# Contents



**Wed. 24 Jan 2024**

**Note**.

All info for the class is available on the canvas page. Notes from the prof are written on the iPad, and PDFs will be provided after each class. Despite this taking notes is helpful.

Offices are hours are Tuesdays in person, and Thursdays on Zoom. Hours may vary.

A text for this class is not *required*. Technically, we are using Fraleigh's *A first course in Abstract Algebra*

No quizzes in this class, weekly Homeworks except on Exam weeks, two midterms, and one final.

Readings on the class schedule are not additional, it's for people that need extra material, or people that missed that day.

# 1 Introduction - Sets and Relations

## 1.1 Sets

**Definition**.

A **Set**. is a well-defined collection of objects called *elements*.

$a \in A$ means "$A$ is a set, $a$ is an element of a set, and $a$ is in $A$.

Examples of sets are

- $\mathbb{Z}$ - The set of all integers, positive, negative, and zero
- $\mathbb{N}$ - The set of natural numbers, $0, 1, 2, \ldots$. **In this class,** $\mathbb{N}$ **starts with** $1$**.**
- $\mathbb{Q}$ - The set of rational numbers.
- $\mathbb{R}$ - The set of real numbers.
- $\mathbb{C}$ - The set of complex numbers.

- $\{1, 2, 3, 4\}$
- $\{a \in \mathbb{Z} \mid a > 2\}$. This is a set of integers *such that* $a > 2$.
- $\varnothing$ - The empty set.
- $\mathrm{GLn}(\mathbb{R})$ - The set of $n \times n$ invertible matrices with real entries. (GL stands for "General Linear".)
- $C(\mathbb{R})$ - The set of continuous functions $f : \mathbb{R} \to \mathbb{R}$.

**Definition**.

A set $A$ is a **subset** of a set $B$ if

$$\forall x \in A, x \in B$$

In other words, everything in $A$ is also in $B$. As notation, we can say either $A \subseteq B$ or $A \subset B$.

A **proper** subset is $A \subset B$ but $A \neq B$. Just write $A \subsetneq B$.

For example, $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. And, importantly, $\varnothing \subseteq A$ for all sets $A$. In other words, the empty set is a subset of *all* sets.

Two sets are equal if $A = B$, or $A \subseteq B$ *and* $B \subseteq A$. This is often how you prove set equality.

### 1.1.1 Set Operations

We have four main operations.

- **Union**: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$.
- **Intersection**: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.
- **Product**: $A \times B = \{(a, b) \mid a \in A, b \in B\}$.
- **Difference**: $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$

Two sets are **disjoint** if $A \cap B = \varnothing$.

If we're working in a particular *universe* $U$ (i.e. all sets are subsets of the universal set $U$) then the *complement* of $A$ is $A^c = \{x \mid x \in U \text{ and } x \notin A\}$.

## 1.2 Relations

**Definition**.

A **relation** between sets $A$ and $B$ is a subset $R \subseteq A \times B$.

If $(a, b) \in R$, then we say that "$a$ is related to $b$", or we write $aRb$, or $a \sim b$.

**Example**.

$R \subseteq \{1, 2, 3\} \times \{2, 3, 4\}$. $R = \{(1, 3), (2, 2), (3, 4)\}$

**Note**.

Relations might not be reflexive! If $(a, b) \in R$, that means $a$ is related to $b$, but it might not be the case that $(b, a) \in R$. In other words, the reverse may not be true!

Another example might be $R \subseteq \mathbb{R} \times \mathbb{R}$, with $R = \{(x, x^3) \mid x \in \mathbb{R}\}$. Oh look! We just rewrote $f(x) = x^3$, so functions are relations.

**Definition**.

A **partition** of a set $A$ is a collection of *disjoint* subsets whose union is $A$.

Another way to think of this is that any element of $A$ is in one and only one of its partitions.

An example of this might be the partition

$$A = \mathbb{Z} = \{x \in \mathbb{Z} \mid x < 0\} \cup \{0\} \cup \{x \in \mathbb{Z} \mid x > 0\}$$

is a partition of $\mathbb{Z}$ into 3 sets.

Another example might be $A = \mathbb{R}$, subsets are $\{x\}$ for each $x \in \mathbb{R}$.

Another, maybe more interesting example might be the following.

**Example**.

Fix $n \in \mathbb{N}$, $n \geq 2$. Let

- $\bar{0} = \{x \in \mathbb{Z} \mid x \text{ is divisible by } n\}$.
- $\bar{1} = \{x \in \mathbb{Z} \mid x - 1 \text{ is divisible by } n\}$.
- $\bar{2} = \{x \in \mathbb{Z} \mid x - 2 \text{ is divisible by } n\}$. On and on until...
- $\overline{n-1} = \{x \in \mathbb{Z} \mid x - (n-1) \text{ is divisible by } n\}$.

**Claim**: This partitions $\mathbb{Z}$ into in $n$ subsets.

**Fri. 26 Jan 2024**

Let's go back to relations, which we put aside to talk about partitions.

**Definition**.

A relation $A \subseteq A \times A$ is called an **equivalence relation** if it satisfies 3 properties

1. **Reflexivity**: $aRA$ for all $a \in A$.
2. **Symmetry**: $aRb$ if and only if $bRa$.
3. **Transitivity**: If $aRb$ and $bRc$, then $aRc$.

The key idea is that equivalence relations on $A$ are *the same* as partitions of $A$. What's going on here?

From an equivalence relation: If $b$ is related to $b$, put them in the same set. Because of symmetry of equivalence relations, order of elements in the set doesn't matter.

Conversely, given a partition say $aRb \Leftrightarrow bRa$ are in the same subset.

**Note**.

We'll be talking a lot about partitions and equivalence relations in this class.

Now we move on to the next step in our intro: functions.

## 1.3 Functions

A function $f : A \to B$ is a relation $R_f \subseteq A \times B$ such that, for all $a \in A$, there is a *unique* $b \in B$ such that $aRb$. Effectively, this means that

1. We pass the vertical line test.
2. The function is defined over its entire domain.

Which are the properties we expect of functions!

**Example**.

Let $f : \mathbb{R} \to \mathbb{R}$, with $R_f = \{(x, x^3) \mid x \in \mathbb{R}\}$. We write $f(a)$ for the value $b$ where $(a, b) \in R_f$.

Given a function $f : A \to B$. We say that

- $A$ is the *domain*.
- $B$ is the *codomain*.
- The *range* is a *subset* of the codomain, only where $f$ outputs values.

The $+$ operation is a function $+ : \mathbb{R} \to \mathbb{R}$, also written as $(a, b) \mapsto a + b$. The multiplication operation $\times : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, also written as $(a, b) \to ab$. These are binary operations, very useful in Group Theory.

**Definition**.

A **binary operation** on a set $A$ is a function $f : A \times A \to A$. Its an operation on two inputs that outputs one thing.

**Note**.

A dot product does not count here! Because the output of the dot product does not come from the same set as the input.

To do more complicated things in real life (such as $a + b + c$), we must parenthesize.

$$f(a, f(b, c)) \text{ or } f(f(a, b), c)$$

Of course this doesn't matter for addition in particular, but it might for other binary operators!

**Example**.

Fix $n \geq 2$ and consider $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ (Note that this is a set of sets!)

We want to come up with binary operations on this set. We have

1. Addition: $+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$, defined as $(\bar{a}, \bar{b}) \mapsto \overline{a + b}$.

   But this isn't well-defined! For instance, what happens if $a + b$ exceeds $n$? To fix this, let's add the following condition:

   Let $\bar{x} = \bar{y}$ if $x, y$ are in the same subset of partitions. (i.e. They have the same remainder mod $n$.)

   **Question**: Is this a well-defined binary operations?

   **Answer**: Yes! But we must check that it doesn't matter how we define our inputs.

2. Multiplication: $\times : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$, defined as $(\bar{a}, \bar{b}) \mapsto \overline{ab}$

**Note**.

We also write $x \equiv y \pmod{n}$ if $\bar{x} = \bar{y}$.

Now we're ready to jump in.

# 2 Properties of Operations on R

Let's look at the properties of $(\mathbb{R}, +)$ and $(\mathbb{R} \setminus \{0\}, \times)$.

$(\mathbb{R}, +)$

1. **Associativity**: $a + (b + c) = (a + b) + c$
2. **Identity**: $a + 0 = a$
3. **Inverses**: $a + (-a) = (-a) + a = 0$
4. **Commutativity**: $a + b = b + a$

$(\mathbb{R} \setminus \{0\}, \times)$

1. **Associativity**: $a \times (b \times c) = (a \times b) \times c$
2. **Identity**: $a \times 1 = a$.
3. **Inverses**: $a \times (1/a) = (1/a) \times a = 1$
4. **Commutativity**: $a \times b = b \times a$

**Definition**.

We say that a binary operation $p : A \times A \to A$ is **associative** if

$$p(a, p(b, c)) = p(p(a, b), c)$$

for any $a, b, c \in A$. In other words, how we parenthesize doesn't matter.

**Definition**.

We say that a binary operation $p : A \times A \to A$ has an **identity** if

$$p(a, e) = p(e, a) = a$$

for any $a \in A$.

**Definition**.

We say that a binary operation $p : A \times A \to A$ has a **inverses** if

1. It has an identity element $e$ (otherwise identity is meaningless!)
2. $$p(a, b) = p(b, a) = e$$

   for any $a \in A$ and some $b \in A$.

We usually write $b$ as $a^{-1}$.

**Definition**.

We say that a binary operation $p : A \times A \to A$ is **commutative** if

$$p(a, b) = p(b, a)$$

| for any $a, b \in A$.

Let's look at properties of $(\mathbb{Z}_n, +)$ and $(\mathbb{Z}_n, \times)$.

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

1. Is Associative.
2. Has an identity: 0.
3. Has an inverse: $\overline{(-a)}$ for any $\bar{a}$.
4. Is Commutative: We can move elements around.

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

1. Is Associative
2. Has an identity: 1.
3. **Does not** have an inverse! Because $\bar{0}$ is still there, we have no inverse.
4. Is Commutative: We can move elements around. In this case, $\bar{a}\bar{b} = \overline{ab} = \overline{ba} = \bar{b}\bar{a}$.

**Question**: If we instead looked at $(\mathbb{Z}_n \setminus \{0\}, \times)$, would there be inverses?

**Answer**: We've messed the whole thing up! This is not even an binary operation anymore. Since we don't have $\bar{0}$, what does $\bar{2} + \bar{2}$ even mean now, if $n = 4$?

We'll study this more in about a week.

Let's look at matrices. $A = \mathrm{Mat}_n(\mathbb{R})$ be the set of $n \times n$ matrices with real elements, with the binary operation being matrix multiplication. Let's look at its properties.

1. Its associative.
2. It has an identity.
3. It **does not** have an inverse.
4. It **is not** commutative.

Now looking at $A = \mathrm{GL}_n(\mathbb{R})$ be the set of $n \times n$ invertible matrices with real entries.

1. Its associative.
2. It has an identity.
3. It **does** have an inverses.
4. It **is not** commutative.

**Proposition**

If $p : A \times A \to A$ is a binary operation with two identities $e, f$, then $e = f$.

**Proof**

$e = p(e, f) = f$, so $e = f$.

**Proposition**

If we have two inverses, then they are the same. More formally: if $p(a,b) = p(b,a) = e$, and $p(a,c) = p(c,a) = e$, then $b = c$

**Proof**

$p(c, p(a,b)) = p(c,e) = c$, but we could have also done $p(p(c,a),b) = p(e,b) = b$, so $b = c$.

**Mon. 29 Jan 2024**

**Note**.

Homework 1 is due this Thursday at 11:59PM, on Gradescope. Because this is the first homework, Gradescope will allow late submissions but just submit it on time.

Last time, we talked about binary operations and their properties. Now, we are going to put everything together and talk about Groups!

# 3 Groups

**Definition**.

A **Group** is a set $G$ with a binary operation $p : G \times G \to G$ that

1. Is *Associative*.
2. Has an *Identity*.
3. Has *Inverses*.

Note that it does **not** have commutatitivity. We'll talk about that later.

Notation-wise, we write $(G, p)$, or just $G$ if the binary operations is understood. Additionally, we often write the operation as $a \cdot b$, $a + b$, or $ab$ instead of $p(a,b)$.

**Definition**.

A Group is **Abelian** if the operation is also *commutative*.

**Note**.

Sometimes, we say that a group is *closed* under its operation. However we don't need this because a binary operation, by definition, is necessarily closed.

Let's look at some examples.

**Example**.

These groups are **Abelian**:

1. $(\mathbb{R}, +)$
2. $(\mathbb{Z}, +)$
3. $(\mathbb{C}, +)$
4. $(\mathbb{R} \setminus \{0\}, \times)$

These groups are **Non-Abelian**:

1. $(\mathrm{GL}_n(\mathbb{R}), \times)$. Recall that this is the set of *non-invertible* $n \times n$ matrices with real entries.

2. $(\mathbb{Z}_n, +)$. Recall that this was the set of classes of partitions modulo $n$.

These are **not Groups**:

1. $(\mathbb{N} \cup \{0\}, +)$, has no inverses.
2. $\mathrm{Mat}_n(\mathbb{R}), \times)$, has no inverses.

**Definition**.

The **Order** of a group, is the *cardinality* of the set $G$, denoted $|G|$.

## 3.1 Cancellation Law

In a group $G$, if $ab = ac$, then $b = c$.

**Proof**

Since $G$ has inverses, there is an element $a^{-1} \in G$ such that $aa^{-1} = e$. So,

$$\begin{aligned} ab &= ac \\ a^{-1}(ab) &= a^{-1}(ac) \\ (a^{-1}a)b &= (a^{-1}a)c \\ b &= c && \text{Defn of Identity} \end{aligned}$$

Let's look at some more examples.

## 3.2 Groups of Matrices

**Example**.

From the groups of matrices, we can also talk about

- $\mathrm{GL}_n(\mathbb{R})$
- $\mathrm{GL}_n(\mathbb{C})$
- $\mathrm{GL}_n(\mathbb{Q})$

Which are all groups.

**Question**: Is $\mathrm{GL}_n(\mathbb{N})$ a group? What about $\mathrm{GL}_n(\mathbb{Z})$?

Recall that GL stands for *general linear*. There is also the *special linear* group SL. This is the set of general linear matrices with determinant 1. Let's look at some examples

**Example**.

1. $\mathrm{SL} = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det(A) = 1\}$

   Recall that $\det(AB) = \det(A)\det(B)$, so this is closed.

## 3.3 Symmetric Groups

**Definition**.

Given the set $\{1, 2, \ldots, n\}$, the group of *permutations* of this set is the **symmetric group** $S_n$, where the binary operation is *function composition*.

A **permutation** is a bijection $\{1, 2, \ldots, n \ \to \{1, 2, \ldots, n\}$. A permutation can be described by a list.

**Example**.

If $n = 3$, we have the permutations

$$\{123, 213, 132, 321, 231, 312\}$$

We say that $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ takes an input from the set and defines the shuffle.

We'll talk more about Symmetric groups later in the semester.

**Note**.

- The Symmetric group is **Non-Abelian**.
- There are $n!$ permutations of $S_n$, so the order of $S_n$ is $|S_n| = n!$
- Why the Symmetric Group is named as it is is a question for another day.

## 3.4 Subgroups

**Definition**.

A **subgroup** is a subset $H$ of a group $(G, p)$ such that:

1. $H$ is closed under $p$.

   If $a, b \in H$, then $p(a, b) \in H$.

   Note that we *need* to explicitly state that a subgroup is closed, because $p$ is **not** closed in $H$, but it *is* by virtue of the values in $H$. However this does not come for free from $p$, unlike with $G$ like before.

2. $H$ has inverses.

   If $a \in H$, then $a^{-1} \in H$.

Note that we also have

1. **The Identity**, by virtue of $H$ being closed and containing inverses.

$$aa^{-1} = e$$

2. **Associativity**, because $(G, p)$ is associative. This property is just inherited from $G$.

So $(H, p)$ is a group!

As notation, we say that $H \leq G$ if $H$ is a subgroup of $G$.

**Example**.

$$\mathrm{SL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{C})$$

Notice the direction of "subset-ness"!

**Example**.

$$\{\bar{0}, \bar{2}\} \leq (\mathbb{Z}_4, +)$$

Let's check this one.

1. **Closure**:

   This is small enough that we can check them all.

   - $\bar{0} + \bar{0} = \bar{0}$
   - $\bar{0} + \bar{2} = \bar{2}$
   - $\bar{2} + \bar{0} = \bar{2}$
   - $\bar{2} + \bar{2} = \bar{4} = \bar{0}$

   Note that we didn't really need to check the middle two, since the group is Abelian, and that property is inherited.

2. **Inverses**

   - $\bar{0} + \bar{0} = \bar{0}$
   - $\bar{2} + \bar{2} = \bar{0}$

So we have a subgroup!

**Example**.

If $G$ is a group and $a \in G$ is an element, then

$$H = \{\dots, a^{-3}, a^{-2}, a^{-1}, e, a^1, a^2, a^3, \dots\}$$

is a subgroup.

As a note

- $a^{-3} = a^{-1}a^{-1}a^{-1}$
- $a^2 = aa$

Furthermore, sometimes, $a^n = e$ for some finite $n$. The smallest such $n$ is called the **order** of $a$.

**Example**.

The order of $\bar{2} \in \mathbb{Z}_4$ is 2.

**Definition**.

We say that a subgroup $H \leq G$ is called **trivial** if $|H| = 1$. Or,

$$H = \{e\}$$

| This is a subgroup of *every group*.

**Note**.

$G \leq G$ for all groups $G$. In other words, a group is always a subgroup of itself.

We can say that $H < G$ is a **proper** subgroup if $H \leq G$ but $H \neq G$ and, additionally for this class, $H$ is non-trivial.

**Wed. 31 Jan 2024**

Today we are going to talk about subgroups of $\mathbb{Z}$ under addition. We want to understand *all* those subgroups. Both the techniques and the results will be useful beyond just this set of groups.

Let $a \in \mathbb{Z}$, and let $a\mathbb{Z} = \{ax \mid x \in \mathbb{Z}\}$ be all the multiples of $a$ (with $0\mathbb{Z} = \{0\}$.)

**Claim.**

$a\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

**Proof.**

We need check two properties.

1. **Closure**: Given $ax, ay \in a\mathbb{Z}$, $ax + ay = a(x + y) \in a\mathbb{Z}$.
2. **Inverses**: Given $ax \in a\mathbb{Z}$, $a(-x) \in a\mathbb{Z}$, and $ax + a(-x) = ax - ax = 0 \in a\mathbb{Z}$.

**Note**.

This is how you should prove your questions relating to subgroups on the homework.

**Claim**.

If $H \leq \mathbb{Z}$ is a subgroup, then $H = a\mathbb{Z}$ for some $a \in \mathbb{Z}$. In other words, this is it! This is *all* the subgroups.

**Proof**.

If $H \leq \mathbb{Z}$, then $0 \in H$. If $H = \{0\}$¡ then $H = 0\mathbb{Z}$ is the trivial subgroup. Otherwise, $H$ contains non-zero integers. Since $H$ contains inverses, it contains positive integers. Let $a$ be the smallest positive integer in $H$. We want to show that $H = a\mathbb{Z}$.

Given $ax \in a\mathbb{Z}$, we can express $ax$ as follows

$$ax = \begin{cases} a + \cdots + a & x > 0 \\ 0 & x = 0 \\ (-a) + \cdots + (-a) & x < 0 \end{cases}$$

In all such cases, $H$ is closed and has inverses/identity, so $ax \in H$ and thus $a\mathbb{Z} \subseteq H$.

The harder way is going backwards.

Given $h \in H$, and assume $|h| > a$ (We can do this because $a$ is the smallest positive integer in $H$.) Write

$$h = ax + r$$

Where $0 \leq r < a$. We know that $h \in H$, and $ax \in H$, so

$$r = h - ax \in H$$

Because $r$ is a combination of two elements in the subgroup! But recall that $r$ is between 0 and $a$. But we said before that $a$ is the smallest positive integer in $H$, so $r$ *must* be zero! In other words $h = ax$ and $h \in a\mathbb{Z}$. Which proves that $H \subseteq a\mathbb{Z}$.

So $H = a\mathbb{Z}$.

**Note**.

This proof is very important and the techniques in it come back! Be sure you understand what's going on.

This is great! We've now categorized every subgroup of the Integers under addition!

Now, given $a\mathbb{Z}$, $b\mathbb{Z}$, form

$$a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$$

This is a subgroup of $\mathbb{Z}$. In fact,

**Theorem**

**Definition**.

If $a, b \neq 0$, then $d$ is the **greatest common divisor** (gcd), of $a$ and $b$,

$$d = \gcd(a, b)$$

If $a, b = 0$, $d = \gcd(a, b)$, then

1. $d$ divides $a$ and $b$, notated as $d \mid a$ and $d \mid b$.

   **Proof**.

   $a \cdot 1 + b \cdot 0 = a \in d\mathbb{Z}$, so $d \mid a$. Similarly for $b$, $a \cdot 0 + b \cdot 1 = b \in d\mathbb{Z}$ so $d \mid b$.

2. if $e \mid a$ and $e \mid b$, then $e \mid d$

   **Proof**

   If $e \mid a$ $e \mid b$, then $e \mid (ax + by) = d$.

3. $\exists x, y \in \mathbb{Z}$ such that $d = ax + by$

   **Proof**.

   $d \in a\mathbb{Z} + b\mathbb{Z}$, so $d = ax + by$, for some $x, y \in \mathbb{Z}$.

**Fact**.

$d$ is the smallest positive value of $|ax + by|$.

This is useful, because if $ax + by = 1$ for some $x, y$, then $\gcd(a, b) = 1$.

**Definition**.

$a, b \in \mathbb{Z}$ are **relatively prime** if $\gcd(a, b) = 1$ and

$$\gcd(a,b) = 1 \Leftrightarrow ax + by = 1$$

for some $x, y \in \mathbb{Z}$.

**Proposition**.

Let $p$ be a prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

**Proof**.

Assume that $p$ is a prime, and $p \mid ab$, but $p \nmid a$.

We will show that $p \mid b$.

The factors of $p$ are 1 and $p$, and $p \nmid a$, so $\gcd(p, a) = 1$ (since the gcd is either 1 or $p$, but if it was $p$, then $p$ would divide $a$.)

So there must exist $x, y \in \mathbb{Z}$ with $px + ay = 1$. Multiplying by $b$, we have $pxb + aby = b$. Now of course, $p \mid pxb$ and, more importantly, $p \mid aby$ since $a$ is a multiple of $p$ so

$$p \mid (pxb + aby) = b$$

So $p \mid b$.

**Similarly**.

$a\mathbb{Z} \cap b\mathbb{Z}$ is also a subgroup of $\mathbb{Z}$, say $m\mathbb{Z}$ and $m = \text{lcm}(a, b)$, the least common multiple of $a$ and $b$: The smallest number which is both a multiple of $a$ and $b$.

**The Euclidean Algorithm**. *To find the* gcd

To understand this, let's look at an

**Example**.

Suppose we want to find the $\gcd(210, 45)$. Write $210 = 45 \cdot 4 + 30$. If $x \mid 210$ and $x \mid 45$, then $x \mid 30$. Now $x \mid 30$ and $x \mid 45$ implies that $x \mid 210$.

Hence $\gcd(210, 45) = \gcd(45, 30)$.

We can do this trick again!

$45 = 30 \cdot 1 + 15$, so $\gcd(45, 30) = \gcd(30, 15) = 15$. So $\gcd(210, 45) = 15$.

**Cyclic Subgroups**.

$G$ is a group, and $a \in G$. The set

$$\langle a \rangle = \{\dots, a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, \dots\}$$

is called the **cyclic subgroup generated by** $a$.

**Note**.

$\langle a \rangle$ is the smallest subgroup of $G$ that contains all these powers of $a$.

$|\langle a \rangle| = |a|$, the smallest positive $n$ such that $a^n = e$, or $\infty$.

**Fri. 2 Feb 2024**

# 4 Cyclic Groups and Subgroups

We're going to repeat a little bit from last class, just to make sure we're on the same page.

**Definition**.

If $G$ is a group and $a \in G$, the set

$$\langle a \rangle = \{\dots, a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, \dots\}$$

Is the cyclic subgroup generated by $a$.

If $G = \langle a \rangle$ for some $a \in G$, we say $G$ is a **cyclic group**.

**Example**.

$G = \mathbb{Z}$, $a = 2$, We have that

$$\langle 2 \rangle = \{\dots, -4, -2, 0, 2, 4, \dots\}$$

In general, $\langle a \rangle = a\mathbb{Z}$, and $\langle 1 \rangle = \mathbb{Z}$, so $\mathbb{Z}$ is a cyclic group.

**Note**.

$\langle a \rangle$ is the smallest subgroup of $G$ containing $a$.

Recall: Let $n \in \mathbb{N}$ be the smallest number such that $a^n = e$ (or $\infty$ if $a^n \neq e$ for all $n$) we say that $n$ is the order of $a$, or $|a| = n$.

**Proposition**

Let $|a| = n < \infty$. Then

1. $a^l = a^m$ if and only if $l - m \equiv 0 \pmod{n}$ .
2. $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$, and $|\langle a \rangle| = n$.

**Proof**

1. If $a^l = a^m$, then $a^l a^{-m} = e$ and so $a^{l-m} = e$. Assume that $l - m \leq 0$.

   If $l - m \not\equiv 0 \pmod{n}$ then $l - m > n$, because $n$ is minimal. Then $l - m = nk + r$, and $r \in \{0, 1, \dots, n-1\}$.

   So

   $$a^r = a^{(l-m)-nk} = \underbrace{a^{l-m}}_{e}\underbrace{(a^n)^{-k}}_{e}$$

   But $r < n$ so in fact $r = 0$. This contradicts $l - m \not\equiv 0 \pmod{n}$ , hence $l - m \equiv 0 \pmod{n}$ .
2. If $l \in \mathbb{Z}$, write $l = nk + r$, $r \in \{0, 1, \dots, n-1\}$, then $a^l = a^{nk+r} = (a^n)^k a^r = e^k a^r = a^r$. So

   $$\langle a \rangle = \{e, a, \dots, a^{n-1}\}$$

If $a^l = a^m$ for $l, m \in \{0, 1, \ldots, n-1\}$, then $l - m \equiv 0 \pmod{n}$ . This only happens for $l = m$, so $|\langle a \rangle| = n$.

This answers the question to the overloading of the word "order" from before. The *order* of an element is in fact the order of the cyclic subgroup that it generates!

**Example**.

If $|a| = n$, then

$$|a^l| = \frac{n}{\gcd(n, l)}$$

This is a good exercise for understanding subgroups. If you understand why it's true, you're in good shape.

**Definition**.

An **infinite cyclic group** is a cyclic group $\langle a \rangle$ where $|a| = \infty$.

For example, $\mathbb{Z}$.

**Finite cyclic groups**, for example $\mathbb{Z}_n = \langle \bar{1} \rangle$

**Example**.

If $G = \mathrm{GL}_2(\mathbb{R})$, then

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

Has infinite order. Raising it to a power keeps generating larger and larger matrices.

However other matrices have finite order. For example, rotation matrices! In fact, it's possible to generate a rotation matrix of any order!

$$B_n = \begin{bmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{bmatrix}$$

Has order $n$. It's a rotation matrix!

## 4.1 Homomorphisms

So far we've been studying groups in isolation, but we may want to make general statements about the relation between different groups.

We want function between groups that "respect" the group operation.

**Definition**.

Given groups $(G, p)$ and $(G', p')$. A **Homomorphism** $\varphi : G \to G'$ is a function such that

$$\varphi(p(a, b)) = p'(\varphi(a), \varphi(b))$$

It doesn't matter if we combine elements before or after the binary operations.

Suppressing $p$ and $p'$, we can write $\varphi(ab) = \varphi(a)\varphi(b)$.

Alternatively, we have the following diagram

$$\begin{array}{ccc} G \times G & \xrightarrow{\quad p \quad} & G \\ \downarrow{\scriptstyle \varphi \times \varphi} & & \downarrow{\scriptstyle \varphi} \\ G' \times G' & \xrightarrow{\quad p' \quad} & G' \end{array}$$

**Example**.

We can express the determinant function as

$$\det : \mathrm{GL}_n(\mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \times)$$

Or

$$A \to \det(A)$$

And we can check that $\det(AB) = \det(A)\det(B)$

Similarly

**Example**.

Consider the function $\exp : (\mathbb{R}, +) \to (\mathbb{R} \setminus \{0\}, \times)$

Or

$$x \to e^x$$

And we can check that $\exp(x + y) = e^x e^y = \exp(x)\exp(y)$

A more general

**Example**.

Given a group $G$, $a \in G$, we have

$$\varphi : (\mathbb{Z}, +) \to G$$

or

$$n \to a^n$$

If $|a| = n$, then $\varphi(\mathbb{Z}_n, +) \to G$, or $\bar{i} \to a^i$.

**Example**.

The **trivial homomorphism** $\phi : G \to G'$ can be defined as $a \to e$ for all $a \in G$.

**Note**.

The difference between an *Isomorphism* and a *Homomorphism* is **not** necessarily a bijection.

**Proposition**

If $\varphi : G \to G'$ is a homomorphism, then

1. $\varphi(a_1, \ldots, a_n) = \varphi(\alpha_1) \cdots \varphi(a_n)$
2. $\varphi(e_G) = e_{G'}$
3. $\varphi(a^{-1}) = \varphi(a)^{-1}$

It's important to note that these aren't by definition, but *derived* from the definition.

**Proof**.

1. This one is by induction, we won't prove it.
2. $\varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$

   We can can "cancel" $\varphi(e_G)$ from both sides and get

   $$e_{G'} = \varphi(e_G)$$

3. $e_{G'} = \varphi(e_G) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$ so $\varphi(a)\varphi(a^{-1}) = e_{G'}$ and so $\varphi(a^{-1}) = \varphi(a)^{-1}$