Math 120A: Group Theory

Eli Griffiths

August 9, 2023

Table of Contents

Introduction 2

1.1 Understanding Relations and Sets 2

Operations 4

2.1 Binary Operation 4

2.1.1 Tabular Representation 5

Binary Structures 6

3.1 Isomorphic Binary Structures 6

Introduction to Groups 7

4.1 Groups 7

4.2 Subgroups 7

4.3 Generators and Cyclic Subgroups 8

Permutations 11

5.1 Groups of Permutations 11

5.1.1 Cayley's Theorem 11

5.2 Cartesian Product of Groups 13

Homomorphisms and Factor Groups 16

6.1 Homomorphisms 16

List of Theorems 18

List of Definitions 18

Introduction

1.1 Understanding Relations and Sets

Definition 1.1 (Relations). A relation between two sets A and B is denoted by $\mathcal{R}$. $\mathcal{R}$ is a subset of $A \times B$ where $(a,b) \in \mathcal{R}$ is read as "a is related to b".

Analysts are initimately familiar with the concept of functions. A function is a relation (which for these purposes will be denoted by ϕ) on a domain X and codomain Y such that

$$(x,y) \in \phi \iff \phi(x) = y.$$

Some often thought of functions are $x \mapsto x^2$ and $x \mapsto e^x$. Consider the following function:

$$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R} : (a,b) \mapsto a+b.$$

While it may not seem like a function in the same vain as $f(x) = x^2$, it is just as valid. Hence operators on sets can be thought as a function and hence a relation on the set (in this instance on $\mathbb{R}$).

Definition 1.2 (Equivalence Relation). A relation $\mathcal{R}$ is called an *Equivalence Relation* if it satisfies the following three properties:

Reflexive	$\forall a \in A, (a,a) \in \mathcal{R}$
Symmetric	$\forall a,b \in A, (a,b) \in \mathcal{R} \implies (b,a) \in \mathcal{R}$
Transitive	$\forall a,b,c \in A, (a,b),(b,c) \in \mathcal{R} \implies (a,c) \in \mathcal{R}.$

Consider the relation $\mathcal{R}$ where

$$x\mathcal{R}y \iff |x| = |y|.$$

Checking the three properties reveals that $\mathcal{R}$ is indeed an equivalence relation.

Reflexivity	$\lvert x\rvert = \lvert x\rvert$
Symmetry	$\lvert x\rvert = \lvert y\rvert \implies \lvert y\rvert = \lvert x\rvert$
Transitivity	$\lvert x\rvert = \lvert y\rvert, \lvert y\rvert = \lvert z\rvert \implies \lvert x\rvert = \lvert z\rvert.$

Theorem 1.1 (Partitions from Equivalence Relations). Let A be a non empty set, and $\sim$ be an equivalence relation on A. Then for each $a \in A$ it follows that $\bar{a} := \{x \in A : x \sim a\} \subseteq A$. These subsets produce a partition of A.

Proof. First show that if $\bar{a} \cap \bar{b} \neq \varnothing$, then $\bar{a} = \bar{b}$. Let $w \in \bar{a} \cap \bar{b}$. Consider an element $x \in \bar{a}$. Then $x \sim a$. Since $w \in \bar{a}$ it follows that $w \sim a$ hence $x \sim w$. Since $w \in \bar{b}$, its true that $w \sim b$, meaning $x \sim b$. Therefore $x \in \bar{b}$, meaning $\bar{a} \subseteq \bar{b}$. Other direction follows in the same manner. ■

Definition 1.3 (Powerset). The powerset of a set A, denoted by $\mathcal{P}(A)$, is the set containing all subsets of A. Equivalently,

$$\mathcal{P}(A) = \{S : S \subseteq A\}.$$

Theorem 1.2. Given a finite, non-empty set A, it follows that $\mathcal{P}(A) = 2^{|A|}$.

Proof. Let A be a finite, non-empty set. Define a binary string structure in the following manner. Given a binary string such as

$$\begin{aligned}(0, 0, 0, \ldots, 0) &\implies \varnothing \\ (1, 0, 0, \ldots, 0) &\implies \{a_1\} \\ (1, 1, 0, \ldots, 0) &\implies \{a_1, a_2\} \\ &\vdots\end{aligned}$$

where $a_1, a_2, \ldots a_n$ denote all the elements in A. Therefore, if a set A has n elements, the cardinality of $\mathcal{P}(A)$ is equivalent to the question "How many binary strings are there with length n". Each entry of the string provides 2 choices, $\{0, 1\}$. Therefore since there are n choices in the entirety of the string, the number of binary strings of length n is equal to 2^n. Therefore $\mathcal{P}(A) = 2^n = 2^{|A|}$. ■

Operations

2.1 Binary Operation

Definition 2.4 (Binary Operation). $*$ is a binary operation if it denotes the mapping $* : S \times S \to S$ into some set S that obeys two rules

1. Exactly *one* element is assigned to each possible ordered pair of elements of S
2. For each ordered pair of elements of S, the element assigned to it is again in S

For example, addition on the reals is a binary operation as it is a mapping defined by

$$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R} : (a, b) \mapsto a + b.$$

Often in abstract algebra, imposing or analyzing structure provides the greatest insight. Therefore there are certain algebraic properties commonly used to identify binary operations. Consider for example the concept of *closure*.

Definition 2.5 (Closure). Let $*$ be a binary operation on S. Let $H \subseteq S$. H is closed under $*$ if for all $(u, v) \in H \times H$ that $u * v \in H$.

Example 2.1. Examine the normal addition and multiplication of integers

$$+, \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}.$$

Consider the subset $H = \{2n + 1 : n \in \mathbb{Z}\} \subseteq \mathbb{Z}$. Firstly one has to ask if either operations are indeed a binary operation on H. In the case of multiplication, one can consider two elemenets $a, b \in H$. Therefore $\exists m, n \in \mathbb{Z}$ such that $a = 2n + 1$ and $b = 2m + 1$. Multiplying them together results in $2(2m^2+2mn)+1$ which is indeed in H. For addition, $5 \in H$ and $3 \in H$, however $3 + 5 = 8 \notin H$.

Remark. Given an arbitrary binary operation $*$, it is not always the case that $a * b = b * a$. If a binary operation indeed does have $a * b = b * a$, it is *commutative*.

Definition 2.6 (Commutative Operation). A binary operation $*$ on S is commutative if $\forall a, b \in S$ that $a * b = b * a$.

Pulling from other well known operations, we can generalize the notion of associativity from multiplication and addition to a general binary operation.

Definition 2.7 (Associativity). A binary operation $*$ on S is associative if $\forall a, b, c \in S$ that $(a * b) * c = a * (b * c)$.

Example 2.2. Consider a (potential) binary operation. Define the set $F = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$. Define the operation $*$ by

$$f * g \mapsto f \circ g.$$

> It is fairly obvious that $*$ is indeed a binary operation as the composition of two real valued functions should still remain real valued. One may want to say $*$ is commutative, however consider the following functions
>
> $$f(x) = x + 1$$
> $$g(x) = x^2.$$
>
> It follows fairly quickly that $f \circ g \neq g \circ f$ in this instance, meaning $*$ can not be commutative. Now a harder question is if $*$ is associative. This would require that for all possible real valued functions f, g, h that $f \circ (g \circ h) = (f \circ g) \circ h$. Surprisingly this is true. Note that
>
> $$\begin{aligned} f \circ (g \circ h) &= f \circ (g(h(x))) \\ &= f(g(h(x))). \end{aligned}$$
>
> and that
>
> $$\begin{aligned} (f \circ g) \circ h &= (f(g(x))) \circ h \\ &= f(g(h(x))). \end{aligned}$$
>
> Hence both are equivalent meaning $*$ is indeed associative.

2.1.1 Tabular Representation

If given a finite set S, a binary operation $*$ on S can be defined by tabulating all possible combinations of elements $a, b \in S$. Consider for example $S = \{a, b\}$. The operation can then be defined as

$*$	a	b
a	b	b
b	a	a

Consider then what the outcome of $a * b$ would be. Using the table, the first element will index the row and the second element will index the column. Therefore $a * b = b$. Consider the following question:

How many possible binary operations can be defined on a finite set?

The tabular representation of a binary operation is useful in this instance. Given the set S that $*$ is over, define $n = |S|$. The table will therefore have n^2 entries in it. Each entry has n choices as it can be any element of S. Therefore since you have n choices n^2 times, therefore

$$\text{Number of possible relations} = n^{n^2}.$$

Remark. Not every binary operation is well defined

Consider for example $* : \mathbb{R} \times \mathbb{R} \to \mathbb{R} : (a, b) \mapsto a^b$. Note that $-1 * \sqrt{2} = (-1)^{\sqrt{2}} \notin \mathbb{R}$, hence $*$ in this case is not well defined.

Binary Structures

3.1 Isomorphic Binary Structures

Definition 3.8 (Binary Algebraic Structure). $\langle S, * \rangle$ is a binary algebraic structure if S is a set and $*$ is a binary operation defined over S.

Definition 3.9 (Homomorphism Property). Two binary structures $\langle S, * \rangle$ and $\langle S', *' \rangle$ are homomorphic if there exists a mapping $\phi : S \longrightarrow S'$ such that

$$\phi(x * y) = \phi(x) *' \phi(y).$$

Definition 3.10 (Isomorphic Binary Algebraic Structures). Two binary structures $\langle S, * \rangle$ and $\langle S', *' \rangle$ are isomorphic if there exists a mapping $\phi : S \longrightarrow S'$ such that it is homomorphic, one-to-one, and onto.

The following example structures are isomorphic

$$\begin{aligned} \langle [0,1], +_1 \rangle &\simeq \langle [0,c], +_c \rangle \\ \langle U_n, \cdot \rangle &\simeq \langle \mathbb{Z}_n, +_n \rangle \\ \langle \mathbb{Z}, + \rangle &\simeq \langle 2\mathbb{Z}, + \rangle. \end{aligned}$$

Consider the structures $\langle \mathbb{Q}, + \rangle$ and $\langle \mathbb{R}, + \rangle$. Are these two structures isomorphic? Indeed they cannot be because $|\mathbb{Q}| = \aleph_0$ and $|\mathbb{R}| \neq \aleph_0$. Therefore there cannot exist a onto-to-one and onto map between the structures, hence they cannot be isomorphic.

In general one can follow a process to show that two binary structures $\langle S, * \rangle$ and $\langle S', *' \rangle$ are isomorphic.

1. Define some function ϕ that will be shown to be an isomorphism from S to S'.
2. Show that ϕ is one-to-one.
3. Show that ϕ is onto.
4. Show that the homomorphic property holds under ϕ. That is that $\phi(x * y) = \phi(x) *' \phi(y)$ for all $x, y \in S$

Introduction to Groups

4.1 Groups

Consider past experiences with basic algebra. Beyond simple computation, computation would be used to solve equations. The simplest possible equations done would be linear equations of the form $a + x = b$. Condsider the example equation $5 + x = 3$. Then one would solve it by doing

$$\begin{aligned} 5 + x &= 3 \\ -5 + (5 + x) &= -5 + 3 \\ (-5 + 5) + x &= -5 + 3 \\ 0 + x &= -5 + 3 \\ x &= -5 + 3 \\ x &= -2. \end{aligned}$$

What was required to solve this equation? There were 3 mains things. Firstly associativity had to be utilized in order to group the -5 and 5 numbers together. Second, there needed to be a *neutral* element, in this instance 0. Thirdly, there needed to be an inverse element, in this instance -5. Therefore this shall be the motivation behind the definition of a group.

Definition 4.11 (Group). A group $\langle G, * \rangle$ is a set G closed under the binary operation $*$ such that it follows three axioms.

1. For all $a, b, c \in G$, we have

$$(a * b) * c = a * (b * c).$$

2. There exists an element $e \in G$ such that for all $x \in G$, we have

$$e * x = x * e = x.$$

3. For each element $a \in G$, there is an element $a' \in G$ such that

$$a * a' = a' * a = e.$$

Example 4.3. Take the structure $\langle Z, * \rangle$ where $a * b = a \cdot b$. The structure is not a group since there is no inverse element for *any* of the elements, therefore it certianly cannot be a group

4.2 Subgroups

Definition 4.12 (Subgroup). A subset H of a group G is a subgroup if it is

1. Closed under the binary operation of G
2. H with the induced operation of G is a group

The notation $H \leq G$ and $G \geq H$ denotes that H is a subgroup of G, and additionally $H < G$ and $G > H$ denote that H is a subgroup of G where $H \neq G$.

To show that a given subset of G is a subgroup over its induced binary operation, one can follow a simple 3 condition process. This process can be shrunken down to one condition as proved in Theorem 4.5.

Theorem 4.3 (Subgroup). A subset H of G is a subgroup of G if and only if

1. H is closed under the binary operation of G
2. The identity element e of G is in H
3. For all $a \in H$ it is true that $a^{-1} \in H$

Example 4.4. Consider the subset of $M_n(\mathbb{R})$ defined as

$$S = \left\{A \in M_n(\mathbb{R}) : A^\top A = I_n\right\}.$$

under the binary operation of matrix multiplication. Check the conditions that S is a subgroup of $M_n(\mathbb{R})$.

(Closure) Let $A, B \in S$. Then

$$\begin{aligned}(AB)^\top AB &= B^\top A^\top AB \\ &= B^\top I_n B \\ &= B^\top B \\ &= I_n.\end{aligned}$$

Therefore $AB \in S$.

(Identity) The identity matrix I_n is in S since $I_n = I_n^\top$, therefore

$$I_n^\top I_n = I_n I_n = I_n.$$

Therefore S has an identity element.

(Inverse) Let $A \in S$.

4.3 Generators and Cyclic Subgroups

Consider the group $\mathbb{Z}_n$ under modular addition. Something of interest to note is that every element in $\mathbb{Z}_n$ can be written as the repeated addition of 1. Take for example $\mathbb{Z}_3 = \{0, 1, 2\}$. It follows then that

$$\begin{aligned}1 &= 1 \\ 1 +_3 1 &= 2 \\ 2 +_3 1 &= 0.\end{aligned}$$

In this instance, the repeated operation of 1 produced all the elements of $\mathbb{Z}_3$. In a sense, the element 1 *generated* the entire group. This idea can be cautified abstractly.

Definition 4.13 (Generator). An element g of a group G is a generator for G if the set

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

Is equivalent to G. That is

$$\langle g\rangle = G.$$

Note that all elements of a group G function as generators that produce a cyclic subgroup.

Example 4.5. Consider the cyclic subgroup of $GL(2,\mathbb{R})$ with the generator

$$\left\langle \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \right\rangle.$$

For simplicity, denote the matrix as a and the identity matrix as e. Note that then

$$\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

meaning that $a^2 = e$, implying that $a^{2n} = e$ and $a^{2n+1} = a$. Additionally, since $a^2 = e$, it follows that $a = a^{-1}$. therefore

$$\left\langle \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\} \leq GL(2,\mathbb{R}).$$

Example 4.6. Consider the cylic subgroup of $GL(2,\mathbb{R})$ with the generator

$$\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle.$$

Note that multiplaction of the matrix results in

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}.$$

In general,

$$\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & m+n \\ 0 & 1 \end{bmatrix}.$$

Therefore if a denotes the generating elements

$$a^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}.$$

Additionally, $a^{-n}a^n = e$, meaning

$$a^{-n} = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}.$$

Hence the group generated by a is

$$\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} : k \in \mathbb{Z} \right\}.$$

Example 4.7. Is the following group cyclic?

$$G = \left\{ a + b\sqrt{2} : a, b \in \mathbb{Z} \right\}.$$

The group is not cylic.

Proof. Assume towards contradiction that G is cylic. Consider two cases for a choice of generator. Assume that $b = 0$. Then all possible generators are in the form a where $a \in \mathbb{Z}$. However $a \neq \sqrt{2} \in G$, hence b cannot be zero. Assume then that $b \neq 0$. Then all generators are of the form $a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$. However, the generator will never result in any integers since $a + b\sqrt{2} \notin \mathbb{Z}$. Therefore the group cannot be cylic since there are no possible generators of the group. ∎

Theorem 4.4. A group with no proper non-trivial subgroups is cyclic

Proof. Let G be a group and assume that it has no proper non-trivial subgroups, meaning that the only subgroups of G are $\{e\}$ and G. The case where $G = \{e\}$ is trivial. Therefore let $g \in G$ such that $g \neq e$. Then $\langle g \rangle \leq G$. However since G has no proper non-trivial subgroups, $\langle g \rangle \neq G$ and hence $\langle g \rangle = G$ ∎

Theorem 4.5 (Singular Subgroup Condition). *H is a subgroup of G if and only if $ab^{-1} \in H$ for all $a, b \in H$.*

Proof. Let G be a group and $H \subseteq G$. Assume that $\forall a, b \in H$ that $ab^{-1} \in H$. Consider the three conditions (out of order in this case) in Theorem 4.3

2.) Let $a \in H$. Then $aa^{-1} \in H$, or equivalently $e \in H$. Therefore H contains the identity element of G.

3.) Let $b \in H$. Since $e \in H$, it follows that $eb^{-1} \in H$, or equivalently $b^{-1} \in H$. Therefore H has an inverse for every element within itself.

1.) Let $a, b \in H$. Since H contains inverses for every element, $b^{-1} \in H$ and also $(b^{-1})^{-1} \in H$. Therefore $a(b^{-1})^{-1} \in H$ or equivalently $ab \in H$. Hence H is closed under the binary operation of G.

Since H satisfies the 3 condition of Theorem 4.3, it follows that $H \leq G$. ∎

Permutations

5.1 Groups of Permutations

Theorem 5.6 (Symmetric Groups). Let A be a set and define

$$S_A = \{\phi : \phi : A \to A, \text{ one-to-one and onto}\}.$$

S_A equipped with the binary operation of composition is a group.

Consider the basic example where $A = \{1, 2, 3\}$. Consider an example element $\phi \in S_A$. It can be defined in the following way

$$\begin{aligned} \phi(1) &\to 1 \\ \phi(2) &\to 3 \\ \phi(3) &\to 2. \end{aligned}$$

Something of interest is a map from S_A can also be naturally expressed as a matrix like the following

$$\phi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

These groups defined over these sets are called **symmetric groups**.

5.1.1 Cayley's Theorem

Arguably one of the most interesting and powerful results in elementary group theory is Cayley's Theorem which makes a statement about *all* groups.

Lemma 5.1. Let G and G' be groups and let $\phi : G \to G'$ be a one-to-one function such that

$$\phi(xy) = \phi(x)\phi(y)$$

for all $x, y \in G$. Then $\phi[G]$ is a subgroup of G and ϕ is an isomorphism from $G \to \phi[G]$

Proof. Let G be a group and define ϕ as above. Consider then $\phi[G]$. Let $a, b \in \phi[G]$. Then there are $u, v \in G$ such that $a = \phi(u)$ and $b = \phi(v)$. Therefore

$$ab = \phi(u)\phi(v) = \phi(uv) \in \phi[G],$$

meaning $\phi[G]$ is a closed binary algebraic structure. Consider the group axioms.

$\mathcal{G}_1$ Associativity is trivial

$\mathcal{G}_2$ Let e be the identity of G and define $e' = \phi(e)$. Note that for all $g' \in G'$ that there exits $g \in G$ such that $g' = \phi(g)$. Therefore

$$e'g' = \phi(e)\phi(g) = \phi(eg) = \phi(g) = g'.$$

Hence every element of $\phi[G]$ has a left identity.

$\mathcal{G}_3$ Let $g' \in \phi[G]$. Then there is $g \in G$ such that $g' = \phi(g)$. Consider $\phi(g^{-1}) = g'' \in \phi[G]$. Then

$$g'g'' = \phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e) = e'.$$

Hence every element of $\phi[G]$ has a left inverse.

Since $\phi[G]$ is closed and satisfies the left sided group axioms, it is a group. ■

Theorem 5.7 (Cayley's Theorem). Any group is isomorphic to a subgroup of some symmetric group.

Cayley's Theorem. Let G be a group. It is sufficient to find a map $f : G \longrightarrow S_G$ that is one-to-one and for all $u, v \in G$ that $f(uv) = f(u)f(v)$. Then by Lemma 5.1, $G \simeq \phi[G]$. Let $\lambda_x : G \longrightarrow G$ such that $\lambda_x(g) = xg$. Let $c \in G$ and note that $\lambda_x(x^{-1}c) = c$, hence λ_x is onto. Let $a, b \in G$ and assume that $\lambda_x(a) = \lambda_x(b)$. Then

$$\begin{aligned} \lambda_x(a) &= \lambda_x(b) \\ xa &= xb \\ a &= b, \end{aligned}$$

meaning λ_x is one-to-one. Note that λ_x represents a permutation of all the elements of G. Now define the mapping

$$f : G \longrightarrow S_G : x \mapsto \lambda_x.$$

Suppose that $f(x) = f(y)$. That is, $\lambda_x = \lambda_y$ as functions mapping $G \longrightarrow G$. This means $\lambda_x(e) = \lambda_y(e)$ which implies $xe = ye$. Therefore $x = y$. Let $g \in G$. Then $\lambda_{xy}(g) = (xy)g$. Note that $\lambda_x(\lambda_y(g)) = (x)(yg) = (xy)g$. Therefore $\lambda_{xy} = \lambda_x\lambda_y$. ■

Orbits

Definition 5.14 (Orbit). Let $\sigma \in S_n$. The orbit of an element a under σ is defined as

$$O_\sigma(a) = \{\sigma^n(a) : n \in \mathbb{Z}\}.$$

Example 5.8. Consider the permutation from S_5

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}.$$

Then the orbit of 1 in this case is

$$1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 1 \xrightarrow{\sigma} \dots.$$

Therefore the chain loops, meaning

$$O_\sigma(a) = \{1, 3\}.$$

Example 5.9. Consider the permutation from S_4

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}.$$

σ has only three orbits. It is obvious that $O_\sigma(1) = \{1\}$ and $O_\sigma(2) = \{2\}$. Additionally, there is a cycle between 3 and 4, hence $O_\sigma(3) = O_\sigma(4) = \{3, 4\}$.

Definition 5.15. Let $\sigma \in S_n$. The permutation σ is called a cycle if it has at most 1 orbit containing more than 1 element.

Lemma 5.2. Two orbits of a permutation are either the same or disjoint.

Proof. Let $\sigma \in S_n$ and consider for $a, b \in S_n$ the orbits $O_\sigma(a)$ and $O_\sigma(b)$. If there exists $x \in O_\sigma(a) \cap O_\sigma(b)$, then there are integers m, n such that

$$x = \sigma^m a = \sigma^n b.$$

Note that for some arbitrary $s \in \mathbb{Z}$ that

$$\sigma^s(a) = \sigma^{s-m}(\sigma^m(a)) = \sigma^{s-m}(\sigma^n(b)) = \sigma^{s-m+n}(b).$$

Since $O_\sigma(a) = \{\sigma^n a : n \in \mathbb{Z}\}$, then $\sigma^s(a) = \sigma^{s-m+n}(b) \in O_\sigma(a)$. Therefore $O_\sigma(a) \subseteq O_\sigma(b)$. The roles of a and b can be swapped to achieve $O_\sigma(b) \subseteq O_\sigma(a)$. Hence the two are equal. If there does not exist an x in the intersection, the two cycles are disjoint. ■

Theorem 5.8 (Permutations as a Cyclic Product). Every permutation σ of a finite set is a product of disjoint cycles.

Proof. Let $\sigma \in S_n$. Consider all orbits of σ,

$$O_\sigma(1), O_\sigma(2), \ldots, O_\sigma(n).$$

■

5.2 Cartesian Product of Groups

Definition 5.16 (Cartesian Product of Sets). The cartesian product of a collection of sets $A_1, A_2, \dots A_n$ is the set of all ordered n-tuples

$$x = (a_1, a_2, \dots, a_n)$$

where $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$ and is denoted as

$$A_1 \times A_2 \times \dots \times A_n = \prod_{i=1}^{n} A_i$$

Since groups add structure to sets, it makes sense to apply the idea of a cartesian product to a collection of groups rather than a collection of sets.

Definition 5.17 (Direct Product of Groups). The direct product of a collection of groups $G_1, \dots, G_n$ is

$$G = \prod_{i=1}^{n} G_i$$

where the binary operation of two elements of G, for example $g, h \in G$, is defined as

$$gh = (g_1 *_1 h_1, g_2 *_2 h_2, \dots, g_n *_n h_n).$$

An important property of the direct product is that itself gives rise to a group structure. This can be checked by examining it under the group axioms.

Theorem 5.9 (Group Structure of Direct Product). The direct product of a collection of groups $G_1, G_2, \dots G_n$ is a group

Proof. Let G be the direct product of a collection of groups $G_1, \dots, G_n$. First examine clsoure. Let $g, h \in G$ and consider gh. Then

$$gh = (g_1 *_1 h_1, g_2 *_2 h_2, \dots, g_n *_n h_n).$$

Since $g_1 *_1 h_1 \in G_1, \dots, g_n *_n h_n \in G_n$, G is closed. Consider the group axioms.

$\mathcal{G}_1$ Let $g, h, z \in G$. Considering $g(hz)$ and $(gh)z$, it arises that they must be equal as each component of the n-tuple are independent with a corresponding binary operation from a group. Since these operations must be associative, the operation of G must also be associative.

$\mathcal{G}_2$ Let $e_1 \in G_1, \dots, e_n \in G_n$ be the identity elements of the collection of groups. Then $e = (e_1, e_2, \dots, e_n) \in G$, therefore G has an identity element.

$\mathcal{G}_3$ Let $a \in G$. Choose a^{-1} as $(a_1^{-1}, \dots, a_n^{-1})$. It follows quickly that $aa^{-1} = e$. Hence every element of G has an inverse.

Since G is closed and follows the group axioms, it is a group. ■

Consider the special case where each group of the collection G_i is an abelian group. In this case, the direct product is sometimes called a *direct sum*, harkening to the abelian nature of addition. The group direct sum of the groups G is itself an abelian group.

Example 5.10. Consider the direct product $\mathbb{Z}_2 \times \mathbb{Z}_2$. By direct enumeration, $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$. Since $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 4, it is either isomorphic to $\mathbb{Z}_4$ or K_4. Since each element is its own inverse, it cannot be cyclic (because $|(a,b)| < 2$) and hence $\mathbb{Z}_2 \times \mathbb{Z}_2 \simeq K_4$.

In this instance, the direct sum of two cyclic groups was not cyclic. Therefore one may conjecture that the direct sum of cyclic groups does not preserve the cyclic property. Consider another simple case.

Example 5.11. Consider the direct product $\mathbb{Z}_2 \times \mathbb{Z}_3$. By direct enumeration, $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0),(1,0),(0,1),(1,1),(1,2),(0,2)\}$. Note that in this case $(1,1)$ and $(1,2)$ generates the direct sum.

Therefore in some cases, the direct sum is cyclic and other cases it is not. Consider the class of direct products of cyclic groups of the same order n. Note the order of $\mathbb{Z}_n \times \mathbb{Z}_n = n^2$. However, given any element $(a,b) \in \mathbb{Z}_n \times \mathbb{Z}_n$, $(a,b)^n = e$. This implies $|(a,b)| \leq n$, hence (a,b) cannot generate the entire group. Since (a,b) was any element, no element generates the group. This explains why in example 5.10 the group was not cyclic. Consider now the following theorem.

Theorem 5.10. The direct product $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if m and n are relatively prime.

Proof. Consider the two directions.

($\Rightarrow$) Assume that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic. Let $(r,s) \in \mathbb{Z}_m \times \mathbb{Z}_n$ where (r,s) is the generator. Consider $(r,s)^{\frac{mn}{d}}$ where $d = \gcd(m,n)$. Note that

$$(r,s)^{\frac{mn}{d}} = (r^{mn}, s^{mn})^{\frac{1}{d}} = (e,e).$$

Therefore the order of $(r,s) \leq \frac{mn}{d}$, meaning $|(r,s)| < mn$ if and only if $d > 1$. However, since (r,s) generates the group, $|(r,s)| = mn$, hence d must be equal to 1. Hence $\gcd(r,s) = 1$.

($\Leftarrow$) Assume that $\gcd(m,n) = d = 1$. Note that the element $(1,1)$ generates a cyclic subgroup. Note that there are integers p,q such that $N = mp = qn$ with $(1,1)^N = e$. Since m and n are coprime, $N = mn$ is the smallest integer such that $(1,1)^N = e$.

Therefore the direct product $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if m and n are coprime. ■

Homomorphisms and Factor Groups

6.1 Homomorphisms

Definition 6.18 (Image and Inverse Image). Let $\phi : X \to Y$ be a mapping from X to Y and let $A \subseteq X$ and $B \subseteq Y$. The image of A in Y is $\phi[A] = \{\phi(a) : a \in A\}$. The inverse image of B in X is $\phi^{-1}[B] = \{x \in X : \phi(x) \in B\}$. The set $\phi[X]$ is sometimes reffered to as the range of ϕ.

Definition 6.19 (Homomorphism). A map ϕ of a group G into another group G' is a homomorphism if $\forall a, b \in G$

$$\phi(ab) = \phi(a)\phi(b).$$

Theorem 6.11 (Properties of Homomorphisms). If ϕ is a homomorphism between two groups G and G', then the following are true

1. If $e \in G$ is the identity, $\phi(e)$ is the identity of G'.
2. If $a \in G$, then $\phi(a^{-1}) = \phi(a)^{-1}$
3. If $H \leq G$, then $\phi[H] \leq G'$.
4. If $K' \leq G' \cap \phi[G]$, then $\phi^{-1}[K'] \leq G$

Proof. Let ϕ be a homomorphism between groups G and G'.

1.) $\forall a \in G, \phi(a) = \phi(ea) = \phi(e)\phi(a)$. Therefore $\phi(e)$ must be the identity in G'

2.) $\forall a \in G, \phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$, therefore $\phi(a^{-1}) = \phi(a)^{-1}$

3.)

4.)

■

Definition 6.20. Let $\phi : G \to G'$ be a homomorphism of groups. Then $\phi^{-1}[\{e'\}] = \{x \in G : \phi(x) = e'\} \leq G$ is the kernel of ϕ, denoted as $\ker(\phi)$.

Theorem 6.12. A homomorphism $\phi : G \to G'$ between groups is a one-to-one map if and only if $\ker(\phi) = \{e\}$.

Proof. Let $\phi : G \to G'$ be a homomorphism of two groups.

($\Rightarrow$) Assume that ϕ is a one-to-one map. Note $\ker(\phi) = \{x \in G : \phi(x) = e'\}$. By theorem 6.11, $\phi(e) = e'$. Since ϕ is one-to-one, this is the only mapping to e', therefore $\ker(\phi) = \{e\}$.

(⇐) Assume that $\ker(\phi) = \{e\}$. Let $a, b \in G$ and assume $\phi(a) = \phi(b)$. Note that

$$e' = \phi(b)\phi(b)^{-1} = \phi(a)\phi(b)^{-1} = \phi(ab^{-1}).$$

Therefore $ab^{-1} \in \ker(\phi)$, meaning $ab^{-1} = e \implies a = b$, hence ϕ is one-to-one.

Both directions are thus proven. ■

Factor Groups

Theorem 6.13 (Factor Group Isomorphism). Let $\phi : G \to G'$ be a group homomorphism. Then the cosets of $\ker(\phi)$ form a factor group, $G/\ker(\phi)$ of which the map $\mu : G/\ker(\phi) \to \phi[G]$ defined by $\mu(aH) = \phi(a)$ is an isomorphism.

Proof. Let $\phi : G \to G'$ be a group homomorphism and let $H = \ker(\phi)$. Consider the mapping $\mu : G/H \to \phi[G]$ where $\mu(aH) = \phi(a)$. First examine if μ is well defined. Let $g_1H, g_2H \in G/H$ and assume that $\mu(g_1H) = \mu(g_2H)$. That is, $\phi(g_1) = \phi(g_2)$. Note that $g_1, g_2 \in H$ and therefore $g_1h_1 = g_2h_2$ for some $h_1, h_2 \in H$ or equivalently $g_1 = g_2h$ for some $h \in H$. Therefore $g_2^{-1}g_1 = h \in H$. Therefore $\phi(g_2^{-1}g_1) = e$, meaning $\phi(g_1) = \phi(g_2)$. One-to-one follows by doing a reversed argument. Examining the homomorphic property, let $g_1H, g_2H \in G/H$. Then $\mu(g_1Hg_2H) = \mu(g_1g_2H) = \phi(g_1g_2) = \phi(g_1)\phi(g_2)$. Also $\mu(g_1H)\mu(g_2H) = \phi(g_1)\phi(g_2)$. ■

Example 6.12. Consider the factor group $\mathbb{Z}_{11} \times \mathbb{Z}_{15} / \langle(1,1)\rangle$. What is its order? Since a factor group is collection of cosets, a partition is formed over $\mathbb{Z}_{11} \times \mathbb{Z}_{15}$ by the subgroup $\langle(1,1)\rangle$. It is then true that $|G| = |H| \cdot |G/H|$. Therefore the order of the factor group should be $\frac{|\mathbb{Z}_{11} \times \mathbb{Z}_{15}|}{|\langle(1,1)\rangle|} = \frac{165}{165} = 1$

List of Theorems

1.1 Theorem (Partitions from Equivalence Relations) 2
4.3 Theorem (Subgroup) 8
4.5 Theorem (Singular Subgroup Condition) 10
5.6 Theorem (Symmetric Groups) 11
5.7 Theorem (Cayley's Theorem) 12
5.8 Theorem (Permutations as a Cyclic Product) 13
5.9 Theorem (Group Structure of Direct Product) 14
6.11 Theorem (Properties of Homomorphisms) 16
6.13 Theorem (Factor Group Isomorphism) 17

List of Definitions

1.1 Definition (Relations) 2
1.2 Definition (Equivalence Relation) 2
1.3 Definition (Powerset) 3
2.4 Definition (Binary Operation) 4
2.5 Definition (Closure) 4
2.6 Definition (Commutative Operation) 4
2.7 Definition (Associativity) 4
3.8 Definition (Binary Algebraic Structure) 6
3.9 Definition (Homomorphism Property) 6
3.10 Definition (Isomorphic Binary Algebraic Structures) 6
4.11 Definition (Group) 7
4.12 Definition (Subgroup) 7
4.13 Definition (Generator) 9
5.14 Definition (Orbit) 12
5.16 Definition (Cartesian Product of Sets) 14
5.17 Definition (Direct Product of Groups) 14
6.18 Definition (Image and Inverse Image) 16
6.19 Definition (Homomorphism) 16