \dots, I$ are the words one passes through on reducing W to its reduction w, we have a string of equalities:

$$\phi_j(W) = \phi_j(w'_1) = \dots = \phi_j(w'_I) = \phi_j(w).$$

This shows that ϕ_j is well-defined on $F(S)$. To show that ϕ_j defines a homomorphism, let $W = w' \cdot w''$ be a concatenation of words, and let w be its reduction. We must prove that

$$\phi_j(w) = \phi_j(w') \cdot \phi_j(w'').$$

By well-definedness, it suffices to show $\phi_j(W) = \phi_j(w') \cdot \phi_j(w'')$. This is obvious, since if

$$w' = s'_1 \cdots s'_{l'}, \quad w'' = s''_1 \cdots s''_{l''}$$

then

$$\begin{aligned}\phi_j(W) &= \phi_j(s'_1) \cdot \dots \cdot \phi_j(s'_{l'}) \cdot \phi_j(s''_1) \cdot \dots \cdot \phi_j(s''_{l''}) \\ &= (\phi_j(s'_1) \cdot \dots \cdot \phi_j(s'_{l'})) \cdot (\phi_j(s''_1) \cdot \dots \cdot \phi_j(s''_{l''})) \\ &= \phi_j(w') \cdot \phi_j(w'')\end{aligned}$$

□

Proposition 6.5. There is a bijection of sets

$$\{\text{Group homomorphisms } F(S) \to G\} \cong \{\text{Set maps } S \to G\}.$$

Proof. We above define a homomorphism $\phi_j : F(S) \to G$ for any function $j : S \to G$. This defines a function

$$\Phi : \{\text{Set maps } S \to G\} \to \{\text{Group homomorphisms } F(S) \to G\}$$

given by $j \mapsto \phi_j$. We define an inverse map Ψ as follows: If ϕ is a group homomorphism, it assigns a value to the reduced word s, for any $s \in S$. So we define $\Psi(\phi) := \psi_\phi$ to be the function sending s to $\phi(s)$. We must show that $\Psi \circ \Phi$ and $\Phi \circ \Psi$ are the identities. Well, given a homomorphism $\phi : F(S) \to G$, let w be the word

$$w = s_1 \dots s_l$$

where the s_i are whatever letters of $\overline{S}$ are in w. we know that

$$\phi(w) = \phi(s_1 \cdot \dots \cdot s_l) = \phi(s_1) \cdot \dots \cdot \phi(s_l)$$

by the group homomorphism property, and the fact that every word is a product of one-letter words. So the value of ϕ on one-letters words——i.e., its value on S——determines its value on all elements of $F(S)$. This shows that $\Phi \circ \Psi$ is the identity. On the other hand, we have defined Φ so that $\Phi(j) = \phi_j$ simply sends one-letter words to the value $j(s)$. Hence $\Psi \circ \Phi$ is also the identity. □

Example 6.13. Let S be a set and G a group. For all functions

$$S \to G$$

$\exists$ a group homomorphism

$$F(S) \to G$$

When $S = \varnothing$, $\exists!$ function

$$\phi \to G$$

What group homomorphism is

$$F(\phi) \to G?$$

It sends the empty word to 1_G.

Proposition 6.6. If w_1 and w_2 have the same reduction, then $w_1 \sim w_2$ is an equivalence relation.

Proof. $w_1 \sim w_2$ is an equivalence relation, since

(1) $w \sim w$ obviously: reduction(w) = reduction(w).

(2) $w_1 \sim w_2 \Rightarrow w_2 \sim w_1$
obviously, since

$$\begin{aligned} &\text{reduction}(w_1) = \text{reduction}(w_2) \\ \Rightarrow &\text{reduction}(w_2) = \text{reduction}(w_1). \end{aligned}$$

(3) $w_1 \sim w_2$, $w_2 \sim w_3 \Rightarrow w_1 \sim w_3$
since

$$\begin{aligned} &\text{reduction}(w_1) = \text{reduction}(w_2) \\ &\text{reduction}(w_2) = \text{reduction}(w_3) \end{aligned} \Rightarrow \text{reduction}(w_1) = \text{reduction}(w_3)$$

(All follows from uniqueness of reduction and the fact that equality is an equivalence relation.) □

Remark. So if $w_1 \rightsquigarrow w_2$ via cancellation, then $w_1 \sim w_2$. (Not necessary conversely.)

Proposition 6.7. Let $F(S)$ be reduced words in $\overline{S}$. $\exists$ bijection

$$F(S) \to \{\text{equivalence classes of words in Word}(\overline{S})\}.$$

Proof. Send $w \mapsto [w]$, i.e. send w to its equivalence class.
Any equivalence class has a unique element of shortest length——the (common) reduction of any $w' \in [w]$.
This defines inverse map. □

Proposition 6.8. The operation

$$\begin{aligned} \{\text{equiv class of words}\} \times \{\text{equiv class of words}\} &\xrightarrow{\text{concatenate}} \{\text{equiv class of words}\} \\ ([w_1], [w_2]) &\longmapsto [w_1 w_2] \end{aligned}$$

is well-defined.

Proof. Let r_1 and r_2 be reduction of w_1', w_2' respectively. Then note

$$r_1 r_2 \text{ can be obtained from } w_1' w_2' \text{ via cancellations.}$$

(Just apply cancellations to the w_1' part of the word, then to the w_2' part of the word.)

Hence for any

$$w_1' \in [w_1], w_2' \in [w_2],$$

we have

$$w_1' w_2' \sim r_1 r_2$$

i.e.

$$[w_1' w_2'] = [r_1 r_2]$$

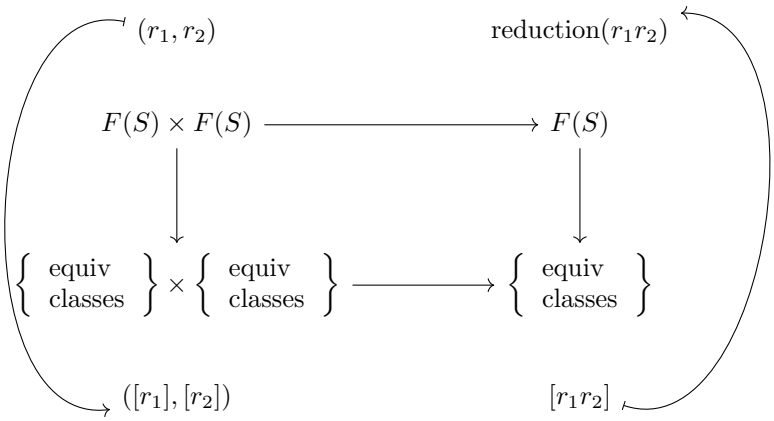
So regardless of which representatives $w_1' \in [w_1]$, $w_2' \in [w_2]$ we choose, the equivalence class of $w_1' w_2'$ is unchanged. □

Corollary 6.9. The free group operation

$$\begin{aligned} F(S) \times F(S) &\to F(S) \\ (r_1, r_2) &\mapsto \text{reduction}(r_1 r_2) \end{aligned}$$

is associative.

Proof.



So we just need to show the operation $([r_1], [r_2]) \mapsto [r_1 r_2]$ is associative. Well,

$$([r_1][r_2])[r_3] = [r_1 r_2][r_3] = [(r_1 r_2) r_3] = [r_1 (r_2 r_3)] = [r_1][r_2 r_3] = [r_1]([r_2][r_3])$$

where the third equality comes from the associativity of concatenating ordinary words. □

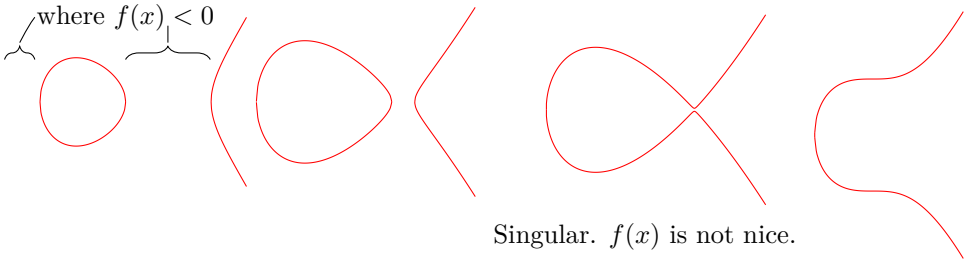
Chapter 7

Elliptic Curves

Definition 7.1. Let $f(x)$ be a nice cubic polynomial in x. The elliptic curve defined by f is the set

$$\mathbb{E} := \{\mathscr{O}\} \cup \{(x, y) \mid y^2 = f(x)\}.$$

Example 7.1. The solutions to $y^2 = f(x)$ look like



Singular. $f(x)$ is not nice.

Note $(x, y) \in \mathbb{E} \Rightarrow (x, -y) \in \mathbb{E}$.

Theorem 7.1. Every elliptic curve is an abelian group.

This is quite surprising. Let me define for you the group operation

$$\mathbb{E} \times \mathbb{E} \to \mathbb{E}$$
$$(P, Q) \mapsto P + Q$$

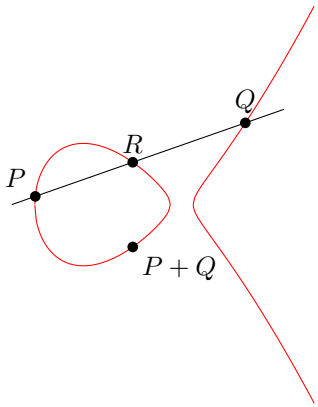
(1) If $P, Q = \mathscr{O}$, then we set

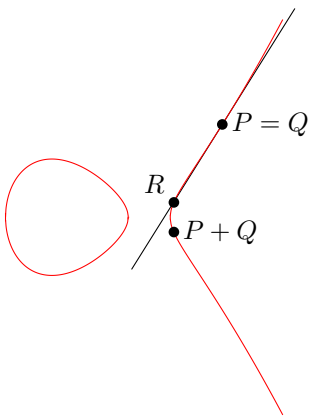
$$\mathscr{O} + \mathscr{O} = \mathscr{O}.$$

(2) If $P = \mathscr{O}$, $Q = (x, y) \in \mathbb{E}$, we set

$$\mathscr{O} + Q = Q + \mathscr{O} = \mathscr{O}$$

(3) If P, Q are on $\{(x, y) \mid y^2 = f(x)\}$: Consider the (unique!) line L_{PQ} containing P and Q.

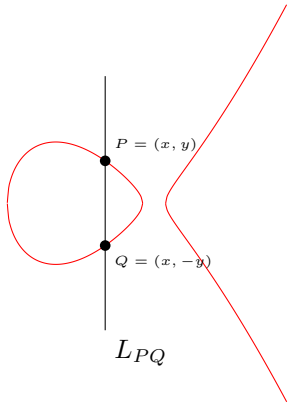




A line L intersects a cubic in three points. Let $R = (x, y)$ be the third. Then we define $P + Q := (x, -y)$. If $P = Q$, we take tangent to P.

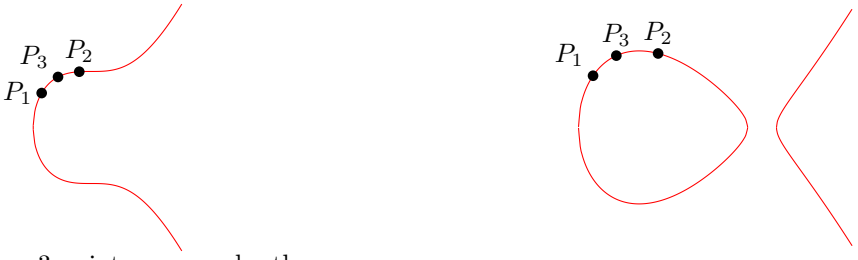
Rules: If L_{PQ} is vertical, so it doesn't intersect a third point in $\mathbb{R}^2$, we declare the third point R to be the "point at ∞" $\mathscr{O}$.

(This isn't really a rule, but rather an interpretation using projective geometry, where parallel lines——like vertical lines——intersect at a point at ∞.)



Note $L_{PQ} = L_{QP}$, so $P + Q = Q + P$.

Hard to prove $\mathbb{E} \times \mathbb{E} \to \mathbb{E}$ is associative.



I'd recommand choosing 3 points near each other.

Proposition 7.2. $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$.

Awesome observation: Assume $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ has $a_i \in \mathbb{Q}$. Suppose $P, Q \in \mathbb{E}$ are rational points (meaning their x- and y-coordinates are rational numbers). Then $P + Q$ is also a rational point!

Proof. L_{PQ} is given by

$$y = mx + t$$

$P, Q \in \mathbb{Q}^2 \Rightarrow m, t \in \mathbb{Q}$. $L_{PQ} \cap \mathbb{E} \ni R$ satisfies equation

$$(mx + t)^2 = a_3x^3 + a_2x^2 + a_1x + a_0$$

$\Rightarrow P, Q, R$ are roots to some cubic $g(x)$ with rational coefficients.
$\Rightarrow$

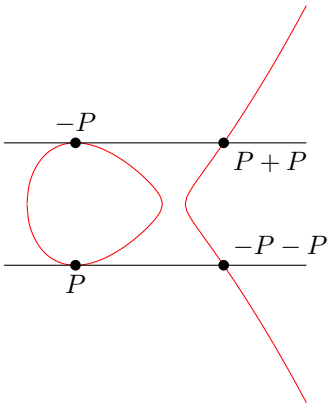
$$(x - x_1)(x - x_2)(x - x_3) = g(x) = b_3x^3 + b_2x^2 + b_1x + b_0$$

But $x_1, x_2 \in \mathbb{Q} \Rightarrow x_3 \in \mathbb{Q}$, since $x_1x_2x_3$ is constant term of $g(x)$! (Better: Since $x_1 + x_2 + x_3 = b_2$ and $x_1, x_2, b_2 \in \mathbb{Q}$.) □

Definition 7.2. If f is a rational cubic (i.e. $a_i \in \mathbb{Q}$), let $\mathbb{E}(\mathbb{Q}) \subset \mathbb{E}$ denote the set

$$(\mathbb{E} \cap (\mathbb{Q} \times \mathbb{Q})) \cup \{\mathscr{O}\}$$

(i.e., the set of all P such that the coordinates of P are rational numbers, along with the point at ∞.)



So we have a subset

$$\mathbb{E}(\mathbb{Q}) \subset \mathbb{E}$$

It's closed under $+$.

It's closed under inverses, since

$$P = (x, y) \in \mathbb{Q} \times \mathbb{Q}$$

$\Rightarrow$

$$-P = (x, -y) \in \mathbb{Q} \times \mathbb{Q}$$

And $\mathbb{E}(\mathbb{Q}) \ni \mathscr{O}$ =identity by definition. So we see

Proposition 7.3. $\mathbb{E}(\mathbb{Q}) \subset \mathbb{E}$ is a subgroup.

Definition 7.3. G is called finitely generated if exists a finite set S and a surjective homomorphism

$$F(S) \to G.$$

Parsing this definition: Let $S = \{s_1, \ldots, S_n\}$ be the finite set and

$$\phi : F(S) \to G$$

the onto homomorphism.

ϕ sends each s_i to some element

$$g_i = \phi(s_i)$$

That ϕ is onto means that $\forall g \in G$, $\exists$ a word w, s.t.

$$\phi(w) = g$$

i.e. g can be written as a finite product of g_i and g_i^{-1}.

So the down-to-earth meaning is that $\exists$ some finite collection

$$g_1, \ldots, g_n \in G$$

s.t. any element of G can be expressed as a product of g_i and their inverses.

Example 7.2. Any finite group G is finitely generated. Take

$$S = G$$

and map

$$\begin{aligned} F(S) &\to G \\ g &\mapsto g. \end{aligned}$$

Example 7.3. Any cyclic group is finitely generated. If

$$G = \langle g \rangle,$$

set $S = \{g\}$,

$$\begin{aligned} F(S) &\to G \\ g &\mapsto g. \end{aligned}$$

Example 7.4. Any finite product of finitely generated groups is again finitely generated

$$G = G_1 \times \cdots \times G_n.$$

Taking generating sets S_i for G_i and define $S = S_1 \cup \cdots \cup S_n$. If $\phi_i : F(S_i) \to G_i$ is a surjection $\forall i$, let

$$\begin{aligned} \phi : F(S) &\to G \\ a_i &\mapsto (1, \ldots, 1, \phi_i(a_i), 1, \ldots, 1) \end{aligned}$$

One of the most important theorem about elliptic curve is

Theorem 7.4 (Mordell's Theorem)**.** $\mathbb{E}(\mathbb{Q})$ is finitely generated.

Crazy surprising——there is some finite collection of rational points $P_1, \ldots, P_n \in \mathbb{E}(\mathbb{Q})$ such that any other rational points can be obtained by adding+subtracting the P_i from each other.

Chapter 8

The Fundamental Group

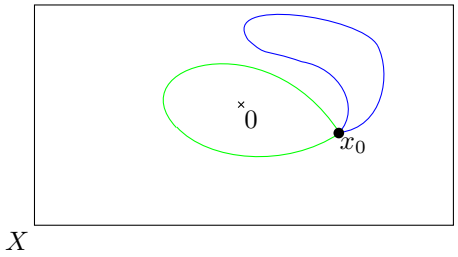
Definition 8.1. Let $X \subset \mathbb{R}^n$ be a subset and fix $x_0 \in X$. A **loop** in X base at x_0 is a continuous function

$$[0,1] \xrightarrow{\gamma} \mathbb{R}^n$$

such that

- $\gamma(t) \in X$, $\forall t \in [0,1]$.
- $\gamma(0) = \gamma(1) = x_0$.

Example 8.1. $X = \mathbb{R}^n \setminus \{0\}$, $x_0 = (1,0)$.



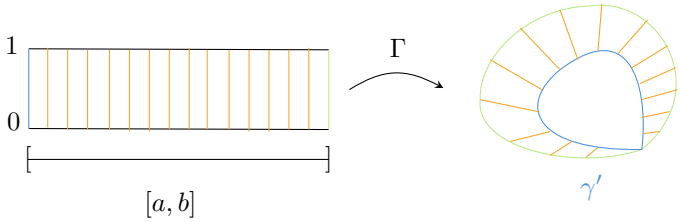
Definition 8.2. Given two curves γ_1 and γ_2, we say γ_1 and γ_2 are **homotopic** if γ_1 can be wiggled into γ_2 without changing $\gamma(0)$ and $\gamma(1)$. i.e., if $\exists$ continuous map

$$\begin{aligned} \Gamma : [0,1] \times [a,b] &\to X \\ (t,s) &\mapsto \Gamma(t,s) \end{aligned}$$

such that

- $\Gamma(t,a) = \gamma_1(t)$.
- $\Gamma(t,b) = \gamma_2(t)$.
- $\Gamma(0,s) = \Gamma(1,s) = x_0$, $\forall s$.

where $[a,b]$ is some interval.



You can think Γ as some "movie" of paths lasting $b-a$ seconds.

Lemma 8.1. Say $\gamma_1 \sim \gamma_2$ if and only if γ_1 is homotopic to γ_2. This is an equivalence relation.

Roughly,

- Any path can be wiggled to itself by the boring wiggle. (No wiggling at all!)
- If γ_1 wiggles to γ_2, the reverse wiggle will wiggle γ_2 to γ_1.
- If γ_1 wiggles to γ_2 and γ_2 wiggles to γ_3, just perform the two wiggles to exhibit a single wiggle from γ_1 to γ_3.

Definition 8.3. Let

$$\pi_1(X, x_0) = \{\text{loop at } x_0\}/\sim .$$

This is called the **fundamental group** of X with base point x_0.

Remark. If X is connected, then $\pi_1(X, x_0) \cong \pi_1(X, x_0')$ for any two basepoints.

Composition is as follows:

$$\begin{aligned} \pi_1(X, x_0) \times \pi_1(X, x_0) &\to \pi_1(X, x_0) \\ ([\gamma_b], [\gamma_a]) &\mapsto [\gamma_b][\gamma_a]. \end{aligned}$$

Given two paths γ_a and γ_b, consider the path

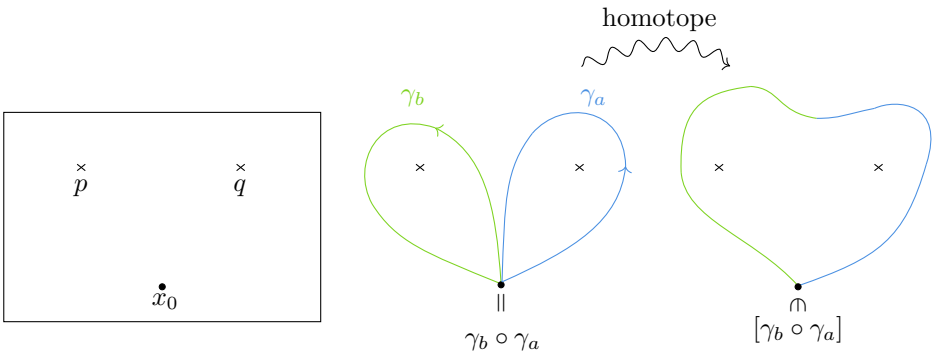
$$\begin{aligned} \widetilde{\gamma_b \circ \gamma_a} : [0,2] &\to X \\ t &\mapsto \begin{cases} \gamma_a(t) & \text{if } t \in [0,1] \\ \gamma_b(t-1) & \text{if } t \in [1,2] \end{cases} \end{aligned}$$

Rescale $[0, 2]$ to $[0, 1]$ to obtain a path

$$\begin{aligned} \gamma_b \circ \gamma_a : [0,1] &\to X \\ t &\mapsto \begin{cases} \gamma_a(2t) & \text{if } t \in \left[0, \frac{1}{2}\right] \\ \gamma_b(2t-1) & \text{if } t \in \left[\frac{1}{2}, 1\right] \end{cases} \end{aligned}$$

We let $[\gamma_b][\gamma_a] = [\gamma_b \circ \gamma_a]$.

Example 8.2. Consider $X = \mathbb{R}^2 \setminus \{p, q\}$, x_0 anywhere.



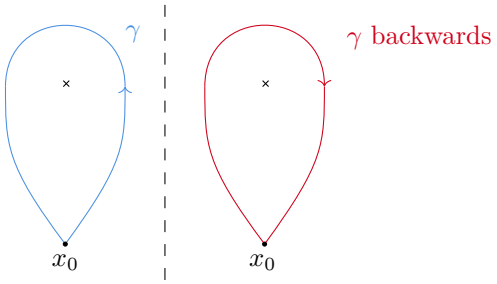
The two diagrams on the right hand side are both representatives of $[\gamma_b \circ \gamma_a]$.

Remark.

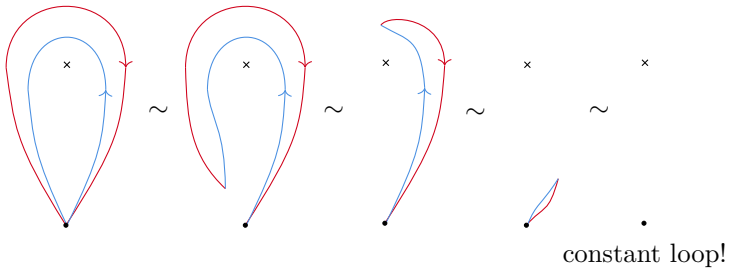
- The constant loop $\gamma(t) = x_0$, $\forall t$ is the identity.

  If γ is a loop and γ_0 is the constant loop, $\gamma_0 \circ \gamma$ is the loop called "Do γ quickly, then do nothing for $\frac{1}{2}$ a second." Well, let Γ be the homotopy that shrinks this "doing nothing" time from $\frac{1}{2}$ to 0 seconds.

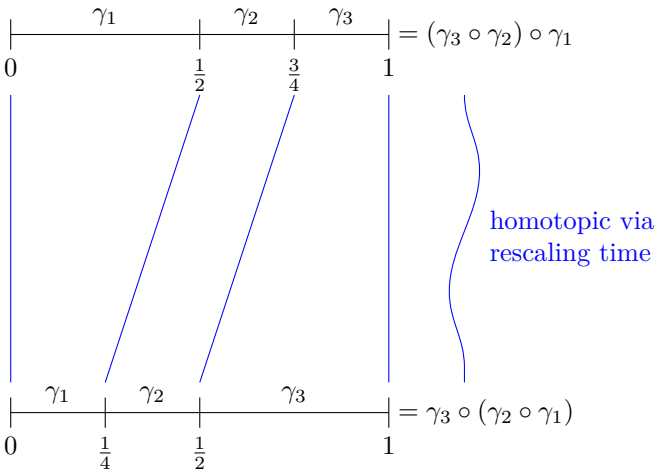
- The inverse of γ is the loop called "do γ backwards."



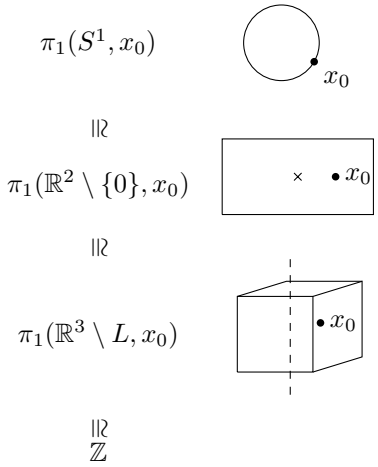
["γ backwards"$\circ\gamma$]=?



- Finally, composition is associative.

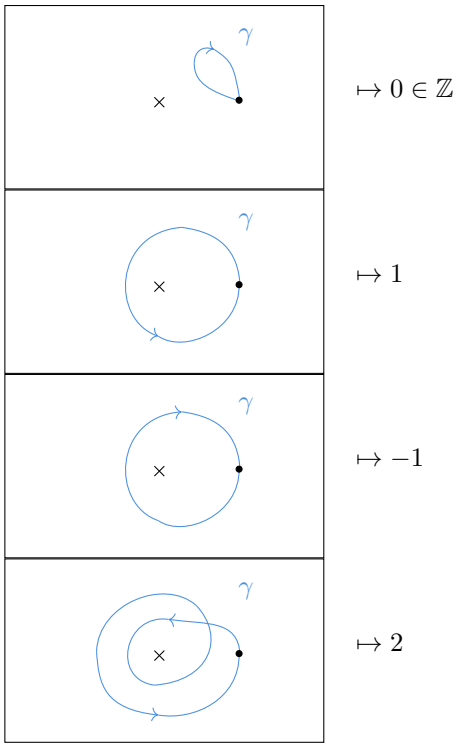


Example 8.3. Note that L represents a line.



I am not proving this isomorphism for you——but roughly, you send a path γ to its "winding number".

Question: "How many time does γ wind around the puncture?"

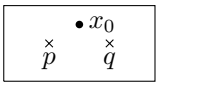


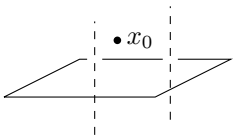
Example 8.4. If γ is differentiable, you can define this as

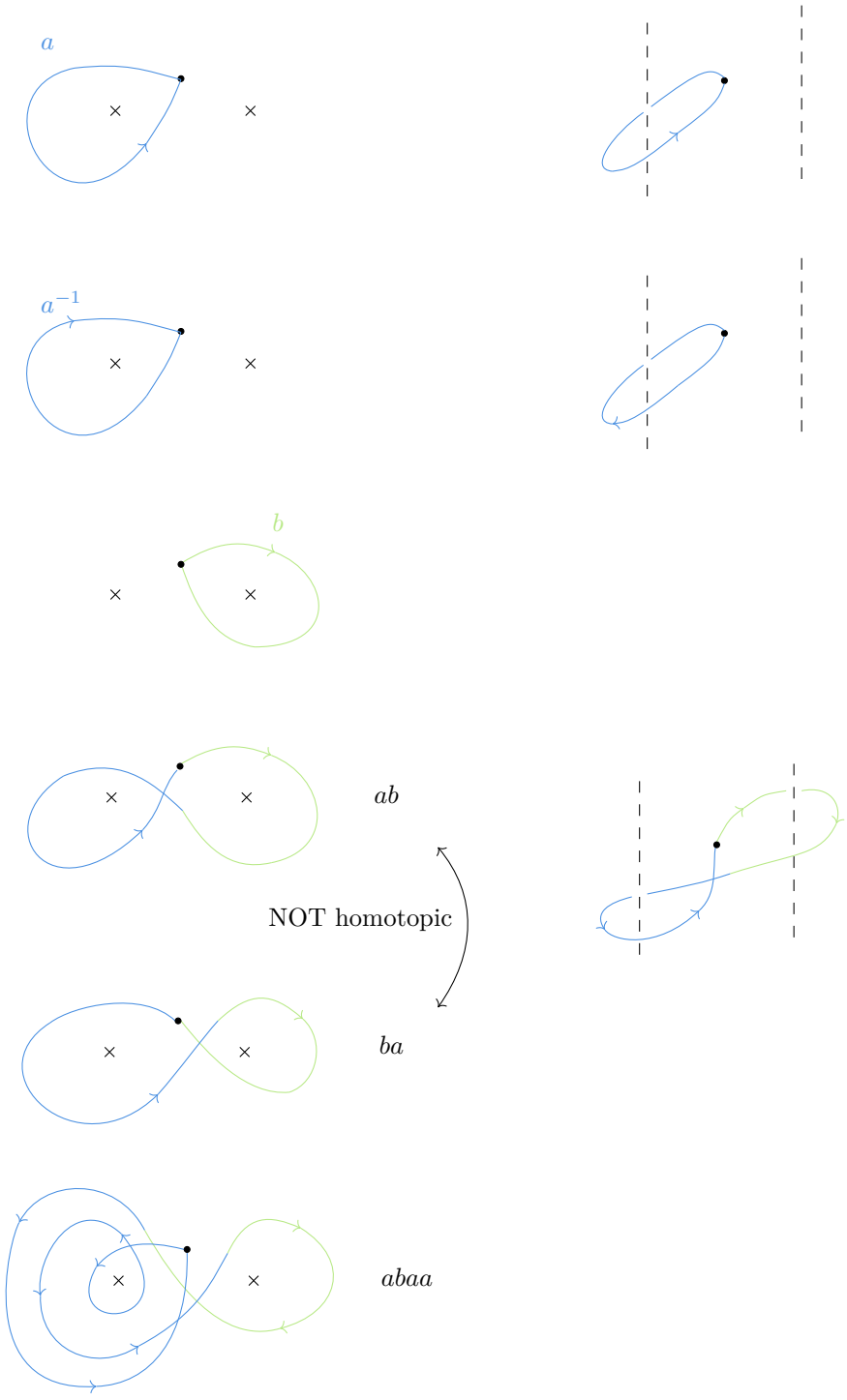
$$\frac{1}{2\pi \mathrm{i}} \int_\gamma \frac{\mathrm{d}z}{z}.$$

Example 8.5.

$$\pi_1(\infty, x_0)$$
$$\wr$$
$$\pi_1(\mathbb{R}^2 \setminus \{p, q\}, x_0)$$
$$\wr$$
$$\pi_1(\mathbb{R}^3 \setminus (L \circ L'), x_0)$$
$$\wr$$
Free groups on two generators






a
a^{-1}
b
ab
NOT homotopic
ba
abaa

Chapter 9

Quotient Groups

9.1 Quotient Groups

Let $H \subset G$ be a subgroup.
Question: When can the orbit set

$$G/H$$

be given a group structure?

Remark. Hg is the orbit of g with respect to the action of H on G. So

$$Hg = \mathcal{O}_g$$

So the question: is there a natural group operation of set of coset of H?
A candidate

$$\begin{aligned} G/H \times G/H &\to G/H \\ (Hg_1, Hg_2) &\mapsto Hg_1g_2 \end{aligned}$$

Is this map well-defined?
No, in general. But it is well-defined in special cases!

Theorem 9.1. If $H \subset G$ is normal, the operation

$$\begin{aligned} G/H \times G/H &\to G/H \\ (Hg_1, Hg_2) &\mapsto Hg_1g_2 \end{aligned}$$

is well-defined and makes G/H into a group.

Proof. To show the operation is well-defined, we need to show: If $Hg_1 = Hg_1'$ and $Hg_2 = Hg_2'$ for some $g_1, g_1', g_2, g_2' \in G$, then

$$Hg_1g_2 = Hg_1'g_2'.$$

Well,

$$Hg_1'g_2' = \{hg_1'g_2' \mid h \in H\}$$

That

$$\begin{aligned} Hg_1 = Hg_1' &\Rightarrow \mathcal{O}_{g_1} = \mathcal{O}_{g_1'} \\ &\Rightarrow g_1, g_1' \text{ are in same orbit} \\ &\Rightarrow g_1' = h_1g_1, \text{for some } h_1 \in H. \end{aligned}$$

Likewise,

$$Hg_2 = Hg_2' \Rightarrow g_2' = h_2g_2, \text{for some } h_2 \in H.$$

So

$$\begin{aligned} Hg_1'g_2' &= \{h \cdot h_1g_1 \cdot h_2g_2 \mid h \in H\} \\ &= \{h \cdot h_1g_1 \cdot h_2g_1^{-1}g_1g_2 \mid h \in H\} \\ &= \{h \cdot h_1h_3g_1g_2 \mid h \in H\} \subset Hg_1g_2 \end{aligned}$$

Since H is normal, we use $h_3 := g_1h_2g_1^{-1} \in H$.

Since Hg_1g_2, $Hg_1'g_2'$ are orbits/equivalence classes,

$$Hg_1g_2 \supset Hg_1'g_2'$$

Hence,

$$Hg_1g_2 = Hg_1'g_2'$$

Done with "well-defined".

Why is it a group?

(1) Associative

$$\begin{aligned}(Hg_1 \cdot Hg_2) \cdot Hg_3 &= Hg_1g_2 \cdot Hg_3 \\ &= H(g_1g_2)g_3 \\ &= Hg_1(g_2g_3) \\ &= Hg_1 \cdot Hg_2g_3 \\ &= Hg_1 \cdot (Hg_2 \cdot Hg_3).\end{aligned}$$

(2) Identity

$$H1_G \cdot Hg = Hg = Hg \cdot H1_G.$$

(3) Inverse

$$\begin{aligned}Hg \cdot Hg^{-1} &= Hgg^{-1} \\ &= H1_G \\ &= Hg^{-1}g \\ &= Hg^{-1} \cdot Hg.\end{aligned}$$

□

Let's see some examples.

Example 9.1. $H = \{\mathrm{id}_G\} \subset G$.

H is normal, since $\forall g \in G$,

$$\begin{aligned}gHg^{-1} &= \{ghg^{-1} \mid h \in H\} \\ &= \{g\mathrm{id}_G g^{-1}\} \\ &= \{\mathrm{id}_G\} \\ &= H\end{aligned}$$

But G/H isn't a special new group, because $\exists$ an isomorphism

$$\begin{aligned}G/H &\to G \\ Hg &\mapsto g\end{aligned}$$

Example 9.2. Let $H = n\mathbb{Z} = \{\text{multiples of } n\} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$. Then $Ha = \{a' \in \mathbb{Z}, \text{s.t. } a' = kn + a, \text{for some } k \in \mathbb{Z}\} = \mathcal{O}_a$.

Proposition 9.2. $\exists$ bijection $\mathbb{Z}/n\mathbb{Z} \to \{0, 1, \ldots, n-1\}$, $\forall n \geqslant 1$.

Proof. Given $\mathcal{O}_a \in \mathbb{Z}/n\mathbb{Z}$, let r_a be the unique number, s.t.

$$a = kn + r_a, k \in \mathbb{Z}, r_a \in \{0, 1, \ldots, n-1\}$$

i.e. the reminder of $a \div k$. (From elementary school.)

So let the bijection be

$$\begin{aligned}\mathbb{Z}/n\mathbb{Z} &\to \{0, 1, \ldots, n-1\} \\ \mathcal{O}_a &\mapsto r_a\end{aligned}$$

- Well-defined?
  If $\mathcal{O}_a = \mathcal{O}_{a'}$,
  $$a' = a + k'n \qquad \text{(by definition of orbit)}$$
  So
  $$\begin{aligned} a' &= k'n + kn + r_a \\ &= (k' + k)n + r_a \end{aligned}$$
  Hence
  $$r_{a'} = r_a$$
  where the unique number in $\{0, 1, \ldots, n-1\}$ such that $a' = kn + r_{a'}$. Therefore, well-defined!
- Injection?
  Given $\mathcal{O}_a$, $\mathcal{O}_b$,
  $$r_a = r_b$$
  $\Rightarrow$
  $$\begin{aligned} a &= kn + r_a \\ b &= ln + r_b \\ &= ln + r_a \end{aligned}$$
  $\Rightarrow$
  $$a - b = (k - l)n$$
  $\Rightarrow$
  $$a \in \mathcal{O}_b$$
  $\Rightarrow$
  $$\mathcal{O}_a = \mathcal{O}_b$$
- Surjection?
  $$\begin{aligned} \mathcal{O}_0 &\mapsto 0 \\ \mathcal{O}_1 &\mapsto 1 \\ \mathcal{O}_2 &\mapsto 2 \\ &\vdots \\ \mathcal{O}_{n-1} &\mapsto n-1 \end{aligned}$$

□

By this theorem, this means
$$\mathbb{Z}/n\mathbb{Z}$$
is a group of order
$$n = |\{0, 1, \ldots, n-1\}|$$
What's the group structure?

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ \text{bijection} \big(\downarrow & & \\ (\mathcal{O}_a, \mathcal{O}_b) & \longmapsto & \mathcal{O}_{a+b} \\ \downarrow & & \downarrow \\ (r_a, r_b) & \longmapsto & r_{a+b} \end{array}$$

$$\{0, \ldots, n-1\} \times \{0, \ldots, n-1\} \longrightarrow \{0, \ldots, n-1\}$$

i.e. the group structure is: Add numbers, then find the remainder when dividing by n.

Definition 9.1. Let $a, b \in \mathbb{Z}$. We write

$$a \equiv b \pmod{n}$$

or

$$a = b \pmod{n}$$

if

$$a - b = kn \quad \text{for some } k \in \mathbb{Z}$$

Equivalently, $a \equiv b \pmod{n} \Leftrightarrow \mathcal{O}_a = \mathcal{O}_b$.

When we write

$$a \pmod{n}$$

We mean the equivalence class

$$\mathcal{O}_a = Ha \in G/H$$

Remark. You might find it annoying to keep track of giant equivalence classes $\mathcal{O}_a$, $\mathcal{O}_b$, etc, in your head all the time. So instead, it may help to think of $\mathcal{O}_a$ simply as a number, namely, the remainder r you get when dividing a by n:

$$a = kn + r$$

This is justified by the bijection

$$\mathbb{Z}/n\mathbb{Z} \cong \{0, \dots, n-1\}$$

So when you see "$a \pmod{n}$", you can just think of the number r. Likewise, the group operations is just "clock arithmetic":

$$(a, b) \mapsto a + b \pmod{n}$$

which you can think as the remainder in $(a + b) \div n$.

9.2 Subgroups Descend to Quotient Groups

Let G be an arbitrary group and $H \triangleleft G$.

Proposition 9.3. There is a bijection between the set of subgroups G containing H and the set of subgroups in G/H.

Proof. Let $p : G \to G/H$ be the group homomorphism given by sending $g \mapsto [g]$.

Given a subgroup $K \subset G$, note the composition of group homomorphisms

$$K \hookrightarrow G \to G/H.$$

Since the image of any group homomorphism is a subgroup, this shows that $p(K)$ is a subgroup of G/H. So we have a function $\{\text{subgroups of } G\} \to \{\text{subgroups of } G/H\}$ given by sending $K \mapsto p(K)$.

We show it is a surjection: Given $K' \subset G/H$, consider the preimage $p^{-1}(K') \subset G$. This is a subgroup of G since if $p(x), p(y) \in K'$, then $p(xy) = p(x)p(y) \in K'$ (because K' is closed under multiplication).

Now it suffices to show that $p^{-1}(p(K)) = K$ for all subgroups $K \subset G$. Obviously, $K \subset p^{-1}(p(K))$. To show the other inclusion, let $x \in p^{-1}(p(K))$. We know by definition of $p(K)$ that there is some $y \in K$ for which $p(x) = p(y)$. Then $p(xy^{-1}) = 1_{G/H}$, so $xy^{-1} \in H$. Since K contains H, $xy^{-1} \in K$, hence $x \in K$. □

Proposition 9.4. There is a bijection between the set of normal subgroups in G containing H and the set of normal subgroups in G/H.

Proof. We show that if K is normal, then $p(K)$ is normal. (This proves we have a function $\{\text{normal subgroups of } G\} \to \{\text{normal subgroups of } G/H\}$.)

Well, if $[k] \in p(K)$, then $[g][k][g]^{-1} = [gkg^{-1}] = [k']$ for some $k' \in K$ since K is normal in G. So $p(K) \subset G/H$ is normal. (Note we are using the fact that $G \to G/H$ is a surjection here——otherwise, we wouldn't know that every element of G/H is in the image of $p(G)$.)

Surjectivity: We show that if $p(K)$ is normal, then $K = p^{-1}(p(K))$ is normal. If $k \in K$ and $g \in G$, we have that $[gkg^{-1}] = [g][k][g^{-1}] = [k']$ for some $[k'] \in p(K)$——i.e., for some $k' \in K$. So $gkg^{-1} \in p^{-1}(p(K)) = K$.

We know that this assignment is an injection. □

9.3 Commutative Diagram

Definition 9.2. Suppose we have groups K, G, H, X with maps of groups

$$\begin{array}{ccc} K & \xrightarrow{\phi} & G \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\psi} \\ H & \xrightarrow{\beta} & X \end{array}$$

We say this diagram commutes if $\psi \circ \phi = \beta \circ \alpha : K \to X$.

Remark. 1 will denote the trivial group. This group is well-defined up to isomorphism!

Now look at the diagram

$$\begin{array}{ccc} K & \xrightarrow{\phi} & G \\ {\scriptstyle !}\downarrow & & \downarrow{\scriptstyle\psi} \\ 1 & \xrightarrow{!} & X \end{array}$$

What does it mean for this diagram to commute? This holds if and only if $\psi \circ \phi$ yields the trivial map that kills everything (sends everything to the identity). Why? Because the morphisms in the left and bottom are the trivial map that kills everything in K and the map that embeds the maps are uniquely defined (assuming they are group homomorphisms), which is denote by the !. So $\psi \circ \phi$ is the constant map at $1_X \in X$.

Alternatively, we have $\text{im}(\phi) \subset \ker(\psi)$. This is close to what we had for exactness.

Example 9.3. $K = G = X = 1$.

Example 9.4. $K = SL_n(\mathbb{R})$, $G = GL_n(\mathbb{R})$, $X = \mathbb{R}^\times$, ϕ is the inclusion and $\psi = \det$.

Example 9.5. Let $K \subset G$ be a normal subgroup, so ϕ is the embedding. Let $X = G/K$ (This is a group since K is normal in G), and ψ is the canonical quotient projection.

9.4 Universal Property of Quotient Groups

Theorem 9.5. Given a commutative diagram

$$\begin{array}{ccc} K & \xrightarrow{\text{normal}} & G \\ \downarrow & & \downarrow{\scriptstyle\psi} \\ 1 & \longrightarrow & X \end{array}$$

There exists a unique homomorphism $\tilde{\psi} : G/X \to X$ such that the diagram

$$\begin{array}{ccc} G & \xrightarrow{\psi} & X \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\tilde{\psi}} \\ G/K & \xrightarrow{\text{id}} & G/K \end{array}$$

commutes.

Alternatively, if $\psi : G \to X$ is such that $K \subset \ker(\psi)$ for a $K \subset G$ a normal subgroup, then there exists a unique map $\tilde{\psi} : G/K \to X$ such that $\psi = \tilde{\psi} \circ \pi$, if $\pi : G \to G/K$ is the canonical map onto the quotient. This is called the **universal property of the quotient group**.

Proof. We want to define this map $\tilde{\psi} : G/K \to X$. Define it by taking a coset $Kg \mapsto \psi(g)$, or alternatively, taking the preimage of any coset in G/K back to G via the canonical map π. We need to show that this is well-defined.

Say that $Kg = Kg'$, or equivalently $g = k \cdot g'$. Does $\psi(g) = \psi(g')$? Well

$$\psi(g) = \psi(k \cdot g') = \psi(k) \cdot \psi(g') = \psi(g'),$$

So everything works! We now need to check that $\tilde{\psi}$ is unique and that $\psi = \tilde{\psi} \circ \pi$. But we have

$$\psi(g) = \tilde{\psi}(Kg) = \tilde{\psi}(\pi(g)),$$

so we just need to show uniqueness. But let's take another such map $\gamma : G/K \to X$, so we have

$$\psi(g) = \gamma(\pi(g)) = \gamma(Kg),$$

so that γ and $\tilde{\psi}$ must agree on all cosets K, then we are done. □

Remark. Uniqueness follows from the constraint of the commutativity of the diagrams in the statement of the theorem.

9.5 Generalizations of Quotient Group

The idea of a universal property allows us to generalize the notion of a quotient group.

Let $G \overset{\chi}{\twoheadrightarrow} H$ be any surjective homomorphism (We will denote this with the two-head arrow now). Then H is a "quotient group" of G, i.e. a diagram

$$\begin{array}{ccc} K & \longrightarrow & G \\ \downarrow & & \downarrow{\scriptstyle \chi} \\ 1 & \longrightarrow & H \end{array}$$

with the analogous universal property. To answer this, what is K? Let's just make it the kernel of χ, so that:

Theorem 9.6. Given $G \overset{\chi}{\twoheadrightarrow} H$, and let $K = \ker(\chi)$. Then the diagram

$$\begin{array}{ccc} K & \xrightarrow{i} & G \\ \downarrow & & \downarrow{\scriptstyle \chi} \\ 1 & \longrightarrow & H \end{array}$$

such that $i : K \to G$ is inclusion, has the same universal property, i.e. given any map $\psi : G \to X$ whose kernel contains K, we have a unique map $\tilde{\psi} : H \to X$ such that

$$\psi = \tilde{\psi} \circ \chi.$$

Proof. How do we define $\tilde{\psi} : H \to X$. Well since χ is surjective, for any $h \in H$, we have $h = \chi(g)$, though g may not be unique! Well, now define

$$\tilde{\psi} := \psi(g).$$

We need to check this is a well-defined homomorphism. So let's say $\chi(g) = \chi(g')$. Then $\chi(g) = \chi(g')$ implies that $\chi(g \cdot (g')^{-1}) = 1_H$ so that $g \cdot (g')^{-1} \in K$, so that $g = g' \cdot k$ for some $k \in K$. The same arguments now just follow from the proof of the previous theorem. □

Corollary 9.7. Suppose $\chi : G \to H$ is surjective and $K = \ker(\chi)$. Then $H \cong G/K$.

Remark. This is so-called the first isomorphism theorem. Let's give the proof with universal properties. We will see it in next chapter again.

Proof. Theorem 9.5 gives a map $G/K \to H$ and theorem 9.6 gives a map $H \to G/K$. Composing these maps gives us a map $G/K \to H \to G/K$, such that the proper commutativity constraints are met. This map is give by composition of the two maps we get from the two theorems, but the identity map $G/K \to H$ also satisfies that constraint. Since the maps were uniquely defined, we must have that the composition is the identity. Symmetrically, we obtain another map $H \to G/K \to H$ that is given by composing in the other direction, but again, $H \to H$ given by the identity also gives another map that meets the sufficient commutativity conditions, so the composition of those maps in the other order is the identity on H. So we have two maps $G/K \to H$ and $H \to G/K$ whose compositions in both orders are the respective identity maps, so that G/K and H are in bijection, but these maps were group homomorphisms, so they are actually isomorphic as groups! □

Remark. This notion of the universal property allows us to distinguish certain objects up to isomorphism uniquely, as we did in the proof of corollary, since the universal property is a statement of existence and uniqueness. If you are wondering, two objects "in a category" are isomorphic if and only if they have the same universal property. In our example, two groups (the quotient group and any group surjected on by G) satisfied the same universal property in this "category of groups", so they were isomorphic![1]

[1] This is a consequence of something very important in category theory called the Yoneda lemma.

Proposition 9.8. Let K, G be any groups and let $\phi : K \to G$ be any group homomorphism. Then there exists another group homomorphism $\psi : G \to H$ such that we have a universal property

$$\begin{array}{ccc} K & \xrightarrow{\phi} & G \\ {\scriptstyle\epsilon}\downarrow & & \downarrow{\scriptstyle\psi} \\ 1 & \longrightarrow & H \end{array}$$

where $\epsilon : K \to 1$ is the trivial homomorphism mapping every element of K to the identity element of the trivial group 1 and the bottom arrow $1 \to H$ is the unique homomorphism from the trivial group to H.

Proof. 1. Constructing H and ψ: Define H as the quotient group

$$H = G/\phi(K)$$

where $\phi(K)$ is the image of K under ϕ, which is a subgroup of G. $G/\phi(K)$ consists of the cosets $g\phi(K)$ for all $g \in G$.

Define $\psi : G \to H$ as the natural projection map

$$\psi(g) = g\phi(K)$$

where ψ sends each element g to its cosets in H and ψ is a surjective homomorphism.

2. Verifying diagram commutativity: We need to show that

$$\psi \circ \phi = \epsilon$$

Compute $\psi(\phi(k))$ for any $k \in K$:

$$\psi(\phi(k)) = \phi(k)\phi(K) = \phi(K)$$

Since $\phi(k) \in \phi(K)$, the coset $\phi(k)\phi(K)$ equals $\phi(K)$, which is the identity element in H. Therefore, $\psi(\phi(k))$ maps every element of K to the identity in H. This matches the composition via ϵ:

$$(\text{Unique map from 1 to } H) \circ \epsilon(k) = 1_H$$

Thus, the diagram commutes.

3. The construction satisfies the following universal property: For any group L and any homomorphism $f : G \to L$ such that $f \circ \phi = \epsilon$, there exists a unique homomorphism $\overline{f} : H \to L$ such that

$$f = \overline{f} \circ \psi.$$

Since (1) $f \circ \phi = \epsilon$, for all $k \in K$:

$$f(\phi(k)) = 1_L$$

This means $\phi(k) \in \ker(f)$ for all $k \in K$. Therefore $\phi(K) \subset \ker(f)$.

(2) Define $\overline{f} : H \to L$ by

$$\overline{f}(g\phi(K)) = f(g)$$

It is well-defined because if $g\phi(K) = g'\phi(K)$, then $g^{-1}g' \in \phi(K)$, so $f(g^{-1}g') = 1_L$, implying $f(g) = f(g')$. Thus, $\overline{f}$ if a well-defined homomorphism.

(3) Uniqueness: If there exists another homomorphism $\overline{f}'$ such that $f = \overline{f}' \circ \psi$, then for all $g \in G$:

$$\overline{f}(g\phi(K)) = f(g) = \overline{f}'(g\phi(K)).$$

Therefore, $\overline{f} = \overline{f}'$. □

Chapter 10

Isomorphism Theorems

10.1 The First Isomorphism Theorem

10.1.1 The Quotient Map as a Group Homomorphism

Proposition 10.1. Let $H \subset G$ be normal. The map

$$\begin{aligned} q : G &\to G/H \\ g &\mapsto Hg \end{aligned}$$

(1) is a group homomorphism.

(2) is a surjection.

(3) has kernel q.

Proof.

(1)
$$\begin{aligned} q(g_1 g_2) &= Hg_1g_2 \\ &= Hg_1Hg_2 \\ &= q(g_1)q(g_2) \end{aligned}$$

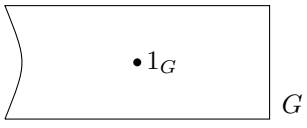
(2) $\forall Hg \in G/H$,
$$Hg = q(g)$$

(3) $q(g) = 1_{G/H} \Leftrightarrow q(g) = H1_G$
$$= H$$
But $Hg = H1_G \Leftrightarrow g$ and 1_G are in same orbit
$$\Leftrightarrow g = h1_G \text{ for some } h \in H$$
$$\Leftrightarrow g \in H$$
So $q(g) = 1_{G/H} \Leftrightarrow g \in H$.

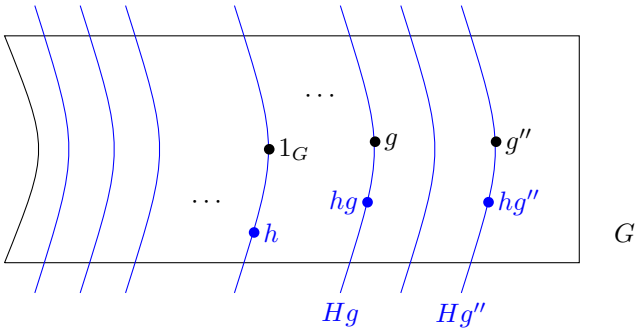
□

10.1.2 Visualization

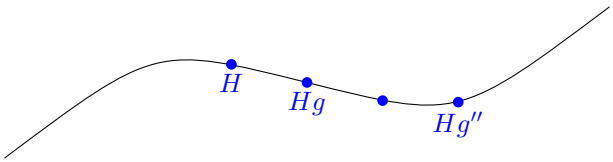
What's the picture?
Image G as some set



A subgroup $H \subset G$ breaks G up into orbits



And G/H collapse all these orbits:



10.1.3 Injectivity and Kernels of Homomorphisms

By the way,

Proposition 10.2. Let $G \xrightarrow{\phi} G'$ be a group homomorphism. Then ϕ is injective if and only if

$$\ker(\phi) = \{1_G\}.$$

Proof. Injective $\Rightarrow \exists! g$ (if any), s.t. $\phi(g) = 1_{G'}$.
Since a group homomorphism always sends 1_G to $1_{G'}$, $g \in 1_G$.
Assume $\ker(\phi) = \{1_G\}$. Then $\phi(g_1) = \phi(g_2) \Rightarrow \phi(g_1)\phi(g_2)^{-1} = 1_{G'}$

$$\begin{aligned} &\Rightarrow \phi(g_1 g_2^{-1}) = 1_{G'} \\ &\Rightarrow g_1 g_2^{-1} \in \ker(\phi) \\ &\Rightarrow g_1 g_2^{-1} = 1_G \\ &\Rightarrow g_1 = g_2 \end{aligned}$$

□

So given any normal H, the quotient homomorphism q exhibit, H as the kernel of same group homomorphism.

10.1.4 Kernels are Normal Subgroups

Question: Is every kernel of a group homomorphism normal?

Proposition 10.3. Let $\phi : G \to G'$ be a group homomorphism. Then $\ker(\phi)$ is normal.

Proof. Need to show: $\forall h \in \ker(\phi)$, $\forall g \in G$, $ghg^{-1} \in \ker(\phi)$.
Well,

$$\begin{aligned} \phi(ghg^{-1}) &= \phi(g)\phi(h)\phi(g^{-1}) \\ &= \phi(g)1_{G'}\phi(g^{-1}) \\ &= \phi(g)\phi(g^{-1}) \\ &= \phi(gg^{-1}) \\ &= \phi(1_G) \\ &= 1_{G'} \end{aligned}$$

So $ghg^{-1} \in \ker(\phi)$. □

Here we only proved that

$$g\ker(\phi)g^{-1} \subset \ker(\phi), \quad \forall g$$

when trying to show $\ker(\phi)$ is normal. But how do we show

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

10.1.5 Equality of Conjugates Implies Normality

Proposition 10.4. Let $H \subset G$ be a subgroup. "$\forall g \in G$, $gHg^{-1} \subset H$" implies "$\forall g \in G$, $gHg^{-1} = H$".

Proof. We need to show that $\forall g \in G$, $H \subset gHg^{-1}$.

So fix $h \in H$. Let $g' = g^{-1}$. By hypothesis,

$$g'H(g')^{-1} \subset H,$$

so

$$g'h(g')^{-1} = h'$$

for some $h' \in H$. Then

$$h = gh'h^{-1}$$

Since

$$\begin{aligned} gh'g^{-1} &= g(g'h(g')^{-1})g^{-1} \\ &= gg^{-1}hgg^{-1} \\ &= h \end{aligned}$$

This shows $h \in gHg^{-1}$. □

10.1.6 Intersection of Normal Subgroups

Corollary 10.5. If H_1, H_2 are normal subgroup of G, so is $H_1 \cap H_2$.

Proof. Let $h \in H_1 \cap H_2$. Then $\forall g \in G$,

- $ghg^{-1} \in H_1$ since H_1 is normal.
- $ghg^{-1} \in H_2$ since H_2 is normal.

Hence $ghg^{-1} \in H_1 \cap H_2$.
$\Rightarrow \forall g \in G$, $gH_1 \cap H_2g^{-1} \subset H_1 \cap H_2$. □

Note that

Proposition 10.6. If H_1, H_2 are just subgroup of G, then $H_1 \cap H_2$ is also a subgroup of G.

Proof. $1_G \in H_1$ and H_2 since both are subgroups.

Hence

$$1_G \in H_1 \cap H_2.$$

If g and g' are in $H_1 \cap H_2$, then

- $gg' \in H_1$ since H_1 is a subgroup
- $gg' \in H_2$ since H_2 is a subgroup

Hence

$$gg' \in H_1 \cap H_2.$$

Likewise for inverses. □

10.1.7 Constructing the Smallest Normal Subgroups Containing a Set

Now let's say you're given a group G, and some arbitrary collection

$$I$$

of elements in G. (I isn't a subgroup or anything necessarily; It's just some random list of elements of G.)

Question: Can you find a normal subgroup of G containing I?

Well, G itself is a normal subgroup of G. And it certainly contains I.

Question: Can we get something smaller?

Yes. Consider the intersection

$$\bigcap H$$

The set $\{H \subset G \mid H \text{ is normal and } H \text{ contains } I\}$ is NOT empty since G is in it. So we get some normal subgroup of G via this intersection (by corollary). Nice construction.

10.1.8 The First Isomorphism Theorem

Proposition 10.7. Let $\phi : G \to G'$ be a surjective group homomorphism. Then $\exists$ an isomorphism $G/\ker(\phi) \xrightarrow{\cong} G'$.

Proof. Given a surjective group homomorphism

$$\phi : G \to G',$$

Let $H = \ker(\phi)$. Note that if $g_2 \in Hg_1$,

$$\phi(g_2) = g_1$$

Because

$$\begin{aligned}\phi(g_2) &= \phi(hg_1), \quad \text{for some } h \in H \\ &= \phi(h)\phi(g_1) \\ &= 1_{G'}\phi(g_1) \\ &= \phi(g_1)\end{aligned}$$

So we have a well-defined map

$$\begin{aligned}\psi : G/H &\to G' \\ Hg &\mapsto \phi(g)\end{aligned}$$

(We showed if $Hg_1 = Hg_2$, then $\phi(g_1) = \phi(g_2)$.) This is a homomorphism, since

$$\begin{aligned}\psi(Hg_1Hg_2) &= \psi(Hg_1g_2) && \text{in } G/H \\ &= \phi(g_1g_2) && \text{Definition of } \psi \\ &= \phi(g_1)\phi(g_2) && \phi \text{ is a homomorphism} \\ &= \psi(Hg_1)\psi(Hg_2) && \text{Definition of } \psi\end{aligned}$$

It is an injection, since

$$\begin{aligned}\psi(Hg_1) = 1_{G'} &\Leftrightarrow \psi(g_1) = 1_{G'} \\ &\Leftrightarrow g_1 \in H \\ &\Leftrightarrow Hg_1 = H1_G, \text{the unit of } G/H\end{aligned}$$

It is a surjection since ϕ is a surjection:

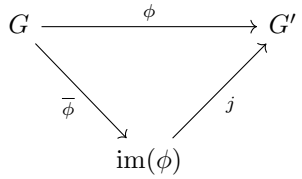
$$\forall g' \in G', \exists \text{ some } g \in G, \text{s.t. } \phi(g) = g', \text{so } \psi(Hg) = g.$$

□

Corollary 10.8 (The First Isomorphism Theorem)**.** Let $\phi : G \to G'$ be any group homomorphism. Then $\exists$ group isomorphism

$$G/\ker(\phi) \cong \text{im}(\phi).$$

Proof. $\text{im}(\phi) \subset G'$ is a subgroup. By the definition of image, the homomorphism $\phi : G \to G'$ factors as follows:



Here, j is the inclusion of $\text{im}(\phi)$ into G. (It's a injective group homomorphism.) $\overline{\phi}$ is the "same" function as ϕ, but has a different target/codomain. So we see $\phi = j \circ \overline{\phi}$.

Also, by definition of image, $\overline{\phi}$ is a surjection. Hence, the proposition says

$$G/\ker(\overline{\phi}) \cong \text{im}(\phi)$$

But $\ker(\overline{\phi}) = \ker(\phi)$, since $j(1_{\text{im}(\phi)}) = 1_{G'}$. □

10.1.9 Application of the First Isomorphism Theorem: Index

Proposition 10.9. Let

$$O_n(\mathbb{R}) := \{n \times n \text{ real matrices } A \text{ such that } A^{\mathrm{T}}A = I\}$$

and

$$SO_n(\mathbb{R}) := \{A \in O_n(\mathbb{R}) \text{ s.t. } \det(A) = 1\}.$$

Then

$$[O_n(\mathbb{R}) : SO_n(\mathbb{R})] = 2.$$

i.e. $SO_n(\mathbb{R})$ is an index 2 subgroup of $O_n(\mathbb{R})$.

Proof. Consider the homomorphism

$$\begin{aligned} \det : O_n(\mathbb{R}) &\to \mathbb{R}^\times \\ A &\mapsto \det(A) \end{aligned}$$

Since the unit of $\mathbb{R}^\times$ is $1 \in \mathbb{R}^\times$, the kernel of det is $SO_n(\mathbb{R})$.

On the other hand,

$$\mathrm{im}(\det) = \{+1, -1\} \subset \mathbb{R}^\times.$$

Since

$$\begin{aligned} [O_n(\mathbb{R}) : SO_n(\mathbb{R})] &= |O_n(\mathbb{R})/SO_n(\mathbb{R})| && \text{by definition of index} \\ &= |O_n(\mathbb{R})/\ker(\det)| \\ &= |\mathrm{im}(\det)| && \text{The First Isomorphism Theorem} \\ &= |\{+1, -1\}| \\ &= 2 \end{aligned}$$

□

10.2 The Second Isomorphism Theorem

10.2.1 The Second Isomorphism Theorem

Fix a group G. Let $S \subset G$ be a subgroup and $N \triangleleft G$ be a normal subgroup.

Proposition 10.10. Let SN be the set of all elements in G of the form sx where $s \in S$ and $x \in N$. This is a subgroup of G.

Proof. Given $s_1, s_2 \in S$ and $x_1, x_2 \in N$, we have that

$$s_1x_1s_2x_2 = s_1s_2s_2^{-1}x_1s_2x_2 = s_1s_2x'x_2$$

for some $x' \in N$ (since N is normal). And $s_1s_2 \in S$ and $x'x_2 \in N$ since both are closed under multiplication. The identity is in SN since $1 \in S$, N and $1 \cdot 1 = 1$. Finally, SN contains inverses because

$$x^{-1}s^{-1} = (s^{-1}x's)s^{-1} = s^{-1}x'$$

where $x' \in N$ is the element such that $x' = sx^{-1}s^{-1}$. □

Proposition 10.11. N is a normal subgroup of SN.

Proof. We know that $gxg^{-1} \in N$ for every $g \in G$ and $x \in N$. Since $SN \subset G$, we in particular have that $gxg^{-1} \in N$ for any $g \in SN$. □

Proposition 10.12. $S \cap N$ is a normal subgroup of S.

Proof. If $x \in S \cap N$, then for all $s \in S$, we know $sxs^{-1} \in N$ since N is normal in G. On the other hand, S is closed under multiplication, so $sxs^{-1} \in S$ as well. This shows $sxs^{-1} \in N \cap S$. □

Theorem 10.13 (The Second Isomorphism Theorem)**.** There exists an isomorphism

$$S/(S \cap N) \cong SN/N.$$

Proof. Consider the composition of homomorphisms

$$S \to SN \to SN/N$$

where the latter is the quotient map and the former is simply the inclusion (note that $S \subset SN$). This composition is a surjection since for any $n \in N$, the element $[sn] \in SN/N$ is equal to the element $[s] \in SN/N$. Its kernel is the set of those elements s which are in N——i.e., $S \cap N$. So we are finished by the first isomorphism theorem. □

Question: Does the equivalence class $[s]$ in the $S/(S \cap N)$ define an equivalence class $[sn]$ in the SN/N? Does the n in $[sn]$ matter?

This gives us a hint for another proof of the second isomorphism theorem:

Proof. Given $[sn] \in SN/N$, consider $[s] \in S/(S \cap N)$.

We claim the assignment $\phi : [sn] \mapsto [s]$ is well-defined. For if $sn = s'n'x$ with $x \in N$, then

$$s = s'(n'xn^{-1}).$$

We must show that the element $n'xn^{-1}$ is in $S \cap N$. Well, we see it must be in S by multiplying both sides on the left by s'^{-1}. We know that it's in N since the elements n', x, n^{-1} are all in N and N is closed under multiplication.

Now we show it is a group homomorphism:

$$\begin{aligned}\phi([s_1n_1][s_2n_2]) = \phi([s_1n_1s_2n_2]) &= \phi([s_1s_2(s_2^{-1}n_1s_2n_2)]) \\ &= \phi([s_1s_2(n's_2)]) \\ &= [s_1s_2] \\ &= [s_1][s_2] \\ &= \phi([s_1n_1])\phi([s_2n_2]).\end{aligned}$$

To show it is an injection, we must know that the kernel is trivial. Well, if $\phi([sn]) = [x]$ for $x \in S \cap N$, then $[sn]$ has a representative of the form xn'; but $x \in X \cap N$, $n' \in N$ implies $xn' \in N$ by the fact that N is closed under multiplication, so $[sn] = [sn'] = 1 \in SN/N$.

To show surjection, note that for any $s \in S$, we have that $s = s1_G \in SN$. So $\phi([s1_G]) = \phi(s)$. □

10.2.2 Application of the Second Isomorphism Theorem

Example 10.1. Let $G = S_4$, the symmetric group on 4 elements. Let S be the subgroup of G generated by the permutation (12) and N be the normal subgroup A_4, the alternating group on 4 elements. We have the isomorphism $S \cong \mathbb{Z}_2$.

Proof.

1. Identify S, N and their intersection:

   $S = \langle(12)\rangle$, which is of order 2.

   $N = A_4$, which is of order 12.

   $S \cap N$: Since (12) is an even permutation only if it can be written as an even number of transpositions. However, (12) is a single transposition, so $(12) \notin A_4$. Therefore, $S \cap N = \{1_G\}$.

2. Compute SN:

   SN consists of all elements that can be written as sn, where $s \in S$ and $n \in N$.

   Since S has order 2 and N has order 12 and $S \cap N = \{1_G\}$, the order of SN is $|S||N|/|S \cap N| = (2 \times 12)/1 = 24$.

   However, G is of order 24, so $SN = G$.

3. Apply the second isomorphism theorem:

$$S \cong S/\{1_G\} \cong S/(S \cap N) \cong (SN)/N \cong G/N \cong S_4/A_4 \cong \mathbb{Z}_2.$$

□

10.3 The Third Isomorphism Theorem

The third isomorphism theorem answers the following question: Let's say I have a nested sequence of subgroups, $K \subset N \subset G$. Well, I could quotient out all of N to get the orbit set G/N. (In the process, all of K is divided out, too, since K is contained in N.) Or I could try to quotient out step by step: First take G/K, and then divide out by what remains of N. Is the end result the same thing? The answer is yes, and if both K and N are normal in G (so that it makes to talk about quotient groups), the end result is the same thing as groups.

10.3.1 The Third Isomorphism Theorem

Proposition 10.14. If there exists subgroups $K \subset N \subset G$. There is an injection

$$f : N/K \to G/K.$$

Proof. For any coset $nK \in N/K$ (where $n \in N$), define:

$$f(nK) = nK \in G/K.$$

This simply means that we are considering the coset nK from N/K as an element in G/K.

If $n_1K = n_2K$ in N/K, then $n_1^{-1}n_2 \in K$. Since $K \subset G$, this also means $n_1K = n_2K$ in G/K. Thus, f is well-defined.

If $f(n_1K) = f(n_2K)$, then $n_1K = n_2K$ in G/K, implying $n_1^{-1}n_2 \in K$. This shows that $n_1K = n_2K$ in N/K. Hence, f is injective.

Therefore, there exists an injection $f : N/K \to G/K$. □

Neither of these are groups, these are just sets. After all we haven't assumed that K is normal in G.

Proposition 10.15. Let $K \subset N \subset G$ be subgroups and K is normal in G. Then $K \triangleleft N$.

Proof. Since $K \triangleleft G$, for any $g \in G$ and $k \in K$, we have:

$$gkg^{-1} \in K.$$

In particular, this holds for any $n \in N$ because $N \subset G$. Thus, for any $n \in N$ and $k \in K$:

$$nkn^{-1} \in K.$$

This shows K is normal in N, so $K \triangleleft N$. □

Now it makes sense to talk about the groups G/K and N/K.

Proposition 10.16. Let $K \subset N \subset G$ be subgroups. The injection $f : N/K \to G/K$ is a group homomorphism.

Proof. For any $n_1K, n_2K \in N/K$, the product in N/K is:

$$(n_1K) \cdot (n_2K) = (n_1n_2)K.$$

Applying f:

$$f((n_1K) \cdot (n_2K)) = f((n_1n_2)K) = (n_1n_2)K.$$

On the other hand:

$$f(n_1K) \cdot f(n_2K) = (n_1K) \cdot (n_2K) = (n_1n_2)K.$$

Since both sides are equal, f is a group homomorphism. □

This exhibits N/K as a subgroup of G/K.

Proposition 10.17. Let $K \subset N \subset G$ be subgroups. There exists a bijection

$$\psi : G/N \to (G/K)/(N/K).$$

Proof. For any coset $gN \in G/N$, define:

$$\psi(gN) = gK \in (G/K)/(N/K).$$

This means that gK is considered as a coset in G/K, identified up to the subgroup N/K.

Well-Defined: If $g_1N = g_2N$, then $g_1^{-1}g_2 \in N$, so g_1K and g_2K are the same in $(G/K)/(N/K)$. Thus, ψ is well-defined.

Injectivity: If $\psi(g_1N) = \psi(g_2N)$, then g_1K and g_2K are the same double coset in $(G/K)/(N/K)$, implying $g_1N = g_2N$. So ψ is injective.

Surjectivity: For any coset gK in $(G/K)/(N/K)$, there is a corresponding $gN \in G/N$ such that $\psi(gN) = gK$. Thus, ψ is surjective.

Hence, ψ is a bijection. □

This is just a function between two sets. To be clear, on the right hand side, we have made use of the action of N/K on G/K, since N/K is a subgroup. The quotient set $(G/K)/(N/K)$ is the usual orbit space of this action.

Proposition 10.18. Let G be finite group and $K \subset N \subset G$ be subgroups, then

$$|G/N| = |G/K|/|N/K|.$$

Proof. $|G/N|$ is the number of cosets of N in G.

$|G/K|$ is the number of cosets of K in G.

$|N/K|$ is the number of cosets of K in N.

Each coset of N in G corresponds to $|N/K|$ cosets of K in G. Hence:

$$|G/K| = |G/N| \cdot |N/K|.$$

Rearranging gives:

$$|G/N| = \frac{|G/K|}{|N/K|}.$$

□

Theorem 10.19 (The Third Isomorphism Theorem)**.** Let G be a group. Let $K \triangleleft G$ and $N \triangleleft G$ such that $K \subset N \subset G$. Then the quotient group N/K is a normal subgroup of G/K and

$$(G/K)/(N/K) \cong G/N.$$

Proof.

1. N/K is a normal subgroup of G/K:

   Since N is a subgroup of G, N/K is a subgroup of G/K.

   For any coset $gK \in G/K$ and $nK \in N/K$, consider the conjugation: $(gK)(nK)(gK)^{-1} = gKnKg^{-1}K = gng^{-1}K$.

   Since $N \triangleleft G$, $gng^{-1} \in N$.

   Therefore, $gng^{-1} \in N/K$.

   Thus, $(gK)(nK)(gK)^{-1} \in N/K$.

   Hence, $N/K \triangleleft G/K$.

2. Define the natural homomorphism $\phi : G/K \to G/N$, where $\phi(gK) = gN$. It is well-defined, i.e., if $gK = g'K$, then $\phi(gK) = \phi(g'K)$.

   If $gK = g'K$, then $g^{-1}g' \in K \subset N$.

   Therefore, $g^{-1}g' \in N$, so $gN = g'N$.

   Hence, $\phi(gK) = gN = g'N = \phi(g'K)$.

3. ϕ is a surjective group homomorphism:

   For any $gK, hK \in G/K$:

   $$\phi((gK)(hK)) = \phi(ghK) = ghN = (gN)(hN) = \phi(gK)\phi(hN).$$

   Therefore, ϕ is a homomorphism.

   For any $gN \in G/N$, there exists $gK \in G/K$ such that $\phi(gK) = gN$. Thus, ϕ is surjective.

4. Determine the kernel of ϕ:
   $\ker(\phi) = \{gK \in G/K \mid \phi(gK) = N\}$.
   $\phi(gK) = gN = N$ implies $g \in N$.
   Therefore, $\ker(\phi) = \{gK \mid g \in N\} = N/K$.

5. Apply the first isomorphism theorem:
   If $\phi : G/K \to G/N$ is a surjective homomorphism with kernel N/K, then
   $$(G/K)/\ker(\phi) \cong \text{im}(\phi) = G/N.$$
   Since $\ker(\phi) = N/K$, we have
   $$(G/K)/(N/K) \cong G/N.$$

□

10.3.2 Application of the Third Isomorphism Theorem

Example 10.2. Let $G = \mathbb{Z}$, $N = 4\mathbb{Z}$, $K = 12\mathbb{Z}$.
$N/K = 4\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}_3$.
$G/K = \mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}_{12}$.
$(G/K)/(N/K) = (\mathbb{Z}_{12})/(\mathbb{Z}_3) \cong \mathbb{Z}_4$.
$G/N = \mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4$.
$(G/K)/(N/K) \cong G/N \cong \mathbb{Z}_4$.

Chapter 11

Short Exact Sequence and Semidirect Product

11.1 Extensions, a.k.a. Short Exact Sequences

Definition 11.1. A **short exact sequence** of groups is a pair of homomorphisms

$$G \to H \to K$$

such that

(1) $G \to H$ is an injection,

(2) $H \to K$ is a surjection, and

(3) the kernel of $H \to K$ is equal (not just isomorphic) to the image of $G \to H$.

A short exact sequence is often written as

$$1 \to G \to H \to K \to 1.$$

Definition 11.2. We will also say that H is an **extension** of K by G.

Question: The reason for the 1 on the ends?

The 1 represents the trivial group with one element. The above sequence is "exact" in the sense that the image of any homomorphism is the kernel of the next. For instance, the portion $1 \to G \to H$ says that the image of $1 \to G$ is the kernel of $G \to H$, i.e. $G \to H$ is injective.

For reasons that will become clearer later, short exact sequences are important because of the following philosophy: We think of the group H as built up of the groups G and K.

Example 11.1. There are short exact sequences:

(1) $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, and[1]

(2) $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.[2]

So we can think of both $\mathbb{Z}/4\mathbb{Z}$ and the Klein four group as built out of two copies of $\mathbb{Z}/2\mathbb{Z}$, but we see there are different groups we can build out of $\mathbb{Z}/2\mathbb{Z}$.

We also have short exact sequences:

(3) $\mathbb{Z}/3\mathbb{Z} \to S_3 \to \mathbb{Z}/2\mathbb{Z}$, [3] and

(4) $\mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.

So we see that there are at least two different ways to build a group of order 6 out of $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$.

Remark. The above examples show:

(1) Extensions do not need to be direct products.

(2) An extension $G \to H \to K$ may not allow for maps $H \leftarrow K$ such that $K \to H \to K = \mathrm{id}_K$.

(3) Extensions of abelian groups can be non-abelian.

[1] The first homomorphism sends $1 \mapsto 2 \in \mathbb{Z}/4\mathbb{Z}$, while the second sends $0, 2 \mapsto 0$ and $1, 3 \mapsto 0 \in \mathbb{Z}/2\mathbb{Z}$.

[2] We send $a \mapsto (a, 0)$ and $(a, b) \mapsto b$.

[3] $A_3 \cong \mathbb{Z}/3\mathbb{Z}$, and this is simply the short exact sequence associated to the inclusion $A_3 \to S_3$.

11.2 Split Short Exact Sequences

Definition 11.3. We say a short exact sequence

$$G \to H \to K$$

splits if there is homomorphism $K \to H$ such that $K \to H \to K = \mathrm{id}_K$.

To make things easier to read, from now on we will write short exact sequence

$$G \to H \to K$$

as

$$L \to H \to R$$

The L is for left, the R is for right. Since $L \to H$ is injective, from now on we will indentify L with its image in H for simplicity of notation.

Example 11.2. Of the examples of the short exact sequences from above

(1) $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$,

(2) $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.

(3) $\mathbb{Z}/3\mathbb{Z} \to S_3 \to \mathbb{Z}/2\mathbb{Z}$,

(4) $\mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.

Only (1) does not split.

Note there is no way to think of R as a subgroup of H a priori. For instance, in the example

$$\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$$

the second copy of $\mathbb{Z}/2\mathbb{Z}$ doesn't naturally "embed" back into $\mathbb{Z}/4\mathbb{Z}$.

Proposition 11.1. $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ doesn't split.

Proof. $\mathbb{Z}/2\mathbb{Z}$ only has elements of order 1 and 2, so no homomorphism $j : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ can have an image containing elements of order $\geqslant 3$.[4]

But let's observe that both $[1]$ and $[3]$ are elements of order 4 inside $\mathbb{Z}/4\mathbb{Z}$:

$$\langle [1] \rangle = \{[1], [2], [3], [0]\}, \quad \langle [3] \rangle = \{[3], [6] = [2], [5] = [1], [0]\}$$

Hence any homomorphism $j : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ must have image contained in $\{[0], [2]\} \subset \mathbb{Z}/4\mathbb{Z}$. But this is the kernel of the map from $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ above; so no j could factor the identity map of $R = \mathbb{Z}/2\mathbb{Z}$. □

Here's a dramatic example:

Example 11.3. The short exact sequence

$$\mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

does not split for any $n \neq -1, 0, 1$.[5]

Since this is our first time trying to understand short exact sequences, let's try to analyze the case where we are allowed to think of R as a subgroup of H. If both L and R are inside H, maybe you will buy the philosophy more that H is "built up" from L and R. So we come to the definition we did before.

Definition 11.4. A short exact sequence **splits** if there is a group homomorphism $j : R \to H$ such that the composition $R \xrightarrow{j} H \to R$ is equal to id_R. We will call a choice of $j : R \to H$ a **splitting**.

So if the short exact sequence is given by homomorphisms $\phi : L \to H$, $\psi : H \to R$, the definitions say that $\psi \circ j = \mathrm{id}_R$. In particular, j is an injection.

[4] After all, if $g^n = 1$, we must have that $j(g)^n = 1$ as well.

[5] Any homomorphism from $\mathbb{Z}/n\mathbb{Z}$ must send an element of order n to some element of finite order. But $\mathbb{Z}$ has no element of finte order except 0, so there is no injection from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}$.

11.3 Semidirect Product

In the above example, clearly there is no way to think about $\mathbb{Z}/n\mathbb{Z}$ as a subgroup of $\mathbb{Z}$.

So we have a new idea. We'd like to be able to recognize semidirect products in nature and we'd like to be able to produce examples! Let's analyze.

As before, let's identify R with $j(R)$ when we have a split short exact sequence. Well, every element of R defines an action on H itself by conjugation: $h \mapsto rhr^{-1}$. But since L is normal, $rLr^{-1} = L$, so this defines an action on L via $C_r : l \mapsto rlr^{-1}$.

Moreover, this is a group isomorphism from L to itself. We could show that this defines a group homomorphism $R \to \mathrm{Aut}(L)$ given by $r \mapsto C_r$. In other words, it is equivalent to show $C_r \circ C_{r'} = C_{rr'}$ which is because: For $h \in R$, we have

$$(C_r \circ C_{r'})(h) = C_r(C_{r'}(h)) = C_r(r'hr'^{-1}) = r(r'hr'^{-1})r^{-1}.$$

Using the associativity of the group operation, this simplifies to

$$(C_r \circ C_{r'})(h) = (rr')h(rr')^{-1} = C_{rr'}(h).$$

This new map $R \to \mathrm{Aut}(L)$ is called the **conjugation action** of R on L. So any splitting gives rise to a homomorphism $R \to \mathrm{Aut}(L)$.[6]

Question: Fix two groups R and L. The natural question is: Does any homomorphism $R \to \mathrm{Aut}(L)$ give rise to a split exact sequence?

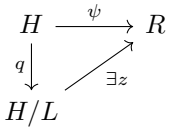
Another observation is that, given a splitting, both R and L become subgroups of H. Moreover, their intersection consists only of 1_H——after all, if a non-identity element $l \in L \cap R$, then the map $R \to H \to R$ could not be injective (l would be in the image of R, hence in the kernel of $H \to L$). Finally, since the orbits of the L action span H itself, we see that $H = \bigcup_{r \in R} Lr$. That is $H = LR$.

Definition 11.5. Let L, R be subgroups of H. We let

$$LR = \{g \text{ such that } g = lr \text{ for some } l \in L, r \in R\}.$$

To prove that $H = LR$ when short exact sequence $L \to H \to R$ splits, we need the following lemma.

Lemma 11.2. Let $L \to H \xrightarrow{\psi} R$ be a short exact sequence. Let $q : H \to H/L$ be the quotient homomorphism sending $h \mapsto Lh$. Then there exists an isomorphism $z : H/L \to R$ such that $z \circ q = \psi$. (That is, there exists a z so that the diagram



is commutative.)

Proof. We are given a short exact sequence $L \to H \xrightarrow{\psi} R$, where $\psi : H \to R$ is surjective with kernel L, and we want to show there exists an isomorphism $z : H/L \to R$ such that $z \circ q = \psi$, where $q : H \to H/L$ is the quotient map.

Since ψ is surjective and $\ker(\psi) = L$, by the first isomorphism theorem, we know that:

$$H/L \cong R.$$

Define a map $z : H/L \to R$ by:

$$z(Lh) = \psi(h).$$

This is well-defined because if $Lh_1 = Lh_2$, then $h_1 h_2^{-1} \in L = \ker(\psi)$, so $\psi(h_1) = \psi(h_2)$.

z is an isomorphism since:

- z is a homomorphism because ψ is a homomorphism.
- z is surjective since ψ is surjective.

[6] Here $\mathrm{Aut}(L)$ refers to the group of group automorphisms, not of set automorphisms.

- z is injective because the kernel of z is exactly L, meaning the only element mapped to the identity in R is L.

For all $h \in H$, $(z \circ q)(h) = z(Lh) = \psi(h)$, so $z \circ q = \psi$.
Thus, z is the desired isomorphism that makes the diagram commute.
By the First Isomorphism Theorem, there exists an isomorphism $z : H/L \to R$ such that $z \circ q = \psi$, proving the lemma. □

Once we have the lemma, we can prove the following corollary:

Corollary 11.3. If $j : R \to H$ is a splitting of the $L \to H \to R$, then

$$H = \bigcup_{r \in R} Lj(r).$$

Proof. By definition of splitting, we have that $\psi \circ j = \mathrm{id}_R$. on the other hand, we know that $\psi = z \circ q$ by the lemma, so we have

$$z \circ q \circ j = \mathrm{id}_R$$

Since z is a group isomorphism, its inverse is a homomorphism and we have an equality of homomorphisms

$$q \circ j = z^{-1}$$

Now we interpret the map $q \circ j$. The homomorphism q sends $h \mapsto Lh$. So the composite $q \circ j$ sends r to the coset $Lj(r) \in H/L$. Well, z^{-1} is a bijection onto H/L, so for any coset $Lh \in H/L$, we have a unique $r \in R$ for which $Lh = Lj(r)$. Since

$$\bigcup_{H/L} Lh = H,$$

this proves that

$$\bigcup_{r \in R} Lj(r) = H.$$

□

In the notes above, we identified elements $r \in R$ with their image in H using j, so we wrote this as

$$\bigcup_{r \in R} Lr = H.$$

Question: Fix $L, R \subset H$. If $L \cap R = \{1\}$, $L \subset H$ is normal and $LR = H$, is H a semidirect product of L and R?
What good questions we ask, when the answers are yes!

Theorem 11.4. Fix a normal subgroup $L \subset H$ and let $R \cong H/L$. The following are equivalent:

(1) A homomorphism $j : R \to H$ splitting a short exact sequence $L \to H \to R$.

(2) An isomorphism $R \to R'$ to a subgroup $R' \subset H$ such that $R' \cap L = \{1\}$ and the set map $L \times R' \to H$ is a surjection.

(3) A group homomorphism $\phi : R \to \mathrm{Aut}(L)$.

Of these, our favorite interpretation is the last since it has no reference to the group H——once we construct a group homomorphism $\phi : R \to \mathrm{Aut}(L)$, one can construct a short exact sequence $L \to H \to R$.
Question: What is group operation on H in terms of R and L?

Proposition 11.5. Any homomorphism

$$\phi : R \to \mathrm{Aut}(L),$$
$$r \mapsto \phi_r.$$

defines a group H and a split short exact sequence

$$L \longrightarrow H \overset{j}{\underset{}{\rightleftarrows}} R$$

Then

(1) the following defines a group structure on the set $H = L \times R$:

$$H \times H \to H$$
$$(l_1, r_1) \cdot (l_2, r_2) := (l_1 \cdot \phi_{r_1}(l_2), r_1 r_2).$$

where the right hand side of equality is almost the group operation of $L \times R$, but before we multiply by l_1, we "twist" l_2 to another element of L——namely, the value of r_1 under the homomorphism $\phi : R \to \mathrm{Aut}(L)$, $\phi_{r_1}(l_2)$. Moreover,

(2) The set $\{(l, 1)\}$ is a normal subgroup isomorphic to L,

(3) The set $\{(1, r)\}$ is a subgroup isomorphic to R.

Proof. **Associativity**:

$$\begin{aligned}(l_1, r_1) \cdot ((l_2, r_2) \cdot (l_3, r_3)) &= (l_1, r_1) \cdot (l_2 \cdot \phi_{r_2}(l_3), r_2 r_3) \\ &= (l_1 \cdot \phi_{r_1}(l_2 \cdot \phi_{r_2}(l_3)), r_1(r_2 r_3)) \\ &= (l_1 \cdot \phi_{r_1}(l_2) \cdot \phi_{r_1}(\phi_{r_2}(l_3)), r_1(r_2 r_3)) \\ &= (l_1 \cdot \phi_{r_1}(l_2) \cdot \phi_{r_1 r_2}(l_3), (r_1 r_2) r_3) \\ &= (l_1 \cdot \phi_{r_1}(l_2), r_1 r_2) \cdot (l_3, r_3) \\ &= ((l_1, r_1) \cdot (l_2, r_2)) \cdot (l_3, r_3)\end{aligned}$$

The third equality is because ϕ_{r_1} is a homomorphism. The forth equality is because $\phi : R \to \mathrm{Aut}(L)$ is a homomorphism.

Identity:

$$\begin{aligned}(1_L, 1_R) \cdot (l, r) &= (1_L \cdot \phi_{1_R}(l), 1_R \cdot r) \\ &= (1_L \cdot l, 1_R \cdot r) \\ &= (l, r)\end{aligned}$$

The second equality is because ϕ is a homomorphism, $\phi_1 = 1$.

Inverses:

Claim 11.6. $(l, r)^{-1} = (\phi_{r^{-1}}(l^{-1}), r^{-1})$.

Proof.

$$\begin{aligned}(l, r) \cdot (\phi_{r^{-1}}(l^{-1}), r^{-1}) &= (l \cdot \phi_r(\phi_{r^{-1}}(l^{-1})), r r^{-1}) \\ &= (l \cdot \phi_{r r^{-1}}(l^{-1}), r r^{-1}) \\ &= (l \cdot l^{-1}, r r^{-1}) \\ &= (1_L, 1_R)\end{aligned}$$

The second equality is because $\phi : R \to \mathrm{Aut}(L)$ is a homomorphism, so $\phi_r \circ \phi_{r'} = \phi_{rr'}$. The third equality is because ϕ is a group homomorphism, so $\phi_1 = \mathrm{id}_L$.

$$\begin{aligned}(\phi_{r^{-1}}(l^{-1}), r^{-1}) \cdot (l, r) &= (\phi_{r^{-1}}(l^{-1}) \cdot \phi_{r^{-1}}(l), r^{-1} r) \\ &= (\phi_{r^{-1}}(l^{-1} l), r^{-1} r) \\ &= (\phi_{r^{-1}}(1_L), 1_R) \\ &= (1_L, 1_R)\end{aligned}$$

The second equality is because $\phi_{r^{-1}} : L \to L$ is a group homomorphism. The last equality is because $\phi_{r^{-1}}$ is a group homomorphism, so $\phi_{r^{-1}} = 1$. □

Therefore, it indeed defines a group. □

Definition 11.6. We denote this group by

$$L \rtimes_\phi R$$

When ϕ is implicit, we write

$$L \rtimes R,$$

and say $L \rtimes R$ is a **semi-direct product of L and R.**

Remark. We use "a" since different ϕ may yield different groups. Though "and" is a conjunction that's usually apathetic of order, L and R play vastly different roles!

Remark. Why $\rtimes$? Usually, people write $N \triangleleft G$ when N is normal subgroup of G. $\rtimes$ is the bastard child of $\triangleleft$ (normal) and $\times$ (product).

Any

$$L \longrightarrow H \underset{}{\overset{j}{\leftarrow\!\!\rightarrow}} R$$

gives rise to a map

$$R \to \mathrm{Aut}(L).$$

How? By conjugation, since

$$\begin{aligned} &L \subset H \text{ is normal,} \\ &C_h : L \to L \\ &\qquad l \mapsto hlh^{-1} \end{aligned}$$

is a group automorphism of L.

By essentially the same arguments in your homework, we have a homomophism

$$\begin{aligned} H &\to \mathrm{Aut}(L) \\ h &\mapsto C_h \end{aligned}$$

The composition

$$R \xrightarrow{j} H \longrightarrow \mathrm{Aut}(L)$$

is the homomorphism ϕ.
Question: How does R act on $L \subset L \rtimes R$?

Proposition 11.7. $(1_L, r) \cdot (l, 1_R) \cdot (1_L, r^{-1}) = (\phi_r(l), 1_R)$. In other words, in $L \rtimes R$, conjugation by r recovers ϕ_r.

Proof.

$$\begin{aligned} (1_L, r) \cdot (l, 1_R) \cdot (1_L, r^{-1}) &= (1_L \cdot \phi_r(l), r \cdot 1_R) \cdot (1_L, r^{-1}) \\ &= (\phi_r(l) \cdot \phi(1_L), rr^{-1}) \\ &= (\phi_r(l \cdot 1_L), 1_R) \\ &= (\phi_r(l), 1_R) \end{aligned}$$

□

We now have enough ingredients to prove the theorem 11.4.
The spine of though is:

- If $L \subset H$ is normal, $H \curvearrowright L$ by conjugation.
- Given a splitting

  $$L \subset H \underset{}{\overset{j}{\leftarrow\!\!\rightarrow}} R$$

  So does R

  $$R \xrightarrow{\phi} \mathrm{Aut}(L).$$

- $L \rtimes R$ is a group where R's conjugation action on L agrees with ϕ.

Now let's prove $H \cong L \rtimes R$!

To see why $L \rtimes R \cong H$, we need a lemma.

Lemma 11.8. $\forall h \in H$, $\exists! l \in L$, $r \in R$, s.t. $h = l \cdot j(r)$.

Proof. We know that the diagram

$$\begin{array}{ccc} H & \xrightarrow{\psi} & R \\ {\scriptstyle q}\downarrow & \nearrow_{z} & \\ H/L & & \end{array}$$

is commutative. (i.e., $z \circ q = \psi$.)

Given a splitting $H \overset{j}{\leftarrow} R$, we see that

$$z \circ q \circ j = \psi \circ j = \mathrm{id}_R$$

Since z is an isomorphism, it has an inverse z^{-1}:

$$q \circ j = z^{-1}$$

z^{-1} is also a group isomorphism.

That z^{-1} is a bijection means $\forall h \in H$, $\exists! r$, s.t. $q \circ j(r) = [h] \in H/L$
$\Rightarrow \exists! r \in R$, s.t. $j(r) \in Lh = [h]$
$\Rightarrow \exists! r \in R$, s.t. $[j(r)] = [h]$
$\Rightarrow \exists! r \in R$, s.t. $h = l \cdot j(r)$, for some $l \in L$.

Of course, given h and $j(r)$, l is uniquely determined:

$$l = h \cdot j(r)^{-1}$$

So indeed, $\forall h \in H$, $\exists! l, r$, s.t. $h = l \cdot j(r)$. □

Now we can prove:

Theorem 11.9. Let $L \longrightarrow H \overset{j}{\underset{}{\leftrightarrows}} R$ be a split short exact sequence and $\phi : R \to \mathrm{Aut}(L)$ the induced action. Then

$$H \cong L \rtimes_\phi R.$$

Proof. Consider the map

$$\begin{aligned} L \ltimes_\phi R &\xrightarrow{\alpha} H \\ (l, r) &\mapsto l \cdot j(r) \end{aligned}$$

Then

$$(l_1 \cdot \phi_{r_1}(l_2), r_1 r_2) \mapsto l_1 \phi_{r_1}(l_2) j(r_1) j(r_2)$$

But by definition,

$$\phi_{r_1}(l_2) = j(r_1) l_2 j(r_1)^{-1}$$

Hence

$$\begin{aligned} \alpha((l_1, r_1) \cdot (l_2, r_2)) &= \alpha((l_1 \phi_{r_1}(l_2), r_1 r_2)) \\ &= l_1 \phi_{r_1}(l_2) j(r_1) j(r_2) \\ &= l_1 j(r_1) l_2 j(r_1)^{-1} j(r_1) j(r_2) \\ &= l_1 j(r_1) l_2 j(r_2) \\ &= \alpha((l_1, r_1)) \cdot \alpha((l_1, r_2)) \end{aligned}$$

So α is a homomorphism.

By lemma 11.8, $\forall h \in H$, $\exists! l \in L$, $r \in R$, s.t.

$$h = l \cdot j(r)$$

Hence α is a bijection. □

This is enough to show that split short exact sequences are the same amount of data as semidirect products:

- Given $L \longrightarrow H \overset{j}{\underset{\psi}{\leftrightarrows}} R$, we get $\phi : R \to \mathrm{Aut}(L)$ by conjugation.

- By theorem, $H \xleftarrow{\alpha} L \rtimes R$ is an isomorphism.
- So we have a surjection $L \rtimes R \xrightarrow{\alpha} H \xrightarrow{\psi} R$.
- Since α is an isomorphism, $\ker(\psi \circ \alpha) = \alpha^{-1}(\ker \psi)$ by lemma 11.8.
$$= \alpha^{-1}(L)$$
$$= \{(l, 1_R)\} \subset L \rtimes R$$
- So we have a short exact sequence
$$L \to L \rtimes R \xrightarrow{\psi\circ\alpha} R$$
$$l \mapsto (l, 1_R)$$
with splitting
$$L \rtimes R \leftarrow R$$
$$(1_L, r) \leftarrow\!\shortmid\, r$$
The situation can be summerized by saying that the following diagram is commutative:

$$\begin{array}{ccccc} L & \longrightarrow & H & \overset{\psi}{\underset{j}{\rightleftarrows}} & R \\ {\scriptstyle \mathrm{id}_L}\downarrow & & {\scriptstyle\alpha}\uparrow\downarrow{\scriptstyle\alpha^{-1}} & & \downarrow{\scriptstyle \mathrm{id}} \\ L & \longrightarrow & L \rtimes R & \overset{\psi\circ\alpha}{\underset{}{\rightleftarrows}} & R \end{array}$$

$$l \longmapsto (l, 1_R)$$

$$(1_L, r) \longmapsto\!\shortmid\, r$$

(i.e. any subsquare you can draw is a commutative square.)

Example 11.4. Recall that $SO_n(\mathbb{R}) \subset O_n(\mathbb{R})$ is a subgroup of index 2. By definition, $SO_n(\mathbb{R}) = \ker(O_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}^\times)$ and any kernel is a normal subgroup. So it is normal.[7] So we have a short exact sequence

$$\begin{array}{ccccccccc} & & & & & & \mathbb{Z}/2\mathbb{Z} & & \\ & & & & & & \wr\| & & \\ 1 & \to & SO_n(\mathbb{R}) & \to & O_n(\mathbb{R}) & \to & \{\pm 1\} & \to & 1 \\ & & & & & & \cap & & \\ & & & & & & \mathbb{R}^\times & & \end{array}$$

This sequence admits many different splittings?

For concreteness, take $n = 2$.

$$SO_2(\mathbb{R}) \longrightarrow O_2(\mathbb{R}) \underset{j}{\overset{\longrightarrow}{\leftarrow}} \mathbb{Z}/2\mathbb{Z}$$

For instance,

$$O_2(\mathbb{R}) \leftarrow \mathbb{Z}/2\mathbb{Z} : j$$
$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \leftarrow\!\shortmid\, [0]$$
$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \leftarrow\!\shortmid\, [1]$$
or
$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \leftarrow\!\shortmid\, [1]$$
or
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \leftarrow\!\shortmid\, [1]$$

[7] Or you may use that any subgroup of index two is normal.

Chapter 12

Simple Groups and Hölder Program

12.1 Simple Groups

There are some groups that can't be built out of any others. For instance, what if H doesn't allow for any (non-trivial) normal subgroups? Then it's impossible to have a short exact sequence unless $H \cong K$ or $G \cong H$. In this sense, groups without normal subgroups are the simplest groups.

Definition 12.1. A group H is called **simple** if it has no non-trivial normal subgroups.

Example 12.1. A cyclic group is simple if and only if it has finite, prime order.[1]

Example 12.2. $\mathbb{Z}$ is not simple.[2]

Example 12.3. A_1, A_2, A_3 are simple.[3]

Example 12.4. A_4 is not simple.[4]

Theorem 12.1. A_n is a simple group for $n \geqslant 5$.

Proof. To prove that the alternating group A_n is simple for $n \geqslant 5$, we need to show that A_n has no normal subgroups other than the trivial subgroup $\{e\}$ and A_n itself.

Let N be a normal subgroup of A_n such that $N \neq \{e\}$. We will show that $N = A_n$, thereby proving that A_n is simple.

1. N Contains a 3-Cycle:

   Since N is nontrivial, there exists a non-identity element $\sigma \in N$. We consider the cycle type of σ in its disjoint cycle decomposition.

Case 1: If σ contains a 3-cycle, then N contains a 3-cycle.

Case 2: If σ does not contain a 3-cycle, we will show that N still contains a 3-cycle through the following steps.

2. Conjugation and Normality:

   Since N is normal in A_n, for any $\tau \in A_n$, the conjugate $\tau\sigma\tau^{-1} \in N$. This property allows us to generate new elements in N from existing ones.

3. Generating 3-Cycles:

   - Expressing Elements as Products of 3-Cycles:

     Any even permutation can be expressed as a product of 3-cycles. For example, a cycle of length $k \geqslant 3$, $(a_1\, a_2\, \ldots\, a_k)$, can be written as:

$$(a_1\, a_2\, a_3)(a_1\, a_3\, a_4)\ldots(a_1\, a_{k-1}\, a_k)$$

[1] If it has prime order, it is simple since it has no subgroups but itself and $\{1\}$. On the other hand, a cyclic group of order n has a subgroup for every number n/k dividing n; for instance, take $\{1, x^k, \ldots\}$ for any generator x. Hence a cyclic group is simple when it has prime order.

[2] It has many subgroups and any subgroup of an abelian group is normal.

[3] A_1 and A_2 both have one element. A_3 is a subgroup of S_3 or index 2 by the first isomorphism theorem——it is a group of order 3, which is cyclic of prime order.

[4] We need to exhibit a non-trivial normal subgroup. There is a unique one: It consisits of elements that are products of 2-cycles. This normal subgroup is isomorphic to the Klein four group and the quotient group is the cyclic group of order 3.

- Commutators to Obtain 3-Cycles:
  Consider σ and an appropriate τ in A_n. The commutator $\gamma = \sigma\tau\sigma^{-1}\tau^{-1}$ is an element of N (since N is normal) and can be a 3-cycle.

4. N Contains All 3-Cycles:

   - Conjugacy Classes:
     In A_n, 3-cycles split into two conjugacy classes, but their union is the set of all 3-cycles. Since N contains at least one 3-cycle and is normal, it must contain all 3-cycles of that conjugacy class.
   - Generating A_n with 3-Cycles:
     The group A_n is generated by its 3-cycles when $n \geqslant 5$. Therefore, the subgroup of A_n generated by all 3-cycles is A_n itself.

5. Conclusion: Since N contains all 3-cycles, N generates A_n. Thus, $N = A_n$.

Therefore, A_n is a simple group for $n \geqslant 5$. □

12.2 Hölder Program

Now that we've seen examples of many groups, we'd like to start classifying them. Can we think of a general strategy that will help us say:"I know all groups?"
Question: How can we classify all groups?

This question doesn't have a satisfactory answer, in some ways. We can try to understand all simple groups and then understand ways in which they can all be built up. The strategy that took flight in the 19th century is called the Hölder program. It seems very natural. The problem is, we don't know how to execute it. We can't even classify all finite simple groups.

Then can we understand all finite simple groups and their extensions? This will at least classify all finite groups. We still don't know how to do this. We can classify all finite simple groups as of 1985-ish, but we still don't know how to solve the problem of classifying all their extensions. To give you some idea of how difficult even classification is, consider that the following theorem led to a Fields Medal for Thompson:

Theorem 12.2 (Feit-Thompson, or the Odd Order Theorem)**.** Every finite, simple, non-abelian group has even order.

So for instance, if you give me a non-abelian group whose order is odd, I know it's not simple.

Definition 12.2. The **Hölder program** for classifying groups is:

(1) Classify all simple groups.

(2) Classify all the ways that one can create extensions of simple groups.

We don't know how to complete this program. For instance, we don't know how to do (1). We only know how to do (1) for finite simple groups and this wasn't done until 1985. Even for finite groups, we haven't done (2).

12.3 Solvable Groups

Following the Hölder Program's focus on understanding and decomposing complex group structures, we now explore solvable groups, which represent groups that can be broken down systematically into simpler abelian components.

Definition 12.3. A group G is called **solvable** if it has a finite sequence of subgroups

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{e\}$$

such that each G_i is normal in G_{i-1} and the corresponding quotient groups G_{i-1}/G are abelian.

Remark. The group is "solvable" because it can be decomposed into smaller, simpler parts, eventually reaching the trivial group.

Example 12.5. Every cyclic group is abelian, so it is trivially solvable.

Example 12.6. S_3 is solvable. Normal series: $S_3 \triangleright A_3 \triangleright \{e\}$. Quotients: $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$ and $A_3/\{e\} \cong \mathbb{Z}/3\mathbb{Z}$. Both are abelian, so S_3 is solvable.

Example 12.7. S_5 is not solvable. The absence of a suitable normal series highlights the difference between solvable and more complex groups.

Proposition 12.3. Every subgroup of a solvable group is solvable.

Proof. A solvable group G has a chain of subgroups:

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{e\},$$

where each quotient G_{i-1}/G_i is abelian.

Let $H \subseteq G$ be a subgroup. We can intersect H with each group in the chain:

$$H \cap G_0 \triangleright H \cap G_1 \triangleright \cdots \triangleright H \cap G_n = \{e\}.$$

Each quotient $(H \cap G_{i-1})/(H \cap G_i)$ is a subgroup of the abelian quotient G_{i-1}/G_i, so it is also abelian.

This gives a normal series for H with abelian quotients, meaning H is solvable. □

Proposition 12.4. Quotients of solvable groups are solvable.

Proof. A group G is solvable if it has a chain of normal subgroups:

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{e\},$$

where each quotient G_{i-1}/G_i is abelian.

Let $N \triangleleft G$ be a normal subgroup, and we want to show that the quotient group G/N is solvable.

Use the chain from G to form a new chain in the quotient:

$$G_0/N \triangleright G_1/N \triangleright \cdots \triangleright G_n/N = \{e\}.$$

Each new quotient:

$$(G_{i-1}/N)/(G_i/N) \cong G_{i-1}/G_i$$

is abelian because the original quotients G_{i-1}/G_i were abelian.

Therefore, the quotient group G/N is solvable. □

This discussion on solvable groups demonstrates how groups can be decomposed into simpler components. While solvable groups are structured and accessible, the study of non-solvable groups, such as simple groups, remains crucial in understanding the broader landscape of group theory.

In the next chapter, we continue exploring more specialized results in group theory with Sylow theorems, which provide deeper insights into the structure of finite groups.

Chapter 13

Sylow Theorems

13.1 Counting

We saw that the orbit-stabilizer theorem answered some non-trivial questions for us: How big is the symmetry group of the tetrahedron?——for instance. Recall that the theorem says that for any group acting on a set X and for any $x \in X$, there is a bijection $G/G_x \cong \mathcal{O}_x$. In particular, if the group G is finite, we have

$$|\mathcal{O}_x| = |G|/|G_x|.$$

These kinds of counting theorems are great in math. They're like "lay-ups" in basketball. They're the easiest shots you can take. Once you reduce a hard problem to just counting, you're in business.

In the proof of Lagrange's theorem, we used the reasoning that any set is a union of its orbits. Hence given a group action of G on a finite set X, we can conclude

$$|X| = \sum_{\text{orbits}} |\mathcal{O}_x|.$$

Let's use this observation some more. The above equation is called the **counting formula**.

13.2 p-group

Definition 13.1. Let p be a prime number. A finite group G is called a **p-group** if

$$|G| = p^n$$

for some integer $n \geqslant 1$. i.e., if its order is a power of p.

Definition 13.2. Let G act on a set X. $x \in X$ is called a **fixed point** of the group action if $gx = x$ for all $g \in G$.

Proposition 13.1. Fix a p-group G. Fix a finite set X whose order is not divisible by p. Then any action of G on X must have at least one fixed point.

Example 13.1. If someone claims to you that they have a p-group acting on the tetrahedron, you can look at the induced action of G on the set of vertices of the tetrahedron. If p is anything other than 2, you know that this group action fixes at least one vertex.

Proof. By the orbit-stabilizer theorem, any orbit $\mathcal{O}_x$ has order dividing the order of the group G. Hence we have that $|\mathcal{O}_x|$ has to equal p^k for some $k \geqslant 0$. Note that we must prove that $|\mathcal{O}_x| = p^0 = 1$ for some $x \in X$ to exhibit a fixed point.

Such an x must exist——otherwise, each $\mathcal{O}_x$ is equal to p^k for $k \geqslant 1$, hence each $\mathcal{O}_x$ is divisible by p. Then the right hand side of the counting formula

$$|X| = \sum_{\text{orbits}} \mathcal{O}_x$$

is divisible by p. But by assumption, $|X|$ cannot be divisible by p. Hence $\mathcal{O}_x$ must be 1. □

Here's another application:

Proposition 13.2. Let G be a p-group. Then G has non-trivial center (i.e., its center must contain more than just the identity element).

Throughout, we let Z stand for the center of G.

Proof. Consider the conjugation action of G on itself. The orbits of this action are precisely the conjugacy classes of G. Hence the counting formula reads

$$|G| = \sum_{\text{conjugacy classes}} |[x]|$$

where $[x]$ is the conjugacy class of x——it is the set of all elements of the form gxg^{-1} for some $g \in G$. $|[x]| = 1$ if and only if x is in the center of G. For if the only element in $\mathcal{O}_x$ is x itself, this means $gxg^{-1} = x$ for all $g \in G$——this of course implies that $gx = xg$.

Finally, we know that $1_G \in G$ is always in the center of G, so the counting formula reads

$$|G| = 1 + \sum_{\text{conjugacy classes} \neq [1_G]} |[x]|.$$

If $|[x]| \geqslant 2$ for all $x \neq 1_G$, then the right hand side is not divisible by p——for it would be a summation of the form

$$1 + \sum_{\text{various } k \geqslant 1} p^k.$$

This is a contradiction since $|G|$ is only divisible by p. Hence there must be some $x \neq 1_G$ for which $|[x]| = 1$; that is, there must be some $x \neq 1_G$ in the center. □

This has a great corollary.

Corollary 13.3. Any group of order p^2 is abelian.

This is highly non-trivial. For instance, imagine proving by hand that a group of order 49 must be abelian.

We knew that every group of order p is abelian, since it must be cyclic. This is the next power up.

Proof. The center of G is a subgroup, so by Lagrange's Theorem, we must have $|Z| = 1$, p, or p^2 since these are the only divisors of p^2.

On the other hand, the proposition tells us that $|Z| \neq 1$, so it must be p or p^2.

Assume $|Z| = p$. We will yield a contradiction. For fixing $x \in G, \notin Z$, let us examine the stabilizer of x under the conjugation action of G. This, we called the centralizer of x last time, and we denote it $Z(x)$. It is the set of all $y \in G$ for which $xy = yx$.

Since the stabilizer of a group action is always a subgroup, by Lagrange's theorem, we know that $|Z(x)|$ must divide p^2. On the other hand, $Z \subset Z(x)$ since any element of the center (by definition) commutes with x. Moreover, $x \in Z(x)$ since x commutes with itself. This proves that $|Z| <_{\neq} |Z(x)|$, so $|Z(x)|$ must be a number bigger than p dividing p^2. We conclude $|Z(x)| = p^2$.

But this means every element of G commutes with x. Hence x must be in the center. □

So this strategy of just "counting" has paid off great dividends. Let's milk it for all we've got. One beautiful outcome of all this milking is Sylow's theorems.

13.3 The First Sylow Theorem

Let p divide $|G|$. We write

$$|G| = p^p \mid n$$

where p^e is the largest power of p dividing $|G|$. In particular, $\gcd(m, p) = 1$.

Definition 13.3. Then a **Sylow p-subgroup**, or **p-Sylow subgroup**), is a subgroup $H \subset G$ such that $|H| = p^e$. In other words, it is a subgroup is the biggest subgroup with size a power of p.

So if there are many different primes p that divide $|G|$, we can try to look for a Sylow p-subgroup for each of these p. As of this comment, we have no idea if there even existence, nor how many there may be inside of G.

Example 13.2. Let $G = S_3$. Then since $6 = 3 \cdot 2$, a Sylow 3-subgroup is a subgroup of order 3 inside G. There is a unique one, given by $H = \{\mathrm{id}, (123), (132)\}$. There are three Sylow 2-subgroups: $\{\mathrm{id}, (12)\}, \{\mathrm{id}, (13)\}, \{\mathrm{id}, (23)\}$.

Theorem 13.4 (The First Sylow Theorem)**.** Let p divide $|G|$. Then there exists a Sylow p-subgroup of G.

Before get into the proof of this theorem, let's introduce two lemmas which will be used in the proof of theorem.

Lemma 13.5. p doesn't divide $|\mathcal{P}_{p^e}(G)|$.

Proof. The number of subsets of order p^e is not divisible by p. Recall $\binom{a}{b}$ =ways to choose b unordered things from a collection of size a. So $\binom{a}{b} = \dfrac{a!}{b!(a-b)!}$. Well, we have

$$\binom{p^e m}{p^e} = \frac{(p^e m)(p^e m - 1)\cdots(p^e m - p^e + 1)}{p^e(p^e - 1)\cdots 1}$$

Note if p divides a numerator term

$$p^e m - k,$$

it also divides

$$p^e - k$$

in the denominator and the same number of times! Why? If

$$k = p'l, \quad p \nmid l.$$

$$p^e m - k = p^i(p^{e-i}m - l)$$
$$p^e - k = p^i(p^{e-i} - l)$$

Note $i < e$, else $p^e - k$ would be negative!

So $\dfrac{p^e m - k}{p^e - k}$ is NOT divisible by p. □

Remark. We argued

$$\binom{p^e m}{p^e} = \frac{p^e m(p^e m - 1)\cdots(p^e m - p^e + 1)}{p^e(p^e - 1)\cdots 1}$$

isn't divisible by p. This came down to

$$p^i \mid p^e m - k \quad \Rightarrow \quad p^i \mid p^e - k.$$

Why is $i < e$? Since otherwise,

$$k = p^{e+a}l \quad \Rightarrow \quad p^e - k = p^e(1 - p^a l) \leqslant 0 \text{ if } a \geqslant 0.$$

More concretely, by definition of binomial coefficient, k has to run from 0 to $p^e - 1$, so k itself must be less than p^e.

Claim 13.6. $U \subset G$ a subset. The stabilizer H of U has order dividing $|U|$.

Proof. If U is fixed by H, then $U = \bigcup_{u \in U} Hu$, and U is partitioned into cosets.

$$U = \bigsqcup Hu$$

So

$$|U| = |H| + \cdots + |H|.$$

□

Let's try to prove this theorem, What should our strategy be? Counting.
The better question is: Count what?

Proof. G acts on $\mathcal{P}_{p^e}(G)$ by left multiplication

$$S \mapsto gS.$$

Since $p \nmid |\mathcal{P}_{p^e}(G)|$ by lemma, $\exists$ orbit $\mathcal{O}_U$, s.t. $p \nmid \mathcal{O}_U$. (Since $|\mathcal{P}_{p^e}(G)| = \sum_{\text{orbits}} |\mathcal{O}_U|$.)

Let $U \in \mathcal{O}_U$. By orbit-stabilizer,

$$|G|/|G_U| = |\mathcal{O}_U|$$

while by other lemma, $U = \bigcup_{\text{cosets}} G_U$. So $|G_U|$ divides $|U| = p^e$. Hence

$$p^e m = |G| = |G_U| \cdot |\mathcal{O}_U|$$

where $|G_U|$ is power of p and $|\mathcal{O}_U|$ is not divided by p.

$$|G_U| = p^e.$$

□

Corollary 13.7. Let p divide $|G|$. Then there exists an element $x \in G$ of order p.

You may not have considered this corollary before. By Lagrange, we know that any element $x \in G$ must divide the order of $|G|$. But given a number dividing $|G|$, is it obvious that there should (or shouldn't) be an element of a specified order p for a prime dividing G?

Proof. Since p divides G, $|H| \geqslant 2$. So we can choose an element $x \in H$ such that $x \neq 1_G$. Moreover, the order of x must divide $|H|$ by Lagrange's theorem. Thus

$$x^{p^k} = 1_G$$

for some $k \geqslant 1$. Just let $y = x^{p^{k-1}}$. Then $y^p = 1_G$. □

Example 13.3. Let

$$G = S_7 \times \mathbb{Z}/14\mathbb{Z}$$

Then

$$\begin{aligned} |G| &= 7! \times 14 \\ &= 7^2 \times 5 \times 3^2 \times 2^5. \end{aligned}$$

The first Sylow theorem guarantees that this group will have

- A subgroup of order 49
- A subgroup of order 5
- A subgroup of order 9
- A subgroup of order 32

Example 13.4. Could you find a subgroup of order 16 in S_7?

Proof.

1. Identify a suitable prime power:
   - The order of S_7 is $7! = 5040$, and 16 is a power of 2, specifically 2^4.
   - We need to find a subgroup of S_7 with order 16, which will be a Sylow 2-subgroup.
2. Look for elements of order 2:
   - In S_7, elements of order 2 are transpositions (2-cycles), which swap two elements and leave the others fixed. For example, $(12) \in S_7$ has order 2.

- A product of disjoint transpositions, such as (12)(34), also has order 2. In general, a product of k disjoint transpositions has order 2^k.

3. Construct a subgroup of order 16:

   - To get a subgroup of order 16, we need a group generated by 4 disjoint transpositions (since $2^4 = 16$).
   - Consider the following disjoint transpositions in S_7: (12), (34), (56), (78).
   - These four disjoint transpositions generate a subgroup of order 16. This subgroup is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, since each transposition generates a cyclic group of order 2, and the transpositions are disjoint (i.e., they commute).

Thus, the subgroup of order 16 in S_7 can be generated by disjoint transpositions, such as $\{(12), (34), (56), (78)\}$, and is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. □

So the first Sylow theorem tells us that Sylow p-subgroups exist——Given group G, s.t.

$$|G| = p^e m, \quad p \nmid m,$$

$H \subset G$ is a Sylow p-subgroup if $|H| = p^e$.

13.4 The Second Sylow Theorem

Theorem 13.8 (The Second Sylow Theorem)**.** Fix a finite group G and a prime p dividing $|G|$.

(1) Any two Sylow p-subgroups are conjugate.

(2) For any subgroup $H \subset G$ which is a p-group. $\exists$ a Sylow p-subgroup containing H.

Proof. Any subgroup $K \subset G$ acts on $G/H = \{\text{left cosets } gH\}$.

$$gH \mapsto (kg)H.$$

If K is a p-group and H is a Sylow p-subgroup, $|K| = p^l$ while $|G/H| = |G|/|H| = p^e m/p^e = m$. Since $p \mid m$, the action of K on G/H has a fixed point: $\exists g$, s.t.

$$k \cdot gH = gH, \quad \forall k \in K.$$

i.e., $\forall k \in K$, $\forall h \in H$, $\exists h' \in H$, s.t.

$$k \cdot g \cdot h = g \cdot h'.$$

$\Rightarrow k = gh'h^{-1}g^{-1}$.
$\Rightarrow k \in gHg^{-1}$.
$\Rightarrow K \subset gHg^{-1}$. □

Note that if $\exists$ only one Sylow p-subgroup, it must be normal. Why?
$\forall g \in G$,

$$C_g : G \to G$$
$$x \mapsto gxg^{-1}$$

is a group isomorphism. So it sends subgroups of order k to subgroups of order k. If $\exists$ only one such subgroup H, C_g must take H to H, $\forall g \in G$, i.e.,

$$gHg^{-1} = H, \quad \forall g \in G.$$

Since H is normal
The second Sylow theorem tells us the converse is true.

Corollary 13.9. If a Sylow p-subgroup H is a normal subgroup G, H is the only Sylow p-subgroup of G.

13.5 Normalizer

Before the third Sylow theorem, we still need to introduce a important concept——normalizer.

Definition 13.4. Let $K \subset G$ be a subgroup. Then

$$N(K) = \{g \in G \mid gKg^{-1} = K\}$$

is called the **normalizer** of K.

Proposition 13.10.

(1) $N(K)$ is a subgroup of G.

(2) $K \lhd N(K)$.

(3) $N(K)$ is stabilizer of K with respect to the conjugation action of G on $\mathcal{P}_{|K|}(G)$, where $\mathcal{P}_{|K|}(G)$ denote the set of all subgroups of G with order equal to $|K|$.

13.6 The Third Sylow Theorem

Before we get to the third Sylow theorem, we may quickly run a useful fact first. We know that semidirect products are recognized as split short exact sequence: $H \cong L \rtimes R \Leftrightarrow \exists$ split short exact sequence $1 \longrightarrow L \longrightarrow H \underset{\longleftarrow}{\overset{j}{\longrightarrow}} R \longrightarrow 1$.
Question: So when can we recognize direct products?

Proposition 13.11. The following statement are equivalent:

(1) $H \cong L \times R$.

(2) $H \cong L \rtimes_\phi R$, where $\phi : R \to \mathrm{Aut}(L)$ is trivial.

(3) $\exists$ split short exact sequence $L \longrightarrow H \underset{\longleftarrow}{\overset{j}{\longrightarrow}} R$, s.t. $j(R) \lhd H$.

Proof. (1)⇒(3)⇒(2)⇒(1)
(1)⇒(3): If $H \cong L \times R$, we have the inclusion

$$\begin{aligned} i : L &\to H \\ l &\mapsto (l, 1_R) \end{aligned}$$

and the projection

$$\begin{aligned} p : H &\to R \\ (l, r) &\mapsto r \end{aligned}$$

both are homomorphism. Then we have a splitting

$$L \xrightarrow{i} H \underset{j}{\overset{p}{\rightleftarrows}} R$$

where $j : R \to H$ is the other "inclusion" homomorphism.
$r \mapsto (1_L, r)$
Moreover, $j(R) \lhd H$. Why?

$$\begin{aligned} (l', r')(1_L, r)(l', r')^{-1} &= (l', r')(1_L, r)(l'^{-1}, r'^{-1}) \\ &= (l' 1_L l'^{-1}, r' r r'^{-1}) \\ &= (1_L, r' r r'^{-1}) \in j(R). \end{aligned}$$

(3)⇒(2): Let $r \in j(R)$, $l \in i(L)$. Then

$$rlr^{-1}l^{-1} = l'l^{-1} \in i(L),$$

since $i(L)$ is normal and

$$rlr^{-1}l^{-1} = rr' \in j(R),$$

since $j(R)$ is normal. So

$$rlr^{-1}l^{-1} \in j(R) \cap i(L)$$

But $j(R) \cap i(L) = \{1_H\}$ since j is a splitting.
$\Rightarrow \quad rlr^{-1}l^{-1} = 1_H, \quad \forall l, r$
$\Rightarrow \quad rlr^{-1} = l, \quad \forall l, r$
$\Rightarrow \quad \phi : R \to \mathrm{Aut}(L)$
is $r \mapsto \mathrm{id}_L, \quad \forall r \in R$
(2)⇒(1): If $\phi(r) = \mathrm{id}_L$, $\forall r$, then

$$\begin{aligned}(l_1, r_1) \cdot (l_2, r_2) &= (l_1 \cdot \phi_{r_1}(l_2), r_1 r_2) \\ &= (l_1 l_2, r_1 r_2)\end{aligned}$$

which is the definition of the multiplication on $L \times R$. □

Now we will state the third Sylow theorem, which will really help us determine the structures of groups.

Theorem 13.12 (The Third Sylow Theorem)**.** Let G be a finite group and p a prime dividing $|G|$. We let

$$\mathrm{Syl}_p(G)$$

denote the set of Sylow p-subgroups of G. Then

(1) $|\mathrm{Syl}_p(G)|$ divides m.

(2) $|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}$.

Remark. (1) implies that G acts on $\mathrm{Syl}_p(G)$ by conjugation and the second Sylow theorem says this action has a single orbit, i.e. $|\mathrm{Syl}_p(G)| = |G|/\text{Stabilizer } G_H$ for some Sylow p-subgroup H. But $H \subset G_H$, so $|G_H| = p^e \cdot m'$.

$$|\mathrm{Syl}_p(G)| = p^e m / p^e \cdot m' = m/m'.$$

For (2), we will show that $\forall H \in \mathrm{Syl}_p(G)$, H is the only fixed point for conjugation action of H on $\mathrm{Syl}_p(G)$. So

$$|\mathrm{Syl}_p(G)| = 1 + \sum \mathcal{O}$$

where $\mathcal{O}$s are all divisible by p.

Proof. Let H be a Sylow p-subgroup. G acts on $\mathrm{Syl}_p(G)$ by conjugation:

$$K \mapsto hKh^{-1}$$

By orbit-stabilizer,

$$|G|/|G_H| = |\mathcal{O}_H| = |\mathrm{Syl}_p(G)|$$

The second equality holds by the second Sylow theorem. Well, $hHh^{-1} = H$, so $H \subset G_H$, so $p^e \mid |G_H|$. Hence,

$$p^e m / p^e m' = |\mathrm{Syl}_p(G)| \quad \Rightarrow \quad m = |\mathrm{Syl}_p(G)| \cdot m'$$

Since G acts on $\mathrm{Syl}_p(G)$, so does $H \subset G$. H is a fixed point. If K is another,

$$H \subset N(K) \text{ and } K \subset N(K).$$

By the second Sylow theorem, H is conjugate to K in $N(K)$. But $K \triangleleft N(K)$, so $H = K$. □

Here's an example application:

Proposition 13.13. If $|G| = 15$, G is cyclic.

Proof. The strategy is determine $\mathrm{Syl}_5(G)$, $\mathrm{Syl}_3(G)$.
For $p = 5$, $|G| = p^e m$

$$= 5^1 \cdot 3.$$

By the third Sylow theorem,

(a) $|\mathrm{Syl}_5(G)|$ divides 3

(b) $|\mathrm{Syl}_5(G)| \equiv 1 \pmod 5$

(a) $\Rightarrow |\mathrm{Syl}_5(G)| = 1$ or 3
(b) $\Rightarrow |\mathrm{Syl}_5(G)| = 5$.
$\Rightarrow \exists!$ subgroup $H_5 \subset G$ of order 5. H_5 is hence normal!
Likewise,

(c) $|\mathrm{Syl}_3(G)|$ divides 5.

(d) $|\mathrm{Syl}_3(G)| \equiv 1 \pmod 3$

$\Rightarrow |\mathrm{Syl}_3(G)| = 1$.
$\Rightarrow \exists!$ subgroup $H_3 \subset G$ of order 3. It's normal.
Since $\gcd(|H_3|, |H_5|) = \gcd(3, 5) = 1$, $H_3 \cap H_5 = \{1_G\}$. Then

$$1 \longrightarrow H_3 \longrightarrow G \underset{\longleftarrow}{\overset{j}{\longrightarrow}} H_5 \longrightarrow 1.$$

Since $H_3, H_5 \triangleleft G$, $G \cong H_3 \times H_5 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$. □

Proposition 13.14. Let $|G| = p \cdot P$ where $p \neq P$ are primes. Then if P is the large prime, $G \cong \mathbb{Z}/P\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

Proof. By the third Sylow theorem,

(a) $|\mathrm{Syl_P}(G)|$ divides p.

(b) $|\mathrm{Syl}_P(G)| \equiv 1 \pmod P$.

(a) $\Rightarrow |\mathrm{Syl}_P(G)| = 1$ or $p < P$
(b) $\Rightarrow |\mathrm{Syl}_P(G)| = 1$ since the only number less than P equal to 1 mod P is 1.
$\Rightarrow \exists! H_P \subset G$ of order P.
$\Rightarrow H_P \triangleleft G$.
So consider short exact sequence

$$1 \to H_P \to G \to G/H_P \to 1.$$

$|G/H_P| = p$, so it is isomorphic to $\mathbb{Z}/p\mathbb{Z}$
$|H_P| = P$, so it is isomorphic to $\mathbb{Z}/P\mathbb{Z}$.
So we have short exact sequence

$$1 \to \mathbb{Z}/P\mathbb{Z} \to G \to \mathbb{Z}/p\mathbb{Z} \to 1.$$

By the first Sylow theorem, splitting j exists. (Since p, P are relatively prime.) □

Chapter 14

Rings

14.1 Definition of Rings

Definition 14.1. A **monoid** is a group without inverses. That is, a monoid is a set M together with a function

$$\cdot : M \times M \to M$$

which has a unit, and which is associative. We say a monoid is **commutative** if $ab = ba$ for all $a, b \in M$.

Definition 14.2. An **associative ring** is a triple $(R, +, \cdot)$ where R is a set, and

(1) $+ : R \times R \to R$ is a function making $(R, +)$ into an abelian group. We call this operation addition, and we call its identity element 0.

(2) $\cdot : R \times R \to R$ is a function making R into a monoid. We call the $\cdot$ operation multiplication, and we denote the unit by 1.

(3) Finally, we demand that multiplication distributes over addition: This means that for all $a, b, c \in R$, we have

$$a(b + c) = ab + ac \quad \text{and} \quad (b + c)a = ba + ca$$

where we have written $a \cdot b$ as ab.

We will often simply write R for a ring, leaving the operations $+$ and $\cdot$ implicit.

Definition 14.3. If $(R, \cdot)$ is an abelian monoid, we call R a **commutative ring**.

When we dealt with groups, I proved the cancellation law right away because it was a useful thing to know. Here's another useful thing to know:

Proposition 14.1. Let R be an associative ring and let 0 be the additive identity for R. Then

$$0 \cdot a = a \cdot 0 = 0$$

for all $a \in R$.

Proof.

$$\begin{aligned} 0 \cdot a &= (0 + 0) \cdot a && \text{(Since } 0 + 0 = 0\text{)} \\ &= 0 \cdot a + 0 \cdot a && \text{(Distributivity)} \end{aligned}$$

By the cancellation law for abelian groups, we can subtract $0 \cdot a$ from both sides of this equation. We are left with $0 = 0 \cdot a$. Analogously, $a \cdot 0 = 0$. □

Remark. We won't get to see why in depth, but rings have incredibly different behaviors based on whether they are commutative or not.

14.2 Examples of Commutative Rings

Example 14.1. Consider the triple $(\mathbb{Z}, +, \cdot)$. This makes $(\mathbb{Z}, +)$ into abelian group and $(\mathbb{Z}, \cdot)$ is certainly a monoid——multiplication has a unit called 1 and it's associative. Distributivity is the usual notion of distributivity you are used to.

Example 14.2. The triple $(\mathbb{Q}, +, \cdot)$ with the usual addition and multiplication is a ring. Likewise for $\mathbb{R}$ and $\mathbb{C}$ with their usual notions of multiplication. These are special kinds of rings, because any element of $R - \{0\}$ has an inverse under multiplication.

Example 14.3 (Polynomial Rings)**.** Let $\mathbb{Z}[x]$ denote the set of polynomials in x with integer coefficients. So an element is an expression

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = \sum_{i=0}^{\infty} a_i x^i$$

where $a_i = 0$ for all i bigger than some finite n. For example, the following are elements in $\mathbb{Z}[x]$:

$$0, 5, 3 + x - 5x^4, x.$$

In the third example, we have $a_0 = 3$, $a_1 = 1$, $a_2 = 0$, $a_3 = 0$, $a_4 = -5$.

Let $q(x)$ be a polynomial with coefficients b_i. Addition of polynomials is defined as follows

$$p(x) + q(x) := \sum_{i=0}^{\infty} (a_i + b_i) x^i.$$

Note that since $a_i = 0$ for i bigger than n, and $b_i = 0$ for all i bigger than some m, the sum is indeed a polynomial, as $(a_i + b_i) = 0$ for all i bigger than $\max(m, n)$.

And the product of two polynomials is defined in the usual way

$$\begin{aligned} p(x) \cdot q(x) &= (a_0 + a_1 x + \cdots + a_n x^n)(b_0 + b_1 x + \cdots + b_m x^m) \\ &= a_0 b_0 + (a_1 b_0 + a_0 b_1) x + \cdots + a_n b_m x^{n+m} \\ &= \sum_{k \geqslant 0} \left(\sum_{i+j=k} a_i b_j \right) x^k. \end{aligned}$$

Proposition 14.2. $\mathbb{Z}[x]$ is a commutative ring. More generally, if R is a commutative ring, the set of polynomials with coefficients in R, $R[x]$, is a commutative ring.

Proof.

1. $R[x]$ is a ring, since

   (1) Addition is closed: For two polynomials $p(x)$ and $q(x)$ in $R[x]$, the sum $p(x) + q(x)$ is a polynomial whose coefficients are the sum of the corresponding coefficients of $p(x)$ and $q(x)$. Since R is a commutative ring and closed under addition, this operation is well-defined in $R[x]$.

   (2) Multiplication is closed: For two polynomials $p(x)$ and $q(x)$, their product $p(x) \cdot q(x)$ is given by

   $$p(x) \cdot q(x) = \left(\sum_{i=0}^{n} a_i x^i \right) \left(\sum_{j=0}^{m} b_j x^j \right) = \sum_{k=0}^{n+m} c_k x^k$$

   where the coefficients c_k are computed as

   $$c_k = \sum_{i+j=k} a_i b_j$$

   Since R is closed under multiplication, the coefficients c_k are elements of R, and therefore the product is a polynomial in $R[x]$.

   (3) Addition is associative and commutative: The addition of polynomials in $R[x]$ is associative and commutative because addition in R is associative and commutative, and the operations on the individual coefficients follow the properties of R.

(4) Multiplication is associative: The multiplication of polynomials in $R[x]$ is associative because the distributive law holds and multiplication in R is associative. Hence for polynomials $p(x)$, $q(x)$ and $r(x)$ in $R[x]$

$$(p(x) \cdot q(x)) \cdot r(x) = p(x) \cdot (q(x) \cdot r(x))$$

(5) Distributivity: Multiplication distributes over addition in $R[x]$ because for polynomials $p(x)$, $q(x)$ and $r(x)$ in $R[x]$:

$$p(x) \cdot (q(x) + r(x)) = p(x) \cdot q(x) + p(x) \cdot r(x)$$

This holds because distributivity applies to the individual coefficients in R.

2. Commutativity of multiplication: For any polynomials $p(x), q(x) \in R[x]$, we have

$$p(x) \cdot q(x) = q(x) \cdot p(x)$$

This follows from the fact that multiplication in R is commutative. In particular, if $p(x) = \sum_{i=0}^{n} a_i x^i$ and $q(x) = \sum_{j=0}^{m} b_j x^j$, then the product is

$$p(x) \cdot q(x) = \sum_{k=0}^{n+m} \sum_{i+j=k} a_i b_j x^k.$$

By the commutativity of multiplication in R, we have $a_i b_j = b_j a_i$ and thus

$$p(x) \cdot q(x) = q(x) \cdot p(x).$$

□

Example 14.4 (Smooth Functions)**.** Here's an example where it's much harder to write down all the elements of the set. Let $C^\infty(\mathbb{R}^n)$ denote the set of all infinitely differentiable functions $f : \mathbb{R}^n \to \mathbb{R}$. Given two functions f and g, we define their sum $f+g$ to be a function that sends $x \in \mathbb{R}^n$ to $f(x)+g(x)$, where this addition takes place in $\mathbb{R}$. Their product fg is the function that sends $x \in \mathbb{R}^n$ to $f(x) \cdot g(x) \in \mathbb{R}$. This is again a ring.

14.3 The Rings $\mathbb{Z}/n\mathbb{Z}$

We've seen three examples of rings that we're used to. They've all been infinite. Let's see some finite examples.

Lemma 14.3. Let $\mathbb{Z}/n\mathbb{Z}$ be the set of integers modulo n. The function

$$\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \qquad \overline{a} \cdot \overline{b} := \overline{a \cdot b}$$

is well-defined.

Remark. We are denoting the equivalence class associated to $a \in \mathbb{Z}$ by a $\overline{a}$. Here, $a \cdot b$ is the usual multiplication of integers and $\overline{a \cdot b}$ denotes its equivalence class mod n.

Proof. We need to show that if $\overline{a} = \overline{a}'$ and $\overline{b} = \overline{b}'$, then

$$\overline{a \cdot b} = \overline{a' \cdot b'}.$$

Well, $a = a'$ modulo n if and only if $a = a' + An$ for some integer A. Likewise, we have that $b = b' + Bn$ for some B. Then

$$ab = (a' + An)(b' + Bn) = a'b' + (a'B + Ab' + AB)n$$

so ab equals $a'b'$ modulo n. □

Corollary 14.4. Let $+$ be the usual addition on $\mathbb{Z}/n\mathbb{Z}$, and let $\cdot$ be the operation above. Then

(1) $(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian group with unit $\overline{0}$.

(2) $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ is an abelian monoid with unit $\overline{1}$.

(3) The operation $\cdot$ distributes over $+$.

Proof.

(1) is something we proved a long time ago.

(2) To prove associativity, note that

$$\begin{aligned}(\overline{a} \cdot \overline{b}) \cdot \overline{c} &= \overline{\overline{a \cdot b} \cdot \overline{c}} \\ &= \overline{\overline{(a \cdot b) \cdot c}} \\ &= \overline{\overline{a \cdot (b \cdot c)}} \qquad (14.1) \\ &= \overline{a} \cdot \overline{\overline{b \cdot c}} \\ &= \overline{a} \cdot (\overline{b} \cdot \overline{c}).\end{aligned}$$

Every line is by definition of $\cdot$, except for (14.1) which uses associativity of multiplication for the integers. Commutativity holds because

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{b \cdot a} = \overline{b} \cdot \overline{a}.$$

Note the middle equality is just commutativity for multiplication for the integers. The unit is 1 because $\overline{a} \cdot \overline{1} = \overline{a \cdot 1} = \overline{a}$.

(3) Distributivity holds because

$$\begin{aligned}\overline{a} \cdot (\overline{b} + \overline{c}) &= \overline{a} \cdot \overline{b + c} \\ &= \overline{\overline{a \cdot (b + c)}} \\ &= \overline{\overline{ab + ac}} \qquad (14.2) \\ &= \overline{\overline{ab}} + \overline{\overline{ac}} \\ &= \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}.\end{aligned}$$

Again, every line is by definition, except (14.2) uses distributivity for the usual integers.

□

14.4 Motivation for Commutative Rings

There is now a philosophy in modern math that properties of spaces can be discerned from properties of their set of functions. For instance, by studying the set of polynomial functions on a space X, one can discern properties about the space X itself. And in fact, every set of functions is always a commutative ring. It is the properties of these rings that determine certain properties of the space X. This is by no means obvious, and some of the most meaningful developments in this direction have only come since the late 1880's——that is nearly two hundred years after Descartes first noticed that algebraic equations can describe concrete geometry. So if you consider that algebra (from the so-called Golden Age of Islam in the 800's-plus) and geometry (from the Greeks) took nearly a thousand years for Descartes to synthesize, and it took us an even two hundred more years to develop a systematic way to understand that rings are a powerful way to study geometry, you might realize you're setting foot on some pretty rad ideas. We won't be able to even begin to penetrate this narrative——of using rings to study geometry——but if you're interested, you can do some reading on commutative algebra and algebraic geometry.

14.5 Examples of Non-commutative Rings

Example 14.5 (Matrix Rings)**.** Fix an integer $n \geqslant 0$ and consider the set $M_{n\times n}(\mathbb{R})$ of all $n \times n$ matrices with entries in $\mathbb{R}$. You can add and multiply matrices, and multiplication of matrices distributes over addition. Hence $M_{n\times n}(\mathbb{R})$ is a ring. To see distributivity explicitly, consider three matrices A, B, C with entries a_{ij}, b_{ij}, c_{ij}. Then the ijth entry of $A(B + C)$ is given by

$$\sum_{k=1}^{n} a_{ik}(b_{kj} + c_{kj}) = \sum_{k=1}^{n} a_{ik}b_{kj} + \sum_{k=1}^{n} a_{ik}c_{kj}$$

but this right hand side is the ijth entry of $AB + AC$. You can likewise show $(B + C)A = BA + CA$.

Example 14.6 (Group Rings)**.** Let G be finite group, and let R be a commutative ring. Then $R[G]$ as a set is the set of all functions from G to R. (So every element $g \in G$ is associated an element $r_g \in R$.) We write such a function as the summation

$$\sum_{g \in G} r_g g.$$

As an example, here is an example of an element of $\mathbb{Z}[S_3]$:

$$5() + 3(12) - 8(123).$$

Addition is the obvious addition——we just add component-wise, so

$$\left(\sum r_g g\right) + \sum (s_g g) = \sum_{g \in G} (r_g + s_g) g.$$

i.e., this is just the addition of functions. Multiplication is not just multiplication of functions. The product of $\sum r_g g$ and $\sum s_g g$ has the coefficient of g given by

$$\sum_{(g_1, g_2) \text{ s.t. } g_1 g_2 = g} r_{g_1} s_{g_2}.$$

Put another way,

$$\left(\sum_{g \in G} r_g g\right)\left(\sum_{h \in G} s_h h\right) = \sum_{g \in G} \sum_{h \in H} r_g s_h (gh) = \sum_{k \in G} \left(\sum_{(g_1, g_2) \text{ s.t. } g_1 g_2 = g} r_g s_h \right) k.$$

Note that this multiplication is not commutative.

14.6 Homomorphisms of Rings

Definition 14.4. Let R and S be rings, and let $f : R \to S$ be a function. We say that f is a **ring homomorphism** if

(1) f is a group homomorphism for addition,

(2) $f(1) = 1$ (so f sends the multiplicative unit of R to that of S), and

(3) $f(ab) = f(a)f(b)$ for all $a, b \in R$.

Definition 14.5. We further say f is an **isomorphism** if f is a bijection.

Now I wanted to say something more about why $\mathbb{Z}/n\mathbb{Z}$ is a ring. How did we see it was a group? By applying a general principle: If $H \triangleleft G$, then G/H is a group.

I want to do the same thing with rings. But for this context, when we say ring, we will mean a commutative ring.

Chapter 15

Ideals and Quotients

15.1 Ideals

You might think something along the lines of: If $S \subset R$ is a "normal" subring, then R/S is going to be some ring. That's the blind analogy to groups. Well, that analogy is wrong.

Definition 15.1. Let R be a commutative ring. A subset $I \subset R$ is called an **ideal** if

(1) I is a subgroup under addition, and

(2) $x \in I$ implies $rx \in I$ for all $r \in R$.

Remark. Note that (2) implies that if $x, y \in I$, then $xy \in I$. So it looks like a closure condition for being a subobject. But I need not have the multiplicative identity of R, so I is definitely not a subring. What (2) is really saying, heuristically, is that I sucks every element of R into I via multiplication.

Proposition 15.1. For every non-zero integer n, let $n\mathbb{Z} \subset \mathbb{Z}$ be those integers which are multiples of n. $n\mathbb{Z}$ is an ideal inside the ring $\mathbb{Z}$.

Proof. (1) $n\mathbb{Z}$ contains 0, and if two numbers are divisible by n, so its their sum. Likewise, if a is divisible by n, so is $-a$. So $n\mathbb{Z}$ is a subgroup under addition. (2) Finally, if r is any integer and x is divisible by n, then rx is divisible by n. □

Remark. Since R is abelian, note that any subgroup I is normal. So there is an abelian group R/I.

Proposition 15.2. Let R be a commutative ring, and $I \subset R$ an ideal. Then the operation

$$\times : R/I \times R/I \to R/I, \qquad \overline{r} \cdot \overline{s} = \overline{rs}$$

along with the usual addition on R/I, makes R/I a commutative ring.

Proof. We need to show that this operation doesn't depend on the choice of representative $r \in \overline{r}$, $s \in \overline{s}$.

So let $r' = r + x$ and $s' = s + y$ where $x, y \in I$. (This just means $\overline{r'} = \overline{r} \in R/I$, and that $\overline{s'} = \overline{s} \in R/I$.) Then

$$r's' = (r + x)(s + y) = rs + xs + ry + xy.$$

Note the last three terms are in I because I is an ideal, and hence their sum is in I because I is a subgroup. So $\overline{r's'} = \overline{rs}$. That is, the operation is well-defined.

We already know that $(R/I, +)$ is an abelian group. So we need to show that $(R/I, \times)$ is an abelian monoid, and that multiplication distributes over addition.

Well, multiplication is associative because

$$(\overline{a}\overline{b})\overline{c} = \overline{ab}\overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a}(\overline{b}\overline{c}).$$

Note that the key step there was invoking the fact that $(R, \times)$ is associative.

It is commutative because

$$\overline{a}\overline{b} = \overline{ab} = \overline{ba} = \overline{b}\overline{a}$$

where again, the middle equality is just using that $(R, \times)$ is commutative.

The multiplicative unite is $\overline{1}$:

$$\overline{1}\overline{a} = \overline{1a} = \overline{a}, \quad \overline{a}\overline{1} = \overline{a1} = \overline{a}.$$

Finally, multiplication distributes over addition because

$$\overline{a}(\overline{b} + \overline{c}) = \overline{a(b+c)} = \overline{ab + bc} = \overline{a}\overline{b} + \overline{b}\overline{c}.$$

□

So to get new and interesting rings, we can look for ideals and then take quotient rings.

Example 15.1. The rings $\mathbb{Z}/n\mathbb{Z}$ is the quotient ring of $\mathbb{Z}$ by the ideal $I = n\mathbb{Z}$.

Example 15.2. $\mathbb{Z} \subset \mathbb{Q}$ is a subgroup, and a subring in fact, but it is definitely not an ideal. This is because if x is an integer and r is a rational number, rx need not be an integer. In fact, subrings are usually not ideals.

15.2 Examples of Ideals and Quotient Rings

Definition 15.2. Let $x \in R$ be an element of a commutative ring. Then ideal generated by x is the subset of all elements of the form rx for some $r \in R$. We write (x) for this ideal.

Proposition 15.3. This is an ideal.

Proof. Let $I = (x)$. I is closed under addition because $rx + sx = (r + s)x \in I$. It contains the additive identity since $0x = 0$. It contains inverses because $-(rx) = (-r)x$. So I is a subgroup under addition. Finally, if $s \in R$ and $rx \in I$, we have that $s(rx) = (sr)x \in I$. □

Example 15.3. Let $R = \mathbb{R}[t]$ be the ring of polynomials in one variable t. Consider the ideal I generated by the polynomial $t^2 + 1$. So

$$I = \{f(t) \text{ such that } f(t) = g(t)(t^2 + 1) \text{ for some polynomial } g(t) \in \mathbb{R}[t].\}$$

Then what is the ring R/I?

Proposition 15.4. The ring $\mathbb{R}[t]/(t^2 + 1)$ is isomorphic to $\mathbb{C}$.

How cool is that? In general, when you have a ring R and you quotient out its polynomial ring by some equation, you "add on" an element to R that satisfies that polynomial equation. This is the beginnings of Galois theory.

15.3 Ideals Geometrically

Question: How should you think of ideals?

Algebraically: A subgroup closed under scaling. $I \subset R$, s.t.

- $rx \in I$, $\forall x \in I$, $r \in R$.
- $(I, +) \subset (R, +)$ subgroup.

You might find this unenlightening. So

Geometrically: Let $R = \{\text{continuous functions from a space } X \text{ to } \mathbb{R}\}$. This R is a ring because

- sum of continuous functions is continuous,
- product of continuous functions is continuous,
- the zero function is the additive identity

$$(0 + f)(x) = 0(x) + f(x) = f(x)$$

So $0 + f = f$. (Likewise, $f = f + 0$.)

- the constant function $1 : x \mapsto 1_{\mathbb{R}}$ is the multiplicative unit
$$(1 \cdot f)(x) = 1(x) \cdot f(x) = 1_{\mathbb{R}} \cdot f(x) = f(x)$$
So $1 \cdot f = f$. (Likewise, $f \cdot 1 = f$.)
- $-f$ sends $x \mapsto -f(x)$, is additive inverse.
- $f \cdot (g + h) : x \mapsto f(x)((g + h)(x)) = f(x)(g(x) + h(x))$, so $f(g + h) = fg + fh$.
$= f(x)g(x) + f(x)h(x)$
- associativity can also be checked easily.

Okay, so $R = \{\text{Continuous functions}\}$.

Let $Y \subset X$ be a subset and define
$$I_Y = \{\text{functions } f \in R \text{ such that } f(y) = 0, \forall y \in Y\}.$$
i.e., $I_Y = \{\text{functions vanishing on } Y\}$.

Proposition 15.5. $I_Y \subset R$ is an ideal.

Proof. Let $f_1, f_2 \in I_Y$. Then $\forall y \in Y$,
$$(f_1 + f_2)(y) = f_1(y) + f_2(y) = 0 + 0 = 0$$
So $f_1 + f_2 \in I_Y$. Likewise,
$$(-f_1)(y) = -f_1(y) = -0 = 0.$$
So $-f_1 \in I_Y$. (Note this implies $0 \in I_Y$. But more straightforwardly, $0(y) = 0$, $\forall y \in Y$, so $0 \in I_Y$.) So $I_Y \subset R$ is a subgroup. We just need to check it's closed under scaling by R.

Given $g \in R$, $f \in I_Y$,
$$\underset{\in R}{(\underbrace{g \cdot f}_{\in})}(y) = \underset{\in R}{\underbrace{g(y) \cdot f(y)}_{\in}} = g(y) \cdot 0 = 0$$
So $gf \in I_Y$. □

Upshot: Every subset $Y \subset X$ gives rise to an ideal $I_Y \subset R$.

Remark. The fact that this example should become a paradigm is not obvious. For example, how do you think of $\mathbb{Z}$ as "functions on some space X"? How is the ideal $p\mathbb{Z}$ gives by some "subset" of X?

Regardless, this kind of thinking has had huge influence on differential geometry, number theory (imagine being able to talk about the geometry of prime numbers!), etc.

Moreover, if we have $Y \subset X$, we should be able to talk about functions on Y——another ring!
Philosophy: Let Y give rise to the ideal I_Y. Then
$$\{\text{functions on } Y\} \cong R/I_Y.$$

Example 15.4 (We deviate from all continuous functions, and just examine polynomial functions.)**.** Let $R = \mathbb{R}[x, y] = \{\text{polynomial functions on } \mathbb{R}^2\}$. Let $Y = \{(x, y) \text{ s.t. } y^2 - x = 0\}$. Then
$$I_Y = \{\text{polynomials } f \text{ such that } f(y^2, y) = 0\} \overset{\text{not obvious}}{=\!=\!=} (y^2 - x)$$
where $(y^2 - x)$ is the ideal generated by the element $y^2 - x \in R$. Roughly, if $f(x, y)$ vanishes on Y, it must be factored by $y^2 - x$. Then
$$\{\text{algebraic/polynomial functions on } Y\} \cong R/(y^2 - x).$$
So why? If f_1, f_2 are functions on X, they restrict to functions on Y. But
$$\begin{gathered} f_1(y) = f_2(y), \quad \forall y \in Y \\ \Updownarrow \\ f_1(y) - f_2(y) = 0, \quad \forall y \in Y \\ \Updownarrow \\ f_1 - f_2 \in I_Y \end{gathered}$$
i.e., f_1 and f_2 define the same function on Y if and only if $[f_1] = [f_2] \in R/I_Y$.

Chapter 16

Fields

16.1 Basic Concept of Fields

Definition 16.1. A commutative ring is called a **field** if $R - \{0\}$ is a group under multiplication.

Example 16.1. $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ are fields, since every non-zero element has a multiplicative inverse.

Example 16.2. $\mathbb{Z}$ is not a field, since any integer that's not ± 1 does not admit a multiplicative inverse.

16.2 Subfields

16.3 Prime Fields

16.4 Characteristic of Fields

16.5 Field Extensions

Chapter 17

Modules

17.1 Modules

Just as groups act on sets, rings act on abelian groups. When a ring acts on an abelian group, that abelian group is called a **module** over that ring.

Now, when a group acts on a set, it had to act by bijections, so it had to respect the property, for instance, of the **cardinality** of the set. But for a ring to act on an abelian group, it respects a different structure——the structure of addition built into the abelian group. This is condition (1) in the definition below.

In this context, we'll set up all the definitions for the algebra of modules, just as we did for groups.

Definition 17.1. Let R be a ring, and let M be an abelian group. A **left action** of R on M is a function

$$\begin{aligned} R \times M &\to M, \\ (r, m) &\mapsto rm \end{aligned}$$

such that for all $r, s \in R$ and $m, m' \in M$, we have

(1) $r(m + m') = rm + rm'$.

(2) $(r + s)m = rm + sm$.

(3) $s(rm) = (sr)m$.

(4) $1m = m$.

When a left action of R on M is specified, we say that M is a **left R-module**.

Remark. Again, you should think of "multiplying by r" as scaling by some ring element. So a module is just some set with an addition, together with a notion of scaling by r.

There's a much more succinct way to put all this. The above is the same data as a ring homomorphism $R \to \mathrm{End}(M)$.

A right R-module is an abelian group M together with a function $M \times R \to M$ satisfying the analogies of (1)-(4) above.

Now this might seem like a lot of data, because we have both R and M floating around. In practice, we often fix a single ring R, and just study relationships between the different M.

Exercise. Let M be a left R-module. Then

$$0m = m \quad \text{and} \quad (-r)m = -(rm).$$

Proof. For emphasis, we will write 0_R to denote the zero element of R. Then we have by (2), we have that

$$0_R m = (0_R + 0_R)m = 0_R m + 0_R m$$

so by the cancellation law, we have that

$$0 = 0_R m$$

where on the left hand side, 0 is the additive identity of M. Similarly,

$$rm + (-r)m = (r - r)m = 0_R m = 0.$$

□

Example 17.1.

(a) Let $R = \mathbb{R}$, and let $M = \mathbb{R}^n$, an n-dimensional vector space over the real numbers. Then we have a function

$$\mathbb{R} \times M \to M, (t, v) \quad \mapsto t\vec{v}$$

i.e. we scale by t. So if $\vec{v} = (v_1, \ldots, v_n)$,

$$t\vec{v} = (tv_1, \ldots, tv_n).$$

This satisfies all the properties above.

(b) Any ring R is a left module over itself.

(c) This is an example that departs from the naivete of "scaling," and hits closer to home to the notion of "acting". Let $\mathbb{R}[t]$ be the polynomial ring over $\mathbb{R}$ with variable t. Choose an $m \times m$ matrix T, which we think of as a linear map $T : \mathbb{R}^m \to \mathbb{R}^m$. Then $\mathbb{R}^m$ is a left $\mathbb{R}[t]$-module by the action

$$(a_0 + a_1 t + \cdots + a_k t^k)v := a_0 v + a_1 T(v) + \cdots + a_k (T \circ \cdots \circ T)(v)$$

where the composition $T \circ \cdots \circ T$ happens k times.

17.2 Submodules

Definition 17.2. Let R be a ring and let M be a left R-module. Then an abelian subgroup $M' \subset M$ is called a submodule of M if for every $r \in R$, we have

$$x \in M' \;\Rightarrow\; rx \in M'$$

Example 17.2.

(a) If $R = \mathbb{R}$ and $M = \mathbb{R}^n$, a submodule is a subset closed under addition, inverses and scaling. This is the same thing as a linear subspace of $\mathbb{R}^n$.

(b) Let R be a commutative ring. Then $I \subset R$ is an ideal if and only if it is a submodule of R.

(c) Let $M = \mathbb{R}^m$ be a module over $\mathbb{R}[t]$ given by a linear transformation $T : \mathbb{R}^k \to \mathbb{R}^k$. Then a submodule is a linear subspace V such that $T(V) \subset V$. In other words, it is a T-invariant subspace of V.

17.3 Module Homomorphisms

Definition 17.3. Let M and N be left R-modules. Then an R-module homomorphism, or a **map of R-modules**, or a **module homomorphism**, is a function

$$f : M \to N$$

such that f is a group homomorphism, and

$$f(rx) = rf(x)$$

for all $r \in R$, $x \in M$

Definition 17.4. An R-module **isomorphism** is a homomorphism which is a bijection.

Definition 17.5. The **kernel** and **image** of an R-module homomorphism $f : M \to N$ is the kernel and image of f as a group homomorphism.

This means $\ker(f) = \{x \text{ such that } f(x) = 0\}$ and $\text{im}(f) = \{y \in N \text{ such that } y = f(x) \text{ for some } x \in M\}$.

Example 17.3.

(a) Let $M \cong \mathbb{R}^n$ and $N \cong \mathbb{R}^m$ with the scaling module structure over $\mathbb{R}$. Then a linear map $M \to N$ is a homomorphism of $\mathbb{R}$-modules.

(b) (No obvious example following example (b) from before.)

(c) Let $M = \mathbb{R}^m$ be a left module over $R = \mathbb{R}[t]$, given by a linear transformation T. Let $N = \mathbb{R}^n$ be a left module over $\mathbb{R}[t]$ given by a linear transformation $S : \mathbb{R}^n \to \mathbb{R}^n$. Then an R-module homomorphism is a linear map

$$f : \mathbb{R}^m \to \mathbb{R}^n$$

with the property that

$$f(T(v)) = S(f(v)).$$

Definition 17.6. Let M and N be left R-modules. Then the set of all R-module homomorphisms is denoted

$$\text{Hom}_R(M, N).$$

Proposition 17.1. $\text{Hom}_R(M, N)$ is a left R-module.

Proof. Definition of Scalar Multiplication:
For $r \in R$ and $f \in \text{Hom}_R(M, N)$, define the scalar multiplication $r \cdot f$ by:

$$(r \cdot f)(m) = rf(m), \quad \text{for all } m \in M.$$

Verification that $r \cdot f$ is an R-Module Homomorphism:
1. Additivity:

$$\begin{aligned}(r \cdot f)(m_1 + m_2) &= rf(m_1 + m_2) \\ &= r[f(m_1) + f(m_2)] \\ &= rf(m_1) + rf(m_2) \\ &= (r \cdot f)(m_1) + (r \cdot f)(m_2).\end{aligned}$$

Thus, $r \cdot f$ is additive.
2. Compatibility with Scalar Multiplication: For all $s \in R$ and $m \in M$:

$$\begin{aligned}(r \cdot f)(sm) &= rf(sm) \\ &= r[sf(m)] \\ &= s[rf(m)] && \text{(since } R \text{ is commutative)} \\ &= s(r \cdot f)(m).\end{aligned}$$

Therefore, $r \cdot f$ is R-linear.
Verification of Module Axioms:
1. Distributivity over Ring Addition:

$$\begin{aligned}((r + s) \cdot f)(m) &= (r + s)f(m) \\ &= rf(m) + sf(m) \\ &= (r \cdot f + s \cdot f)(m).\end{aligned}$$

2. Distributivity over Module Addition:

$$\begin{aligned}(r \cdot (f + g))(m) &= r(f + g)(m) \\ &= r[f(m) + g(m)] \\ &= rf(m) + rg(m) \\ &= (r \cdot f)(m) + (r \cdot g)(m).\end{aligned}$$

3. Associativity of Scalar Multiplication:

$$\begin{aligned}((rs)\cdot f)(m) &= (rs)f(m)\\ &= r(sf(m))\\ &= r\cdot(s\cdot f)(m).\end{aligned}$$

4. Identity Element:

$$(1_R\cdot f)(m) = 1_R f(m) = f(m).$$

Conclusion:
Since all module axioms are satisfied, $\mathrm{Hom}_R(M,N)$ is a left R-module under the scalar multiplication defined above. □

17.4 Direct Sums and Free Modules

Definition 17.7. Let M and N be left R-modules. Then we define the **direct sum**

$$M\oplus N$$

to be equal to $M\times N$ as a group, and to have the R-module structure

$$r(m,n) := (rm, rn).$$

Proposition 17.2. $M\oplus N$ is an R-module.

Proof. We know it's an abelian group. On the other hand,

$$1(m,n) := (1m, 1n) = (m,n)$$

since M and N are modules. And we have

$$\begin{aligned}r((m,n)+(m',n')) &= r(m+m', n+n')\\ &= (r(m+m'), r(n+n'))\\ &= (rm+rm', rn+rn') \qquad (3)\\ &= (rm,rn)+(rm',rn')\\ &= r(m,n)+r(m',n').\end{aligned}$$

Note (3) is where we used that M and N are left R-modules. □

Example 17.4. If $R=\mathbb{R}$, and M and N are also $\mathbb{R}$ considered as a module over itself, then

$$\mathbb{R}\oplus\mathbb{R}\cong\mathbb{R}\times\mathbb{R}\cong\mathbb{R}^2$$

as a group, and we have the usual scaling actions

$$r(x_1,x_2) = (rx_1, rx_2).$$

Remark. We have an obvious isomorphism

$$(M\oplus N)\oplus O\cong M\oplus(N\oplus O),\quad (m,n,o)\mapsto(m,n,o).$$

Definition 17.8. Let R be a ring. Then the direct sum module

$$R^n := R\oplus\cdots\oplus R$$

is called the **free R-module of rank n**.

17.5 Universal Property of Free Modules

Question: Why is this called a free R-module?

Proposition 17.3. Let M be an R-module. Then any ordered n-tuple of elements $x_1, \ldots, x_n \in M$ uniquely determines an R-module homomorphism

$$X : R^n \to M$$

given by

$$(0, \ldots, 0, 1, 0, \ldots, 0) \mapsto x_i$$

where the 1 is in the i^{th} coordinate.

Remark. This is the same property as for the free group on n generators: Any ordered n-tuple of elements of a group G determines a unique map from F_n to G.

Proof. Given $(x_1, \ldots, x_n)$, define $X : R^n \to M$ by

$$X(a_1, \ldots, a_n) := a_1x_1 + \cdots + a_nx_n \in M.$$

This is a group homomorphism because

$$\begin{aligned} X((a_1, \ldots, a_n) + (b_1, \ldots, b_n)) &= (a_1 + b_1)x_1 + \cdots + (a_n + b_n)x_n \\ &= (a_1x_1 + \cdots + a_nx_x) + (b_1x_1 + \cdots + b_nx_n) \\ &= X(a_1, \ldots, a_n) + X(b_1, \ldots, b_n). \end{aligned}$$

where the middle equality is using the property of M being an R-module. This is also an R-module homomorphism because

$$\begin{aligned} X(r(a_1, \ldots, a_n)) &= X((ra_1, \ldots, ra_n)) \\ &= (ra_1)x_1 + \cdots + (ra_n)x_n \\ &= r(a_1x_1 + \cdots + a_nx_n) \\ &= rX((a_1, \ldots, a_n)). \end{aligned}$$

Again, the penultimate equality is using the fact that M is an R-module. □

17.6 Free Module on 0 generators

Exercise. Let M be a left R-module. Show that

$$r0_M = 0_M, \quad \text{and} \quad r(-x) = -rx.$$

Proof. An R-action on M is the same thing as a ring homomorphism $R \to \text{End}(M)$. In particular, every $r \in R$ determines an abelian group homomorphism. Hence scaling by r preserves the additive identity of M, and additive inverses.

If you prefer a more computational proof, you can observe

$$r0_M + r0_M = r(0_M + 0_M) = r0_M.$$

So by cancellation for abelian groups, we can subtract $r0_M$ from both sides to obtain

$$r0_M = 0_M.$$

So

$$r(-x) + rx = r(-x + x) = r0_M = 0_M,$$

which shows that $r(-x)$ is the additive inverse to rx. □

Remark. We know what $R^{\oplus n}$ is for $n \geqslant 1$. But what about $n = 0$?

Well, we should look for an R-module $R^{\oplus 0}$such that there is a bijection

$$\text{Hom}_R(R^{\oplus 0}, M) \cong \text{Map}_{\text{Sets}}(\varnothing, M).$$

But there is one and only one function from the empty set to any set. So we must look for a module $R^{\oplus 0}$ which has one and only one module homomorphism to any M. The only such module is the zero module——i.e., the trivial abelian group with the module action $r0 = 0$.

Chapter 18

Vector Spaces

18.1 Spans and Linear Independence and Bases

Definition 18.1. Fix $x_1, \ldots, x_n \in M$.

(1) We say this collection **spans** M if the map $X : R^n \to M$ is a surjection.

(2) We say that this collection is **linearly independent** in M if the map $X : R^n \to M$ is an injection.

(3) We say this collection is a **basis** for M if X is both an injection and a surjection.

You'll recognize these terms from linear algebra. And in terms of equations, these definitions mean exactly what you'd imagine:

Proposition 18.1. Let M be a left R-module, and let $x_1, \ldots, x_n \in M$ be an ordered collection.

(1) The collection spans M if and only if for every $y \in M$, there exists a collection $a_1, \ldots, a_n \in R$ so that
$$y = a_1x_1 + \cdots + a_nx_n.$$

(2) The collection is linearly independent if and only if the equation
$$0 = a_1x_1 + \cdots + a_nx_n$$
has one and only one solution: $(a_1, \ldots, a_n) = (0, \ldots, 0)$.

(3) The collection is a basis if and only if for any $y \in M$, the equation
$$y = a_1x_1 + \ldots + a_nx_n$$
has one and only one collection $(a_1, \ldots, a_n)$ solving it.

Proof. The first is the definition of surjection. The latter claim follows because a homomorphism is injective if and only if the kernel is trivial, and $(0, \ldots, 0) \in R^n$ is the additive identity of R^n. The last claim is the definition of a bijection. □

Definition 18.2. We say that a module is finitely generated if there is some number $n \in \mathbb{Z}_{\geqslant 0}$ and a surjective R-module homomorphism $R^n \to M$.

This is also in analogy to groups. A group G is finitely generated if and only if there is some finite collection of elements g_i such that all other elements can be expressed as products of g_i and their inverses. Likewise, M is finitely generated if there is a finite collection x_i such that every element of M can be obtained by taking linear combinations of x_i.

Example 18.1. Not every module over R admits a basis. This is in contrast to vector spaces. For example, if $R = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$, then for any $x \in M$, the equation
$$ax = 0$$
has many solutions——a could equal $n, 2n, \ldots$.

Take-away: Not every finitely generated R-module admits a basis.

18.2 Vector Spaces and Subspaces

Definition 18.3. A commutative ring is called a **field** if $R - \{0\}$ is a group under multiplication.

Definition 18.4. Let F be a field. A module over F is called a **vector space** over F.

Definition 18.5. Let V be a vector space. Then a submodule of V is called a linear subspace of V.

18.3 Spanning Sets are Bigger Than Independent Sets

The following is the most importance consequences of being a field, as opposed to a ring:

Theorem 18.2. Let F be a field, and let M be a vector space over F. If $v_1, \ldots, v_n$ span and $w_1, \ldots, w_m$ are linearly independent, then $n \geqslant m$.

Proof. Let $y_1, \ldots, y_m$ be linearly independent, and let $v_1, \ldots, v_n$ be spanning. By re-ordering v_i if necessary, we can assume that

$$y_1 = a_1 v_1 + \ldots + a_n v_n$$

for $a_1 \neq 0$. Then $y_1, v_2, \ldots, v_n$ is also spanning, for we can obtain v_1 as a linear combination of the y_1 and the v_i——just divide the above equation by $a_1 \neq 0$ and rearrange terms.

Let $M_1 \subset M$ be the submodule generated by y_1——i.e., the image of $R \to M$ defined by $1 \mapsto y_1$—— and consider the quotient

$$M/M_1$$

(It can be proved that this is also an R-module——i.e., a vector space.) Then $\overline{y_2}, \ldots, \overline{y_m}$ are still linearly independent, for a linear combination of them equals zero if and only if

$$a_1 y_1 = a_2 y_2 + \ldots + a_m y_m$$

for some $a_1 \in F$, and such an equation can hold only when all the $a_i = 0$, since the y_i are assumed linearly independent. Note $\overline{y_1} = 0, \overline{v_2}, \ldots, \overline{v_n}$ are still spanning, so $\overline{v_2}, \ldots, \overline{v_n}$ is spanning. So we have $n - 1$ vectors spanning M/M_1, and we have $m - 1$ linearly independent vectors in it.

By repeating the trick above, if we have m linearly independent elements in a vector space spanned by n elements, we can obtain $m - k$ linearly independent elements in a quotient vector space spanned by $n - k$ elements. So which of these numbers will hit 0 first? If $n - k = 0$ first, we are in a quotient vector space spanned by 0 elements—— i.e., the zero vector space——so we must conclude $m - k = 0$ as well, for there are no linearly independent vectors in the zero vector space. And in this case, $m = n$. If $m - k$ reaches zero before $n - k$ does, we have that $m \leqslant n$. □

18.4 Dimension

Corollary 18.3. If M is a finitely generated vector space, then any two bases of M have the same number of elements in it.

Proof. If the $\{v_i\}$ and $\{w_i\}$ above are both spanning and linearly independent, we have $n \geqslant m$ and $m \geqslant n$. Hence $m = n$. □

Definition 18.6. Let V be a finitely generated F-module——i.e,. a finitely generated vector space. We call such a V a **finite-dimensional** vector space, and define the **dimension** of V

$$\dim_F V$$

to be the number of elements in any basis for V.

Remark. This is the single most important fact in linear algebra: That we have a notion of dimension. It took us thousands of years to know what we mean by an n-dimensional space, so don't take this lightly!

Example 18.2. The 0-dimensional vector space is the module given by the trivial abelian group, $M = \{0\}$.

Corollary 18.4. If M is a finitely generated vector space, any linearly independent collection $w_1, \ldots, w_m$ can be completed to a basis——that is, we can find $w_{m+1}, \ldots, w_n$ so that the resulting collection $w_1, \ldots, w_n$ is both linearly independent and spanning.

Proof. Since M is finitely generated, there is some N for which we have a surjection $F^N \to M$. So any set of linearly independent vectors must have size $\leqslant N$ by the theorem. If $X_m : F^m \to M$ is the map determined by $w_1, \ldots, w_m$, and if X_m is not surjective, choose an element w_{m+1} not in $\operatorname{im}(X_m)$. Note the resulting collection $w_1, \ldots, w_{m+1}$ is still linearly independent, for if

$$a_1 w_1 + \ldots + a_{m+1} w_{m+1} = 0$$

then we have

$$a_1 w_1 + \ldots + a_m w_m = -a_{m+1} w_{m+1}$$

If $a_{m+1} = 0$, by linear independence of the w_i, we know all $a_i = 0$. On the other hand, if $a_{m+1} \neq 0$ we arrive at a contradiction by dividing:

$$\frac{a_1}{-a_{m+1}} w_1 + \ldots + \frac{a_m}{-a_{m+1}} w_m = w_{m+1}$$

The left hand side is in the image of X_m, but w_{m+1} was chosen not to be.

So we have an injective homomorphism $X_{m+1} : F^{m+1} \to M$. If X_{m+1} is not surjective, we repeat the argument. It must become a surjective map at some $m + k \leqslant N$ by the theorem. So let k be the integer at which X_{m+k} first becomes a surjection. By the above argument, it is still an injection, so we have a basis determined by the generators $w_1, \ldots, w_{m+k}$. □

18.5 Some Corollaries

What are we going to do? Well, you have studied matrices whose entries are real numbers before. You did a lot with them-multiply them, add them, and also figure out when they're invertible. I claim that almost everything you could do with real matrices, you can pretty much do with matrices with coefficients in any field.

Corollary 18.5. Any finitely generated module over a field F is isomorphic to F^n for some n.

Proof. Begin with the linearly independent set 0 and complete to a basis. A basis defines an isomorphism from F^n to your module. □

Remark. This is definitely not true for R-modules if R is not a field——after all, any finite abelian group is a $\mathbb{Z}$-module, but any free $\mathbb{Z}$-module is the zero module or an infinite module.

Corollary 18.6. If $V' \subset V$ is a subspace,

$$\dim V' = \dim V \quad \Leftrightarrow \quad V = V'.$$

Proof. One implication is obvious. For the other direction, let $y_1, \ldots, y_n$ be a basis for V'. Since these vectors are linearly independent, they can be completed to a basis in V by one of the corollaries above. But this basis must have exactly n elements in it by the definition of dimension——in other words, the y_i are already a basis. □

Corollary 18.7. Let $V' \subset V$ be a subspace. Then $\dim V' + \dim V/V' = \dim V$.

Proof. Let $v_1, \ldots, v_{\dim V'}$ be a basis for V'. Let $\overline{u_1}, \ldots, \overline{u_{\dim V/V'}}$ be a basis for V/V'. Then choosing representatives u_i for $\overline{u_i}$, the set

$$v_1, \ldots, v_{\dim V'}, u_1, \ldots, u_{\dim V/V'}$$

is a basis for V. It obviously spans since for each $a \in V, \overline{a}$ is a linear combination of $\overline{u_i}$, hence a is in the V'-orbit of some linear combination of the u_i. It is linearly independent because if we have that

$$0 = a_1 v_1 + \cdots + a_{\dim V'} v_{\dim V'} + b_1 u_1 + \cdots + b_{\dim V/V'} u_{\dim V/V'}$$

then

$$\overline{0} = a_1 \overline{v_1} + \cdots + a_{\dim V'} \overline{v_{\dim V'}} + b_1 \overline{u_1} + \cdots + b_{\dim V/V'} \overline{u_{\dim V/V'}}$$

The a_i terms go to zero since $\overline{v_i} = 0$, hence we get an equation saying a linear combination of the $\overline{u_i}$ is zero. This means each b_i must be zero by linear independence of the $\overline{u_i}$. The original equation then says that $0 = \sum a_i v_i$, so by linear independence of the v_i, the a_i must be zero. □

Corollary 18.8 (Rank-nullity Theorem)**.** Let $f : V \to W$ be a map of F-modules and assume V is finitely generated. Then $\dim \ker f + \dim \mathrm{im} f = \dim V$.

Proof. By the first isomorphism theorem, we know there is a group isomorphism $V/\ker f \cong \mathrm{im} f$. But this homomorphism is also an F-module map, as you can check by hand. Thus $\mathrm{im} f \cong V/\ker f$. □

Corollary 18.9 (Criterion for isomorphisms)**.** Let $f : V \to W$ be a linear map between finite-dimensional vector spaces. Then f is an isomorphism if and only if f is injective and $\dim V = \dim W$.

Proof. By the rank-nullity theorem, the image of f has dimension V since f is injective. □

18.6 The Take-away

The take-away from all the above is how powerful the notion of dimension is. Whether your field be something familiar like $\mathbb{R}$, or something foreign (for now) like $\mathbb{Z}/p\mathbb{Z}$; whether the linear map be something as familiar as a matrix, or something that you didn't realize was linear like evaluating polynomial functions, we have a powerful way of studying linear maps.

18.7 Determinants

The other powerful tool we have from linear algebra is the notion of determinant. Well, the determinant only required a notion of multiplying by -1 (taking additive inverses), multiplying entries of a matrix, and adding things together. So we should be able to define a determinant for any matrix with coefficients in a ring R.

As it turns out, some formulas may not hold true if the ring R isn't commutative——the order of multiplication is important——so we'll restrict ourselves to commutative rings.

Definition 18.7. Let R be a commutative ring. A $k \times k$ **matrix** in R is a collection of elements

$$A_{ij} \in R$$

where $i \in 1, \ldots, k$ and $j \in 1, \ldots, k$. We'll represent a matrix by the symbol

$$A = (A_{ij}) .$$

Example 18.3. A 3×3 matrix in R can be drawn in the usual way:

$$\begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{pmatrix}$$

Definition 18.8. The **ring** of $k \times k$ matrices in R, denoted $M_{k\times k}(R)$, has addition given by

$$(A_{ij}) + (B_{ij}) = (A_{ij} + B_{ij}) \quad (A_{ij})\,(B_{ij}) = \left(\sum_{l=1}^{k} A_{il} B_{lj} \right)$$

That is, addition is the usual entry-by-entry addition. In the product, the i, jth entry is given by taking the jth column of B and pairing it with the ith row of A.

Definition 18.9 (Cofactor matrix)**.** Let A be a $k \times k$ matrix. The (i, j)th **cofactor matrix** of A is the matrix obtained by deleting the ith row and jth column of A. When A is implicit, we will write

$$C_{i,j}$$

for the $(k-1) \times (k-1)$ matrix given by the (i, j) th cofactor matrix of A.

Definition 18.10. The **determinant** of a 1×1 matrix in R is the unique element A_{11} of the matrix.

Inductively: Let A be a $k \times k$ matrix. Then the determinant of A is defined to be the sum

$$\det A = A_{11} \det C_{1,1} - A_{21} \det C_{2,1} + \cdots + (-1)^{1+k} A_{k1} \det C_{k,1}.$$

Using summation notation,

$$\det A := \sum_{i=1}^{k} (-1)^{i+1} A_{i1} \det C_{i,1}.$$

This defines a function

$$\det : M_{k\times k}(R) \to R.$$

Example 18.4. If A is a 2×2 matrix,

$$\det(A) = A_{11}A_{22} - A_{12}A_{21}$$

We won't prove the following theorems, but the same proofs you did for real numbers carries through:

Theorem 18.10. Let A and B be $k \times k$ matrices. Then

$$\det(A) \det(B) = \det(AB)$$

and

$$\det\left(A^{\mathrm{T}}\right) = \det(A).$$

Theorem 18.11. Let $\mathrm{adj}(A)$ be the $k \times k$ matrix whose (i, j)th entry is given by

$$(-1)^{i+j} \det C_{j,i}.$$

Then

$$A \cdot (\mathrm{adj}A) = (\mathrm{adj}A) \cdot A = \det A \cdot I$$

where $\det A \cdot I$ is the diagonal matrix with entries given by the element $\det A \in R$.

Remark. In case you haven't seen this last statement before, let me give a small idea of how the proof goes. The (i, j)th entry of the first multiplication is given by

$$\sum_{l=1}^{k} A_{il}(\mathrm{adj}A)_{lj} = \sum_{l=1}^{k} A_{il}(-1)^{j+l}\mathrm{det}C_{j,l}$$

So for instance, the $(1, 1)$ entry is precisely the definition of the determinant of A. By using properties about swapping rows only changing the determinant by a sign, you can prove that every diagonal entry is the determinant of A.

For the off-diagonal entry, you observe that the summation above becomes the determinant for a matrix with two equivalent rows; hence equals zero.

Corollary 18.12. Let $A \in M_{k\times k}(R)$. Then A is an invertible matrix if and only if $\det A \in R$ has a multiplicative inverse.

Proof. Let $B = \det A^{-1}\mathrm{adj}A$. Then

$$BA = \det A^{-1}\mathrm{adj}A \cdot A = \det A^{-1} \det A \cdot I = I.$$

Likewise for BA. □

Example 18.5. If A is a matrix with only integer entries, then there exists an inverse matrix with integer entries if and only if $\det A = \pm 1$.

Example 18.6. Let A be a matrix with entries in $\mathbb{Z}/n\mathbb{Z}$. It is invertible if and only if its determinant is relatively prime to n.

Chapter 19

PIDs

19.1 Polynomial Rings

Let F be a field. Let $F[t]$ be the ring of polynomials.

Theorem 19.1. If $I \subset F[t]$ is an ideal, $\exists p(t) \in F[t]$ such that

$$I = (p(t))$$

i.e., every ideal is generated by a single element.

Proof. If $I = (0)$, done. So we can assume $\exists$ elements of degree $\geqslant 0$. Let $p(t)$ be an element of I with least degree,

$$p(t) = a_0 + a_1 t + \cdots + a_d t^d, \quad d > -\infty.$$

Since $p(t) \in I$,

$$p(t) \subset I.$$

Now let $f(t) \in I$. Consider the division algorithm:

$$\begin{array}{r|l} & \frac{b_n}{a_d}t^{n-d} + \frac{Q_{n-1}}{a_d}t^{n-d-1} + \frac{Q_{n-2}}{a_d}t^{n-d-2} + \ \cdots \ + \frac{Q_{n-d}}{a_d}t^0 \\ a_d t^d + \cdots + a_1 t + a_0 & \begin{array}{l} b_n t^n \ + \ b_{n-1}t^{n-1} \ + \ \cdots \ + \ b_{n-d}t^{n-d} \ + \ b_1 t \ + \ b_0 \\ -b_n t^n \ + \ \frac{a_{n-1}b_n}{a_d}t^{n-1} \ + \ \cdots \ + \ \frac{a_0 b_n}{a_d}t^{n-d} \ + \ 0 \ + \ \cdots \ + \ 0 \\ \hline (Q_{n-1})t^{n-1} + \cdots + (\quad)t^{n-d} + \cdots + (\quad)t + (\quad) \\ -Q_{n-1}t^{n-1} + \frac{a_{n-1}Q_{n-1}}{a_d}t^{n-2} + \cdots + ()t^{n-d-1} + 0 + \cdots + 0 \\ \hline (Q_{n-2})t^{n-2} + \cdots \end{array} \end{array}$$

where $f(t) = b_n t^n + \cdots + b_0$ and $Q_{n-1} = b_{n-1} - (a_d)^{-1}a_{n-1}b_n$.

Then

$$f(t) = p(t)q(t) + r(t)$$

where $\deg(r(t)) < \deg(p(t))$. But $p(t)$ had least degree, so $r(t) = 0$. □

Definition 19.1. $f(t) \in F[t]$ is called **irreducible**, or **prime**, if

$$f(t) = a(t)b(t)$$

then either $a(t)$ or $b(t)$ is a constant polynomial. i.e., if no polynomial degree d, $0 < d < \deg f$, divides f.

Theorem 19.2. Any $f(t)$ admits a factorization into irreducible polynomials.

Proof. Prove by induction: For degree 0 (constant polynomials), $f(t)$ is either zero or a unit (invertible), so the factorization is trivial.

Assume every polynomial of degree less than n can be factored into irreducibles. For a polynomial $f(t)$ of degree n:

- If $f(t)$ is irreducible, we're done.
- If not, $f(t)$ can be written as $f(t) = g(t)h(t)$ with $\deg(g), \deg(h) < n$. By the inductive hypothesis, $g(t)$ and $h(t)$ can be factored into irreducibles.

Thus, any $f(t)$ can indeed be factored into irreducible polynomials over F. □

19.2 Similarities Between $\mathbb{Z}$ and $F[t]$

Exercise. Let R be a commutative ring, and let $x_1, \ldots, x_n$ be a finite collection of elements. Define for yourself the ideal generated by $x_1, \ldots, x_n$. Prove that it's an ideal.

Solution. Since we have n elements in R, they uniquely defined a module homomorphism

$$R^{\oplus n} \to R.$$

We let the ideal generated by $x_1, \ldots, x_n$ be the image of this homomorphism. The image of R is a submodule of R, and by definition, a submodule of R is an ideal.

Definition 19.2. We let $(x_1, \ldots, x_n) \subset R$ denote the ideal generated by the elements $x_1, \ldots, x_n$. Explicitly, it is the set of all elements in R that can be expressed as

$$a_1 x_1 + \ldots + a_n x_n$$

for $a_i \in R$.

Let F be a field. The point is to show that $\mathbb{Z}$ and $F[t]$ are very similar rings. This may be a surprising statement at first glance, but we'll see what we mean. Let me say one important thing: There is an analogy between

(1) The **size** of an integer (or the log of the size of an integer), and

(2) The **degree** of a polynomial.

For instance, for any two integers $x, y \in \mathbb{Z}$, we have that

$$\log(|xy|) = \log|x| + \log|y|.$$

And for any two polynomials in $F[t]$, we have that

$$\deg(fg) = \deg f + \deg g.$$

The size of integers allows us to use induction when we want to prove statements about all integers. Though we've taken log above, log preserves order, so the multiplicative property above is still useful for inductive proofs. Likewise, the degree of a polynomial will allow us to prove statements about all polynomials by induction.

19.3 Review of Preliminary Definitions

Definition 19.3. Let R be a commutative ring. A **zero divisor** is an element $x \in R$ such that

$$xy = 0$$

for some $y \neq 0$.

Example 19.1. Here are some simple examples:

(1) If R has more than one element, then 0 is always a zero divisor, since $0y = 0$ for any $y \in R$. (R needs to have more than one element to guarantee that y can be chosen to be non-zero.)

(2) If $R = \mathbb{Z}/n\mathbb{Z}$ where n is not prime, then choose two integers x, y so that $xy = n$, where neither x nor y is ± 1. Then $\overline{x}$ and $\overline{y}$ are zero divisors in R, for $\overline{x} \neq 0$, $\overline{y} \neq 0$, but $\overline{xy} = \bar{n} = 0$.

Definition 19.4. A commutative ring R is called a **principal ideal domain**, or **PID**, if

(1) If $I \subset R$ is any ideal, then $I = (x)$ for some $x \in R$.

(2) The only zero divisor in R is 0.

Remark. The word domain means there are no non-zero zero divisors. Sometimes you'll hear the term integral domain, which means a commutative ring with no non-zero zero divisors.

The "principal ideal" part of the term means that every ideal is "principal"——i.e., generated by one element.

Example 19.2. By far these are the two most important examples of principal ideal domains:

(1) $R = \mathbb{Z}$. We know any subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some n. Moreover, $n\mathbb{Z} = (n)$, since by definition, any element of $n\mathbb{Z}$ is of the form a for some integer a. Since any ideal is in particular a subgroup of R, we have that every ideal in $\mathbb{Z}$ is principal.

(2) $R = F[t]$ for F a field. Then $F[t]$ is a PID by a theorem, which I now recall:

Theorem 19.3. Let F be a field. Then any ideal $I \subset F[t]$ is generated by a single element.

Proof. Since F is a field, the polynomial ring $F[t]$ has the Division Algorithm: for any polynomials f, g with $g \neq 0$, there exist unique polynomials q, r in $F[t]$ such that $f = qg + r$, where either $r = 0$ or $\deg(r) < \deg(g)$.

Now, let I be any ideal in $F[t]$. If $I = \{0\}$, then I is generated by 0. If $I \neq \{0\}$, consider the set of degrees of nonzero polynomials in I:

$$D = \{\deg(f) \mid f \in I, f \neq 0\}.$$

Since D is a nonempty subset of $\mathbb{N}_0$, it has a minimal element d. Choose $g \in I$ such that $\deg(g) = d$. We claim that $I = (g)$, the ideal generated by g.

First, $(g) \subseteq I$ because I is an ideal and $g \in I$.

Conversely, for any $f \in I$, using the Division Algorithm, write $f = qg + r$ where $\deg(r) < \deg(g)$ or $r = 0$. Since $f, qg \in I$ (because I is an ideal), it follows that $r = f - qg \in I$. If $r \neq 0$, then $\deg(r) < \deg(g) = d$, which contradicts the minimality of d. Therefore, $r = 0$, so $f = qg$ is in (g).

Thus, $I = (g)$, showing that every ideal in $F[t]$ is principal. □

19.4 The Euclidean Algorithm

One major reason that $\mathbb{Z}$ and $F[t]$ are such similar rings is that they both have a division-remainder algorithm, or the Euclidean algorithm. Recall the following statement, which we have known since the cradle:

Theorem 19.4 (Divisions and Remainders for Integers)**.** Let x be an integer, and n any other integer. Then there exists integers q, r such that

$$x = nq + r$$

where $0 \leqslant r < n$.

Remark. We used this heavily when we proved that the only subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$.

The following is the analogous statement for polynomials, where (log of) the size of an integer is replaced by the degree of a polynomial.

Theorem 19.5. Let F be a field, and $g \in F[t]$ a polynomial with coefficients in F. Then for any polynomial $f \in F[t]$, there exists polynomials q, $r \in F[t]$ so that

$$g = fq + r$$

where $0 \leqslant \deg r < \deg f$.

Remark. That is, we can always divide a polynomial g by another polynomial f, and look at the remainder.

Proof. If $\deg g < \deg f$, we are finished, simply by setting

$$g = f0 + g.$$

That is, we can't divide a smaller-degree polynomial by a bigger-degree polynomial, so we just end up dividing trivially, and the remainder is g itself. So we need to prove the case when $\deg g \geqslant \deg f$.

We proceed by induction on the degree of the polynomial g. That is, having fixed f, we have seen that the statement is true for all g with $\deg g < \deg f$ (the base cases). We will assume it true for all g with $\deg g \leqslant e-1$, and prove it true for those g with $\deg g = e$.

Let

$$f = a_d t^d + \ldots + a_1 t + a_0, \quad a_d \neq 0$$

and

$$g = b_e t^e + \ldots + b_1 t + b_0, \quad b_e \neq 0$$

so that f and g are degree d and e polynomials, respectively. Since both a_d, $b_e \in F$ are non-zero, and since F is a field, there exists a unique number q_{e-d} so that

$$q_{e-d} a_d = b_e.$$

So consider the polynomial

$$q_{e-d} f = b_e t^d + q_{e-d} a_{d-1} t^{d-1} + \ldots + q_{e-d} a_1 t + q_{e-d} a_0.$$

Multiply this polynomial by t^{e-d} to obtain

$$q_{e-d} t^{e-d} f = b_e t^e + q_{e-d} a_{d-1} t^{e-1} + \ldots q_{e-d} a_1 t^{e-d+1} + q_{e-d} a_0 t^{e-d}.$$

Note that this polynomial has the same degree as g, and the same highest degree coefficient b_e that g has. So we can subtract it from g to obtain a lower-degree polynomial, $g' := g - q_{e-d} t^{e-d} f$. By induction on degree, there is a polynomial Q and a polynomial r so that

$$g' = Qf + r$$

where r has degree less than f. Then we can write

$$\begin{aligned} g &= \left(q_{e-d} t^{d-e}\right) f + g - \left(q_{e-d} t^{d-e}\right) f \\ &= \left(q_{e-d} t^{d-e}\right) f + g' \\ &= \left(q_{e-d} t^{d-e}\right) f + Qf + r \\ &= \left(q_{e-d} t^{d-e} + Q\right) f + r \end{aligned}$$

so set

$$q = q_{e-d} t^{t-e} + Q$$

and we have

$$g = qf + r$$

where $\deg r < \deg f$. We are finished. □

19.5 Primes and Factorization in PIDs

Definition 19.5. An element $x \in R$ is called a **unit** if there is some $y \in R$ for which

$$xy = yx = 1_R.$$

Example 19.3. The units of $\mathbb{Z}$ are the elements ± 1. Likewise, the units of a field F are the non-zero elements of F.

Proposition 19.6. Let $R = F[t]$. Then the units of R are the constant, non-zero polynomials.

Proof. If $fg = 1$, we must have that $\deg f + \deg g = \deg 1 = 0$. Hence both $\deg f$ and $\deg g$ must be zero——i.e., f and g must be constant. But constant polynomials form a subring $F \subset F[t]$, so two constant polynomials can multiply to one if and only if they are non-zero (since any non-zero element in F has a multiplicative inverse). □

Now I want to generalize the notion of being a prime in $\mathbb{Z}$ to arbitrary rings.

Definition 19.6. An element $x \in R$ is called **prime**, or **irreducible**, if

(1) x is not a unit, and

(2) the only elements dividing x are units, or unit multiples of x. Explicitly, if

$$x = ab$$

for some $a, b \in R$, then either a or b must be a unit.

Example 19.4. Here are some examples of primes in rings:

(1) Let $R = \mathbb{Z}$. If x is a prime number, or the negative of a prime number, then the only numbers dividing x are ± 1 and $\pm x$. Necessarily, if $x = ab$, then either a or b must equal ± 1, which are the units of $\mathbb{Z}$. Hence the prime elements of $\mathbb{Z}$ (under this definition) are prime numbers or their negatives. Note that zero is not a unit.

(2) Let $R = F[t]$. Then the only units of $F[t]$ are constant, non-zero polynomials. So f is a prime, or irreducible, if and only if the only polynomials dividing f have equal degree to f, or are constant polynomials.

(3) As a subexample, if $\deg f = 1$, then f is irreducible. For if $gh = f$, then $\deg g + \deg h = \deg f = 1$. But this means that one of g or h must have degree 0 . That is, any linear polynomial is irreducible.

Theorem 19.7 (Unique Factorization for PIDs)**.** Let R be a PID. Then for any non-zero element $x \in R$, there exists a finite collection of distinct prime elements $p_1, \ldots, p_k \in R$ so that

$$x = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}, \quad n_i \geqslant 1$$

and so that no p_i is a unit multiple of p_j for $i \neq j$. The n_i are unique, and the elements p_i are unique up to multiplication by units and reordering.

Proof. Let $x \in R$, $x \neq 0$. If x is a prime, we're finished: Set $p_1 = x$.

Otherwise, $x = a_1 b_1$ for some non-unit elements a_1, $b_1 \in R$. If both are prime, we're done. Let's say a_1 isn't prime. Then $a_1 = a_2 b_2$, where a_2, b_2 are not units. What does this mean?

$$a_1 \in (a_2)$$

so $(a_1) \subset (a_2)$.

Note importantly that this inclusion is proper, so $(a_1) \neq (a_2)$. Why is that? Otherwise, we would have

$$(a_2) \subset (a_1) \Longrightarrow a_1 = c a_1 b_2 = a_1 c b_2 \Longrightarrow (1 - c b_2)\, a_1 = 0. \Longrightarrow (1 - c b_2) = 0$$

so b_2 would be a unit. (Note that in the last $\Longrightarrow$, we're using the fact that R is a domain.)

And if a_2 is not prime, we would again have $a_2 = a_3 b_3$, with a proper inclusion $(a_2) \subset (a_3)$. Going on in this way, each time we write $a_i = a_{i+1} b_{i+1}$, we have a chain of inclusions

$$\cdots \subset (a_i) \subset (a_{i+1}) \subset \cdots$$

But as we saw before, at some point (a_n) must equal (a_{n+1}), which violates the proper inclusion property, for then $(a_{n+1}) \subset (a) \subset (a_n) \Longrightarrow (a_{n+1}) = (a_n)$.

What this means is that some a_n has to be prime at a finite stage n.

What we've shown is:

Every non-zero element x can be written

$$x = p_1 y_1 \tag{$\star$}$$

where p_1 is prime.

But we may have no control on y_1. Now we need to show that x can be written as a finite product of primes. (Repeating the above process, it's not clear that we get to finitely many primes in finite time!) Well, if y_1 isn't irreducible, we can write

$$y_1 = p_2 y_2$$

where p_2 is a prime (by using $(\star)$ above). If y_2 isn't irreducible, we can go on in this way, and we have again a chain

$$(x) \subset (y_1) \subset (y_2) \subset \cdots$$

of proper inclusions. If y_n isn't a prime at some point we have a contradiction, since there can be no infinite ascending chain of ideals like this in a PID (as we've shown above). So set $p_{n+1} = y_n$, and we have written

$$\begin{aligned} x &= p_1 y_1 \\ &= p_1 p_2 y_2 \\ &= \cdots \\ &= p_1 p_2 \cdots p_n y_n \\ &= p_1 p_2 \cdots p_n p_{n+1} \end{aligned}$$

which shows any element x can be written as a product of primes. □

The core of proof is the following:

Proposition 19.8. Fix a principal ideal domain R. Assume we have an increasing sequence of ideals

$$I_1 \subset I_2 \subset \cdots .$$

Then there is some finite n for which $I_n = I_{n+1} = \cdots$.

Proof. Let $I = \bigcup I_j$. Since R is a PID, there is a single element a that generates I, so $I = (a)$. But $a \in I$, which means $a \in I_n$ for some finite n (by definition of union). Then we'd have

$$(a) \subset I_n \subset (a)$$

so $I_n = (a)$. But if $I_n \subset I_{n+j} \subset (a) = I_n$, we have that $I_n = I_{n+j}$ for all j. □

Remark. Any commutative ring R satisfying this ascending chain condition——that is, the property that any ascending chain of ideals must terminate is called Nötherian, after Emmy Nöther (who is arguably the most famous woman in mathematics and physics). If you take any kind of course in algebraic geometry, you'll see plenty more of Nötherian rings.

Example 19.5. As a consequence:

(1) If $R = \mathbb{Z}$, recall that a prime element of R is simply a prime number, or a negative of a prime number. Thus the theorem is saying that any integer $x \in \mathbb{Z}$ can be written as a product of powers of primes:

$$x = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}.$$

If each p_i is taken to be a positive prime number, this is often called the prime factorization of x. In context of the theorem, however, note we could replace p_1 and p_2 by $-p_1$ and $-p_2$, and we would still be able to express x as a product of powers of primes. In this sense, the choice of the p_i is only unique up to multiplying by units. Of course, for the integers, we can choose to order each p_i so that the $p_i < p_{i+1}$ and we have a preferred ordering, but this is not true in general PIDs.

(2) If $R = F[t]$, this is saying that every polynomial can be written as a product of irreducible polynomials p_i :

$$f = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}.$$

(3) As an example, if $F = \mathbb{C}$, then any polynomial can be written as a product of linear polynomials:

$$f = (t - \alpha_1)^{n_1} \dots (t - \alpha_k)^{n_k} .$$

I caution you that for other fields, we may not be able to decompose f into linear polynomials.

Exercise. Here are some opening exercises:

(1) Let F be a field and $g \in F[t]$. Show that $g(x) = 0$ if and only if the polynomial $t - x$ divides the polynomial $g(t)$ in $F[t]$. (Hint: The division algorithm.)

(2) Fix a commutative ring R. Fix $a, b \in R$. Show

$$(a) = (b)$$

if and only if $a = ub$ for some unit u.

(3) Let R be a commutative ring. Prove a unit cannot be a zero divisor. What is the contrapositive?

(4) Prove that any field is a PID.

Solution. (1) This is certainly true for $\deg g = 0$, for $g(x) = a_0 = 0$ if and only if $g = 0$, while $(t - x)0 = 0$, so $t - x$ divides g.

Now assume $\deg g \geqslant 1$. Use the division algorithm:

$$g = (t - x)q + r$$

Then

$$g(x) = (x - x)q(x) + r(x) = 0q(x) + r(x) = r(x)$$

This means $r(x) = 0$. But $\deg r < \deg(t - x)$, meaning $r(x)$ must be a degree 0 polynomial for which x is a root——this means $r = 0$ as a polynomial, and

$$g = (t - x)q$$

(2) Since $a = ub$, we see that $a \in (b)$. Thus $(a) \subset (b)$. (For if $y = ra$, then $y = rub = (ru)b$, so any multiple of a is a multiple of b.)

Likewise, $u^{-1}a = b$, so we see that $b \in (a)$, thus $(b) \subset (a)$.

(3) If x is a unit, $xy = 1$ for some $y \in R$. Then for any $a, axy = a1 = a$. On the other hand if $ax = 0$, we also have that $axy = 0y = 0$. Hence $a = 0$, so x cannot be a zero divisor.

(4) A commutative ring is a field if and only if its only ideals are $\{0\}$ and R itself. Well, $\{0\}$ is principal since $\{0\} = (0)$. Also, $R = (1)$ for any ring.

So we only need to show that there are no zero divisors aside from zero. But in a field, every non-zero element is a unit, so there are no zero divisors.

19.6 Modules over PIDs

The following theorem shows that every finitely generated module over a PID has a simple form. (If all rings had modules as simple as this, the world would be a wonderful place.)

Theorem 19.9 (Classification of Finitely Generated Modules over PIDs)**.** Let R be a PID, and let M be a finitely generated R-module. Then there exists a finite collection of primes $p_1, \ldots, p_k \in R$, with p_i possibly equaling p_j, and numbers $n_0, \ldots, n_k$ such that

$$M \cong R^{n_0} \oplus R/\left(p_1^{n_1}\right) \oplus R/\left(p_2^{n_2}\right) \oplus \cdots \oplus R/\left(p_k^{n_k}\right)$$

Moreover, this decomposition is unique up to re-ordering and unit multiples of p_i.

Remark. What do we explicitly mean by uniqueness? Given some other decomposition

$$M \cong R^{m_0} \oplus R/\left(q_1^{m_1}\right) \oplus \ldots \oplus R/\left(q_j^{m_j}\right)$$

where each q_i is a prime, then we have

(1) $m_0 = n_0$,

(2) $j = k$, and

(3) There is some re-ordering of the i so that $n_i = m_i$, and that p_i and q_i are unit multiples of each other.

I emphasize that p_i could equal p_j for $i \neq j$. In other words, modules aren't like numbers——they don't admit unique prime factorizations in which $p \cdot \cdots \cdot p$ can be grouped into p^k; the repetition of primes is important.

Example 19.6 ($R = F$ a Field)**.** If F is a field, what are the prime elements? There are no prime elements, since prime elements are in particular non-zero, non-unital elements. So every finitely generated module over F must be of the form

$$M \cong F^{n_0}$$

which is just the statement that every finitely generated F-module admits a finite basis. n_0 is the dimension of the vector space.

Example 19.7 ($R = \mathbb{Z}$)**.** What are the primes of $\mathbb{Z}$? Numbers of the form $\pm p$ for p a prime number. (Note that $(p) = (-p)$.) So the above theorem is stating that any finitely generated $\mathbb{Z}$-module——that is, any finitely generated abelian group-is of the form

$$M \cong \mathbb{Z}^{n_0} \oplus \mathbb{Z}/p_1^{n_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p_k^{n_k}\mathbb{Z}$$

Uniqueness means, for example, that

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \quad (p_1 = p_2 = 2, \text{while } n_0 = 0, n_1 = n_2 = 1)\,.$$

and

$$\mathbb{Z}/4\mathbb{Z} \quad (p_1 = 2, \text{while } n_0 = 0, n_1 = 2.)$$

are not isomorphic $\mathbb{Z}$-modules (i.e., not isomorphic abelian groups). This, we already knew-for instance, $\mathbb{Z}/4\mathbb{Z}$ is cyclic, while the former group is not. Note that the former group is also an example of when $p_i = p_j$ for $i \neq j$.

Example 19.8. Again let $R = \mathbb{Z}$. We can classify every abelian group of order 8 now:

	n_0	$p_1, p_2, \ldots, p_k$	$n_1, \ldots, n_k$
$\mathbb{Z}/8\mathbb{Z}$	0	2	3
$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	0	2, 2	2, 1
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	0	2, 2, 2	1, 1, 1

Example 19.9. As another example, let $M = \mathbb{Z}/6\mathbb{Z}$. This is not of the form stated in the theorem. In fact, M is isomorphic to

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

Exercise. Classify all abelian groups of order

$$7 \times 7 \times 11 \times 11 = 5929.$$

Solution. Need to find all combinations of p_i, n_i such that

$$\begin{aligned} 5929 &= |\mathbb{Z}/(p_1^{n_1}) \oplus \cdots \oplus \mathbb{Z}/(p_k^{n_k})| \\ &= p_1^{n_k} \cdot \cdots \cdot p_k^{n_k}. \end{aligned}$$

	(p_1, n_1)	(p_2, n_2)	(p_3, n_3)	(p_4, n_4)
$\mathbb{Z}/49\mathbb{Z} \oplus \mathbb{Z}/121\mathbb{Z}$	$(7, 1)$	$(11, 2)$	–	–
$\mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/121\mathbb{Z}$	$(7, 1)$	$(7, 1)$	$(11, 2)$	–
$\mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/11\mathbb{Z} \oplus \mathbb{Z}/11\mathbb{Z}$	$(7, 1)$	$(7, 1)$	$(11, 2)$	$(11, 1)$
$\mathbb{Z}/49\mathbb{Z} \oplus \mathbb{Z}/11\mathbb{Z} \oplus \mathbb{Z}/11\mathbb{Z}$	$(7, 2)$	$(11, 1)$	$(11, 1)$	–

Note: $\mathbb{Z}/p^2\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$.

Exercise. Which of these is $\mathbb{Z}/5929\mathbb{Z}$ isomorphic to?

Solution. We showed $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$ if $\gcd(m, n) = 1$. So

$$\mathbb{Z}/49\mathbb{Z} \oplus \mathbb{Z}/121\mathbb{Z} \cong \mathbb{Z}/5929\mathbb{Z}.$$

Let F be a field, and let V be a F-vector space. (This just means V is a module over F.) Then any

$$A : V \to V, \quad F - \text{linear map},$$

defines a $F[t]$-module structure on V: If $f = a_d t^d + \cdots + a_1 t + a_0$,

$$fv := a_d A^d(v) + \cdots + a_1 A(v) + a_0 v.$$

where

$$A^i = \underbrace{A \circ \cdots \circ A}_{i \text{ times}}$$

So let V be a finite dimensional vector space over F. Fix an F-linear $A : V \to V$ to make V an $F[t]$-module.

Proposition 19.10. *V is finitely generated as an $F[t]$-module.*

Proof. Let $v_1, \ldots, v_n$ be a finite basis. Then

$$V = \{b_1 v_1 + \cdots + b_n v_n \mid b_1, \ldots, b_n \in F\}.$$

In particular, if $f_i = b_i$ are constant polynomials,

$$V = \{f_1 v_1 + \cdots + f_n v_n\}$$

So the function

$$\begin{aligned} F[t] \oplus \cdots \oplus F[t] &\to V \\ e_i &\mapsto v_i \end{aligned}$$

is a surjection. □

Corollary 19.11. *V is isomorphic (as an $F[t]$-module) to*

$$F[t]/(p_1^{n_1}) \oplus \cdots \oplus F[t]/(p_k^{n_k}) \oplus F[t]^{n_0}$$

for $p_i \in F[t]$ irreducible, $n_i \geqslant 1$, $n_0 \geqslant 0$.

Remark. $n_0 = 0$; Why? V is a finite dimensional vector space over F, but $F[t]$ isn't, so V couldn't contain a subspace isomorphic to $F[t]$.

In general, identifying irreducible polynomials can be hard: For instance, when is $x^3 + 2x^2 + x + 1$ irreducible over $\mathbb{Z}/p\mathbb{Z}$? We'd probably check case by case.

19.7 When the PID is a Polynomial Ring

The only other PID we've talked about is $R = F[t]$. What are the primes of $F[t]$? In general, this is a hard question. A first prerequisite for f to be a prime is that it have no roots in F-otherwise, as we saw earlier, f can be factored by a linear polynomial, which is not a unit in $F[t]$.

But there are a class of fields in which you can characterize the irreducible elements of $F[t]$ easily:

Definition 19.7. A field F is called **algebraically closed** if every polynomial $f \in F[t]$ has a root.

The obvious example is $F = \mathbb{C}$. The perhaps surprising theorem is:

Theorem 19.12. *Any field F admits an injective ring homomorphism into an algebraically closed field.*

Remark. Note that not every field F admits an injective ring homomorphism into $\mathbb{C}$. For instance, if $F = \mathbb{Z}/2\mathbb{Z}$, the multiplicative unit $\overline{1}$ satisfies the property that $\overline{1} + \overline{1} = 0$. Any ring homomorphism $\phi : \mathbb{Z}/2\mathbb{Z} \to \mathbb{C}$ must satisfy the property that $\phi(\overline{1}) + \phi(\overline{1}) = \phi(0)$, which is impossible, since a ring homomorphism must also satisfy the constraint that $\phi(\overline{1}) = 1_{\mathbb{C}}$.

In other words, there must be some other field, other than $\mathbb{C}$, which has a root to any polynomial, and which admits an injective map from $\mathbb{Z}/2\mathbb{Z}$. Seems mysterious, doesn't it?

Proposition 19.13. *If F is algebraically closed, the only irreducible elements of $F[t]$ are (non-zero) linear polynomials.*

Proof. We know already that any non-zero linear polynomial is irreducible for any pair $f = ab$ either a or b must have degree 0, meaning any factorizations of f involves a unit.

On the other hand, if f has degree $\geqslant 2$, we know f has a root by definition of algebraically closed field, so we can always write

$$f = (t - x)q$$

for some q with degree $\deg f - 1$. Neither $t - x$ nor q can be units since they are not constant polynomials (they have non-zero degree) so no polynomial of higher degree can be a prime. □

Corollary 19.14. If F is algebraically closed, then any finitely generated module over F is isomorphic to

$$F[t]^{n_0} \oplus F[t]/(t-\lambda_1)^{n_1} \oplus \ldots \oplus F[t]/(t-\lambda_k)^{n_k}$$

for some choice of elements $\lambda_i \in F$ and integers $n_1, \ldots, n_k \geqslant 1$.

Why might this be helpful for us? Well, a good example of an $F[t]$-module is an F-vector space V together with a linear map $A : V \to V$. In other words, this helps us classify linear maps A!

Corollary 19.15. If F is algebraically closed and V is a finite dimensional vector space with $A : V \to V$ F-linear, then

$$V \cong F[t]/(t-\alpha_1)^{n_1} \oplus \cdots \oplus F[t]/(t-\alpha_k)^{n_k}$$

for some $\alpha_i \in F$.

Remark. If $f = a_1 t - a_0$, then $a_1^{-1} f = t - a_1^{-1} a_0$, (assuming $a_1 \neq 0$) so $(f) = (a_1^{-1} f) = (t - a_1^{-1} a_0)$. That is, we can always assume $a_1 = 1$.

Let's see some examples: We want to study

$$F[t]/(t-\alpha)^n$$

as a F-module, and as an $F[t]$-module. Note the $F[t]$-module structure on $F[t]/(p^n)$ is

$$\begin{aligned} F[t] \times F[t]/(p^n) &\to F[t]/(p^n) \\ (f, \overline{g}) &\mapsto (\overline{fg}). \end{aligned}$$

Proposition 19.16. If $\deg p = d$,

$$F[t]/(p^n) \cong F^{n \cdot d}$$

as a F-vector space.

Proof. Any $f \in F[t]$ can be written $f = p^n \cdot q + r$, where $\deg r < \deg p^n = nd$. Since r, q are unique given p^n, f, the function

$$\overline{f} \mapsto r, \quad F[t]/(p^n) \to \{\text{polynomial of degree} \leqslant nd-1\} \cong F^{nd}$$

gives a bijection. □

Example 19.10. $V = F[t]/(t)$. $\alpha = 0$, $n = 1$. What is $F[t]$-action?

(1) $F[t]/(t) \cong \{\text{constant polynomial}\}$
$\cong F$.

(2) $t \cdot \overline{a_0} = \overline{ta_0} = \overline{0}$ since $a_0 t \in (t)$. i.e., multiplication by $t \leftrightarrow A : F \to F$.
$a_0 \mapsto 0$

Example 19.11. $V = F[t]/(t-\alpha)$.
Multiplication by $t \leftrightarrow A : V \to V$. i.e., $A : F \to F$.

$$\begin{aligned} \overline{a_0} \mapsto \overline{ta_0} &= \overline{(t-\alpha)}\overline{a_0} + \alpha\overline{a_0} \\ &= \alpha\overline{a_0} \end{aligned} \qquad a_0 \mapsto \alpha a_0$$

Example 19.12. Let

$$V = F[t]/(t-\alpha)^n.$$

Then V has a basis

$$\begin{array}{cccccc} \overline{1}, & \overline{t-\alpha}, & \overline{(t-\alpha)}^2, & \cdots, & \overline{(t-\alpha)}^{n-1}. \\ \| & \| & & & \| \\ V_0 & V_1 & & & V_{n-1} \end{array}$$

Moreover,

$$\begin{aligned} tv_i = t\overline{(t-\alpha)}^i &= (t-\alpha)\overline{(t-\alpha)}^i + \alpha\overline{(t-\alpha)}^i \\ &= \overline{(t-\alpha)}^{i+1} + \alpha\overline{(t-\alpha)}^i \\ &= v_{i+1} + \alpha v_i \end{aligned}$$

So

$$A = \begin{pmatrix} \alpha & 1 & 0 & \cdots & 0 \\ 0 & \alpha & 1 & \cdots & 0 \\ 0 & 0 & \alpha & \cdots & 0 \\ & & & \ddots & \\ 0 & \cdots & 0 & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \alpha \end{pmatrix}$$

where α on diagonal, 1 right above diagonal.

Chapter 20

Cayley-Hamilton Theorem

20.1 Matrix for Linear Transformation

Definition 20.1. Let M be a F vector space, and fix a basis $\vec{v}_1, \ldots, \vec{v}_k$ for M. (Assume M finite dimension.) Then given any linear transformation

$$A : M \to M,$$

the **matrix for A with respect to** $\vec{v}_1, \ldots, \vec{v}_k$ is the matrix for which

$$A\vec{v}_i = \sum_{j=1}^{k} A_{ji}\vec{v}_j.$$

Example 20.1. $(A) = \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{pmatrix}$. Then $A\vec{v}_1 = A_{11}\vec{v}_1 + A_{21}\vec{v}_2 + A_{31}\vec{v}_3$.

Exercise. Write out the matrix for multiplication by t on each of the following $F[t]$-modules with indicated bases:

(1) $M = F[t]/(t)$, $\vec{v}_1 = \overline{1}$.

(2) $M = F[t]/(t-\alpha)$, $\vec{v}_1 = \overline{1}$.

(3) $M = F[t]/(t-\alpha)^2$, $\vec{v}_2 = \overline{1}$, $\vec{v}_1 = \overline{t-\alpha}$.

(4) $M = F[t]/(t-\alpha)^3$, $\vec{v}_3 = \overline{1}$, $\vec{v}_2 = \overline{t-\alpha}$, $\vec{v}_1 = \overline{(t-\alpha)^2}$.

Solution. In general, the action of $F[t]$ on $F[t]/I$ is $f \cdot \overline{g} = \overline{fg}$.

(2) $t \cdot \overline{1} = \overline{t1} = \overline{t-\alpha} + \overline{\alpha} = \alpha\overline{1}$.
So t sends $\overline{1}$ to $\alpha\overline{1}$, i.e.,

$$(A) = (\alpha).$$

(3) $t \cdot \overline{1} = \overline{t1} = \overline{t-\alpha} + \overline{\alpha} = \vec{v}_1 + \alpha\vec{v}_2$. So $(A) = \begin{pmatrix} ? & 1 \\ & \alpha \end{pmatrix}$.

$$t \cdot \overline{(t-\alpha)} = (t-\alpha) \cdot \overline{(t-\alpha)} + \alpha \cdot \overline{(t-\alpha)} = \overline{(t-\alpha)}^2 + \alpha\overline{(t-\alpha)}.$$
$$= 0 + \alpha\vec{v}_1$$

$$\Rightarrow A = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}.$$

Proposition 20.1. In basis for $M = F[t]/(t-\alpha)^n$ given by $\overline{(t-\alpha)}^{n-1}$, $\overline{(t-\alpha)}^{n-2}$, …, $\overline{(t-\alpha)}^{1}$, $\overline{1}$, the linear transformation

$$M \to M$$
$$\vec{v} \mapsto t\vec{v}$$

has the matrix

$$\begin{pmatrix} \alpha & 1 & 0 & & 0 & 0 \\ 0 & \alpha & 1 & & 0 & 0 \\ 0 & 0 & \alpha & & 0 & 0 \\ & & & \ddots & & \\ 0 & 0 & 0 & & \alpha & 1 \\ 0 & 0 & 0 & & 0 & \alpha \end{pmatrix}$$

where α along diagonal, 1 directly above each α except the topmost α.

Proof.

$$\begin{aligned} tv_i = t\overline{(t-\alpha)^{n-i}} &= ((t-\alpha)+\alpha)\overline{t-\alpha}^{n-i} \\ &= (t-\alpha)\overline{(t-\alpha)}^{n-i} + \alpha\overline{(t-\alpha)}^{n-i} \\ &= \overline{(t-\alpha)}^{n-i+1} + \alpha\vec{v}_i \\ &= \begin{cases} \vec{v}_{i-1} + \alpha\vec{v}_i & i \leqslant n-1 \\ \alpha\vec{v}_n & i = n \end{cases} \end{aligned}$$

□

Remark. If M, N are finite dimensional $F[t]$-modules and $\exists$ bases $v_1, \ldots, v_m$ for M, s.t. "multiplication $w_1, \ldots, w_n$ for N by t" is given by a matrix A for M, then on $M \oplus N$, t acts by the matrix matrix B for N

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

i.e., block diagonal.

20.2 Jordan Normal Form

Knowing any $F[t]$-module is isomorphic to $\bigoplus_i F[t]/(p_i n_i)$, we have

Corollary 20.2. Let $T : F^n \to F^n$ be a F-linear transformation, F algebraic closed. Then $\exists$ basis for F^n such that

$$\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & A_e \end{pmatrix}$$

where $A_1 = \begin{pmatrix} \alpha_1 & 1 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 1 \\ 0 & \cdots & 0 & \alpha_1 \end{pmatrix}$, $A_2 = \begin{pmatrix} \alpha_2 & 1 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 1 \\ 0 & \cdots & 0 & \alpha_2 \end{pmatrix}$,..., $A_e = \begin{pmatrix} \alpha_e & 1 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 1 \\ 0 & \cdots & 0 & \alpha_e \end{pmatrix}$.

Definition 20.2. This is called **Jordan normal form of** T.

20.3 Characteristic Polynomial

Definition 20.3. Characteristic polynomial

$$\det(tI - A) \in F[t]$$

Example 20.2. If $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$, then $tI - A = \begin{pmatrix} t - A_{11} & A_{12} \\ A_{21} & t - A_{22} \end{pmatrix}$. So

$$\det(tI - A) = t^2 - (A_{11} + A_{22})t + (A_{11}A_{22} - A_{12}A_{21}).$$

Remark. If A is $k \times k$ matrix, the i^{th} coefficient of characteristic polynomial is an invariant number of A that remains unchanged under conjugation.

$$\det(B(tI - A)B^{-1}) = \det BB^{-1} \det(tI - A) = \det(tI - A).$$

Definition 20.4. Any $A \in M_{k\times k}(F)$ determines

$$f : F[t] \to M_{k\times k}(F),$$

since $F[t]$ is a PID, $\ker(f) = (p)$, $p \in F[t]$.

Taking p to be unique one, s.t.

- $p = t^d + a_d t^{d-1} + \cdots$,
- $\ker(f) = (p)$,

We say p is **minimal polynomial** of A.

20.4 Cayley-Hamilton Theorem

Theorem 20.3 (Cayley-Hamilton)**.** Any matrix A satisfies its characteristic polynomial.

Remark. The theorem holds even when F is not algebraically closed!

Proof. In basis given by above,

$$\det(tI - A) = \prod_{i=1}^{e} (t - \alpha_i)^{n_i}.$$

So need to show

$$\prod_{i=1}^{e} (A - \alpha_i I)^{n_i} = 0.$$

But $\overline{1}_1, \ldots, \overline{1}_e$ generate v as a module, and

$$(A - \alpha_i I)^{n_i} \overline{1}_j = 0.$$

(Since $(A - \alpha_i I)^{n_i - 1}(\overline{1}_i)$ is an eigenvector.) □

Example 20.3. If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, its characteristic polynomial is $t^2 - t(a + d) + (ad - bc)$. The theorem states that

$$A^2 - A(a + d) + I(ad - bc) = 0 \in M_{2\times 2}(F).$$

Example 20.4. Alternatively, if $A \in M_{k\times k}(F)$, then its characteristic polynomial is of the form

$$t^k + b_{k-1}t^{k-1} + \cdots + b_1 t + b_0.$$

The theorem says that $\forall \vec{v} \in F^k$, we have

$$A^k \vec{v} + b_{k-1}A^{k-1}\vec{v} + \cdots + b_1 A\vec{v} + b_0 \vec{v} = 0.$$

Corollary 20.4. The minimal polynomial of A divides its characteristic polynomial.

Proposition 20.5. Let $A \in M_{k\times k}(F)$. A is invertible if and only if the columns of A form a basis.

Proof. Let T_A be the linear transformation $F^k \to F^k$ given by A. Need to show that T_A is invertible——i.e., that T_A is an injection and a surjection. Well,

$$T_A(\vec{e}_i) = \vec{v}_i \quad \text{if } v_i \text{ are columns of } A.$$

$$\begin{pmatrix} \vdots & & \vdots \\ \vec{v}_1 & \cdots & \vec{v}_k \\ \vdots & & \vdots \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} \\ \vec{v}_i \\ \\ \end{pmatrix}$$

So $T_A(\sum b_i \vec{e}_i) = \vec{0} \Leftrightarrow \sum b_i \vec{v}_i = 0 \Leftrightarrow b_i = 0$.

Since $\ker T_A = \{0\}$ and T_A is a linear map between F^k and F^k (which have same dimension), T_A is invertible. □

Proposition 20.6. Let A' be a matrix for T_A in some basis $v_1, \ldots, v_k$. Let $B = \begin{pmatrix} \vdots & & \vdots \\ \vec{v}_1 & \cdots & \vec{v}_k \\ \vdots & & \vdots \end{pmatrix}$. Then

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

Proof.

$$\begin{aligned} BAB^{-1}(\vec{v}_i) &= BA\vec{e}_i \\ &= B(\sum A_{ji}\vec{e}_j) \\ &= \sum A_{ji}\vec{v}_j \\ &= A'(\vec{v}_i). \end{aligned}$$

□

Proposition 20.7. If B is invertible and $A' = BAB^{-1}$, then

$$\det(tI - A') = \det(tI - A) \in F[t].$$

Proof. In general,

$$\begin{aligned} \det(BCB^{-1}) &= \det B \det C \det B^{-1} \\ &= \det B \det B^{-1} \det C \\ &= \det BB^{-1} \det C \\ &= \det I \det C \\ &= \det C \end{aligned}$$

So

$$\det(B(tI - A)B^{-1}) = \det(tI - A)$$

while

$$\begin{aligned} \det(B(tI - A)B^{-1}) &= \det(BtIB^{-1} - BAB^{-1}) \\ &= \det(tI - BAB^{-1}). \end{aligned}$$

□

So to compute characteristic polynomial of arbitrary $A \in M_{k\times k}(F)$? Well, if F is algebraic closed, we know

$$A = BA'B^{-1}$$

where

$$A' = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \cdots & \ddots & \vdots \\ 0 & \cdots & 0 & A_e \end{pmatrix}$$

is block diagonal, with

$$A_i = \begin{pmatrix} \alpha_i & 1 & 0 & \cdots & 0 \\ 0 & \alpha_i & 1 & \cdots & 0 \\ 0 & 0 & \alpha_i & \cdots & 0 \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & \alpha_i \end{pmatrix}, \quad \alpha_i \in F.$$

where α_i along diagonal, 1 right above diagonal. So we need only see

$$\begin{aligned} \det(tI - A') &= \det \begin{pmatrix} t-\alpha_1 & -1 & \cdots & 0 \\ 0 & t-\alpha_1 & \cdots & 0 \\ \vdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & -1 \\ 0 & \cdots & \cdots & t-\alpha_e \end{pmatrix} \\ &= (t-\alpha_1)^{n_1} \cdot (t-\alpha_2)^{n_2} \cdot \cdots \cdot (t-\alpha_e)^{n_e} \end{aligned}$$

Since $tI - A'$ is upper-triangular, its det is $\prod$ of its diagonal entries.

To show that

$$(A - \alpha_1)^{n_1} \cdot \cdots \cdot (A - \alpha_e)^{n_e} = 0$$

We need only show that $\forall \vec{v}$, we have

$$(A - \alpha_1)^{n_1} \cdot \cdots \cdot (A - \alpha_e)^{n_e} \vec{v} = 0$$

Well, choose a basis

$$\begin{aligned}
\vec{v}_{1,n_1} &= \overline{1}, \ldots, \vec{v}_{1,1} = \overline{(t-\alpha_1)}^{n_1 - 1} \in F[t]/(t-\alpha_1)^{n_1} \\
&\vdots \\
\vec{v}_{e,n_e} &= \overline{1}, \ldots, \vec{v}_{e,1} = \overline{(t-\alpha_e)}^{n_e - 1} \in F[t]/(t-\alpha_e)^{n_e}
\end{aligned}$$

Then $\{\vec{v}_{i,n_j}\}$ form a basis for the vector space on which A acts. Moreover,

$$\begin{aligned}
&(A - \alpha_1)^{n_1} \cdot \cdots \cdot (A - \alpha_i)^{n_i} \cdot \cdots \cdot (A - \alpha_e)^{n_e} \vec{v}_{i,j} \\
=&(A - \alpha_1)^{n_1} \cdot \cdots \cdot (A - \alpha_e)^{n_e} (A - \alpha_i)^{n_i} \vec{v}_{i,j} \\
=&(A - \alpha_1)^{n_1} \cdot \cdots \cdot (A - \alpha_e)^{n_e} \vec{0} \\
=&\vec{0}
\end{aligned}$$

The second and third equality is because we know (by choice of basis),

$$A\vec{v}_{i,j} = \vec{v}_{i,j-1} + \alpha_i \vec{v}_{i,j}.$$

On the other hand

$$A\vec{v}_{i,1} = \alpha \vec{v}_{i,1}.$$

So

$$(A - \alpha_i)\vec{v}_{i,j} = \begin{cases} \vec{v}_{i,j-1} & j > 1 \\ 0 & j = 1 \end{cases}$$

So we've shown that if F is algebraic closed, any $A \in M_{k\times k}(F)$ satisfies $\det(tI - A)$. But if F isn't? Well, let $\overline{F}$ be an algebraic closed field into which F injects. Then we have injections

$$M_{k\times k}(F) \hookrightarrow M_{k\times k}(\overline{F})$$

and

$$F[t] \hookrightarrow \overline{F}[t].$$

We can think the first map of any matrix with entries in F as one with entries in $\overline{F}$. Likewise, we can think the second map of any polynomial with F coefficients as having $\overline{F}$ coefficients. Putting it all together,

$$\begin{array}{ccccc}
A & \longmapsto & (A, \det(tI - A)) & \xmapsto{\text{evaluate}} & ? \\
\\
M_{k\times k}(F) & \longrightarrow & M_{k\times k}(F) \times F[t] & \longrightarrow & M_{k\times k}(F) \\
\downarrow & & \downarrow & & \downarrow \\
M_{k\times k}(\overline{F}) & \longrightarrow & M_{k\times k}(\overline{F}) \times \overline{F}[t] & \xrightarrow{\text{evaluate}} & M_{k\times k}(\overline{F}) \\
\\
A & \longmapsto & (A, \det(tI - A)) & \longmapsto & 0
\end{array}$$

is commutative. So $? \to 0$ implies $?$ must have been zero. Most succinctly: Plugging in a matrix into its characteristic polynomial yields the same result whether we think of the matrix as having F or $\overline{F}$ entries.