MATH 113: Introduction to Abstract Algebra

Michael Pham

Fall 2024

Contents

Week 1
Introductions

1.1 Lecture – 8/29/2024

1.1.1 What is Algebra?

To begin with, when we see the word "algebra", we think of equations.

Example 1.1 (Where Algebra Comes In). Suppose we were asked to solve the following equation:

$$x(x+y) = yx$$

A typical way of solving it would be as follows:

$$x(x+y) = yx \tag{1.1}$$
$$x^2 + xy = yx \tag{1.2}$$
$$x^2 = yx + (-1)(xy) \tag{1.3}$$
$$x^2 = yx + (-1)(yx) \tag{1.4}$$
$$x^2 = 0 \tag{1.5}$$
$$x = 0 \tag{1.6}$$

When going through this basic example, we note in (1.4), we are assuming that $xy = yx$; this is where the idea of "algebra" actually comes into play! We are assuming here that we have commutativity.

Similarly, in (1.6), we are assuming that $x^2 = 0 \implies x = 0$. Once again, we are making assumptions that these properties hold and we are working with some underlying structure in-place.

This is algebra.

! We note that $xy = yx$ doesn't always hold! For example, let us look at matrix multiplication:

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

However, we see that if we multiplied them in the other order, we would instead get:

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

! We also note that $x^2 = 0 \implies x = 0$ isn't true! Again, we can look towards matrices for a counterexample:

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

Now, we look at the following example:

Example 1.2 (Sneak Peek into Groups)**.** Let us consider the following equation: $x + a = b$.

To solve for x, we can proceed as follows:

$$\begin{aligned} x + a &= b \\ (x + a) + (-a) &= b + (-a) && \textit{(Inverse)} \\ x + (a + (-a)) &= b + (-a) && \textit{(Associativity)} \\ x + 0 &= b + (-a) \\ x &= b + (-a) && \textit{(Identity)} \end{aligned}$$

In each line, we note the property needed to make the step. We also note here that this foreshadows the concept of "groups" – sets with some operation satisfying the three properties mentioned above.

Example 1.3 (Some Counterexamples)**.** We can think of some basic examples of sets which don't satisfy (at least one of) the properties:

- $(\mathbb{N}, +)$ doesn't satisfy inverses.
- $(\mathbb{N}, \times)$ doesn't satisfy inverses.
- $(\mathbb{R}^{n\times n}, \times)$ doesn't satisfy associativity.

1.1.2 Some Proofs Techniques

Going into this course, writing proofs will play an important part. As such, it is important to recall certain proof techniques:

- Proof by Contradiction
  - For example, we can use this to prove that $\sqrt{2}$ is irrational.
- Proof by Cases
  - For example, we can use this to prove that $x(x+1)$ is even.

- (Strong) Induction
  - For example, we can use this to prove that $\sum_{i=1}^{n} = \frac{n(n+1)}{2}$.

1.2 Lecture – 8/30/2024

1.2.1 Administrivia

Textbooks Used

For the purposes of this course, we will mostly be working with Judson's *Abstract Algebra: Theory and Applications*. The book will be referred to as [Open].
Another very good textbook that will sometimes be referenced is Dummit and Foote's *Abstract Algebra*. This will be referred to by [DF].

We also note that any schedule provided for the timeline of topics is approximate; pacing may vary!

1.2.2 Pre-Examples

In this lecture, we will be looking at the concept of equivalence classes.

Example 1.4 (The Rationals $\mathbb{Q}$). To begin with, let us consider the set $\mathbb{Q}$ and how we can describe the elements in it.

A naive approach is to simply state that for $q \in \mathbb{Q}$, we can write it such that $p \in \mathbb{Z}$ and $q \in \mathbb{N}$.

However, this doesn't fix a relatively important issue: with this approach, $\frac{1}{2} \neq \frac{2}{4}$, despite us treating them as being the same.

This is where equivalence classes will come into play.

1.2.3 Sets

Definition 1.5 (Set). We define a set as a collection of elements.

A set X can be written in the following ways:

$$\begin{aligned} X &= \{x_1, \ldots, x_n\} \\ &= \{x_i\} \\ &= \{x : \varphi(x)\} \end{aligned}$$

Definition 1.6. For sets X, Y, we let $X \times Y$ to be the Cartesian product defined as:

$$X \times Y = \{(x, y) : x \in X \wedge y \in Y\}.$$

We note that (x, y) is an ordered pair. That is, $(x, y) \neq (y, x)$.

1.2.4 Maps

Definition 1.7 (Map)**.** A map $f : X \to Y$ is a rule that assigns a unique element of Y to each element of X.

It is important to note that a map **must** assign every element in the domain to some element in the codomain. And we note that it must be a *unique* element as well; we can't map one element in the domain to multiple in the codomain.

Types of Maps

Definition 1.8 (Surjectivity)**.** We say that a map $f : X \to Y$ is surjective iff for all $y \in Y$, there exists some $x \in X$ such that $f(x) = y$.

Definition 1.9 (Injectivity)**.** We say that a map $f : X \to Y$ is injective iff for $x_1, x_2 \in X$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$.

Similarly, we can take the contrapositive and say that if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$.

Definition 1.10 (Bijectivity)**.** We say that a map $f : X \to Y$ is bijective iff it is both injective and surjective.

1.2.5 Equivalence Relations

Definition 1.11 (Equivalence Relation)**.** We define an equivalence relation R (or $\sim$) on a set X to be a subset $R \subseteq X \times X$ such that it has the following properties:

- Reflexivity: $\forall x(\langle x, x\rangle \in R)$
- Symmetry: $\forall x \forall y(\langle x, y\rangle \in R \implies \langle y, x\rangle \in R)$.
- Transitivity: $\forall x \forall y \forall z(\langle x, y\rangle \in R \land \langle y, z\rangle \in R \implies \langle x, z\rangle \in R)$.

We say that $x \sim y$ iff $\langle x, y\rangle \in R$.

Definition 1.12 (Equivalence Class)**.** We say that an equivalence class of $x \in X$ is a set defined as follows:

$$[x] = \{y \in X : (x, y) \in R\} = \{y \in X : x \sim y\}$$

Definition 1.13 (Quotient)**.** A quotient of X by an equivalence relation R is $X/\sim$, which is the set of all R-equivalence classes.

Example 1.14 (Ages on Humans)**.** Suppose that we are looking at the set of all human beings. We denote this by S.

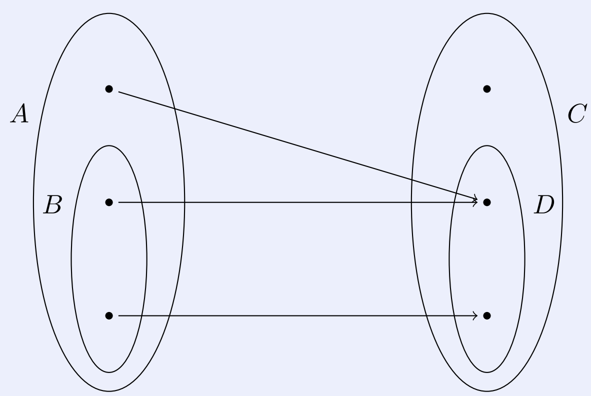
Now, one way to partition them up is to group them into their ages. Then, we can think of each age as being an equivalence class, containing all the human beings that fall under said age. Furthermore, the set of all of the ages can be thought of as the quotient.

Week 2
Second Week Woes

2.1 Lecture – 9/4/2024

2.1.1 Warm Up

Problem 2.1 (Types of Maps)**.** Suppose we have the following map:



Based off of this graph, suppose we had the following maps:

1. $f : A \to C$.
2. $f : A \to D$.
3. $f : B \to C$.
4. $f : B \to D$.

Now, we want to determine whether the maps are injective, surjective, bijective, or none.

Solution. For $f : A \to C$, we see that since two elements are mapped to the same element in D, it isn't an injection. Furthermore, not all elements of C are being mapped to by f, so it is not a surjection either. Thus, it is **neither**.

For $f : A \to D$, we see that it isn't injective due to the same reason provided previously. However, all elements of D are mapped to by some element of A. Thus it is a **surjection**.

For $f : B \to C$, we see that not all elements of C are mapped to by an element in B. However, each element in B map to a different element in C. Thus, it is an **injection**.

For $f : B \to D$, we see that it's still injective by the previous reason. However, since all elements of D are being mapped to by some element in B, it is surjective as well. Thus, it is a **bijection**. ■

2.1.2 $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$

Algebraic Structures

First, let us provide some notation. When we have something like $(\mathbb{Z}, +)$ or $(\mathbb{Z}, \times)$, these are algebraic structures. This is simply a set – so in this case, $\mathbb{Z}$ – equipped with some operation ($+$ and $\times$ in our examples).

> **!** Note that $\mathbb{Z}$ is a countably infinite set.

$(\mathbb{Z}, +)$ versus $(\mathbb{Z}, \times)$

We can do a comparison of the two structures as follows:

$(\mathbb{Z}, +)$:

- Identity: 0.
  - $a + 0 = a$.
- Inverse: $(-a)$
  - $a + (-a) = 0$
- Commutativity
  - $a + b = b + a$

$(\mathbb{Z}, \times)$:

- Identity: 1.
  - $a \times 1 = a$.
- Inverse: None.
- Commutativity
  - $a \times b = b \times a$

2.1.3 Generators

When we write $\mathbb{Z} = \langle 1 \rangle$, this is denoting that 1 generates $(\mathbb{Z}, +)$ as a group.

To make this more concrete, we note that for all $n \in \mathbb{Z}$, we can write n as a sum of n 1's (or (-1)'s).

We note that for $(\mathbb{Z}, \times)$, we can generate it by considering the set of all prime numbers.

By the Fundamental Theorem of Arithmetic, we note htat for all $n \in \mathbb{Z}$, we can write it as follows:

$$n = (\pm 1) \prod_{i=1}^{m} p_i^{a_i},$$

where $m \in \mathbb{N}$, p_i is some prime, and $a_i \in \mathbb{N}$.

> **Theorem 2.1** (Number of Primes). There are infinitely many primes.

Proof. We can proceed by contradiction.

Let us suppose that there are finitely many primes. Then, suppose that we have k primes. We can thus list them $p_1, \ldots, p_k$.

Now, let us consider the product $P = p_1 \cdots p_k$. Then, let us denote $q = P + 1$. By construction then, we note that q is not divisible by any of our $p_1, \ldots, p_k$.

From here, we have two cases:

1. q is a prime number.
2. q is not a prime number.

In the first case, if q is prime, then there is a contradiction. Thus, it follows that there must be infinitely many primes.

In the second case, we note that if q isn't prime, there must exist some prime factor p which divides q. However, by construction, this p cannot be in our list of primes, and thus we have a contradiction.

Therefore, we conclude that there are infinitely many primes. ■

2.1.4 What is $\mathbb{Z}/n\mathbb{Z}$?

We say that $\mathbb{Z}/n\mathbb{Z}$ is the remainder of dividing any $m \in \mathbb{Z}$ by n (where n is some natural number).

With this in mind, let us provide the following definition:

> **Definition 2.2** (Divides By)**.** We say that $n \mid a$ if $(\exists x \in \mathbb{Z})\,(a = xn)$.
>
> More concretely, we note that our remainder is equal to zero in our division algorithm:
>
> $$a = xn + r.$$

Now, we give the following equivalence relation for $\mathbb{Z}$:

> **Definition 2.3.** $\forall a, b \in \mathbb{Z}$, we say that $a \sim b$ iff $n \mid (a - b)$.

Before we proceed further, we should actually confirm if this defines an equivalence relation or not:

1. First, for reflexivity, we see that $(a - a) = 0$. And trivially, we see that $n \mid 0 \implies a \sim a$. Thus, we see that, indeed, $n \mid (a - a)$; $a \sim a$.
2. Next, symmetry. Suppose that $a \sim b$. Then, this means that there exists some $x \in \mathbb{Z}$ such that $xn = a - b$. This means then that $-xn = b - a$, and $-x \in \mathbb{Z}$ as well. Thus, indeed, we see that $n \mid (b - a) \implies b \sim a$.
3. Finally, for transitivity, suppose that $a \sim b$ and $b \sim c$. Then, we note that there exists some x and y such that $a - b = xn$ and $b - c = yn$. Then, $(a - b) + (b - c) = xn + yn$. This becomes $a - c = n(x + y)$, and by closure of $\mathbb{Z}$ under addition, we note that, indeed, $n \mid (a - c) \implies a \sim c$ as desired.

Thus, we see that we do indeed have an equivalence relation.

Equivalence Classes

Now, we look at the equivalence classes of $\mathbb{Z}$ under the given equivalence relation. We observe that for $n = 5$, we have:

$$\begin{aligned}
[0] &= \{\ldots, -5, 0, 5, \ldots\} \\
[1] &= \{\ldots, -4, 1, 6, \ldots\} \\
&\vdots \\
[4] &= \{\ldots, -1, 4, 9, \ldots\}
\end{aligned}$$

And we note that $\cdots = [-5] = [0] = [5] = \cdots$. The same logic applies to the other equivalence classes.

And with all of this, we can finally define $\mathbb{Z}/n\mathbb{Z}$ as the set of equivalence classes for n under the equivalence relation $\sim$.

2.2 Required Reading – 9/6/2024

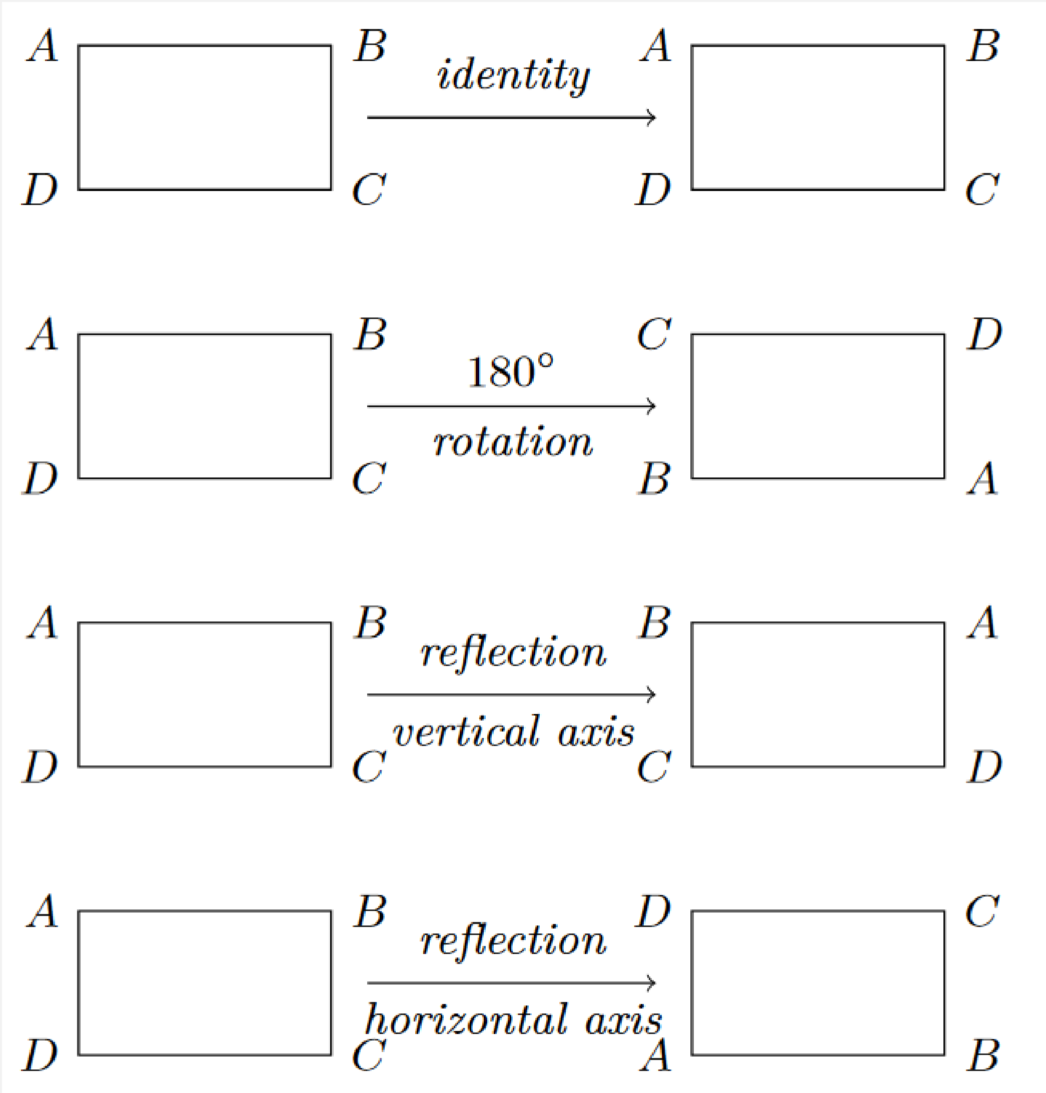
2.2.1 Symmetries

A natural way of thinking about groups is to consider symmetries.

Definition 2.4 (Symmetry)**.** We define a symmetry of a geometric figure to be a rearrangement of the figure which preserves the arrangement of its sides and vertices, along with its distances and angles.

Definition 2.5 (Rigid Motion)**.** A map from the plane to itself preserving the symmetry of an object is called "rigid motion."

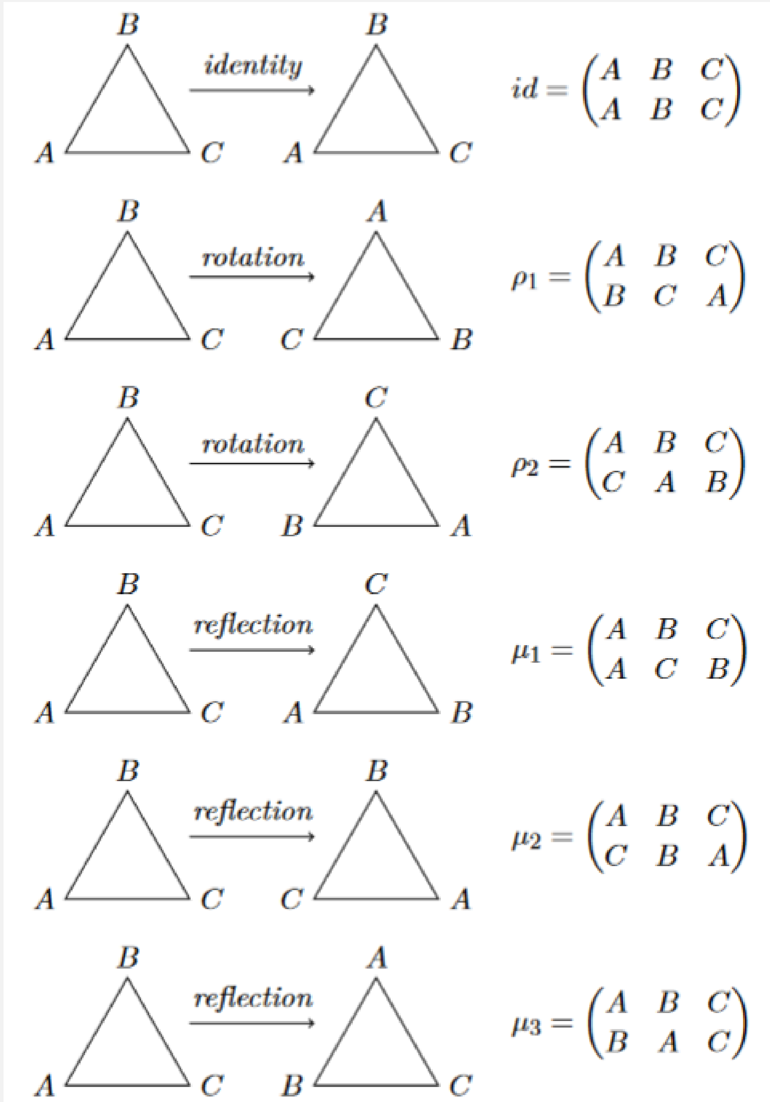
Figure 2.1: Rigid Motions of Rectangle



We observe from the figure above how while the transformations provided preserves the orientation of the rectangle and the relationships among it vertices, if we did something like a $90°$ rotation, it wouldn't be considered a symmetry.

Let us look at a different examples with triangles:

Figure 2.2: Symmetries of a Triangle



First, note that we can encode the transformation using a matrix. Let us look at the following:

$$\begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$$

We observe that this is telling us that we are mapping corner A to C, B to B, and C to A.

Definition 2.6 (Permutation)**.** A permutation of a set S is some bijection $\pi : S \to S$.

An interesting thing to note, which is shown in the figure, is that every permutation (of which there are $3! = 6$) corresponds to some symmetry of our triangle.

Now, a question to ask would be what happens if we combine two different motions for our triangle? For example, let us consider $\mu_1\rho_1$ (that is, we apply ρ_1 onto the triangle, followed by μ_1).

Well, we can proceed as follows:

$$\begin{aligned}\mu_1\rho_1(A) &= \mu_1(B)\\ &= C\\ \mu_1\rho_1(B) &= \mu_1(C)\\ &= B\\ \mu_1\rho_1(C) &= \mu_1(A)\\ &= A\end{aligned}$$

Thus, we note that we get the same transformation as if we simply did μ_2. Note that this is pretty intuitive that composing permutations will result in some new transformation, since they are just bijections from S onto itself.

! We note that we are composing functions when looking at multiple permutations being applied. Thus, we read from right to left.

2.2.2 Definitions and Examples

Groups

As hinted at previous, the integers mod n and the symmetries of a triangle (or rectangle) are all examples of what we call a "group."

Definition 2.7 (Binary Operation). A binary operation (sometimes called a law of composition) on a set G is a function $G \times G \to G$ which assigns to each pair $(a, b) \in G \times G$ a unique element $a \circ b$ (or ab) in G. This is called the composition of a and b.

Definition 2.8 (Group). A group $(G, \circ)$ is defined then as a set G together with some binary operation $(a, b) \mapsto a \circ b$ which satisfies the following three properties:

- Associativity: $(a \circ b) \circ c = a \circ (b \circ c)$, for all $a, b, c \in G$.
- Identity: There exists some identity element $e \in G$ such that $a \circ e = a = e \circ a$, for all $a \in G$.
- Inverse: For every element $a \in G$, there exists some inverse a^{-1} such that $a \circ a^{-1} = e = a^{-1} \circ a$.

Definition 2.9 (Abelian). We note that if a group happens to satisfy commutativity (that is, $a \circ b = b \circ a$), then the group is an abelian group. They are also referred to as being commutative groups.

Examples

Example 2.10 (The Integers $\mathbb{Z}$). First, we note that $(\mathbb{Z}, +)$ forms a group (as seen previously). And in fact, it is actually an abelian group.

On the other hand, $(\mathbb{Z}, \times)$ doesn't, as it fails the inverse check.

Similarly, $\mathbb{Z}/n\mathbb{Z}$ also forms a(n abelian) group. It is often convenient to describe a group in terms of an addition or multiplication table; these are called Cayley tables, specifically.

Example 2.11 (Matrices). We denote $\mathbb{M}_2(\mathbb{R})$ to be the set of all 2×2 matrices. Then, let $GL_2(\mathbb{R})$ to be the subset of $\mathbb{M}_2(\mathbb{R})$ which contains only invertible matrices.

Then, this means that $GL_2(\mathbb{R})$ is in fact a (nonabelian) group under matrix multiplication.

We note that matrix multiplication is associative. Furthermore, we have the identity matrix:

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

And for every matrix A, we have an inverse A^{-1} defined as:

$$A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

2.2.3 Basic Properties of Groups

Proposition 2.12. The identity element in G is unique.

Proof. Suppose for the sake of contradiction that the identity element isn't unique. Then, there exists e, e' (with $e \neq e'$) such that $eg = g = ge$ and $e'g = g = ge'$, for all $g \in G$.

Then, we observe the following: if e is the identity element, then we have that:

$$ee' = e'$$

However, since e' is also the identity element, we see then that:

$$ee' = e$$

In other words, we have:

$$ee' = e = ee' = e'$$

In other words, we have $e = e'$; thus, the identity element is in fact unique. ■

Similarly, we have the following proposition:

Proposition 2.13. For any element $g \in G$, its inverse g^{-1} is unique.

The proof for this is similar to the one for proving uniqueness of the identity.

Proposition 2.14. Let G be a group. If $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. Suppose that G is a group, and we have $a, b \in G$.

Then, we observe the following:

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} \\ &= a(ea^{-1}) \\ &= aa^{-1} \\ &= e\end{aligned}$$

$$\begin{aligned}(b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}a)b \\ &= b^{-1}(eb) \\ &= b^{-1}b \\ &= e\end{aligned}$$

Then, since inverses are unique, we observe then that $(ab)^{-1} = b^{-1}a^{-1}$. ■

Proposition 2.15. Let G be a group. Then, for any $a \in G$, we have that $(a^{-1})^{-1} = a$.

Proof. We proceed as follows:

$$\begin{aligned}(a^{-1})(a^{-1})^{-1} &= e \\ a(a^{-1})(a^{-1})^{-1} &= ae \\ (aa^{-1})(a^{-1})^{-1} &= a \\ e(a^{-1})^{-1} &= a \\ (a^{-1})^{-1} &= a\end{aligned}$$

■

Proposition 2.16. Let G be a group, and $a, b \in G$. Then, the equations $ax = b$ and $xa = b$ have unique solutions.

Proof. Let us suppose that $ax = b$. Then, to show that a solution indeed exists, we proceed as follows:

$$\begin{aligned}a^{-1}(ax) &= a^{-1}b \\ (a^{-1}a)x &= a^{-1}b \\ ex &= a^{-1}b \\ x &= a^{-1}b\end{aligned}$$

Then, let us suppose that there exists x_1, x_2 not equal to each other which both satisfy the equation. Then, we have:

$$\begin{aligned}ax_1 &= b = ax_2 \\ x_1 &= a^{-1}b = x_2 \\ x_1 &= x_2\end{aligned}$$

The proof for $xa = b$ is similar. ■

Proposition 2.17. If G is a group, and $a, b, c \in G$, then $ba = ca$ implies that $b = c$, and $ab = ac$ implies that $b = c$.

Proof. We observe that if $ba = ca$, then we get the following:

$$\begin{aligned} ba &= ca \\ baa^{-1} &= caa^{-1} \\ b &= c \end{aligned}$$

The proof for $ab = ac$ implying $b = c$ is similar. ■

Exponential Notations

We can use exponential notations for groups just as we do in ordinary algebra. Suppose that G is a group, and $g \in G$.

Then, we let $g^0 = e$, and for any $n \in \mathbb{N}$, we define $g^n = g \cdot g \cdots g$ (n times). Similarly, $g^{-n} = g^{-1} \cdot g^{-1} \cdots g^{-1}$ (n times).

Theorem 2.18. In a group, the usual laws of exponents hold:

1. $g^m g^n = g^{m+n}$, for all $m, n \in \mathbb{Z}$.
2. $(g^m)^n = g^{mn}$, for all $m, n \in \mathbb{Z}$.
3. $(gh)^m = (h^{-1}g^{-1})^{-m}$, for all $m, n \in \mathbb{Z}$.

! We note that only in the case of *abelian* groups do we have that $(gh)^n = g^n h^n$.

2.3 Lecture – 9/6/2024

2.3.1 Warm-Up

Problem 2.2. Suppose that we are working in $\mathbb{Z}/10\mathbb{Z}$.

Answer the following questions:

1. $3 \in [14]$?
2. $-4 \in [14]$?
3. $[14] = \{...\}$?
4. Describe $14 \cap \mathbb{N}$ as a subset of $\mathbb{Z}$.

Solution. We provide the solutions below:

1. No; $3 \notin [14]$. It is in $[13]$ though.
2. No; $-4 \notin [14]$. It is in $[16]$ though.
3. $[14] = \{\ldots, -6, 4, 14, \ldots\}$. Alternatively, we can think of this as $[14] = \{n \in \mathbb{Z} : (\exists k \in \mathbb{Z})(n = 4 + 10k)\}$.

4. $[14] \cap \mathbb{N}$ can be thought of as all of the (positive) numbers that ends in 4. More formally, this can be expressed as the following set:

$$[14] \cap \mathbb{N} = \{n \in \mathbb{Z} : (\exists k \in \mathbb{N})(n = 4 + 10k)\}.$$

■

Notations on Modulo

We note that we'll be using $a \equiv b \mod n$ to mean the same as $a \sim b$.

2.3.2 $\mathbb{Z}/n\mathbb{Z}$: Act II

Proposition 2.19. $\mathbb{Z}/n\mathbb{Z}$ has exactly n elements.

Proof. Before proving this proposition, we make the following claim:

Lemma 2.20. Suppose that $[i] \cap [j] \neq \emptyset$. Then, it follows that $[i] = [j]$.

Proof. To prove this claim, let us take any $x \in [i] \cap [j]$. Then, we observe that $x = i + na$, for some $n \in \mathbb{Z}$. Similarly, $x = j + nb$, for some $b \in \mathbb{Z}$.

Then, we have that $x = i + na = j + nb$. Then,

$$\begin{aligned} i + na &= j + nb \\ i - j &= j + nb - na \\ &= n(b - a) \end{aligned}$$

Then, we see that $n \mid (i - j)$. In other words, $i \sim j \implies [i] = [j]$. □

Next, let us introduce the next lemma:

Lemma 2.21. If $i \neq j$ and $0 \leq i, j \leq n - 1$, then $[i] \cap [j] = \emptyset$.

Proof. Let us suppose for the sake of contradiction that $[i] \cap [j] \neq \emptyset$.

Then, it follows that $[i] = [j]$ by Lemma . However, this implies then that for some $x \in [i] \cap [j]$, we have that $i \sim j$. In other words, we have that $i - j = n(b - a)$.

However, we note that $n > |i - j| = |n \cdot (b - a)|$. This means then that $1 > |b - a|$. However, this means that $|b - a| = 0 \implies b = a$.

But then we have:

$$\begin{aligned} i + na &= j + nb \\ i + na &= j + na \\ i &= j \end{aligned}$$

But this is a contradiction with the claim that $i \neq j$. Thus, we conclude that, indeed, $[i] \cap [j] = \emptyset$. □

Finally, we introduce the final lemma:

Lemma 2.22. Every $x \in \mathbb{Z}$ belongs to one of the equivalence classes $[0], \ldots, [n-1]$.

Proof. We can prove this using the Division Algorithm as follows:

□

Now, putting this all together, we observe that by Claim 2, $\mathbb{Z}/n\mathbb{Z}$ has at least n elements. And by Claim 3, we observe that there is at most n elements.

Thus, we conclude that $\mathbb{Z}/n\mathbb{Z}$ has n elements as desired. ■

! We note that $\mathbb{Z}/n\mathbb{Z}$ consists of **subsets** of $\mathbb{Z}$, *not* elements.

Operations on $\mathbb{Z}/n\mathbb{Z}$

We observe that $[a] + [b] = [a+b]$. This lends us to the following proposition:

Proposition 2.23. Addition is well-defined on $\mathbb{Z}/n\mathbb{Z}$. In other words, $[a] + [b] = [a+b]$ for different elements of $[a]$ and $[b]$.

Proof. Let us suppose we have $a_1, a_2 \in [a]$ and $b_1, b_2 \in [b]$.

Then, we observe the following:

$$\begin{aligned} [a_1] + [b_1] &= [a_1 + b_1] \\ &= [(a_2 + kn) + (b_2 + ln)] \\ &= [a_2 + b_2] \end{aligned}$$

■

WEEK 3

WEEK THREE

3.1 Lecture – 9/9/2024

3.1.1 Warm-Up

Problem 3.1. For which a, b does:

1. $\log(ab) = \log a + \log b$.
2. $e^{a+b} = e^a \cdot a^b$.

Solution. We note that for $\log(ab)$, this holds for all $a, b \in \mathbb{R}^+$ (that is, the positive reals).
On the other hand, for e^{a+b}, we note that this holds for all $a, b \in \mathbb{R}$. ■

3.1.2 Groups

Review

Recall from a previous lecture that we stated that $(\mathbb{Z}/n\mathbb{Z}, +)$ has some important properties:

- Identity: We see that 0 is the identity element. That is, we observe that $[0] + [a] = [a] + [0] = [a]$.
- Inverse: For every $[a]$, there exists an element $[-a]$ such that $[a] + [-a] = [-a] + [a] = [0]$.
- Commutativity: We observe that $[a] + [b] = [b] + [a]$.

On the other hand, we look at $(\mathbb{Z}/n\mathbb{Z}, \times)$:

- Identity: We see that $[1] \times [a] = [a] \times [1] = [a]$.
- Inverse: Not all of them have inverses; it depends on our choice of n (namely, we require n to be ...)
- Commutativity: We see that $[a] \cdot [b] = [b] \cdot [a]$.

Now, we recall that previously, we said that $(\mathbb{Z}, +)$ is generated by the element 1. That is, $(\mathbb{Z}, +) = \langle 1 \rangle$. On the other hand, we say that $(\mathbb{Z}/n\mathbb{Z}, +) = \langle [1] : [1] + \ldots + [1] = 0 \rangle$.

And in $(\mathbb{Z}, \times)$, we observe any n can be expressed as a product of some primes. In the case of $(\mathbb{Z}/n\mathbb{Z}, \times)$, we observe that since $[a] \times [b] = [a \times b]$, we note that since $[k]$ can be expressed as a product of primes, then it can be expressed as a product of finitely many classes of prime numbers.

Definitions

Definition 3.1 (Groups). A group $(G, *)$ is a set G with a binary operation $* : G \times G \to G$ which satisfies the following properties:

- Associativity: $a * (b * c) = (a * b) * c$.
- Identity: There exists an $e \in G$ such that for all $a \in G$, $e * a = a * e = a$.
- Inverse: For every $a \in G$, there exists an $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

Definition 3.2 (Homomorphism). A homomorphism f from one group $(G, *)$ to another group $(H, \circ)$ is a map of sets $f : G \to H$ such that:

$$\forall a, b \in G : f(a * b) = f(a) \circ f(b).$$

Example 3.3. Going back to our warm-up, we see that $\log(a \times b) = \log(a) + \log(b)$. So, we see that there is a homomorphism between $(\mathbb{R}^+, \times)$ and $(\mathbb{R}, +)$.

Similarly, we see that $e^{a+b} = e^a \times e^b$. Then, there is a homomorphism between $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$.

3.2 Lecture – 9/11/2024

3.2.1 Warm-Up

Problem 3.2. What is $(-i)^{39}$?

Solution. We observe that this is equal to:

$$\begin{aligned}(-i)^{39} &= (-1)^{39}(i)^{39} \\ &= (-1)(-i) \\ &= i\end{aligned}$$

■

Problem 3.3. Solve for $x \in \mathbb{Z}/10\mathbb{Z}$:

1. $5x \equiv 0 \mod 10$
2. $5x \equiv 1 \mod 10$

Solution. We observe that:

1. $x \equiv 0 \mod 10$, $x \equiv 2 \mod 10$, $x \equiv 4 \mod 10$, $x \equiv 6 \mod 10$, and $x \equiv 8 \mod 10$. That is, x is any even number. To show why, we observe the following:

$$\begin{aligned}5x &= 10n \quad \forall n \in \mathbb{Z} \\ x &= 2n \quad \forall n \in \mathbb{Z}\end{aligned}$$

   So, we see that x is any even number (and thus the solutions proposed are the only ones).

2. From the previous part, we see then that there are no solutions for $5x \equiv 1 \mod 10$. To show fully, we observe that from the previous part, if x is even then we have $5x \equiv 0 \mod 10$. Then, if x is odd, we see that $x = 2m + 1$. Then, we have $5x = 10m + 5 \equiv 5 \mod 10$.

   Thus, we see that there are no solutions to $5x \equiv 1 \mod 10$.

■

3.2.2 Basic Properties of Groups

Proposition 3.4. The identity e in any group G is unique.

Solution. Suppose for contradiction that there exists identities e and e'.

Then, we observe that:

$$e_1 = e_1 e_2 = e_1 e_2 = e_2$$

But then, $e_1 = e_2$, which is a contradiction. Thus, we have proven that $e_1 = e_2$. ■

Proposition 3.5. For any element $g \in G$, its inverse g^{-1} is unique.

Solution. Let us take an element $a \in G$. Now, we suppose that there exists inverses a^{-1} and a'^{-1} not equal to each other such that $aa^{-1} = a'a^{-1} = e$.

Then, we see the following:

$$\begin{aligned} a^{-1} &= a^{-1}e \\ &= a^{-1}(aa'^{-1}) \\ &= (a^{-1}a)a'^{-1} \\ &= a'^{-1} \end{aligned}$$

■

Proposition 3.6. For any $a, b \in G$, we have $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. We observe that:

$$\begin{aligned} (ab)^{-1}(ab) &= e \\ (ab)^{-1}(ab)b^{-1} &= eb^{-1} \\ (ab)^{-1}a &= b^{-1} \\ (ab)^{-1}aa^{-1} &= b^{-1}a^{-1} \\ (ab)^{-1} &= b^{-1}a^{-1} \end{aligned}$$

■

Proposition 3.7. For any $a \in G$, we have $(a^{-1})^{-1} = a$.

Solution. We observe the following:

$$\begin{aligned}(a^{-1})(a^{-1})^{-1} &= e \\ a(a^{-1})(a^{-1})^{-1} &= a \\ (aa^{-1})(a^{-1})^{-1} &= a \\ (a^{-1})^{-1} &= a\end{aligned}$$

■

Corollary 3.8. In any group G and any $a, b \in G$, there exists a unique x such that $ax = b$.

Solution. We proceed as follows:

$$\begin{aligned}ax &= b \\ a^{-1}(ax) &= a^{-1}b \\ (a^{-1}a)x &= a^{-1}b \\ ex &= a^{-1}b \\ x &= a^{-1}b\end{aligned}$$

And by uniqueness of inverses, we know that a^{-1} is unique. Furthermore, we know that the identity e is unique. Thus, $x = a^{-1}b$ is unique. ■

3.3 Lecture – 9/13/2024

3.3.1 Warm-Up

Suppose that we have chairs $C_1, C_2, \ldots, C_k$, and persons $P_1, P_2, \ldots, P_k$.

Problem 3.4. How many ways are there to put P_1, P_2, P_3 to chairs C_1, C_2, C_3? How many ways are there for up to the k^{th} person?

Solution. First, we have $3! = 6$ ways. For up to k, we have $k!$.

An intuitive way of viewing this is that the first person has k chairs they can sit on. Then, the next have $k-1$, and so on until the last person only has 1 choice left. ■

3.3.2 Symmetric Groups

For this lecture, let X denote a set.

Then, we define a symmetric group as follows:

Definition 3.9 (Symmetric Group)**.** $\mathrm{Sym}(X) = S_x = S_{|X|}$ is a group of all bijections $f : X \to X$, with the operation $*$ of map composition.

We see that this is indeed a map. First, we see that associativity comes from the fact that composition is indeed associative.

Next, for the identity, we note that the identity map exists, and thus is the identity element of our group.

Finally, for inverses, we note that all bijections have inverses.

> **Example 3.10.** Let $X = \{1\}$ be a finite set. Then, the bijection we have is simply the map $f : X \to X$ which maps 1 back to itself. It's just the identity map. We see then that $S_1 = \{\mathrm{id}\}$.
>
> Let $X = \{1, 2\}$. Then, we see that have the identity map, along with the map f which maps 2 to 1, and 1 to 2. These types of maps are called *transpositions*, which switches only two elements.

3.3.3 Thinking about the Elements of S_X

One way to think of the elements is just being bijections from $X \to X$.

Matrix Representation

However, we can also visualize them as a matrix. For example, if we have four elements, let us denote a bijection σ which the following rule:

$$\begin{aligned} 1 &\mapsto 2 \\ 2 &\mapsto 4 \\ 3 &\mapsto 1 \\ 4 &\mapsto 3 \end{aligned}$$

Then, we have:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{bmatrix}$$

Where we see that the top row is the original set, and the bottom row is the image under σ.

Cycle Notation

Going back to our example previously, we can express it as the following: $(1\,2\,4\,3)$. We see that this is because 1 goes to 2, then 2 goes to 4, then 4 goes to 3, and 3 goes back to 1.

Let us consider another example:

$$\begin{aligned} 1 &\mapsto 3 \\ 3 &\mapsto 1 \\ 2 &\mapsto 4 \\ 4 &\mapsto 2 \end{aligned}$$

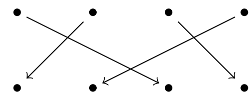
Then, we can express it in cycle notation as: $(1\,3)(2\,4)$.

Strings

Let us consider the following example:

$$\begin{aligned} 1 &\mapsto 2 \\ 2 &\mapsto 4 \\ 3 &\mapsto 1 \\ 4 &\mapsto 3 \end{aligned}$$

We can in fact think of this as a graph as follows:



An advantage of this is that it becomes easy to visualize things such as composition of maps. Furthermore, inverses are easy to see as well.

Week 4

Week For Suffering

4.1 Lecture – 9/16/2024

4.1.1 Warm-Up

Problem 4.1. Prove that $3\mathbb{Z} = \{k \in \mathbb{Z} : 3 \mid k\}$ is a group with the $+$ operation.

Solution. First, we prove that there exists an identity. We observe that $3(0) = 0$, so we see that $0 \in 3\mathbb{Z}$. Furthermore, note that $0 + k = k$ for all $k \in \mathbb{Z}$. Thus, since $3\mathbb{Z} \subseteq \mathbb{Z}$, we note that 0 is also the identity in $3\mathbb{Z}$.

Next, we observe that for any $k \in 3\mathbb{Z}$, we observe that there exists $a \in \mathbb{Z}$ such that $3a = k$. Then, we observe that if we let $b = -a$, then we have $3b = -k$. Thus, we see that $-k \in 3\mathbb{Z}$ as well. Then, we see that $k + (-k) = 0$. Thus, it passes the inverse check.

Finally, we note that $+$ is associative on $\mathbb{Z}$, and thus it follows that it is associative on $3\mathbb{Z}$ as well. ■

Problem 4.2. How to find new examples of groups?

Solution. We can look at existing groups, and then form subgroups from them. ■

4.1.2 Subgroups

Definition 4.1. A subgroup H of a group G is a group H with a group operation $*$ restricted from G.

Example 4.2 (Restriction)**.** Let us suppose some set X with a function f mapping X to $\mathbb{R}$. So, we have $f : X \to \mathbb{R}$. Then, there are times where we are only interested in some subset $Y \subset X$. Then, we look at $f : Y \to \mathbb{R}$.

Then, we have two notations:

- $f : Y \to \mathbb{R}$.
- $f \restriction Y$

So, for example, let consider $G = (G, *)$. Then, we have $* : G \times G \to G$. Now, we restrict it to $* : H \times H \to H$. We note that we have to enforce mapping to H, since H is in fact a group.

Example 4.3. ($n\mathbb{Z}$) Let us consider $(\mathbb{Z}, +)$. Then, let us look at $(3\mathbb{Z}, +)$. This is in fact a subgroup of $(\mathbb{Z}, +)$. From the warm-up, we see that $(3\mathbb{Z}, +)$ is in fact a group.

More generally, let us consider $n \in \mathbb{Z}$. Then, $n\mathbb{Z} = \{k \in \mathbb{Z} : n \mid k\}$. Then, it is a subgroup a subgroup of $(\mathbb{Z}, +)$.

Example 4.4. (A Non-Example) Let us consider $(\mathbb{Z}, +)$. Let us consider $(\mathbb{Z}/3\mathbb{Z}, +)$. We note that $(\mathbb{Z}/3\mathbb{Z}, +)$ is a group. We also note that we have closure, and so we see that $(\mathbb{Z}/3\mathbb{Z}, +)$ is... a subgroup?

However, we note that $+$ isn't the same operation as we have on $(\mathbb{Z}, +)$. Furthermore, we see that $\mathbb{Z}/3\mathbb{Z} \not\subseteq \mathbb{Z}$.

Definition 4.5 (Subgroup Lattice)**.** We define a subgroup lattice of a group G to be:

$$(\{e\}, *) \subset \cdots (H, *) \subset (K, *) \cdots \subset (G, *)$$

On the left-hand side is the trivial subgroup, the smallest possible subgroup. Then, the largest subgroup is the group itself. And everything in-between is what we call proper subgroups.

Definition 4.6 (Proper Subgroup)**.** Proper subgroups are subgroups which are not the group itself and not the trivial subgroup.

Proposition 4.7. We say that $H \subseteq G$ is a subgroup if and only if:

- $e_G \in H$.
- If $h_1, h_2 \in H$, then $h_1 h_2 \in H$.
- If $h \in H$, then $h^{-1} \in H$

Proof. First, let us suppose that $H \subseteq G$ is a subgroup. Then, we'll prove that the three properties hold.

Proof. First, let us show that $e_G \in H$. We observe that since H is a subgroup, we have that $e_H \in H$ and that for all $h \in H$, we have $e_H h = h e_H = h$.

Furthermore, we note that $e_H \in G$, so we see that $e_G e_H = e_H e_G = e_H$.

Now, we observe the following:

$$e_G e_H = e_H e_G = e_H$$

Furthermore, we have:

$$e_H e_H = e_H$$

So, we have:

$$\begin{aligned} e_G e_H &= e_H e_H \\ e_G(e_H e_H^{-1}) &= e_H(e_H e_H^{-1}) \\ e_G &= e_H \end{aligned}$$

Next, let us consider inverses. Since H is a subgroup, we know then that if $h \in H$, we have an inverse h' such that $hh' = h'h = e$. And we note by the uniqueness of inverses in G, we have that $h' = h^{-1}$.

Finally, for closure, we note that it follows from the fact that H is in fact a group. □

■

Proposition 4.8. $H \subseteq G$ is a subgroup if and only if $H \neq \emptyset$ and $\forall a, b \in H$, we have $ab^{-1} \in H$.

Solution. First, let us show that if $H \neq \emptyset$ and $\forall a, b \in H$, we have $ab^{-1} \in H$, then we have H is a subgroup.

Proof. First, since $H \neq \emptyset$, let us then consider $h \in H$. Then, $hh = hh^{-1} = e \in H$.

Next, let us consider $h \in H$. Then, we observe that since we know $e \in H$, we have that $eh^{-1} = h^{-1} \in H$.

Finally, let us consider $h_1, h_2 \in H$. We want to show that $h_1 h_2 \in H$ (i.e. we have closure). Since H respects inverses, we see that if $h_2 \in H$, we have $h_2^{-1} \in H$ as well.

Then, we see that $h_1, h_2^{-1} \in H$. Then, we have $h_1(h_2^{-1})^{-1} = h_1 h_2 \in H$.

Therefore, we note that H is in fact a subgroup. □

■

4.2 Lecture – 9/18/2024

4.2.1 Warm-Up

Problem 4.3. Find all subgroups of S_3.

Solution. First, let us list out all elements in S_3 (in cycle notation):

1. (1)
2. $(1\,2)$
3. $(1\,3)$
4. $(2\,3)$
5. $(1\,2\,3)$
6. $(1\,3\,2)$

First, we note that we have the trivial subgroup and S_3 itself.

Next, we have observe that $\{(1), (1\,2)\}$ forms a subgroup. Similarly, $\{(1), (1\,3)\}$ and $\{(1), (2\,3)\}$ does too.

Next for the three-cycle, we note that the set $\{(1), (1\,2\,3), (1\,3\,2)\}$ forms a subgroup as well. ■

4.2.2 Cyclic Subgroups

Let us take any $a \in G = (G, *)$. Then, we observe the following:

Lemma 4.9 (Exponentiation)**.** We note that $a^x * a^y = a^{x+y}$, for all $x, y \in \mathbb{Z}$.

Definition 4.10 (Cyclic Subgroup)**.** A cyclic subgroup generated by a is a set $\langle a \rangle$ defined as:

$$\langle a \rangle = \left\{ a^k : k \in \mathbb{Z} \right\}.$$

Theorem 4.11 (Minimality of $\langle a \rangle$)**.** The set $\left\{ a^k : k \in \mathbb{Z} \right\}$ is in fact the minimal subgroup of G containing a.

Solution. First, we will prove that the cyclic subgroup is in fact a subgroup.

Proof. We note that by Proposition 4.8, we have that if $\langle a \rangle \neq \emptyset$, and for all $a, b \in \langle a \rangle$, we have that $ab^{-1} \in \langle a \rangle$, then we can conclude that $\langle a \rangle$ is in fact a subgroup.

Now, we first observe that evidently, $\langle a \rangle \neq \emptyset$. Now, let us take $x, y \in \langle a \rangle$. Then, we observe that $x = a^n$ and $y = a^m$ for $n, m \in \mathbb{Z}$.

So, we see that $xy^{-1} = a^n a^{-m} = a^{n-m} \in \langle a \rangle$, since $n - m \in \mathbb{Z}$.

Thus, since $xy \in \langle a \rangle \implies xy^{-1} \in \langle a \rangle$, we have that $\langle a \rangle$ is a subgroup. □

Now, we check minimality. But, this is trivial: for any subgroup H of G, we note that if it contains a, then it must contain all powers of a by closure and its inverse a^{-1} existing. Thus, H must contain $\langle a \rangle$. Therefore, $\langle a \rangle$ is the minimal subgroup containing a. ■

Remark 4.12. We denote H being a subgroup of G as $H \leq G$. Note that this is different from $H \subseteq G$, which says H is a subset of G.

Definition 4.13 (Order)**.** Let $a \in G$. Then, we say that the order of a (in G) is the minimal $n \in \mathbb{N}$ such that $a^n = e$.

Example 4.14. Let us consider:

1. $(G, *) = (\mathbb{Z}, +)$.
2. $(G, *) = (\mathbb{Z}/n\mathbb{Z}, +)$

First, we note that $(\mathbb{Z}, +) = \langle 1 \rangle$. Then, we note that $1 \in \mathbb{Z}$ has infinite order, since no matter how much we add, we are never getting back to $e_G = 0$.

Secondly, for $(\mathbb{Z}/n\mathbb{Z}, +) = \langle [1] : [1] + \ldots + [1] = [0] \rangle$. Here, we see that $[1] \in \mathbb{Z}n\mathbb{Z}$ has order n.

Definition 4.15 (Cyclic Group)**.** We say that any group G is cyclic if and only if there exists some $g \in G$ such that $G = \langle g \rangle$.

Example 4.16. Going back to the previous example, both of them are cyclic groups, since they are generated by 1 and $[1]$ respectively.

Example 4.17. Looking at S_3, we note that it isn't cyclic; there are no single element which generates the entire group.

Furthermore, we note that it isn't abelian.

Theorem 4.18 (Cyclic Groups are Abelian)**.** Every cyclic group is abelian.

4.3 Lecture – 9/20/2024

4.3.1 Warm-Up

Problem 4.4. Let $F : (\mathrm{GL}(2, \mathbb{R}), \times) \to (\mathrm{GL}(2, \mathbb{R}), \times)$, such that $F(A) = A \times A$. Show whether it is a homomorphism or not.

Solution. We observe the following:

$$\begin{aligned} F(AB) &= ABAB \\ &\neq AABB \\ &= F(A)F(B) \end{aligned}$$

We observe that this is because operations are not commutative necessarily. ■

4.3.2 Homomorphisms

Definition 4.19 (Isomorphism)**.** We say that an isomorphism is a bijective homomorphism.

If we know that φ is an isomorphism from G to K – that is, $\varphi : (G, *) \to (K, \circ)$ – then we denote this as $G \cong K$.

Remark 4.20. If we have an isomorphism from G to K, then we have an isomorphism from K to G as well.

Proposition 4.21. Say we have $\varphi : G \to H$ which is a homomorphism. Then, we have:

1. $\varphi(e_G) = e_H$
2. $\varphi(g^{-1}) = \varphi(g)^{-1}$
3. If $K \leq G$, then $\varphi(K) \leq H$
    - Since $G \leq G$, then $\varphi(G) \leq H$.
4. If $M \leq H$, then $\varphi^{-1}(M) = \{g \in G : \varphi(g) \in M\}$ is a subgroup of G.

Solution. We will prove the properties.

Proof. Let e_H and e_G be identities of H and G respectively. Then, we observe the following:

$$\begin{aligned}\varphi(e_G) &= \varphi(e_G)\\ \varphi(e_Ge_G) &= \varphi(e_G)\\ \varphi(e_G)\varphi(e_G) &= \varphi(e_G)\\ \varphi(e_G) &= e_H\end{aligned}$$

□

Next, for inverses, we observe that:

Proof. Let us consider:

$$\begin{aligned}\varphi(e_G) &= e_H\\ \varphi(e_G) &= \varphi(g)(\varphi(g))^{-1}\\ \varphi(gg^{-1}) &= \varphi(g)(\varphi(g))^{-1}\\ \varphi(g)\varphi(g^{-1}) &= \varphi(g)\varphi(g)^{-1}\\ \varphi(g^{-1}) &= \varphi(g)^{-1}\end{aligned}$$

□

For the last property, we will prove it only for the kernel of φ:

Proof. First, we observe that $M = \{e_H\}$, and we have that:

$$\varphi^{-1}(\{e_H\}) = \{g \in G : \varphi(g) = e_H\} = I.$$

Now, we note that since $\varphi(e_G) = e_H$, we know then that $e_G \in \varphi^{-1}(\{e_H\})$. So, we know that the set is non-empty.

Next, to show closure, we suppose that we have elements $g_1, g_2 \in I$. Then, we know that $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = e_He_H = e_H$. So, we have closure.

Finally, to show inverses, suppose that we have $g_2 \in I$. Then, we note that since $g_2 \in I$, we now observe that $\varphi((g_2)^{-1}) = \varphi(g_2)^{-1} = (e_G)^{-1} = e_G$. So, we have that $(g_2)^{-1} \in I$ too.

Thus, we have satisfied all properties of a subgroup, and thus can conclude that, indeed, $\varphi^{-1}(M)$ is a subgroup. □

■

Remark 4.22. When we write $\varphi(K)$, we are saying the image of K under φ. If we are looking at the entire group, this is simply the image of φ.

And note when we say $\varphi^{-1}(M)$, this is the pre-image of M under φ.

Definition 4.23 (Kernel)**.** We define the kernel of a homomorphism to be the pre-image of the identity. That is, $\varphi^{-1}(\{e\})$.

WEEK 5

WEEK FIVE

5.1 Lecture – 9/23/2024

5.1.1 Warm-Up

Problem 5.1. Consider the set $\mathrm{GL}(2, \mathbb{R})$, which is the set of invertible 2×2 matrices with real entries. Now, we define H to be the diagonal subgroup:

$$H = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \neq 0 \right\}$$

Then, check whether it's true that $g_1 \in g_2 H$ for the following:

1. $g_1 = \begin{bmatrix} 9 & 10 \\ 21 & 7 \end{bmatrix}$, and $g_2 = \begin{bmatrix} 3 & 5 \\ 7 & 4 \end{bmatrix}$
2. $g_1 = \begin{bmatrix} 39 & 560 \\ 91 & 448 \end{bmatrix}$, and $g_2 = \begin{bmatrix} 3 & 5 \\ 7 & 4 \end{bmatrix}$

Solution. First, we observe the following:

$$\begin{bmatrix} 3 & 5 \\ 7 & 4 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} 3a & 5b \\ 7a & 4b \end{bmatrix}$$

Then, we note that for $a = 3$ and $b = 2$, we indeed have that $g_1 \in g_2 H$.
Similarly, for the second problem, note that we have that $a = 13$ and $b = 112$ works. ■

5.1.2 Cosets

Definition 5.1 (Cosets)**.** Let $G = (G, *)$ be a group, $H \leq G$ be a subgroup of G.
Then, we define a left H-coset gH to be:

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

Lemma 5.2. Let $g_1, g_2 \in G$ and $H \leq G$. The following are equivalent:

- $g_1H = g_2H$.
- $Hg_1^{-1} = Hg_2^{-1}$.
- $g_1H \subset g_2H$.
- $g_2 \in g_1H$.
- $g_1^{-1}g_2 \in H$.

Theorem 5.3. Left H-cosets partition G.

This means that there exists a set $\{g_i\}$ of elements of G such that $G = \bigsqcup g_iH$. Note that this means that $g_iH \cap g_jH = \emptyset$, for $i \neq j$.

Example 5.4. Suppose we have $G = (\mathbb{Z}, +) = \mathbb{Z}$, and $H = (7\mathbb{Z}, +)$. Then, by Theorem 5.3, we know that there exist some set of elements such that $\mathbb{Z}$ can be partitioned into the left H-coset of each of these elements.

More precisely, let us consider $1H = \{\ldots, -6, 1, 8, \ldots\}$, and we just shift the multiple of sevens by the g chosen for our left H-coset. With this in mind, we note that each of these cosets are in fact disjoint from one another. Furthermore, note that their union is precisely $\mathbb{Z}$.

And in fact, we have $\{1, 2, 3, 4, 5, 6, 7\}$ such that the coset of each of these element form G.

Remark 5.5. The set of left H-cosets is denoted G/H. Its cardinality $|G/H| = [G : H]$ (the index of H in G).

Example 5.6. With this in mind, let us consider $\mathbb{Z}/7\mathbb{Z}$; this is why we denote it as such. And we know why now given the idea of cosets.

Theorem 5.7 (Lagrange's Theorem). If G, H are finite groups, with $H \leq G$, then we have:

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

Corollary 5.8. The most important corollary is that if we take any finite group G and subgroup H, we know that the number of elements in H divides the number of elements in G. That is:

$$|H| \mid |G|.$$

5.2 Lecture – 9/25/2024

5.2.1 Warm-Up

Problem 5.2. Are the sets $\mathbb{Z}/6\mathbb{Z}$ and S_n isomorphic, for $n \geq 3$?

Solution. No; recall that if $\mathbb{Z}/6\mathbb{Z}$ and S_n are isomorphic, then if $\mathbb{Z}/6\mathbb{Z}$ is abelian (which it is), then S_n must be too (which it isn't). ∎

5.2.2 Isomorphisms

Recall that we defined an isomorphism to be a bijective homomorhism, and provided the following example:

Example 5.9. We have an isomorphism between $(\mathbb{R}, +)$ and $\mathbb{R}_{>0}, \times$.

Example 5.10. We also have the following isomorphism from homework:

$$\begin{aligned} \exp : \mathbb{Z}/n\mathbb{Z} &\to \langle (1\,2\,\ldots\,n) \rangle \\ [a] &\mapsto (1\,2\,\ldots\,n)^n \end{aligned}$$

We note that it is injective since we can think of the operation as right shifts. Then, after n shifts, we return to the same position. In other words, for two cycles to be equal to each other, their exponents must be equivalent to each other under $\mod n$.

With that in mind, we note that if we have $x \neq y \mod n$, then it follows that $(1\,2\,\ldots\,n)^x \neq (1\,2\,\ldots\,n)^y$.

Theorem 5.11 (Cyclic Groups and $\mathbb{Z}$)**.** If G is a cyclic group, then there are two possibilities:

1. If G is of finite order n, then it is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.
2. If G is of infinite order, then it is isomorphic to $\mathbb{Z}$.

Theorem 5.12 (Isomorphisms Preserve Structure)**.** If G is isomorphic to H, then the following must be true:

- If G is abelian, then H is too.
- If G is cyclic, then H is too.

5.2.3 External Direct Products

The idea is to decompose into small simple pieces. So, if we have a big structure, it's much easier to consider smaller constituents of it.

In the case of external direct products, we want to create a larger group out of two smaller ones.

Definition 5.13 (External Direct Products)**.** Let $(G, \circ), (H, *)$ be groups. Then, we define its direct product $G \times H$ to be:

$$G \times H = \{(g, h) : g \in G \wedge h \in H\}$$

with the operation $\cdot$ to be as follows:

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

Proof. For associativity, it follows from the operations of G and H being associative. We note that since the operation is independent for each coordinates.

For identity, we note that the element (e_G, e_H) serves as the identity element.

For inverses, for every $(g, h) \in G \times H$, we take the inverse $(g^{-1}, h^{-1}) \in G \times H$. We know this exists by G, H being groups. ■

5.3 Lecture – 9/27/2024

Definition 5.14. Let $H \leq G$. We say that H is normal (in G) iff $\forall g \in G : gH = Hg$ iff $g \in G \forall h_1 \in H \exists h_2 \in H : gh_1 = h_2 g$.

5.3.1 Warm-Up

Problem 5.3. What subgroups of $(\mathbb{Z}/6\mathbb{Z}, +)$ are normal?

Solution. We note that all subgroups are in fact normal. This follows from commutativity of the operation. ■

Problem 5.4. What subgroups of S_3 are normal?

Solution. The subgroup $S = \{(1), (1\,2\,3), (1\,3\,2)\}$ is normal. ■

Proposition 5.15. If G is abelian, then every subgroup is normal.

Proof. We see that for all $g \in G$ and for all $h \in H \leq G$, we have that $gh = hg$. So trivially, we see that $gH = Hg$. ■

5.3.2 Normal Subgroups

So, why are we looking at normal subgroups? Namely, we are we looking at how $\forall g \in G$, $gHg^{-1} \subseteq H$.

Well, note that $G/H = \{eH, g_1 H, \ldots\}$. Now, we want to turn G/H into a group by introducing some operation $*$ such that $g_1 H * g_2 H = (g_1 g_2)H$.

Example 5.16. Note that we've looked at an example before.

Let us look at $G = \mathbb{Z}$ and $H = n\mathbb{Z}$. That is, we look at $G/H = \mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n]\}$. Then, we see how $[k] + [l] = (k + n\mathbb{Z}) + (l + n\mathbb{Z}) = (k + l)n\mathbb{Z}$.

However, it works iff $\forall g \in G, gHg^{-1} \subseteq H$.

Definition 5.17. Let $f : G \to H$ be a homomorphism. Then, $\mathrm{Im}(f) = \{h \in H : \exists g \in G : f(g) = h\}$. Also, we say that $\mathrm{Ker}(f) = \{g \in G : f(g) = e_H\}$.

Theorem 5.18 (First Isomorphism Theorem)**.** If $f : G \to H$ is a homomorphism, then $G/\mathrm{Ker}(f) \cong \mathrm{Im} f$. That is, there exists some isomorphism $\Psi : G/\mathrm{Ker} f \to \mathrm{Im} f$.

Proof. To prove this, we will first introduce the following lemma:

Lemma 5.19. $\mathrm{Ker} f$ is a normal subgroup.

Proof. We use the condition that for all $g \in G$, we have $g(\mathrm{Ker} f)g^{-1} \subseteq \mathrm{Ker} f$.

Let us take any $a \in \mathrm{Ker} f$. We see then that $f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g)f(g^{-1}) = f(g)(f(g))^{-1} = e_H$. Thus, we see that, indeed, it lies in the kernel. □

■

WEEK 6

WEEK SIX SUFFERING

6.1 Lecture – 9/30/2024

Problem 6.1. Show that $D(2, \mathbb{R}) \cong \mathbb{R}^\times \times \mathbb{R}^\times$. Note that $D(2, \mathbb{R})$ denotes all invertible diagonal 2×2 matrices with $\mathbb{R}$-entries.

Solution. We can consider the set of all matrices in the following form where $a, b \neq 0$:

$$\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$$

and the form:

$$\begin{bmatrix} 1 & 0 \\ 0 & b \end{bmatrix}$$

We denote them as H, K respectively. Note that H, K are in fact subgroups.

Then, we see that the intersection is only the identity matrix since for the two matrices to be equal, we must require $a = 1$ and $b = 1$. Finally, note that:

$$\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$
$$\begin{bmatrix} 1 & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$

Then, we see that there exists an isomorphism between $D(2, \mathbb{R})$ and $H \times K$.

Finally, we define a map $\varphi(h) \mapsto a$ and $\psi(k) \mapsto b$. These are both isomorphisms, and thus we can conclude that there exists an isomorphism between $H \times K$ and $\mathbb{R}^\times \times \mathbb{R}^\times$. Then, we have an isomorphism between $D(2, \mathbb{R})$ and $\mathbb{R}^\times \times \mathbb{R}^\times$. ■

Problem 6.2. Show that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \ncong \mathbb{Z}/4\mathbb{Z}$.

Solution. We see that the former has elements of at most order 2, whereas the latter has elements of order 4. Thus, there can't be an isomorphism between the two. ■

6.1.1 Internal Direct Products

Definition 6.1. Let G be a group, with $H, K \leq G$. G is the internal direct product of H and K iff

1. $G = H \cdot K = \{h \cdot k : h \in H, k \in K\}$.
2. $H \cap K = \{e_G\}$.
3. $hk = kh$ for any $h \in H$ and $k \in K$.

! Note that $H \cdot K \neq H \times K$! The left is an internal product, whereas the right is an external product.

! Note that the third condition isn't telling us that G is abelian; we aren't considering elements such as hh or kk, or elements not in the subgroup.

Theorem 6.2. If G is the internal direct product of H and K, then $G \cong H \times K$.

Proof. First, note that since G is an internal direct product of H and K, then $g = hk$ for some $h \in H$ and $k \in K$.

We will first define a map $\varphi(g) : G \to H \times K$ by $g \mapsto (h, k)$. Now, we will first show that $\varphi(g)$ is well-defined:

Proof. To show well-definedness, we observe that for $hk = g = h'k'$, we see that:

$$
\begin{aligned}
hk &= h'k' \\
k(k')^{-1} &= h^{-1}h'
\end{aligned}
$$

Now, we observe that $k(k')^{-1} \in K$ and $h^{-1}h' \in H$. Then, we note that $H \cap K = \{e_G\}$, so $k(k')^{-1} = h^{-1}h' = e_G$.

Then, we observe that $h' = h$ and $k' = k$. Therefore, $(h, k) = (h', k')$. □

Next, we will show that it is homomorphic:

Proof. Let us take g_1, g_2 and see that:

$$
\begin{aligned}
\varphi(g_1 g_2) &= \varphi(h_1 k_1 h_2 k_2) \\
&= \varphi(h_1 h_2 k_1 k_2) \\
&= (h_1 h_2, k_1 k_2) \\
&= (h_1, k_1)(h_2, k_2) \\
&= \varphi(g_1)\varphi(g_2)
\end{aligned}
$$

□

■

6.2 Lecture – 10/2/2024

Theorem 6.3 (Fundamental Theorem of Finite Abelian Groups)**.** Every finite abelian group G is isomorphic to:

$$G \cong \mathbb{Z}p_1^{a_1} \times Zp_2^{a_2} \times \cdots \times \mathbb{Z}p_k^{a_k}$$

where $p_1, \ldots, p_k$ are primes (not necessarily distinct), and $a_1, \ldots, a_k$ are natural numbers.

In the case where G is finitely generated, we have that:

$$G \cong \mathbb{Z}^b \times \mathbb{Z}p_1^{a_1} \times \cdots \times \mathbb{Z}p_k^{a_k}$$

Example 6.4. For example, consider $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$. Then, $p_1 = 2$ and $a_1 = 2$.

In the case where, say, $\mathbb{Z}/4\mathbb{Z}$, we see that $p_1 = 2$ and $a_1 = 2$. Now, suppose we had $\mathbb{Z}/6\mathbb{Z}$, then using the theorem, we see that $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Proof. As a quick proof, we note that $\mathbb{Z}/6\mathbb{Z} = \{[0], [1], \ldots, [5]\}$. Then, we consider following subgroups $H = \{[0], [3]\}$ and $K = \{[0], [2], [4]\}$.

First, we see that every element in $\mathbb{Z}/6\mathbb{Z}$ is the result of some $h + k$ for $h \in H$ and $k \in K$.

Next, we see that they only intersect on the identity element $[0]$.

Finally, commutativity comes from both being abelian. $\square$